NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PERSONNEL IDENTITY MANAGEMENT AND THE EXPEDITIONARY STRIKE GROUP

by

Glen E. Neises

September 2007

Thesis Advisor:	Buddy Barreto
Second Reader:	Thomas Housel

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Personnel Identity Management and the Expeditionary Strike Group		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Glen E. Neises			
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)

Identity management (IM) plays a critical role in virtually every management process involving personnel. "Identity management" means the ability to uniquely and unambiguously identity people and entities and their interactions and interrelationship, and also the ability to track their mobility in a timely fashion. Currently, Expeditionary Strike Group (ESG) personnel IM suffers from a lack of: technology, systems integration, and training. The purpose of this thesis is to identify best practices and technologies to help resolve ESG personnel IM problems. Chapter I defines IM and explains why IM is important for the Department of Defense (DoD). Chapter II provides an overview of DoD human resource management and Defense Manpower Data Center information systems. Chapter III provides an introduction to the challenges associated with the ESG, personnel IM and information technology (IT). Chapter IV provides an introduction to metrics, Business Process Redesign and Knowledge Value Added. Those concepts are used to derive an answer to the question, "What does the Non Combatant Evacuation Operation Tracking System do for ESG commanders?" Chapter V summarizes the challenges associated with ESG personnel IM and IT, recommends changes and summarizes the main points of the thesis.

14. SUBJECT TERMS Identity Management, Expeditionary Strike Group, Non Combatant Evacuation Operation Tracking System, Defense Biometric Identification System, Knowledge Value Added, Business Process Redesign			**15. NUMBER OF PAGES** 91
			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

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)

Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PERSONNEL IDENTITY MANAGEMENT AND THE EXPEDITIONARY STRIKE GROUP

Glen E. Neises
Captain, United States Marine Corps
B.S., The Citadel, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2007

Author: Glen E. Neises

Approved by: Buddy Barreto
Thesis Advisor

Thomas Housel
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Identity management (IM) plays a critical role in virtually every management process involving personnel or material, particularly in the Department of Defense (DoD). "Identity management" means the ability to uniquely and unambiguously identity people and entities and their interactions and interrelationship, and also the ability to track their mobility in a timely fashion. Currently, Expeditionary Strike Group (ESG) IM suffers from inefficient data sharing because of a lack of systems integration, just as in the civilian domain. For many ESG IM processes, technology is not being used at all. Large reports and manifests are being generated by hand, are then re-typed and E-mailed, to manually update systems. The lack of timely fielding equipment and proper training is resulting in problems with implementing IM information technology (IT) solutions.

The purpose of this thesis is to establish and identify best practices and technologies to help resolve ESG IM problems. The scope for this thesis is limited to personnel IM issues at the operational, unit level to show ESG Commanders and other decision makers how best practices and technologies can be implemented. These best practices and technologies may provide similar results outside the ESG and be applicable to other DoD operations and the civilian domain as well.

Chapter I provides background information to define the many different aspects of IM and explains why IM is important for the DoD. Chapter II provides an overview of

DoD human resource management and Defense Manpower Data Center (DMDC) information systems. It also reviews the Non Combatant Evacuation Operation Tracking System (NTS) and the Defense Biometric Identification System (DBIDS). Chapter III provides an introduction to the ESG and then explains how IM plays a role in everyday operations. The challenges of ESG personnel IM and IT are addressed, including the NTS and the DBIDS. Chapter IV provides a brief introduction to metrics, Business Process Redesign (BPR) and the Knowledge Value Added (KVA) theory. Those concepts are used in a study to derive an answer to the question, "What does the NTS do for ESG commanders?" Chapter V summarizes the challenges with personnel IM, IT and the ESG, and recommends changes for the DBIDS and NTS. Finally, the conclusion summarizes the main points of the thesis.

TABLE OF CONTENTS

I. BACKGROUND 1
A. CHAPTER INTRODUCTION 1
B. IDENTITY MANAGEMENT 1
C. THE IMPORTANCE OF IDENTITY MANAGEMENT IN THE DEPARTMENT OF DEFENSE 4
D. CHAPTER SUMMARY 5

II. PERSONNEL IDENTITY MANAGEMENT AND DEPARTMENT OF DEFENSE INFORMATION SYSTEMS 7
A. CHAPTER INTRODUCTION 7
B. PERSONNEL IDENTITY MANAGEMENT AND DEPARTMENT OF DEFENSE INFORMATION SYSTEMS 7
1. The Non Combatant Evacuation Operation Tracking System 13
2. The Defense Biometric Identification System 15
C. CHAPTER SUMMARY 17

III. PERSONNEL IDENTITY MANAGEMENT AND THE EXPEDITIONARY STRIKE GROUP 19
A. CHAPTER INTRODUCTION 19
B. THE EXPEDITIONARY STRIKE GROUP 19
C. PERSONNEL IDENTITY MANAGEMENT AND THE EXPEDITIONARY STRIKE GROUP 20
1. Peer Access and Ship Boarding / Departing 21
2. Personnel Cross Deck 21
3. Amphibious Operations 22
4. Port Visits and Leave and Liberty Call 22
5. Special Operations 23
6. Morning Report / Man Over-board 23
7. Movement to Theatres Ashore 23
D. THE CHALLENGES OF PERSONNEL IDENTITY MANAGEMENT INFORMATION TECHNOLOGY AND THE EXPEDITIONARY STRIKE GROUP 24
1. The Defense Biometric Identification System and the Expeditionary Strike Group 24
2. The Non Combatant Evacuation Operation Tracking System and the Expeditionary Strike Group 25
E. CHAPTER SUMMARY 27

IV. A STUDY OF THE NON COMBATANT EVACUATION OPERATION 29
A. CHAPTER INTRODUCTION 29
B. AN INTRODUCTION TO METRICS, KNOWLEDGE VALUE ADDED AND BUSINESS PROCESS REDESIGN 29

1. Information Technology and Metrics 29
2. The Knowledge Value Added Process 30
3. Business Process Redesign 31
C. A STUDY OF THE NON COMBATANT EVACUATION OPERATION .32
D. CHAPTER SUMMARY 33

V. RECOMMENDATIONS AND CONCLUSION 35
A. CHAPTER INTRODUCTION 35
B. SUMMARY OF EXPEDITIONARY STRIKE GROUP PERSONNEL IDENTITY MANAGEMENT AND INFORMATION TECHNOLOGY CHALLENGES 35
C. RECOMMENDED CHANGES FOR EXPEDITIONARY STRIKE GROUP PERSONNEL IDENTITY MANAGEMENT INFORMATION TECHNOLOGY 36
1. Recommended Changes to the Defense Biometric Identification System 36
2. Recommended Changes to the Non Combatant Evacuation Operation Tracking System 40
3. Conclusions 43

APPENDIX A. NON COMBATANT EVACUATION OPERATION TRACKING SYSTEM AND KNOWLEDGE VALUE ADDED 51
A. INTRODUCTION 52
B. THE PROJECT 52
1. Reception Station 54
2. Registration Station 54
3. Debriefing Station 54
4. Medical Station 54
5. Transportation Station 55
6. Comfort Station 55
C. THE SOLUTION 57
D. RADICAL REDESIGN 60
E. CONCLUSION 63

APPENDIX B. ADDITIONAL DIAGRAMS 67

LIST OF REFERENCES 71

INITIAL DISTRIBUTION LIST 75

LIST OF FIGURES

Figure 1. The Defense Biometric Identification System standard "As-Is" ship configuration.....36
Figure 2. Example Defense Biometric Identification System "To-Be" ship configuration.....37
Figure 3. The Recommended Defense Biometric Identification System "To-Be" Expeditionary Strike Group interoperability.....38
Figure 4. Recommended Defense Biometric Identification System "To-Be" wireless capability.....39
Figure 5. Example upgrade for the Non Combatant Evacuation Operation Tracking System [From 21]..40
Figure 6. Example of Non Combatant Evacuation Operation Tracking System real-time data feed for situational awareness and evacuee tracking.....42
Figure 7. Example of Non Combatant Evacuation Operation simulation using Arena software.....43
Figure 8. “As-is” Process Flow Chart.....53
Figure 9. “AS-is” Knowledge Value Added Spreadsheet.....56
Figure 10. Incremental To-Be.....58
Figure 11. Incremental To-Be.....59
Figure 13. Redesign Flowchart.....61
Figure 14. Radical Redesign.....62
Figure 15. Redesign Spreadsheet.....63
Figure 16. “As-is” Processing.....67
Figure 17. Non Combatant Evacuation Tracking System Processing.....68
Figure 18. I-Gauss Views.....70

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Time and Cost Savings.....65

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

ARRS	Automated Repatriation Reporting System
BPR	Business Process Redesign
CONUS	Continental United States
DBIDS	Defense Biometric Identification System
DEERS	Defense Eligibility Enrollment
DMDC	Defense Management Data Center
DOD	Department of Defense
ECC	Evacuation Control Center
ESG	Expeditionary Strike Group
ID	Identification Card
IEEE	Institute of Electrical and Electronics Engineers
IM	Identity Management
IP	Internet Protocol
IT	Information Technology
KVA	Knowledge Value Added
MEU	Marine Expeditionary Unit
NCE	Non Combatant Evacuee
NEO	Non Combatant Evacuation Operation
NPS	Naval Post Graduate School
NTS	Non Combatant Evacuation Operation Tracking System
OUSD P&R	Office of the Under Secretary of Defense for Manpower Personnel and Readiness
PKI	Public Key Infrastructure
RAPIDS	Real-Time Automated Personnel Identification System
RFID	Radio Frequency Identification
ROI	Return on Investment
ROK	Return on Knowledge

SOC	Special Operations Capable
VIP	Very Important Person
WiFI	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WWW	World Wide Web

I. BACKGROUND

A. CHAPTER INTRODUCTION

This chapter explores the motivation and provides background information to define the many different aspects of IM. It also explains why IM is important for the DoD.

B. IDENTITY MANAGEMENT

The stabilization and security of society is needed because modern man is gripped with the fear of terrorism and random acts of violence. Historically, wars were fought against rogue nations or militant factions. Today, we often do not know whom or why we are fighting. The enemy is no longer clearly defined by uniform or geographic location. The insurgency of terrorists and their acts of violence are transcending race, culture and national borders. Conventional methods of intelligence gathering and warfare are no longer adequate to fight the global war on terror [1].

In the wake of the tragic events of September 11, 2001, debate has risen regarding the efficacy and legality of a national identification card - something that is more comprehensive than a driver's license, a Social Security card or a passport. Such debate has centered around finding the appropriate balance between maintaining personal freedoms as guaranteed by the U.S. Constitution and protecting national security. Proponents contend that a card using "biometric" surveillance technologies such as electronic retinal scans or fingerprints could help reduce and/or track illegal immigrants or potential terrorists.

Conversely, opponents assert that such a card could infringe upon civil liberties with minimal impact on reducing terrorism [2].

IM in the public domain is known by the name of National Identity Management. Following the September 11, 2001 attacks, attempts are being made worldwide to improve the quality of National Identity Management, particularly through the application of biometrics to identity documents [3].

For the purpose of this thesis, the definition of IM means the ability to uniquely and unambiguously identify people and entities, identify their interactions and interrelationships, and track their mobility in a timely fashion [1].

Furthermore, IM provides the focus to deal with system-wide data quality and integrity issues often encountered by fragmented databases and workflow processes [3].

In information systems, IM is the management of the identity life cycle of entities (subjects or objects) during which, an identity is established, the identity is described, or the identity is destroyed [1].

In the real world context of engineering online systems, IM can be given three perspectives:

1. The pure identity paradigm - creation, management and deletion of identities without regard to access or entitlements;

2. The user access (log-on) paradigm - a smart card and its associated data that a customer uses to log-on to a service or services (a traditional view);

3. The service paradigm - a system that delivers personalized, role-based, on-line, on-demand, multimedia (content), presence-based services to users and their devices [3].

The basic requirements of an IM system include appropriate response time, required accuracy, comprehensiveness of the identification, and the appropriate level of protection for the identification cycle [1].

1. The appropriate response time: the response time should be quick enough to be useful. The system must be capable of distributing information close to real time, and to any relevant agency in the world [1].

2. The accuracy of the identification: the identification must be robust and reliable. If there are any mistakes in identification, they must be tracked and retrofitted into the system as quickly as possible. Multiple means, such as image, video, voice, spread spectrum and multiple channels of identification should be used to cross reference and validate the reliability of the identity [1].

3. The comprehensiveness of the identification: all possible technologies, such as digital, chemical, physical, biological and sensors at different scales of wavelengths must be used and coordinated. People and objects should not only be identified in isolation but their inter-relationships with cumulative time history profiles should be identified, updated and maintained [1].

4. The appropriate level of protection - the highest level of cryptographic systems should be used. New modalities and generations of cryptosystems need to be

invented. Public Key Infrastructure (PKI) and the concept of digital signatures should protect information [1].

C. THE IMPORTANCE OF IDENTITY MANAGEMENT IN THE DEPARTMENT OF DEFENSE

IM in the DoD is much more than security and biometrics. IM is important because it plays a critical role in virtually every operational and management function involving personnel or material. IM in the DoD is not always a highly technical or complex process. However, it is an integral part of the daily identification, accountability and tracking of its personnel and equipment.

For instance, identification cards (ID)s allow service members access to enter installations and board vessels. The same personnel may be manifested for morning accountability records, logistical planning or for pay and administrative purposes. Once deployed, the same personnel may be tracked by the operations center as they move through a theatre of operations.

Visual inventories of serialized equipment are done daily to track ownership, accountability and serviceability. Most pieces of equipment needing repair are entered and tracked in the maintenance cycle using a serial number.

All of the management and operational processes above are daily functions and are mission critical for the DoD.

IM also provides the focus to develop, implement and integrate new and different technologies into powerful, IM information systems. For instance, DoD logisticians are quickly finding out the benefits of integrating Radio Frequency Identification (RFID) technology into supply chain management and Enterprise Resource Planning systems.

The latest technologies in biometrics, sensors, optics, chemical identification, encryption, RFID, PKI, and biological evidences must all be integrated under the same architecture to create a powerful IM information system that would be useful to the DoD. Without a focus on IM, new technologies and their related information systems will remain fragmented and never truly reach their potential of effectiveness.

D. CHAPTER SUMMARY

In summary, IM is defined as the ability to uniquely and unambiguously identity people and entities, identify their interactions and interrelationships, and track their mobility in a timely fashion [1].

IM in the DoD is important because it plays a critical role in virtually every operation and/or management function involving personnel or material. IM provides the focus to integrate new and multiple technologies into one enterprise-wide IM information system.

THIS PAGE INTENTIONALLY LEFT BLANK

II. PERSONNEL IDENTITY MANAGEMENT AND DEPARTMENT OF DEFENSE INFORMATION SYSTEMS

A. CHAPTER INTRODUCTION

Chapter II introduces more background information and provides an overview of DoD human resource management and DMDC information systems. It also reviews two personnel IM programs that are sponsored by the DMDC, the NTS and the DBIDS.

B. PERSONNEL IDENTITY MANAGEMENT AND DEPARTMENT OF DEFENSE INFORMATION SYSTEMS

The U.S. DoD is the largest employer in the world. There are approximately 4.3 million uniformed service personnel and civilian contractors working at more than 40,000 locations in countries around the world [4]. Imagine the complexities involved in the management of personnel for an organization the size of the DoD. At the enterprise level, even the most basic management responsibilities for personnel identification, tracking, accountability and security becomes overwhelming. Raising and supporting an army and providing and maintaining a navy are only a few of the responsibilities of Congress.

One way Congress is able to manage such a tremendous task is through the delegation of responsibilities to the U.S. Secretary of Defense. As the Secretary of Defense oversees the management of personnel and readiness for the DoD, responsibilities are further delegated to the Office of the Under Secretary of Defense for Manpower Personnel and Readiness (OUSD P&R).

More specifically, the OUSD P&R is the secretary’s senior policy advisor on recruitment, career development,

pay and benefits for 1.4 million active duty military personnel, 1.3 million guard and reserve personnel and 680,000 DoD civilians and is responsible for overseeing the state of military readiness [4]. The management of DoD personnel and readiness is a monumental task and the OUSD P&R relies on the information technologies of the DMDC to help accomplish this mission.

Information technologies that support the management of personnel are an integral part of the DMDC mission. The mission of the DMDC is: to collect and maintain an archive of automated manpower, personnel, training, and financial databases for the DoD; support the information requirements of the OUSD P&R and other DoD manpower, personnel, and training communities with accurate, timely, and consistent data; and, operate DoD-wide personnel programs and conduct research and analysis as directed by the OUSD P&R [4].

Information technologies are an integral part of the DMDC's mission and are vital to the management of personnel and readiness in the DoD. The DMDC’s systems environment is characterized as: highly available, secure, heterogeneous, and distributed. Information technologies are implemented by the systems and technical support division, and include networking, telecommunications, database, web and security [5].

The heart of the DMDC’s production network consists of two Sun Enterprise 10000 servers, one main and one backup, with 32 UltraSPARC II processors. Both mainframes are partitioned across the application and database domain, and are running the Solaris operating system and a 300 GB Oracle8i database [6].

According to Willis, the supervisor of the programming and systems analysis, “Most of the data resides on a

mainframe maintained at the Naval Post Graduate School (NPS) in Monterey, California. The other mainframe is located at the DMDC, in Seaside, CA and houses mostly current information."

Gentry, the repository supervisor at the NPS, emphasizes the importance of the mainframe's physical security. "Very few people know that the main repository is at the NPS, very few people have physical access to the room where the mainframe is housed, and only a select few of my database administrators have the access to view the data." Even Gentry does not have the authority to view the repository's data.

The production network is managed by the programming and systems analysis division in cooperation with Electronic Data Systems, or is outsourced [6]. The production network supports hardware and software from many different vendors, including Adobe, Cisco, Compaq, Gateway, Hewlett Packard, International Business Machines, Microsoft, Novell, Oracle, and Sun Microsystems. The production network is comprised of 170 servers, 13.9 terabytes of storage, 20 routers, 17 switches, 6 firewalls and over 1200 personal computers and printers [5].

To meet the growing needs of the DMDC, a research and development team looks for ways to implement state of the art technologies such as gigabit Ethernet, next generation internet, telephony, voice over internet protocol, and wireless applications [5].

The DMDC database is the largest repository of personnel and financial data in the DoD. Ninety-five different database files are subdivided into six different categories: personnel, pay, financial, training, occupation and other. Database files are compiled from hundreds of

submissions each month that are received from approximately 400 different organizations, both inside and outside of the DoD. Data is submitted in many different formats, electronically, mailed on tape, compact disk, diskette or server used on a cyclical basis. The DMDC houses approximately 22 million record files, 34 database instances, and over 300 database schemas, all of which are quality controlled, maintained, and historically archived [5].

The main problem DMDC analysts encounter is the difficulty of integrating data elements from various data files. Data elements do not follow standard naming conventions, do not employ standard methods for representing domain values, nor use common encoding structures. The integration of data elements from disparate data files is laborious, time-consuming, and requires skill and experience to understand how data elements in one file relate to data elements in another. To solve this problem, the DMDC utilizes a pay data warehouse, effectively merging data elements from both the pay and personnel data files [7].

The DMDC's pay data warehousing methodology is a highly complex process and can be summarized into five different steps. According to Inmon, "The starting point for the design and development of the data warehouse environment is the data model…the data model acts as the road map for development [8]." In the first step, the pay data warehouse requirements are defined, the data schema is selected and the data model is constructed. The second step determines which raw data will be used to populate the warehouse. The third step "filters and cleanses" the data submissions to transform the raw data into a suitable

format before integration into the pay data warehouse. The fourth step populates the pay data warehouse, which consists of temporarily storing the cleansed data in a staging environment. The data is then verified against standard data elements, and once validated is moved to the appropriate location. In the final step, data is ready to be accessed from the pay data warehouse. Analysts use either query languages or access tools to interface with the table structures to view, extract, manipulate, or graphically represent the data. Two different types of tools are required: an ad-hoc query tool, to meet reporting requirements, and a web-enabled, multi-dimensional database tool, to meet recurring reporting needs [7]. The DMDC uses SAS tools and software to handle the various projects and requests. SAS specializes in business intelligence software and services and is able to turn data into information [9].

The DMDC creates and maintains over 70 web based delivery system applications. Virtually all data delivery systems are web-enabled and simply require the user to have internet access, which makes it easy for customers to access information. Password and smart-card technologies are used to restrict the access only to users on a need-to-know basis. Outputs can be generated in almost any form that is convenient for the customer, such as a spreadsheet, report, graphic, or in frequency distributions. Most of the services are free of charge and can be delivered in virtually any form [5].

According to Dove, chief of the management information and analysis division, “At any time, our division of 50 people will have 250 different projects to which we’re trying to respond to as quickly as possible. Some questions take five minutes and some take six months [9]."

Operational programs at the DMDC are formed from a conglomerate of different departments and information technologies. Specific databases, files and computer programs are put together to create specialized information systems that match large sets of files [5].

For example, Operation Mongoose combats fraud in government financial systems. The DoD has 135 different financial processing systems that pays its hired personnel and contractors. Operation Mongoose collects and matches all financial systems files to make sure there is no duplicate billing, and ensures personnel and contractors aren’t getting paid by two pay centers for the same work [5].

The DMDC has approximately 48 different operational programs. Operational programs at DMDC are comprised of many different databases, files, and computer programs that are put together in a system. Programs can range from benefits reporting systems to fraud detection efforts to actuarial evaluations. In general, the operational programs managed by DMDC usually result in a service or benefit (or in some cases the denial of the same) being provided directly to members of the DoD. Other examples of DMDC operational programs include the Basic Allowance for Housing benefits reporting systems, developing aptitude tests for entry into the military, travel charge card verification, and managing the military identification card issuance program. Attitudinal and opinion surveys are used

to formulate, monitor, and refine policies and programs affecting DoD personnel and their families, such as those assisting departing DoD personnel transition back into the civilian sector [5].

The DoD's efforts to find enterprise-wide, IT solutions for personnel IM is currently sponsored by the DMDC. DMDC personnel IM programs include the Contractor Verification System, Common Access Card Personal Identification Number Reset, DMDC Web Guard System, DBIDS, Defense Cross-Credentialing Identification System, Defense National Visitors Center, Real-Time Automated Personnel Identification System (RAPIDS) Card Program and the NTS [5].

The information that the DMDC maintains for each member determines; access to secure facilities and computer systems, eligibility for valuable benefits including health care, use of military grocery and department stores, and access to recreational facilities [10].

Although there are many operational IM programs sponsored by the DMDC, this thesis focuses on two, the NTS and the DBIDS.

1. The Non Combatant Evacuation Operation Tracking System

The primary purpose of the NTS is to provide individual accountability of the noncombatant evacuee (NCE) by creating and maintaining a database of noncombatants assembled during an evacuation operation, and subsequently tracking the noncombatant's movement throughout the evacuation pipeline. The NTS is an automated data processing hardware and software package designed to assist war-fighting Combatant Commanders and Joint Task Force

commanders by providing them visibility of noncombatant personnel, allowing them to focus assets needed to support the Non Combatant Evacuation Operation (NEO) [5].

NTS collects NCE personal information from identification documents (military IDs & passports) that meet current DoD standards using commercial off-the-shelf devices. As new technologies and policies are instituted, the NTS grows and adapts. NCE information collected at the Evacuation Control Center (ECC) is transmitted to the in-theater NTS server and mirrored on the DMDC Continental U.S. (CONUS) shadow server. The NTS and servers are capable of providing real-time reports and queries. A World Wide Web (WWW) reporting capability allows authorized commanders and agencies access to the evacuation information evacuation [5].

NTS has successfully participated in several Courageous Channel exercises and Cobra Gold exercises. Further, the NTS was instrumental in evacuating over 1200 U.S. Noncombatants from Turkey [5].

The NTS can transfer data to other DoD systems, since its data elements were designed using standard DoD attribute naming conventions with the goal of operating in a shared data environment. NTS data are routinely sent to the Global Transportation Network, and the Automated Repatriation Reporting System (AARS) to close out NEOs [5].

The ARRS is a related DMDC program. This system provides a nationwide database that can be used by key agencies, such as the DoD, Department of State, Department of Health and Human Services, and the American Red Cross, to provide aid and support to evacuees from overseas areas.

The ARRS collects and processes information on evacuees from overseas countries arriving in the CONUS, Alaska, and Hawaii through a number of ports of entry [5].

2. The Defense Biometric Identification System

Currently, more than 1.2 million U.S. military personnel, family members and contractors are registered in DBIDS. DBIDS is the largest physical access system in the DoD, providing theater-wide physical access for nearly two million base workers and visitors in Europe and Asia. Soon to be deployed at some 4700 bases worldwide, it uses existing DoD-issued identification credentials, including digital photos and digital fingerprints, drawing on some of the largest stores of biometrics data used in the DoD. DBIDS is scalable and can cover a building, an installation, or an entire theater of operations. The rules-driven system is configurable by local authorities to meet their business rules for access, allowing the level of authentication to vary by threat level or at the local commander’s discretion. DBIDS is an identity and access management solution developed to assist in the securing of DoD installations. DBIDS is used to improve physical security by providing a tool for capturing, authenticating, monitoring and reporting on activities related to personnel and visitors accessing DoD facilities [5].

DBIDS is a rules-based access and IM system. The solution is used to capture and securely store biometric data such as photographs, fingerprints and hand geometry, as well as demographic data and other information that can be used for identification or law enforcement purposes. DBIDS supports the use of wireless handheld scanning devices at installation access/entry control points to

assist security personnel in validating the identity and access privileges of personnel and visitors attempting to enter an installation. DBIDS can verify captured data internally against the DBIDS database and externally against available authoritative sources such as the Defense Enrollment Eligibility Reporting System (DEERS). DBIDS automates the personnel registration process making DBIDS registration easy and in conformity with local procedures and policies. DBIDS uses the latest bar code scanning technologies at registration and entry control points to capture and authenticate current DoD card holder information. For non-DoD ID holders, the DBIDS solution can be used to produce local installation access cards or temporary passes [5].

Security organizations oversee day-to-day operations through the real-time access to person, vehicle and weapons registration data. The DBIDS solution can be configured to alert registration personnel and entry control point guards when individuals seeking to update their information or enter an installation have been flagged as debarred or with some other important consideration [5].

The RAPIDS Program is related to DBIDS. RAPIDS is the DoD's enterprise solution for issuing Uniformed Services Identification and Privilege Cards to all Service members, active and Reserve; civilian employees; retired members; eligible family members; and selected contractors. RAPIDS issues over four million IDs per year. In addition, RAPIDS provides the means to collect family member information to ensure eligible family members are categorized and entered properly into DEERS, and issued IDs. DMDC supports over 2,000 workstations, installed at over 1,400 sites in over

25 countries worldwide. These sites include fixed sites, shipboard sites, deployable sites and reception battalions [5].

The DEERS database serves as the central DoD repository of personnel and medical data. The DEERS Person Data Repository contains one database record for each Uniformed Service member (active duty, retired or a member of a reserve component), U.S.-sponsored foreign military, DoD and Uniformed Services civilians, other personnel as directed by the DoD and their eligible family members [5].

C. CHAPTER SUMMARY

In summary, the DoD relies heavily on the information systems of the DMDC to help manage its human resources. The DoD's efforts to find an enterprise wide, IT solution for personnel IM is currently sponsored by the DMDC. Two DMDC IM programs of interest for this thesis are the NTS and DBIDS. DMDC IM programs are evolving by integrating new technology, combining enterprise-wide databases, files, and computer programs.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PERSONNEL IDENTITY MANAGEMENT AND THE EXPEDITIONARY STRIKE GROUP

A. CHAPTER INTRODUCTION

This chapter provides a brief introduction to the ESG and then explains how IM plays a critical role in everyday operations. The challenges of personnel IM IT are addressed, including the NTS and the DBIDS.

B. THE EXPEDITIONARY STRIKE GROUP

In January of 1996, The 31st Commandant of the Marine Corps, General Krulak, published Operational Maneuver from the Sea. In the White Papers … From the Sea and Forward … From the Sea, the Navy and Marine Corps presented a common vision for a future in which skillfully handled naval forces would enable the U.S. to exert it's influence in the littoral regions of the world. Building upon the foundation laid by those papers, Operational Maneuver from the Sea deals with the full spectrum of challenges that we will have to face, the dangers and opportunities created by new technologies, and the very exciting prospect of adapting the tradition of maneuver warfare, not merely to amphibious operations, but to all aspects of warfare in, and around, costal waters [11].

Since August of 2003, the United States Marine Corps has been engaged with the United States Navy to provide this nation with a force in readiness, known as the ESG. The ESG is a relatively new concept, which combines the capabilities of surface action groups, submarines, and maritime patrol aircraft with those of the Amphibious Ready Groups and Marine Expeditionary Units (MEU) Special

Operations Capable (SOC) to provide greater combat capabilities to theater combatant commanders. The creation of the ESG included a series of experiments allowing Naval Services to analyze the impact of the ESG model during the work up, deployment and employment phases. From these experiments, critical information was gathered to support the future implementation of the concept and highlight any changes that are required in service doctrine, organization, training, material, leadership, education, personnel and facilities [12].

The Navy and Marine Corps ESG is a highly capable, very flexible and extremely efficient fighting organization. Mostly because of new technology; command and control systems, communications equipment, weapons, supply and logistics systems, intelligence systems, medical services, pay and administrative services, have evolved considerably over the past decade. Skill sets for personnel have evolved as well. Only streamlined standard operating procedures have survived the blistering speed of operations and the high turnover of personnel. Experienced staff continues to pass down the highest standards of leadership, accountability, security and safety to ensure the good order and discipline of the operating forces.

C. PERSONNEL IDENTITY MANAGEMENT AND THE EXPEDITIONARY STRIKE GROUP

Even though most systems and skill sets have evolved, and standard operating procedures have been streamlined, the basic requirements for personnel IM have not changed. Personnel identification, accountability and tracking are basic requirements for IM. Those requirements are also an integral part of leadership, security, logistics,

operations, pay, administration and situational awareness. It doesn't matter if you're a platoon commander with personnel on three different ships, moving to three different destinations, or if you are the MEU Commanding Officer, in charge of thousands of personnel deployed all over the world, personnel identification, accountability and tracking must be accurate and timely. You must know where your personnel are at all times. The following scenario descriptions are not meant to be all encompassing, but represent the most basic requirements for personnel identification, accountability and tracking.

1. Peer Access and Ship Boarding / Departing

To gain access to the peer where a ship is docked, personnel must show a military ID to pass a security checkpoint. If you do not have a valid ID then your name must be on an access roster maintained by security personnel. The same is true for boarding a ship. The ID card is checked by security personnel to ensure it has not been tampered with and that it is valid by visually matching the ID photograph to the face of the person requesting access.

2. Personnel Cross Deck

While underway, when personnel move from ship to ship, they usually fly on a helicopter or ride on a small boat. There are many personnel involved in this procedure. An Officer or Staff Non Commissioned Officer in Charge of the personnel transferring is usually present at the point of embarkation to physically verify the movement of their personnel. The Embarkation Officer or Combat Cargo Officer or representative also verifies who is transferring, and updates the unit logistics reports and ensures they board

their transportation safely. The Embarkation Officer or the Combat Cargo Officer usually generates a roster of personnel to be cross decking prior to their departure so they just verify that the roster is accurate. If not, they must verify IDs and generate rosters by hand through a quick muster. Also, the unit administrative and operations center personnel must keep track of who is moving from ship to ship to update their records. The Commanding Officer or Commander of Troops and or other staff officers verify and keep track of who is cross decking.

3. Amphibious Operations

Amphibious operations are much like cross decks, however, entire expeditionary units move to the beach via landing craft. This is usually accomplished in a series of waves because of the large number of personnel that must go ashore. If possible, the Embarkation Officer or Combat Cargo Officer already has a roster of personnel so they are just verifying that the roster is accurate. However, most embarkation plans change and their rosters are no longer accurate. Massive rosters are often generated by hand as personnel present their IDs and board the landing craft.

4. Port Visits and Leave and Liberty Call

The same procedures exist for peer access and ship boarding procedures, however, an added set of procedures are required. The Officer of the Day sets up a check point on the quarter deck and verifies the ID of all personnel leaving and returning from liberty. A logbook entry or laptop computer keeps track of the time and day of check-in and check-out. At the expiration of liberty the Commander

of Troops and the Commanding Officer are promptly notified who, if any personnel are in an unauthorized absence status.

5. Special Operations

The ESG may be called upon to conduct a number of different types of special operations. In the event of a NEO, all evacuees must be screened for verification of identity, documentation, and prioritization as they are processed through the evacuation control center. Normally hand generated rosters, log books or computer flat files are used to record evacuee information and generate manifests.

6. Morning Report / Man Over-board

Each morning personnel accountability and strength reports are submitted to administration. Small unit leaders report up the chain of command via a standard format. Once, administration receives and tallies up the strength reports, personnel not physically attached or co-located with the unit are annotated and reported to the Commanding Officer with their current location status. The same process is done for a man over board operation. The difference is the entire process of verification and reporting must be completed in minutes to quickly determine who has fallen over-board.

7. Movement to Theatres Ashore

In the event all expeditionary forces must move via air transportation to get to inland theatres, all personnel must be properly identified, and manifested for air travel. This process normally takes several days to move thousands of personnel as flight manifests are either hand written or typed using personal computer databases or flat files.

In reality, there are more scenarios that could be included in this list. However, it should now be obvious that personnel identification, accountability and tracking are: critical for leadership, accountability, security, logistics, administration, operations and situational awareness, continuously changing every day, physically verified to ensure accuracy, recorded as changes in status occurs, shared as close to real-time as possible, and kept secure because of the nature of the environment.

D. THE CHALLENGES OF PERSONNEL IDENTITY MANAGEMENT INFORMATION TECHNOLOGY AND THE EXPEDITIONARY STRIKE GROUP

Some of the basic requirements for personnel IM have been outlined in the previous paragraph. By adding technology to automate those requirements or to add a new capability, value has been added to the procedure. However, there will never be one particular IT solution to solve every requirement, and there will always be trade-offs. For instance, a new IT may enable the ESG to collaborate in real-time and facilitate information sharing that has never been possible before. However, in order to use that capability, it may require more bandwidth and or cost you more time and money to operate. Understanding the benefits and challenges of new IT can help determine if the program is going to be successful. The following paragraphs explain some of the trade-offs and or unique challenges faced by the ESG when implementing IM IT.

1. The Defense Biometric Identification System and the Expeditionary Strike Group

In port, thousands of personnel are authorized to board or depart a ship by visually matching the picture on

an ID to the personnel requesting access. By adding technology and automating this procedure, security and access control would improve to a certain degree. However, even if DBIDS is linked to an authoritative source, such as a known terrorist database, limited progress will be made in stopping random acts of terrorism. Studies have shown that terrorist bombers did not hide or try to change their identity when carrying out an attack [13].

The DBIDS will also add many new requirements and complexity to the process. The DBIDS and Smart Card technologies require the installation and maintenance of a new database server for each ship in the ESG. The addition of a new server in an already cramped radio room may require the removal of another piece of hardware from a different system. If DBIDS is only used in port and sits idle for the majority of the deployment, a determination must be made if DBIDS is more important than another system. DBIDS would also require the added personnel requirements of a database administrator and someone to operate a Smart Card issue point. DBIDS access control hardware must be mobile as the access control point moves and requires a steady power source and a network connection. A backup power supply is required because a power outage could cease the operation of the system. Security personnel must be trained and be proficient at the operation and maintenance of the DBIDS.

2. The Non Combatant Evacuation Operation Tracking System and the Expeditionary Strike Group

In the event of a NEO, all evacuees must be screened for the verification of identity, documented, and prioritized, as evacuees are processed through the ECC.

Joint Publication 3-68, Non Combatant Evacuation Operations, directs "A deployable NTS should be located at the ECC, unless lack of time and inadequate security preclude its use." A large scale NEO, involving thousands of evacuees and multiple evacuation sites, becomes impossible without the NTS.

ESGs are normally equipped with the NTS, however, it has not been utilized for any evacuations conducted by an ESG. Hand generated rosters, computer flat files along with laptop computers and peer-to-peer networks are normally employed for ECC processing. As explained previously, there are many benefits to using the NTS, however, there are also many additional requirements to automate the process and ensure the system works correctly. For example, in order to successfully employ the NTS: inventories of hardware must completed along with systems testing prior to an operation, setting up web access to track evacuees on-line must be coordinated in advance, ensuring you have access to commercial satellites must be coordinated in advance, ensuring you have enough wrist bands for every evacuee must be properly estimated, ensuring you have the right number of personnel and system components must be determined in advance, arrangements to embark the system must be coordinated in advance, you must ensure you have a steady power source for the duration of the operation, and you may need to coordinate on-site technical support prior to an operation. This list is not all inclusive, but the key to ensuring all NTS requirements are met prior to any actual operation is through training and operational testing. The ESG must dedicate time and personnel to learn how to operate the system under different operating environments, given different possible

NEO scenarios. The ideal time and place to start NTS training is during the MEU SOC qualification period, because the entire unit will make it a priority to be employed and will learn through experience all of the requirements to ensure its success. Even with all of the requirements in place, and NTS training is incorporated with SOC qualifications, Department of State personnel must have confidence in the system and understand its capabilities and limitations, long before an actual evacuation occurs. Without Department of State cooperation, the NTS may be discouraged and/or not used at all.

E. CHAPTER SUMMARY

In summary, IM plays a critical role in everyday operations of the ESG. Personnel identification, accountability and tracking are basic requirements for IM. By adding technology to automate those requirements or to add a new capability, value has been added to the process. However, there will never be one particular IT solution to solve every requirement and there will always be trade-offs. Understanding the benefits and challenges of new IT can help determine if a program is going to be successful. Finally, unique challenges for the ESG and the DBIDS and NTS are addressed.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. A STUDY OF THE NON COMBATANT EVACUATION OPERATION

A. CHAPTER INTRODUCTION

Chapter IV provides a brief introduction to metrics, BPR and the KVA theory. Those concepts are then used in a study to derive an answer to the question, "What does the NTS do for ESG commanders?"

B. AN INTRODUCTION TO METRICS, KNOWLEDGE VALUE ADDED AND BUSINESS PROCESS REDESIGN

The ESG is faced with the dilemma of scarce resources. Selecting the appropriate IT program to maximize performance has never been more critical. IT often looses its significance as a major contributing factor in operations because it's predominantly considered a support function. Consequently, each year budgets are squeezed and IT gets labeled as a "cost," instead of being identified as the "critical enabler" it should be [14].

ESG personnel with previous deployment experience may not believe there is any need to add technology because expeditionary forces have been successful without it. The addition of technology would only complicate their already difficult time on deployment. Commanders and other stake holders focus on the "bottom line" and want to know what the costs are and what the payoffs will be.

1. Information Technology and Metrics

IT stakeholders must learn to not only identify the cost of IT, but the value IT brings to the organization. Metrics are important because they can measure the bottom-line impact of IT to reveal its true value and enable

allocation of resources in the most essential areas [15]. There are many approaches for quantifying IT payoffs, ranging from highly scientific to purely subjective. Examples of qualitative performance measures include improvements in efficiency, reductions in time, reductions in personnel, generally doing more with less. An example of a quantitative metric, the most prominent investment financial ratio used by the private sector, is return on investment (ROI). ROI is defined as the ratio of money gained or lost on an investment relative to the amount of money invested. The DoD has difficulties using ROI as a metric of performance because they provide a public service and do not generate revenues.

2. The Knowledge Value Added Process

One way the DoD can measure process outputs in common units generated through technological or human resources, is through the use of the Return on Knowledge (ROK) metric, which is provided by the KVA process. KVA can be defined as a new method of gathering historical data about the outputs of an organization's processes. These new data are described in a common unit of measure that reflects the amount of organizational knowledge required to produce the outputs. Once organizational knowledge has been quantified using KVA, it can be monetized, via a market comparables valuation approach, and used in common performance ratios such as ROI and in new ratios such as ROK. ROK describes "returns" in terms of the number of units of knowledge that are generated by the cost to generate the same [16]. The KVA methodology can provide decision makers with quantitative tools to make informed and accurate decisions in the management of IT investments. The KVA process has

been used in the management of DoD IT portfolios, when historically these decisions were exclusively based on costs, schedule, and capabilities [17].

3. Business Process Redesign

BPR is used as a tool by organizations that have the desire to make improvements in their organizational processes to achieve higher levels of effectiveness and efficiency [16]. Teng et al. defines BPR as "the critical analysis and radical redesign of existing business processes to achieve breakthrough improvements in performance measures [18]." Davenport and Short prescribe a five-step approach: Develop the Business Vision and Process Objectives, Identify the Processes to be Redesigned, Understand and Measure the Existing Processes, Identify IT Levers, and Design and Build a Prototype of the New Process [19]. Hammer considers IT as the key enabler of BPR which he considers as "radical change." He prescribes the use of IT to challenge the assumptions inherent in the work processes that have existed since long before the advent of modern computers and communications technology [20]. Davenport & Short argue that BPR requires taking a broader view of both IT and business activity, and of the relationships between them. IT should be viewed as more than an automating or mechanizing force: to fundamentally reshape the way business is done. IT and BPR have recursive relationship. IT capabilities should support business processes, and business processes should be in terms of the capabilities IT can provide [19].

C. A STUDY OF THE NON COMBATANT EVACUATION OPERATION

The NEO study located in the appendix uses the concepts of BPR to identify ways to improve the NTS and increase its attractiveness. The study also uses KVA and ROK to further derive an answer to the question, "What does the NTS do for ESG commanders and other IT stake holders?"

Using BPR it is evident the NEO could benefit greatly from the use of IT. The study reports the NTS improves the accuracy of information during the registration process, eliminates the queue of evacuees waiting to be processed, helps to allay the evacuees fears because they are more quickly manifested and provided a boarding pass or bracelet, provides a web-enabled database to confirm who was processed and allows personnel with higher level access to get a more detailed picture on the status of the evacuation.

The problem is that the NTS's deliverables are services, instead of tangible units of output that can be measured, such as dollars. In order to quantify and measure the outputs/benefits of the NTS the KVA process and ROK metric is used. By comparing the measurements before and after BPR and using an average of 1500 evacuees as the baseline, the study found that the NTS saves as much as $14,665 per NEO. Another interesting discovery includes the potential benefits of radical redesign for the NEO and NTS. By incorporating the Trusted Traveler business model, a pre-registration and biometric identification IT, the NTS could save over $18,000 per NEO while greatly enhancing the ability to process over 100,000 evacuees.

D. CHAPTER SUMMARY

In summary, The ESG is faced with the dilemma of scarce resources. Selecting the appropriate IT program to maximize performance has never been more critical [13]. Commanders and other stake holders focus on the "bottom line" and want to know what the costs are and what the payoffs will be. IT stakeholders must learn to not only identify the cost of IT, but the value IT brings to the organization. Metrics are important because they can measure the bottom-line impact of IT to reveal its true value and enable allocation of resources in the most essential areas [14]. The DoD has difficulties using ROI as a metric of performance because they provide a public good to the people and do not generate revenues. One way the DoD can demonstrate discernable outputs is through the use of the ROK metric, which is provided by the KVA process. The KVA process has been used in the management of DoD IT portfolios, when historically, these decisions were based on costs, schedule, and capabilities [17]. BPR is used as a tool by organizations that have the desired to make changes in their organizational processes to achieve higher levels of effectiveness and efficiency [16]. The NEO study by located in the appendix uses the concepts of BPR to identify ways to improve the NTS and increase its attractiveness. The study also uses KVA and ROK to further derive an answer to the question, "What does the NTS do for ESG commanders and other IT stake holders?"

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS AND CONCLUSION

A. CHAPTER INTRODUCTION

This chapter summarizes the significant challenges associated with ESG personnel IM, provides recommended changes for the DBIDS and NTS programs and explains the potential benefits. Finally, the conclusion recaps the main points of the thesis.

B. SUMMARY OF EXPEDITIONARY STRIKE GROUP PERSONNEL IDENTITY MANAGEMENT AND INFORMATION TECHNOLOGY CHALLENGES

IT is not used by the ESG to automate the identification, verification, recording, reporting or tracking of personnel, when required for: peer access and ship boarding / departing, personnel cross-deck, amphibious operations, port visits and liberty call, special operations, morning report / man over-board or for movement to theatres ashore, etc, etc. Individuals, departments, commands and ships, manually collect and update personnel information independently, on "stand alone" systems, resulting in many redundant but different personnel databases. IT is not being used to increase: the speed of sharing information, situational awareness or for the accuracy of information. Personnel IM IT programs are designed solely to serve one function and have difficulties interacting with other systems. All IT programs have trade-offs and will never solve every problem. IT budgets are constrained and there is strong resistance to add IT to personnel identification, accountability and tracking. Commanders, ESG planners and Department of State personnel

have not identified the value of, or the need to use personnel IM IT programs in training and operations.

C. RECOMMENDED CHANGES FOR EXPEDITIONARY STRIKE GROUP PERSONNEL IDENTITY MANAGEMENT INFORMATION TECHNOLOGY

To address the challenges associated with IM IT and the ESG the following paragraphs provide recommended changes for the DBIDS and NTS.

1. Recommended Changes to the Defense Biometric Identification System

Figure 1 represents a standard DBIDS configuration and the "As-Is" operational system located on an ESG ship.

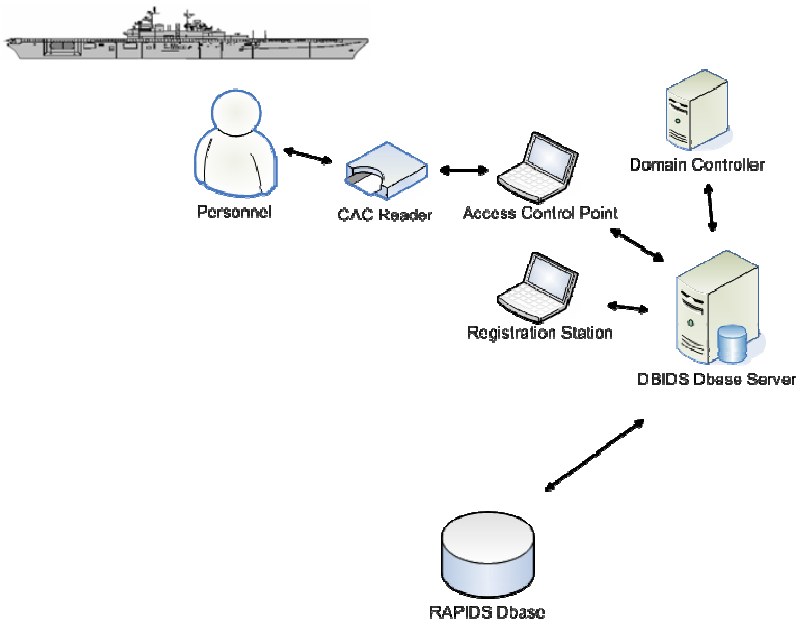


Figure 1. The Defense Biometric Identification System standard "As-Is" ship configuration

A modification to the DBIDS standard "As-Is" ship configuration addresses many of the challenges associated

with IM IT and the ESG. Figure 2 below is one example of how to modify the standard DBIDS ship configuration.

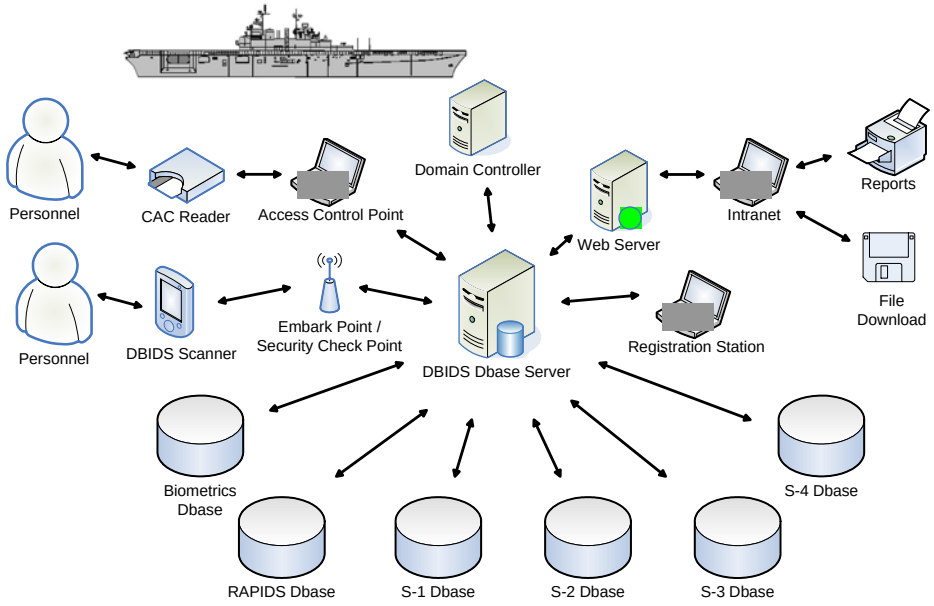


Figure 2. Example Defense Biometric Identification System "To-Be" ship configuration

Changes to the "As-Is" system includes: the addition of web-enabled database technologies, mirroring and/or swapping databases with the DBIDS database, linking to an authoritative biometric database and extending the distance of the wireless DBIDS scanner.

By adding web-enabled database technologies, the DBIDS database serves other purposes than just port security and is utilized throughout the duration of the deployment. Personnel data collected by DBIDS scanners and database administrators is the single most authoritative source of personnel data on the ship because it processes changes in personnel status in real-time and database information is shared instantly via a website. The utilization of the ship's intranet is ideal for this application. Intranet

services are rarely overburdened and in the event of a loss in satellite connectivity, DBIDS and personnel IM are still functional for each ship. Figure 3 below represents a higher level of situational awareness for ESG personnel identification, accountability and tracking.

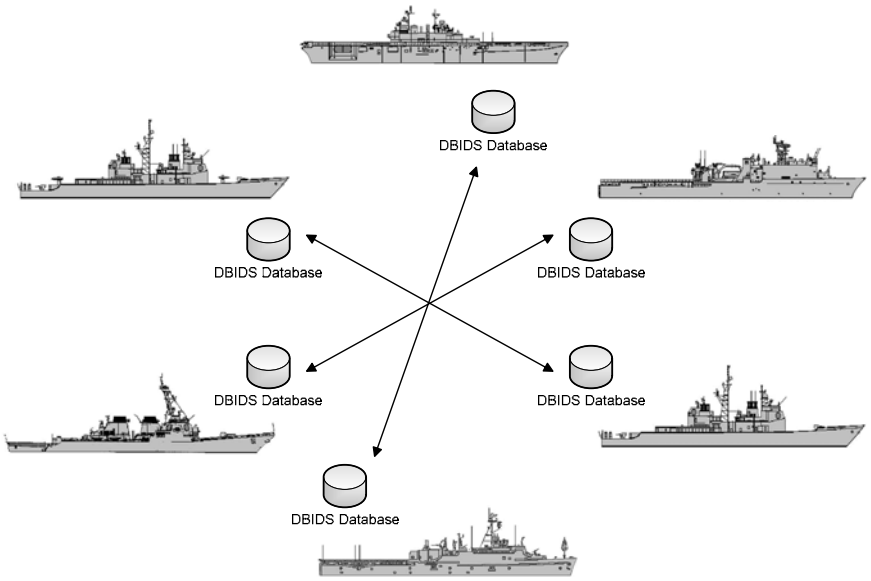


Figure 3. The Recommended Defense Biometric Identification System "To-Be" Expeditionary Strike Group interoperability

Web-enabled database technologies and the internet allow commanders and managers at all levels to share the same visibility of personnel status, on every ESG ship. Web-enabled technology also allows for collaboration and situational awareness tools, providing a common operational picture of the ships status and for the tracking of personnel.

Maintaining a security perimeter around the ship is one of the highest priorities of the ESG. While in foreign

ports, ESG security forces setup physical blockades and provide 24-hour personnel and vehicle access control at the peer. The current DBIDS configuration is not designed to support this operation. By extending the wireless range of the DBIDS scanner using the Institute of Electrical and Electronics Engineers (IEEE) 802.16 Worldwide Interoperability for Microwave Access (WiMAX) standard, ship security and access control are now employed by DBIDS around the entire edge of the security perimeter as seen in Figure 4 below.

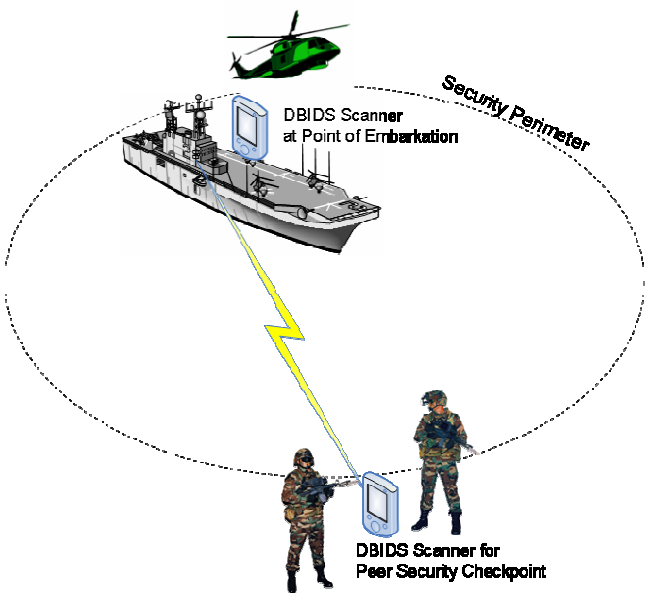


Figure 4. Recommended Defense Biometric Identification System "To-Be" wireless capability

Wireless networking technologies such as WiMAX creates mobile DBIDS scanners for use at all points of embarkation on ship, also seen in figure 4. In the event of cross deck or amphibious operations, only one person is required to physically verify who is departing, IDs are scanned and the information is updated instantly in the DBIDS database. For leave and liberty applications, a DBIDS scanner is

located at every ship access control point to automatically track who did not return from leave and liberty on time. At the expiration of leave or liberty, commanders know instantly who did not return on time by accessing the DBIDS website.

2. Recommended Changes to the Non Combatant Evacuation Operation Tracking System

In the appendix, BPR and KVA is used to identify beneficial changes to the NEO and NTS. To make those changes possible, system upgrades are required for the NTS. Figure 5 below is one example of how to upgrade the NTS.

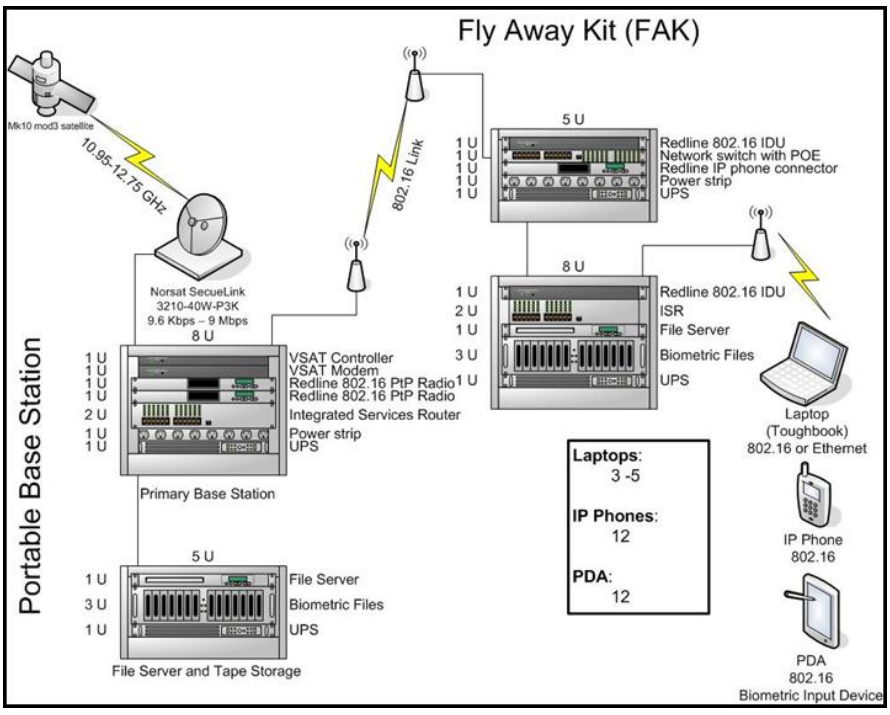


Figure 5. Example upgrade for the Non Combatant Evacuation Operation Tracking System [From 21]

The incorporation of a biometric file server is required for the incorporation of the Trusted Traveler business model in the NEO. A biometric file server stores

and retrieves evacuee biometric data that is collected during the pre-registration process. This allows biometric scanning technologies to reduce the time required to quickly identify and process the evacuee through the ECC. Coordinated efforts by foreign country governments and the Department of State for NEO pre-registration is a key enabler. A web-based, self-service oriented, biometric registry system for data collection allows for easy registration by foreign travelers.

The NTSs bandwidth is improved by replacing the current Inmarsat unit with Norsat's Secure Link Portable iDirect (IP) Data Terminal, which provides data rates of 9.6 Kbps to 8.448 Mbps. The increased bandwidth allows for the incorporation of additional supporting technologies.

Web-enabled technology such as collaboration and situational awareness tools are incorporated to provide a common operational picture of the NEO and tracking of evacuees. Much like the Texas Evacuation Tracking System, geospatial technology through the integration of geographic information system databases, provides status and tracking displays linked to a barcode [22]. Figure 6 below shows an example of a common operational picture and the tracking of evacuee movements in real-time.

Figure 6. Example of Non Combatant Evacuation Operation Tracking System real-time data feed for situational awareness and evacuee tracking

IEEE 802.16 WiMAX wireless networking technology provides secure, high data rate, wireless computing. Wireless technology increases the speed of setting up multiple NTS registration stations at an ECC site by eliminating the need for complex wiring configurations. Additionally, wireless technology enables the use of internet protocol (IP) telephones and biometric scanning devices. WiMAX technology is preferred over Wireless Fidelity (WiFI) because of the built in security features and the increased range for portable devices.

Finally, software simulation tools for personal computers such as Arena or Extend software should be developed and included with the NTS for planning purposes. Figure 7 below is a model of the NEO developed with Arena software.

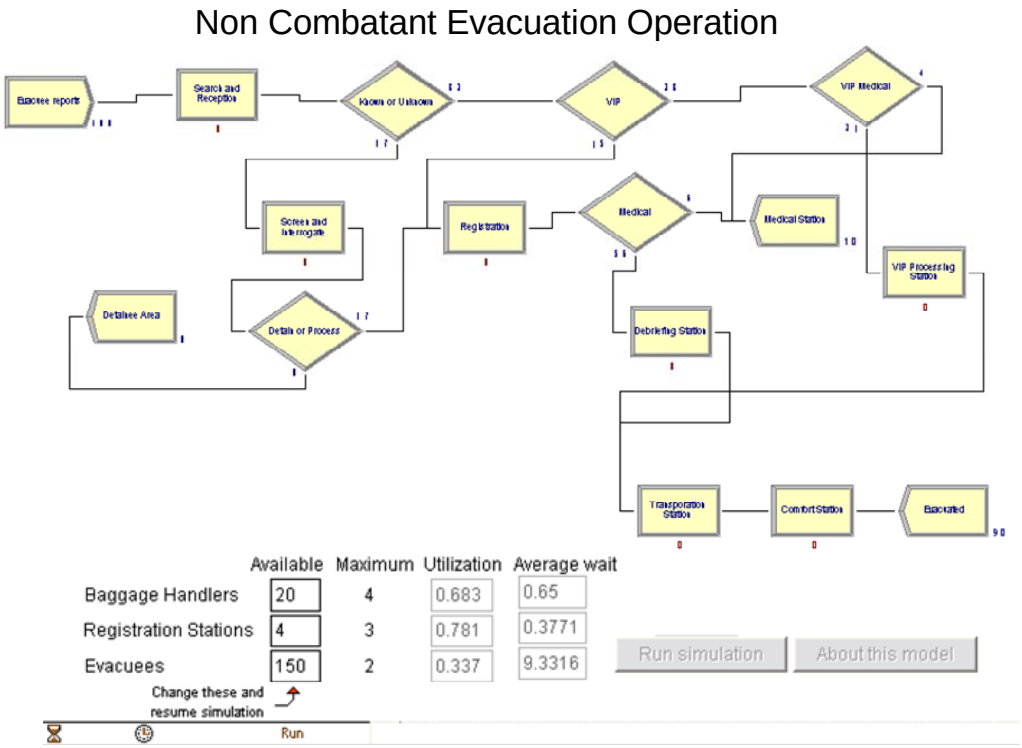


Figure 7. Example of Non Combatant Evacuation Operation simulation using Arena software

Elaborate simulation tools developed by Operations Research experts are used by ESG NEO planners to quickly identify manpower, time and NTS system configuration requirements, based on the given operational scenario.

3. Conclusions

The purpose of this thesis is to establish and identify best practices and technologies to help resolve ESG IM problems. The scope is limited to personnel IM issues at the operational level to show ESG commanders and other IT stake holders how best practices and technologies can be implemented. However, the best practices and technologies may provide similar results outside of the ESG and may be applicable to other public or private domains.

Chapter I explores the motivation and background information to define the many different aspects of IM. For this thesis, the definition of IM is the ability to uniquely and unambiguously identity people and entities, identify their interactions and interrelationships, and track their mobility in a timely fashion [1]. IM plays a critical role in virtually every management process involving personnel or material and is applicable to all types of organizations, public or private. Personnel IM IT can be a critical enabler for many universal functions, including: security, law enforcement, intelligence, human resource management, business administration, logistics, supply, and others.

IM provides the focus to integrate new and multiple technologies into one enterprise wide information system. For example, the U.S. Secretary of the Navy recently issued an initiative to formalize a long term strategy to meet the operational and support requirements necessary for identity sensitive applications across the Navy and Marine Corps. Initial efforts are focused on the development of an enterprise wide IM systems architecture in support of: base and vessel access controls, law enforcement, emergency operations, expanded maritime interception operations, raids, civil support and humanitarian support operations. An incremental approach will allow for the future integration of other applications and technology such as RFID for the identification and tracking of equipment and supplies [23].

Chapter II provides an overview of DoD human resource management and the current efforts of the DMDC to provide enterprise wide personnel IM IT solutions. The DMDC sponsored RAPIDS, NTS and DBIDS are programs of interest to

ESG commanders and other IT stake holders because they are already in use with operational forces. The systems continue to evolve as the program managers look for ways to integrate new technology, databases, files, and computer programs.

Chapter III introduces the unique requirements for ESG personnel IM IT. ESG personnel identification, accountability and tracking are basic requirements for leadership, management, administration, logistics, embarkation, security, operations, medical and other functional areas. The ideal personnel IM system for the ESG automates personnel identification and tracking and the sharing of that data in real time, across different departments, branches of service and ships. The ideal system provides a higher level of operational efficiency and situational awareness, but also introduces many new challenges associated with the use of IT, including a higher level of commitment by ESG forces to ensure the program's success.

There are many challenges associated with ESG personnel IM IT, but the biggest challenge starts with IT program development and implementation at the DoD enterprise level. Legacy systems, including personnel IM information systems, are traditionally pushed down to ESG forces vertically or "stove piped" to provide a solution to one functional area, such as the DBIDS for security and access control. Each functional area, such as: administration, logistics, security and operations has their own "stove piped" system with individual data sets. ESG IM suffers from inefficient data sharing from a lack of horizontal systems integration. For many ESG IM processes, technology is not used at all. Large reports and manifests

are generated by hand, re-typed and E-mailed, to manually update other systems. The lack of timely fielding equipment and proper training is resulting in problems with implementing IM IT solutions.

The U.S. Federal government continues to struggle with similar legacy systems issues, but on a much larger scale. After the attacks of September 11th, the U.S. Department of Homeland Security identified the need for a new National IM information system to track "persons of interest" across the DoD, Federal Bureau of Investigation, Central Intelligence Agency, local law enforcement, and other government agency systems. The efforts by the Department of Homeland Security to create a new National IM information system were never realized because of the complexities involved with systems and data integration across the various agencies legacy systems. There are no simple solutions to fix the problems associated with legacy systems and data integration in the public or private sector.

To make a positive impact on solving enterprise wide personnel IM issues, the DoD should look to America's most successful private sector organizations who realize the benefits associated with enterprise architecture and software product lines. Product line architectures, such as those provided by Oracle and SAP, achieve significant cost and effort reductions through large scale reuse of software product assets. Developers quickly assemble high quality solutions from a suite of existing software components [24]. Organizations with enterprise resource planning systems share common data between operations, human resources, supply, logistics, procurement, financial, order management, inventory and facilities management

systems and are experiencing the benefits of integrating RFID technology as for supply chain management.

Chapter IV explains the importance of using metrics to understand and identify the true value of IT. In the appendix, BPR is used in a NEO study to identify ways to improve the NTS and increase its attractiveness. The study also uses KVA and ROK to derive an answer to the question, "What does the NTS do for ESG commanders and other IT stake holders?" By comparing the measurements taken before and after BPR and using an average of 1500 evacuees as the baseline, the study found positive results for ESG commanders. The NTS saves a significant amount time and money per NEO. Other potential benefits were discovered through the radical redesign of the NTS. By incorporating the Trusted Traveler business model, a pre-registration and biometric identification IT, the NTS saves even more time and money and greatly enhances the ability to process over 100,000 evacuees. The tools of BPR and KVA can be used by any public or private entity to help determine if the NTS is a "good fit" for their own operational environment.

Finally, Chapter V provides recommendations to establish and identify best practices and technologies to help resolve ESG IM problems. The recommendations are focused on resolving personnel IM issues at the operational level to show ESG commanders and other IT stake holders how best practices and technologies can be implemented. However, the best practices and technologies may provide similar results outside of the ESG and may be applicable to other public or private domains.

A new ship configuration for the DBIDS allows for the addition of web-enabled database technologies and the mirroring of databases to provide a higher level of

situational awareness. The DBIDS, collects, processes and shares changes in personnel status as they occur across all ships of the ESG. A new DBIDS website is accessible through the intranet and provides the ability to customize queries and print reports. This also facilitates the integration of personnel status with the common tactical picture provided by software like Command and Control Personal Computer. Mirroring and/or swapping the DBIDS database with legacy and or other systems helps to solve some of the issues with systems and data integration. The DBIDS database is the single most authoritative personnel database in the ESG and is available to download as a database file to integrate with other software programs like Microsoft access. Linking to an authoritative biometric database would allow for the integration of new technologies, such as the Trusted Traveler business model or checking against a known terrorist database at a biometric fusion center. The authoritative biometric information is downloaded and stored on ship to quickly process the matching of biometric data. Adding a wireless network allows the DBIDS scanner to move around anywhere on the ship, to capture changes in personnel status in all scenarios, not just for ship boarding and departing. While in port, the extended operational range of the DBIDS scanner from its access point allows for an added layer of security to extend out to the edge of the ships safety perimeter.

The NTS upgrade includes the incorporation of a biometric file server for the Trusted Traveler business model and also provides the ability to quickly check against a database of known terrorists. A pre-registration biometric enrollment website for foreign travelers is a key

enabler to make the Trusted Traveler business model successful. An increase in bandwidth provides for the integration of web-enabled database technologies, such as situational awareness tools that provide a common tactical picture and the tracking of evacuees. The incorporation of wireless networking technology provides for the extended use of wireless devices such as biometric readers and IP telephones. Finally, software simulation tools for personal computers such as Arena or Extend software are developed and included with the NTS for planning purposes. Elaborate simulation tools developed by Operations Research experts are used by ESG NEO planners to quickly identify manpower, time and NTS system configuration requirements, based on the given operational scenario.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. NON COMBATANT EVACUATION OPERATION TRACKING SYSTEM AND KNOWLEDGE VALUE ADDED

NAVAL POSTGRADUATE SCHOOL

BUSINESS PROCESS RE-ENGINEERING WITH E-BUSINESS TECHNOLOGIES

THE NTS

BY

MAJ JEFF WITHEE
CAPT CHUCK HILL
CAPT GLEN NEISES
CAPT EDDIE PENA

FOR PROFESSOR:

DR. TOM HOUSEL

MARCH 2007

A. INTRODUCTION

The project we decided to work on is the NTS based out of Fort Ord's DMDC. Our point of contact was U.S. Army Major, Larry Chinnery. When we spoke to Major Chinnery he expressed his desire to increase the military's use of the NTS by demonstrating the benefits of the system and to improve it in any way possible in order to increase its attractiveness. Major Chinnery explained that, for larger operations, the system would streamline the process considerably and that even for smaller NEOs this system will increase access to the information gathered and the status of the operation for stakeholders.

B. THE PROJECT

In order to fully comprehend the system we studied the NEOs documented on Globalsecurity.org. On the high end, there was the evacuation of Vietnam in 1975 which totaled over 175,000 evacuees. On the low end, there was the evacuation in Bangui, CAR in 2002 which totaled 39 evacuees. After studying all of the reports we decided that the Vietnam and Bangui NEOs were outliers that could be excluded so as not to skew the statistical analysis. From those reports, and after speaking with the system experts, we came up with an average number of evacuees per NEO for the purpose of this project.

The Navy/Marine Corps team is the branch of the armed services that most commonly conducts NEOs due to their worldwide presence and expeditionary nature. However, the instruction manual on the subject is a joint publication

titled "Joint Tactics, Techniques and Procedures for NEOs." From this document and the NTS documentation we were able to get a clear picture of the "As is" process.

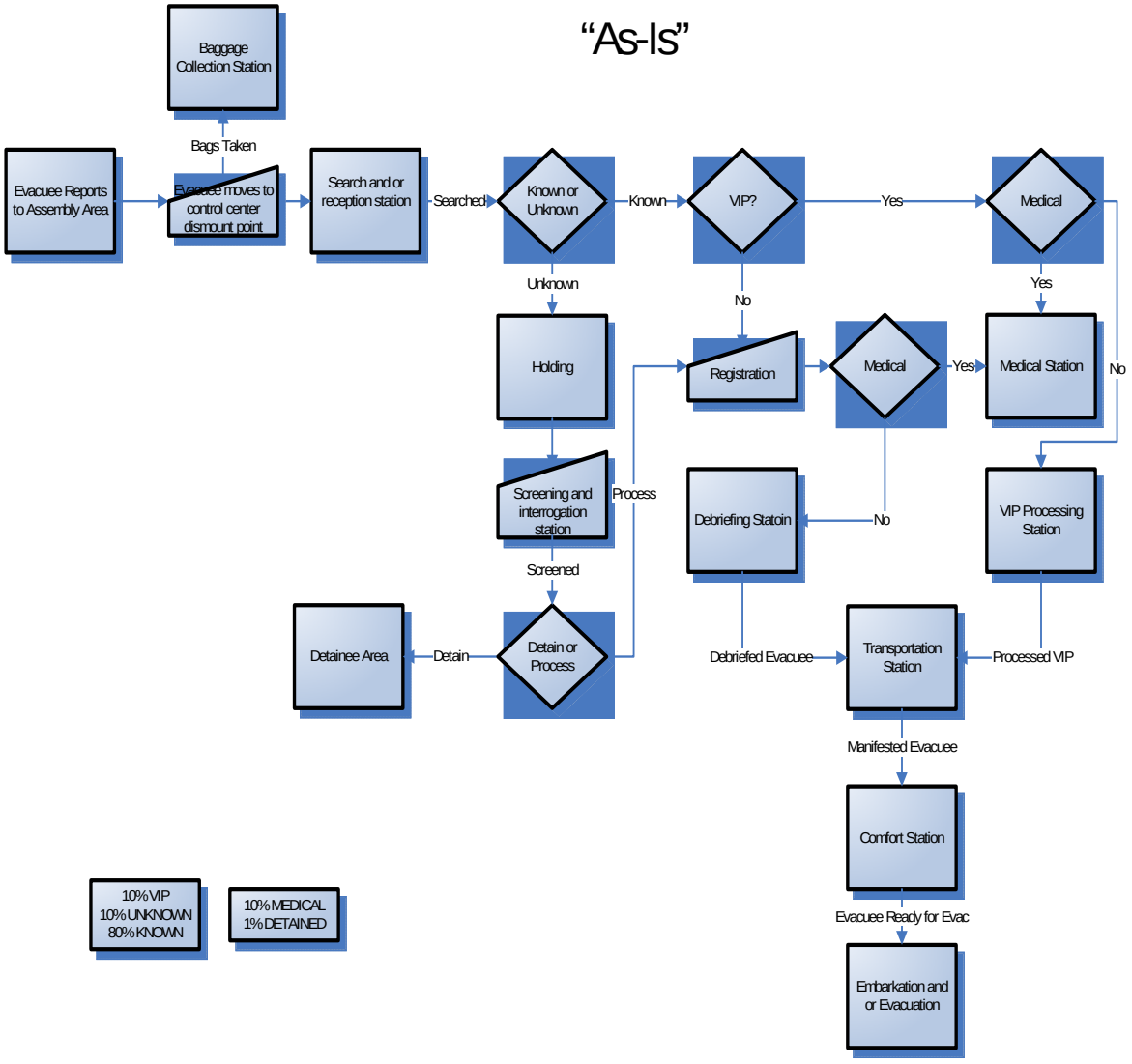


Figure 8. "As-is" Process Flow Chart

Below are short descriptions of the major stations of a NEO. The descriptions come directly from the joint publication on NEOs:

1. Reception Station

The reception station personnel collect all available information from the marshalling teams who escort the evacuees. From there, the evacuees are moved into a holding area where the evacuees are searched, segregated by family, group, or classification (Very Important Person (VIP), medical, no identification, etc) and given an initial brief to describe the process and ease fears about the evacuation.

2. Registration Station

Here, evacuees will complete all administrative paperwork required to evacuate.

3. Debriefing Station

This station is optional, depending on the situation and the time available to conduct the evacuation. It should be staffed by counterintelligence personnel who are able to speak the local language. Each evacuee should be debriefed to obtain information that may affect the evacuation force, its mission, the evacuees, or other activities in the country.

4. Medical Station

The medical station provides emergency medical treatment and immunizations required by the safe haven country. As required, injured or ill evacuees may proceed through the medical station for first aid and to identify medical conditions that may have an effect on the evacuation process. Serious medical cases receive top

priority for evacuation. However, the medical officer ensures that any seriously ill, injured, or wounded persons complete processing.

5. Transportation Station

Transportation personnel prepare each group of evacuees for embarkation aboard aircraft, ships, or surface vehicles.

6. Comfort Station

The comfort station is a temporary waiting area for evacuees until they board evacuation transportation. Comfort station personnel should make the evacuees' stay as untroubled as possible and provide some degree of privacy.

It was evident that the "As-Is" process could benefit greatly from the use of modern IT such as the NTS and could make even further gains from a radical redesign. Our first task was to come up with an accurate representation of their process for a KVA analysis. Using the process flowchart we developed a KVA spreadsheet in Microsoft Excel. Our KVA spreadsheet depicting their "As-Is" process is shown on the following page:

Processes	ALT	Percentage of	K Fired	ALT * Fired	Percent	#Emp	Cost/Pd	Process	Market Premium	Market Comp	Process	ROK	ROI
	Hours	Total LT	Per Hour		Allocation		Per Hour	Cost	Comp	Total Revenue	Revenue		
Baggage Collection	10	1%	60	600	2.64%	13	$ 20.00	$ 260.00	$ 28.00	$ 364.00	$33.60	12.92%	-87.08%
Search & Receive	23	3%	36	828	3.64%	7	$ 25.00	$ 175.00	$ 18.00	$ 126.00	$46.37	26.50%	-73.50%
Screen & Interrogate	48	7%	2	96	0.42%	2	$ 35.00	$ 70.00	$ 40.00	$ 80.00	$5.38	7.68%	-92.32%
Register	2	0%	48	96	0.42%	4	$ 12.00	$ 48.00	$ 12.00	$ 48.00	$5.38	11.20%	-88.80%
Medical Admission	40	6%	4	160	0.70%	2	$ 18.00	$ 36.00	$ 20.00	$ 40.00	$8.96	24.89%	-75.11%
VIP Processing	3	0%	24	72	0.32%	2	$ 22.00	$ 44.00	$ 30.00	$ 60.00	$4.03	9.16%	-90.84%
Debrief	80	11%	36	2,880	12.65%	3	$ 35.00	$ 105.00	$ 40.00	$ 120.00	$161.28	153.60%	53.60%
Transportation Arrangement	480	68%	36	17,280	75.90%	6	$ 30.00	$ 180.00	$ 30.00	$ 180.00	$967.67	537.60%	437.60%
Comfort Evacuees	1	0%	36	36	0.16%	5	$ 12.00	$ 60.00	$ 13.00	$ 65.00	$2.02	3.36%	-96.64%
Embark Into Transportation	20	3%	36	720	3.16%	6	$ 22.00	$ 132.00	$ 32.00	$ 192.00	$40.32	30.55%	-69.45%
Total	707	100%		22,768	100.00%			$1,110.00		$1,275.00			

Figure 9. “AS-is” Knowledge Value Added Spreadsheet

Figure 6 represents the process of the flowchart with Knowledge Value attributes assigned to the process. These are the core processes associated with conducting a typical NEO. We used rank order of learning complexity, actual learning time, and normalized learning time. We found that using the current process the "bottle-neck" was the registration station that only allowed 36 people to be processed per hour. This problem will be addressed by the IT solution developed by the DMDC.

C. THE SOLUTION

The incremental solution for this process has already been developed by the DMDC but we felt it was not being used effectively. The few times the NTS was used in a real world scenario and in training exercises, it was used as part of the registration process. This method did not fully leverage the benefits this system was capable of. Instead, we recommended that the registration station NTS be moved to the beginning. The benefits of this are that it improves the accuracy of information that used to be entered manually, eliminates the traffic jam at the registration station, decreases the cost of conducting the NEO, and adds the intangible benefit of allaying the evacuees fears much sooner because they are manifested and assigned a boarding pass/bracelet upon completing this station. Our incremental solution is depicted below:

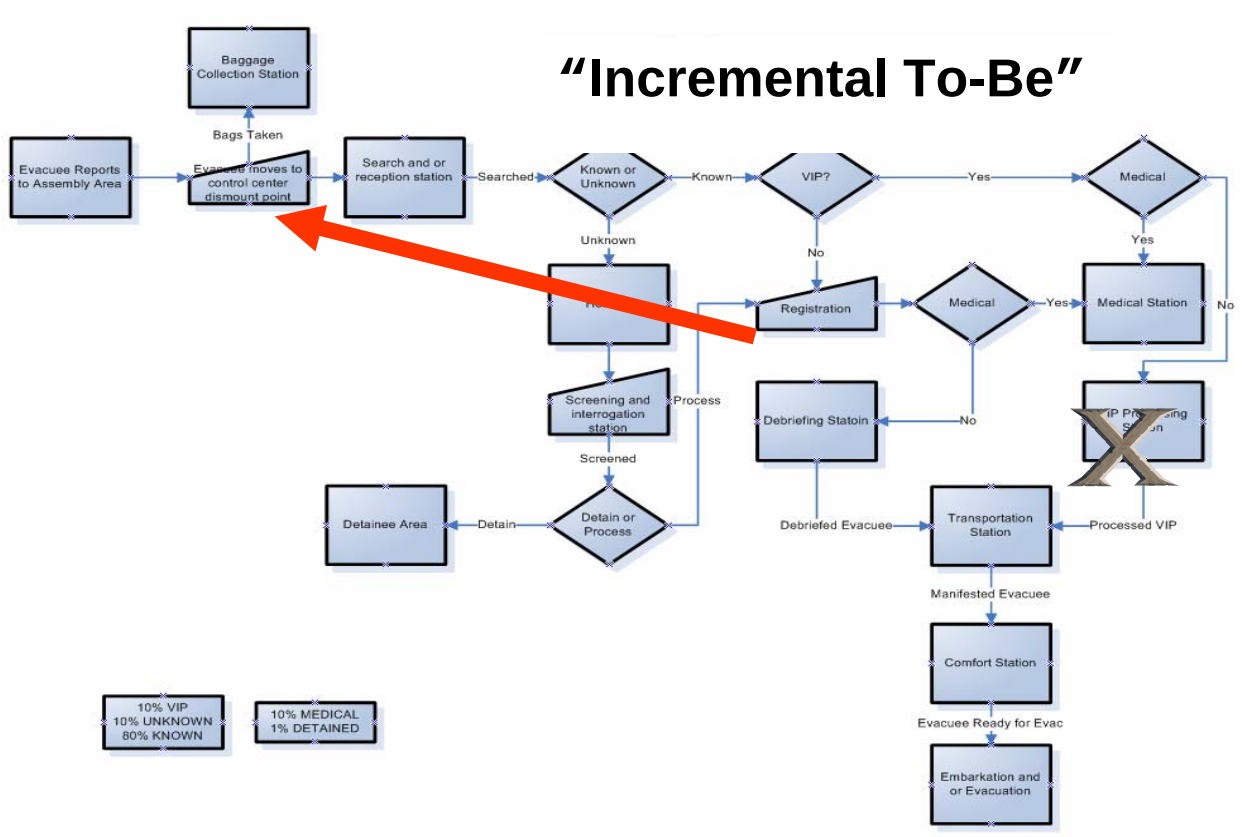


Figure 10. Incremental To-Be

The areas we targeted were the registration station and the VIP processing station. We reasoned that by utilizing IT in the form of the NTS, we could streamline and automate the process considerably. In addition to the benefits cited above, the NTS would allow stakeholders and family abroad to view the progress of the NEO as well as the information gathered at any point in the process. This would be done via a web-enabled database that families could access to confirm that their loved one was processed for evacuation. It would also allow personnel with higher level access to get a more detailed picture of the status

of the evacuation thereby eliminating the need to constantly call someone at the site to find out the current progress.

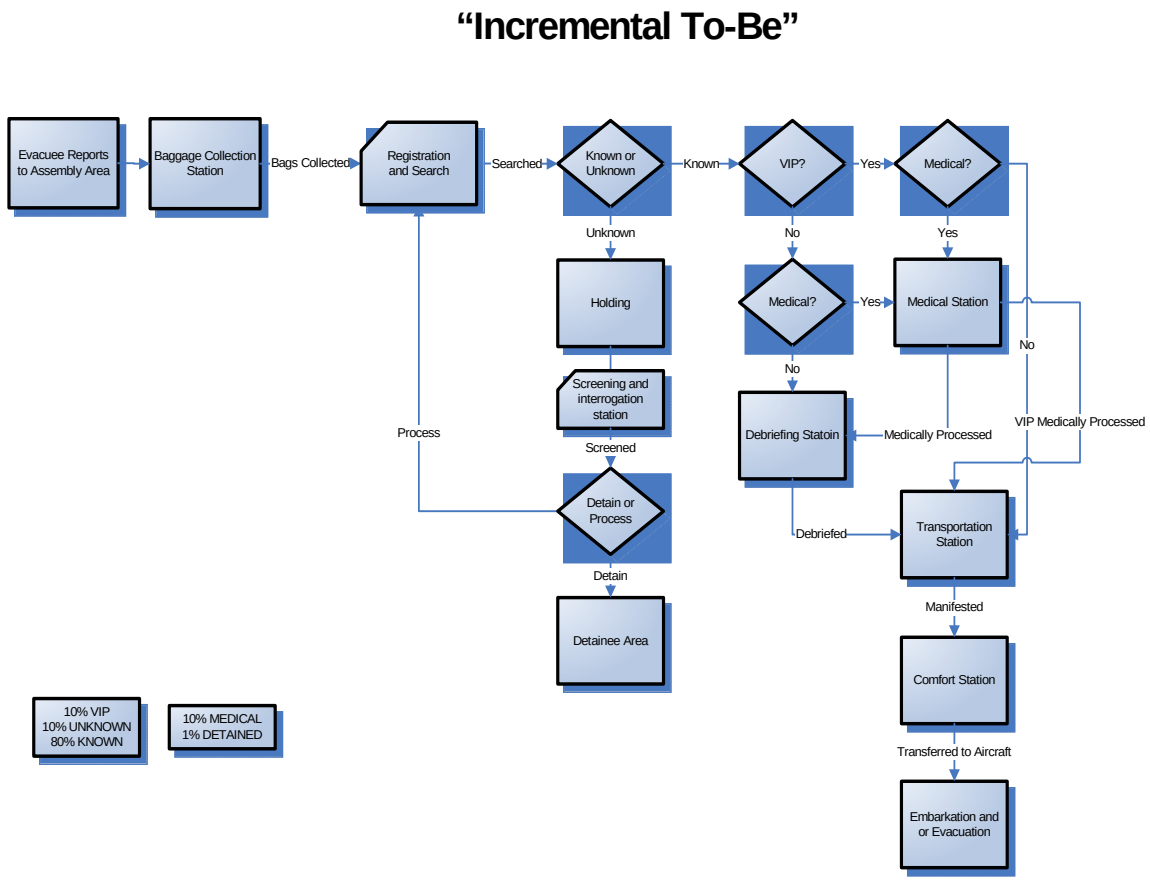


Figure 11. Incremental To-Be

Based on our new "To-Be" process flowchart, we developed a new "To-Be" KVA analysis, depicted below (Figure 12). As can be seen, our solution made heavy use of IT. The processes we re-engineered showed an average increase in the use of IT of nearly 80%.

KVA with NEO Tracking System

Processes	ALT Hours	K Fired Per Hour	ALT * Fired	Process Cost	Market Comp Total Revenue	Percentage Of IT	Cost Of IT	Amortized Cost	Cost Per Fire	ROK	ROI
Baggage Collection	10	60	600	$ 260.00	$ 364.00					12.69%	-87.31%
Register & Search	55	60	3,300	$ 250.00	$ 180.00	33.00%	$42,694.00	$ 4,269.40	$ 2.85	48.64%	-51.36%
Screen & Interrogate	48	2	96	$ 70.00	$ 80.00					7.54%	-92.46%
Medical Admission	40	4	160	$ 36.00	$ 40.00					24.44%	-75.56%
Debrief	80	60	4,800	$ 105.00	$ 120.00					251.43%	151.43%
Transportation Arrangement	480	60	28,800	$ 180.00	$ 180.00					880.00%	780.00%
Comfort Evacuees	1	60	60	$ 60.00	$ 65.00					5.50%	-94.50%
Embark Into Transportation	20	60	1,200	$ 132.00	$ 192.00					50.00%	-50.00%
Total	734		39,016	$1,093.00	$1,221.00						
					$2,145.88						

Figure 12. "To-Be" Knowledge Value Added Spreadsheet

After analyzing the charts we noticed that the limiting factor was still the registration station but that it had improved considerably and was now able to handle 60 evacuees per hour.

D. RADICAL REDESIGN

Next, we developed a radical redesign of the process. As is common when trying to improve public systems we considered what were the "best practices" in the civilian arena for a system similar to the one we were studying. The San Jose Airport currently has a Trusted Traveler system called "Clear" that we thought could yield some benefits in our project. After studying this and other "Trusted Traveler" systems we produced a radical redesign of the system (depicted below). The "Trusted Traveler" program basically qualifies, segregates, and vets all evacuees prior to them needing evacuation so that time can be saved compared to having to conduct these tasks during the actual evacuation. By instituting this program, you would not only move the registration process to the

beginning of the process but you would also eliminate/combine some stations and be able to move the transportation station further up as well.

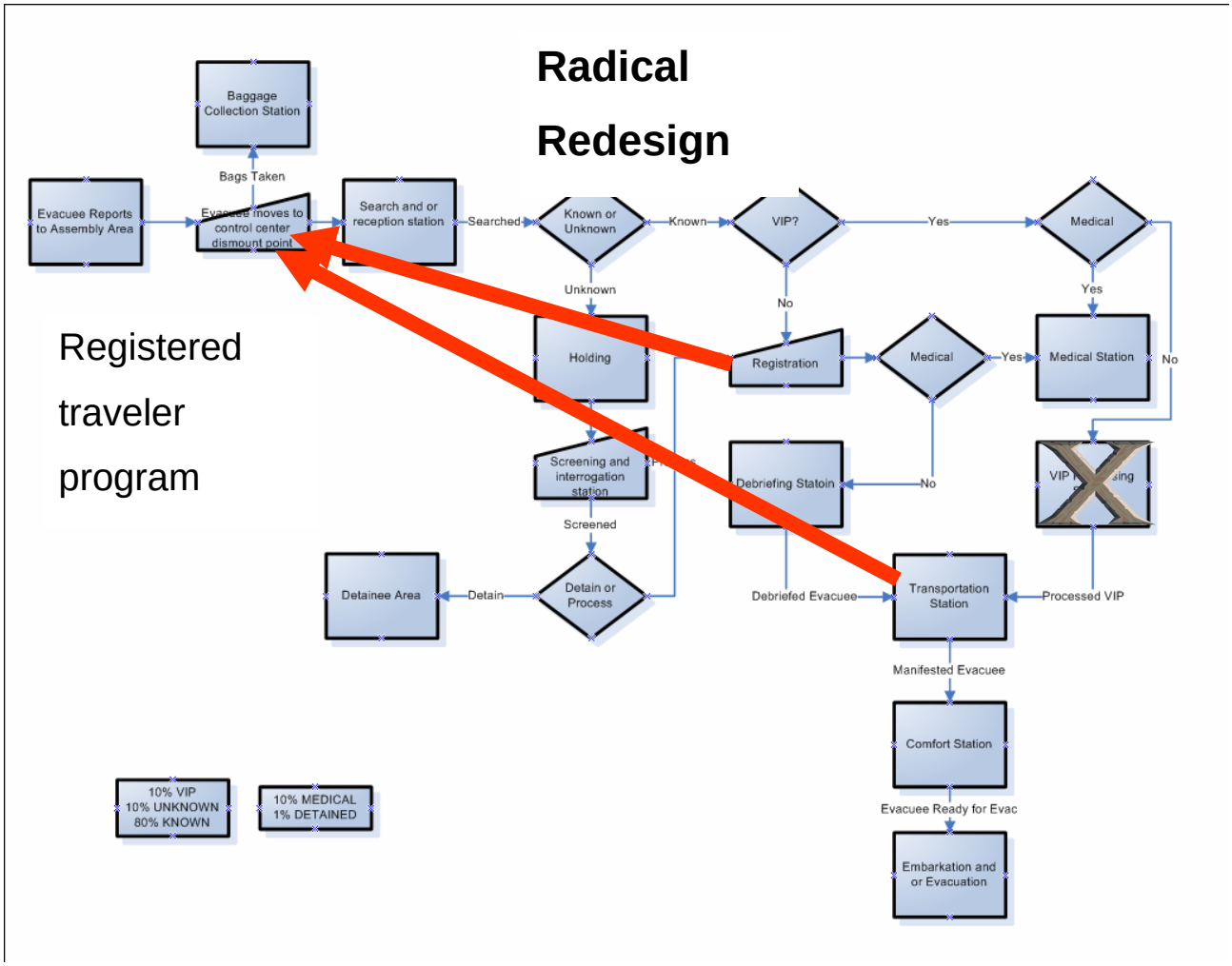


Figure 13. Redesign Flowchart

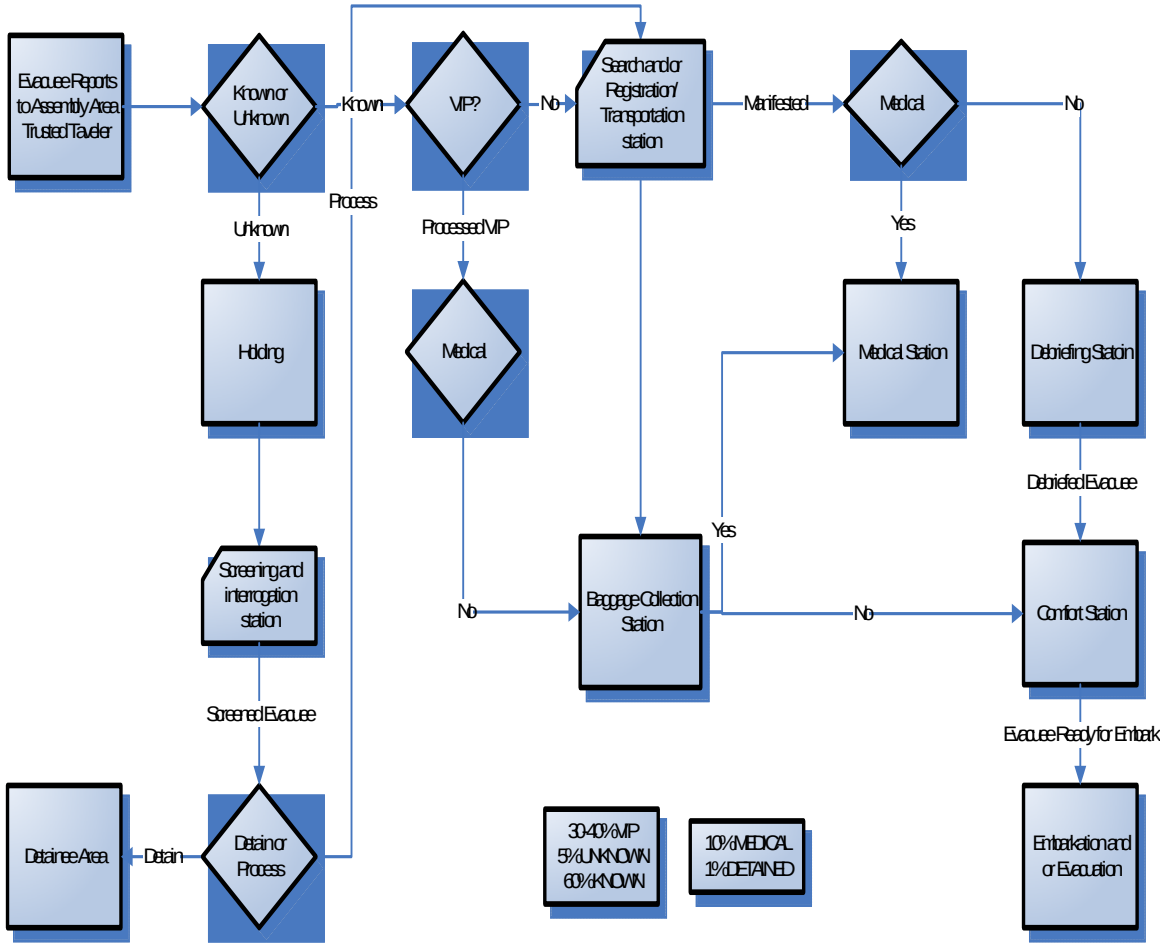


Figure 14. Radical Redesign

As can be seen in the flowchart, instituting a “Trusted Traveler” Program at embassies worldwide would considerably streamline and expedite the NEO process even further. An additional and intangible benefit of combining the NTS system with a redesign of the system is that it gives evacuees peace of mind much sooner than the “As-is” process.

KVA of Radical Redesign

Processes	ALT Hours	K Fired Per Hour	ALT * Fired	Process Cost	Market Comp Total Revenue	Percentage Of IT	Cost Of IT	Amortized Cost	Cost Per Fire	ROK	ROI
Trusted Traveler Check-In	625	100	62,500	$ 25.00	$ 28.00	95.00%	$28,872.00	$ 2,887.20	$ 5.77	687.50%	587.50%
Baggage Collection	10	90	900	$ 340.00	$ 476.00					14.56%	-85.44%
Register & Search	70	60	4,200	$ 250.00	$ 180.00	33.00%	$42,694.00	$ 4,269.40	$ 4.27	61.91%	-38.09%
Screen & Interrogate	48	2	96	$ 70.00	$ 80.00					7.54%	-92.46%
Medical Admission	40	4	160	$ 36.00	$ 40.00					24.44%	-75.56%
Debrief	80	90	7,200	$ 105.00	$ 120.00					377.14%	277.14%
Comfort Evacuees	1	90	90	$ 60.00	$ 65.00					8.25%	-91.75%
Embark Into Transportation	20	90	1,800	$ 132.00	$ 192.00					75.00%	-25.00%
Total	894		76,946	$ 993.00	$1,153.00						
					$4,232.03						

Figure 15. Redesign Spreadsheet

E. CONCLUSION

After comparing the three methods using an average of 1500 evacuees as the baseline, we find that the incremental redesign saves us $14,665 per NEO and the radical redesign saves us over $18,000 per NEO. At first glance it would seem that the incremental redesign using just the NTS and moving the registration process to the front would be close enough without adding additional training time and cost. However, the real benefit to the radical redesign would be in a scenario where there were a large number of evacuees, like Vietnam in the past or a possible South Korea evacuation in the future (estimates range from 100,000 to 200,000 evacuees). The analogy would be the difference between a Ford Pinto, Taurus, and Mustang GT. The “As-is”

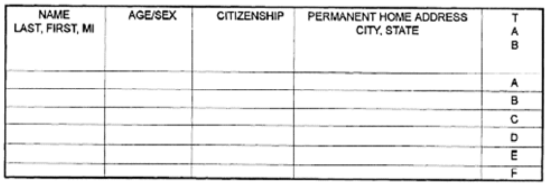
is a Pinto, the incremental is a Taurus and the radical redesign is a Mustang GT. The Pinto will get you where you need to go but it can not get you there quickly nor efficiently. The Taurus will perform well the majority of the time but it lacks speed. The Mustang gives you the speed you need when you have a large distance to cover (e.g. many evacuees) but it costs a little more and consumes more gas (takes longer to train people). However, when you have 150,000 evacuees or even 15,000 evacuees – you will want the speed that the Mustang gives you. For the purposes of this project we estimated that a third of the potential evacuees would be "Trusted Travelers." If you want the equivalent of the Mustang GT with a hybrid engine you simply need to increase the number of travelers you pre-register and this will increase your throughput and decrease your costs considerably – especially once you address the new bottleneck of baggage handling which is a low knowledge process that can be solved with a platoon of strong Marines or sailors. In short, do not wait until you need the speed and efficiency of the radical redesign. Start the "Trusted Traveler" program now and reap the benefits from day one while simultaneously enabling our military forces to better handle a larger crisis if it were to arise. The following spreadsheets illustrate the time and cost savings of each of the follow on systems:

Method					
	Number of Evacuees	**Cost/Hour**	**Hours to Evacuate**	**Cost of System**	**Total Cost**
As-is	1500	$1,110	**42**	**0**	**$46,250**
NTS	1500	$1,093	**25**	**4269**	**$23,056**
NTS & Trusted Traveler	1500	$993	**17**	**7156**	**$9,394**
	Number of Evacuees	**Cost/Hour**	**Hours to Evacuate**	**Cost of System**	**Total Cost**
As-is	15000	$1,110	**417**	**0**	**$462,500**
NTS	15000	$1,093	**250**	**4269**	**$268,981**
NTS & Trusted Traveler	15000	$993	**167**	**7156**	**$158,344**
	Number of Evacuees	**Cost/Hour**	**Hours to Evacuate**	**Cost of System**	**Total Cost**
As-is	150,000	$1,110	**4167**	**0**	**$4,625,000**
NTS	150,000	$1,093	**2500**	**4269**	**$2,728,231**
NTS & Trusted Traveler	150,000	$993	**1667**	**7156**	**$1,647,844**

Table 1. Time and Cost Savings

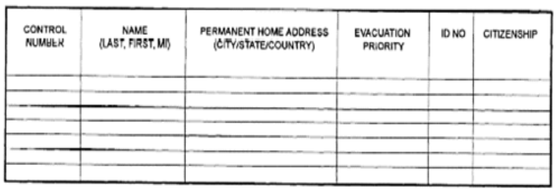
Again, these estimates are developed using 36, 60, and 90 per hour as the throughput for “As-is,” NTS, and radical redesign respectively. The radical redesign could easily be doubled by increasing the number of trusted travelers you pre-register while increasing the number of baggage handlers.

APPENDIX B. ADDITIONAL DIAGRAMS



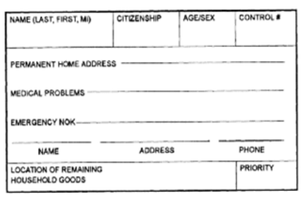
NAME LAST, FIRST, MI	AGE/SEX	CITIZENSHIP	PERMANENT HOME ADDRESS CITY, STATE	T A B
				A
				B
				C
				D
				E
				F

Sample evacuee log book



CONTROL NUMBER	NAME (LAST, FIRST, MI)	PERMANENT HOME ADDRESS (CITY/STATE/COUNTRY)	EVACUATION PRIORITY	ID NO	CITIZENSHIP

Evacuee Register



NAME (LAST, FIRST, MI)	CITIZENSHIP	AGE/SEX	CONTROL #

PERMANENT HOME ADDRESS

MEDICAL PROBLEMS

EMERGENCY NOK

NAME ADDRESS PHONE

LOCATION OF REMAINING HOUSEHOLD GOODS

PRIORITY

Evacuee Information Card

PASSENGER MANIFEST

1. MISSION NUMBER	2. AIRCRAFT/VEHICLE/VESSEL NO.	3. POINT/POE	4. DESTINATION/POD

5. LINE NO. a.	GRADE b.	NAME c.	SSN d.	e. CHECKED BAGGAGE PIECES	WEIGHT	PAX WEIGHT f.	REMARKS g.
		TOTAL FROM FRONT					
		TOTAL FROM BACK					
		TOTALS					TOTAL WEIGHT PASSENGERS AND ALL BAGGAGE

6. I CERTIFY THAT NO UNAUTHORIZED WEAPONS/AMMUNITION/EXPLOSIVE DEVICES, OR OTHER PROHIBITED ITEMS ARE IN THE POSSESSION OF THOSE PERSONNEL FROM WHOM I AM THE DESIGNATED MANIFESTING REPRESENTATIVE OR TROOP COMMANDER, AND THAT THEIR AUTHORIZED WEAPONS HAVE BEEN CLEARED.

a. DATE (YYYYMMDD)	b. PRINTED NAME (Last, First, Middle Initial)	c. GRADE	d. SIGNATURE

DD FORM 2131, SEP 1998 (EG) PREVIOUS EDITION IS OBSOLETE. WHS/DIOR, Oct 98

Passenger Manifest

*FM 90-29

Figure 16.   “As-is” Processing

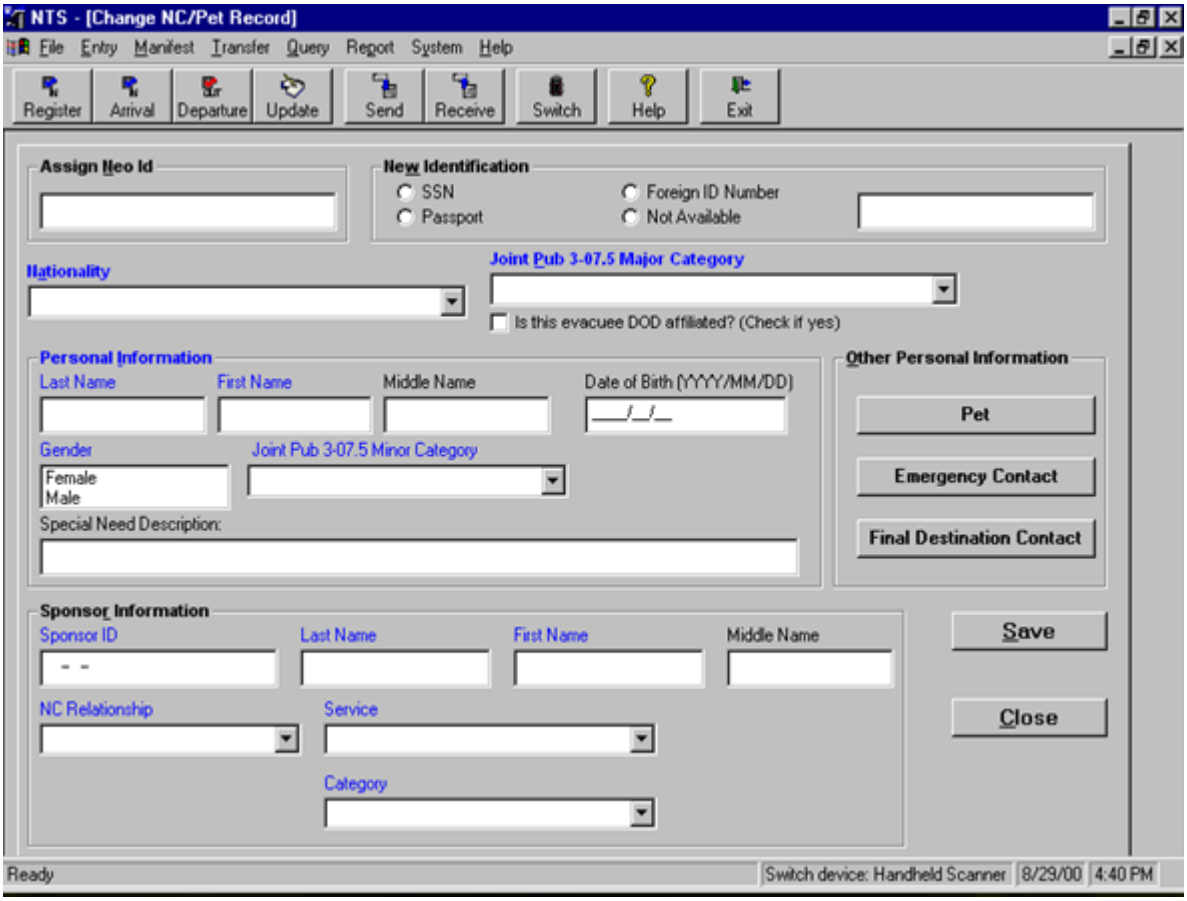
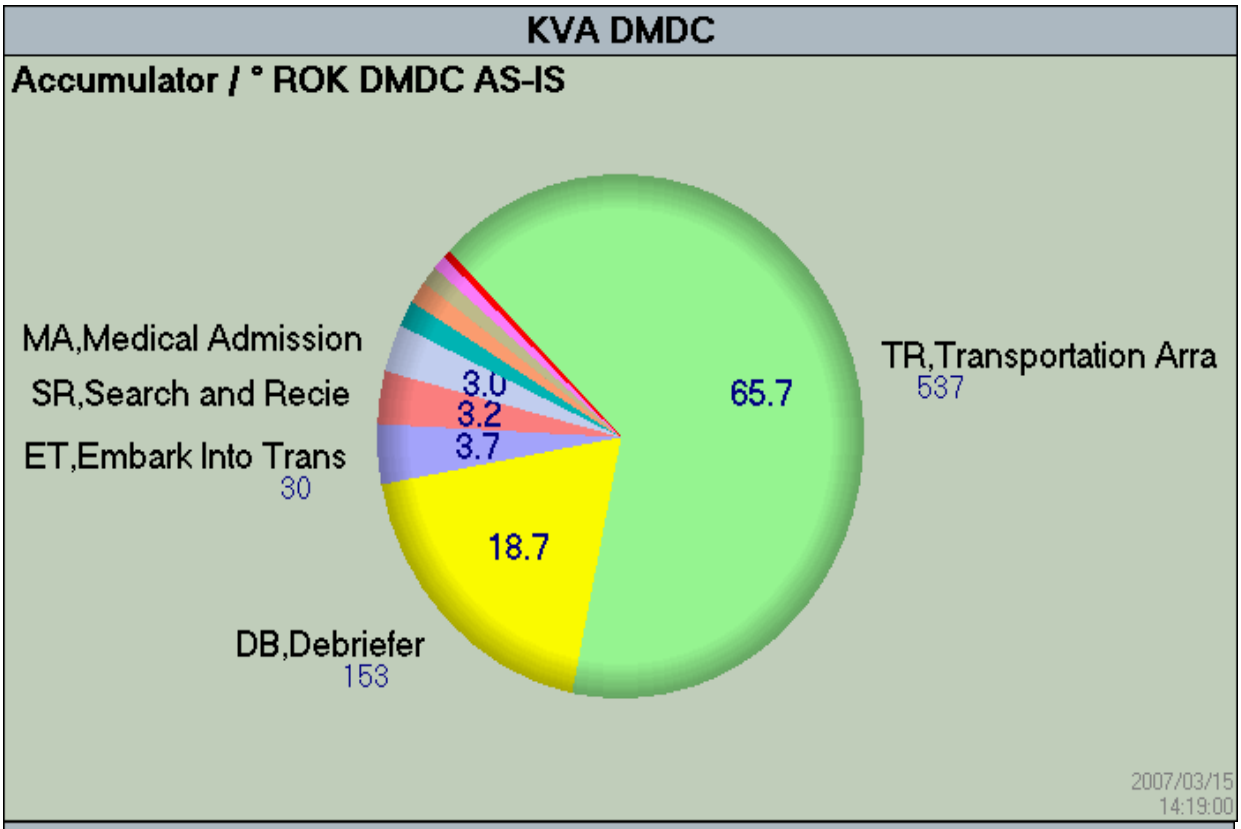
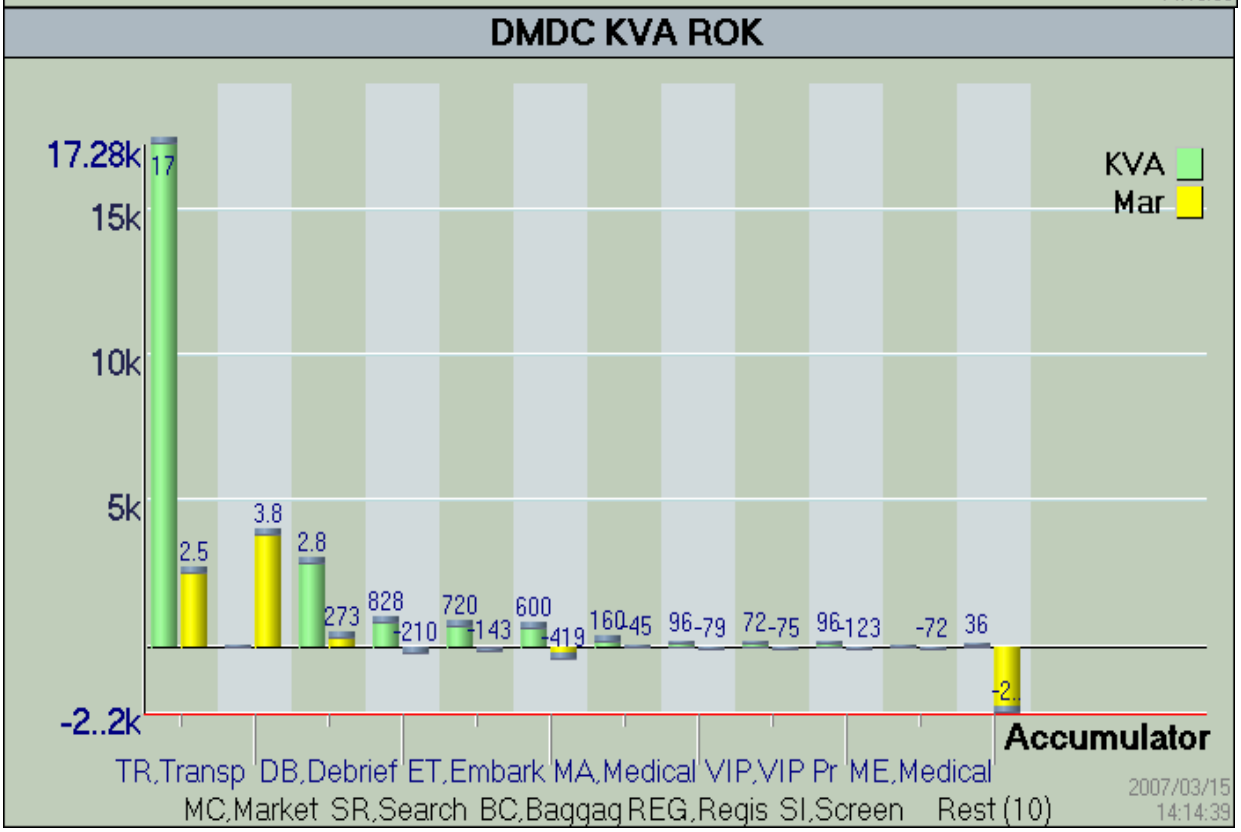


Figure 17. Non Combatant Evacuation Tracking System Processing


KVA DMDC
Accumulator / ° ROK DMDC AS-IS
MA,Medical Admission
SR,Search and Recie
ET,Embark Into Trans
30
3.0
3.2
3.7
65.7
18.7
TR,Transportation Arra
537
DB,Debriefer
153
2007/03/15
14:19:00


DMDC KVA ROK
17.28k
15k
10k
5k
-2..2k
KVA
Mar
17
2.5
3.8
2.8
273
828
210
720
143
600
419
160
45
96
79
72
75
96
123
72
36
-2..
Accumulator
TR,Transp
DB,Debrief
ET,Embark
MA,Medical
VIP,VIP Pr
ME,Medical
MC,Market
SR,Search
BC,Baggag
REG,Regis
SI,Screen
Rest (10)
2007/03/15
14:14:39

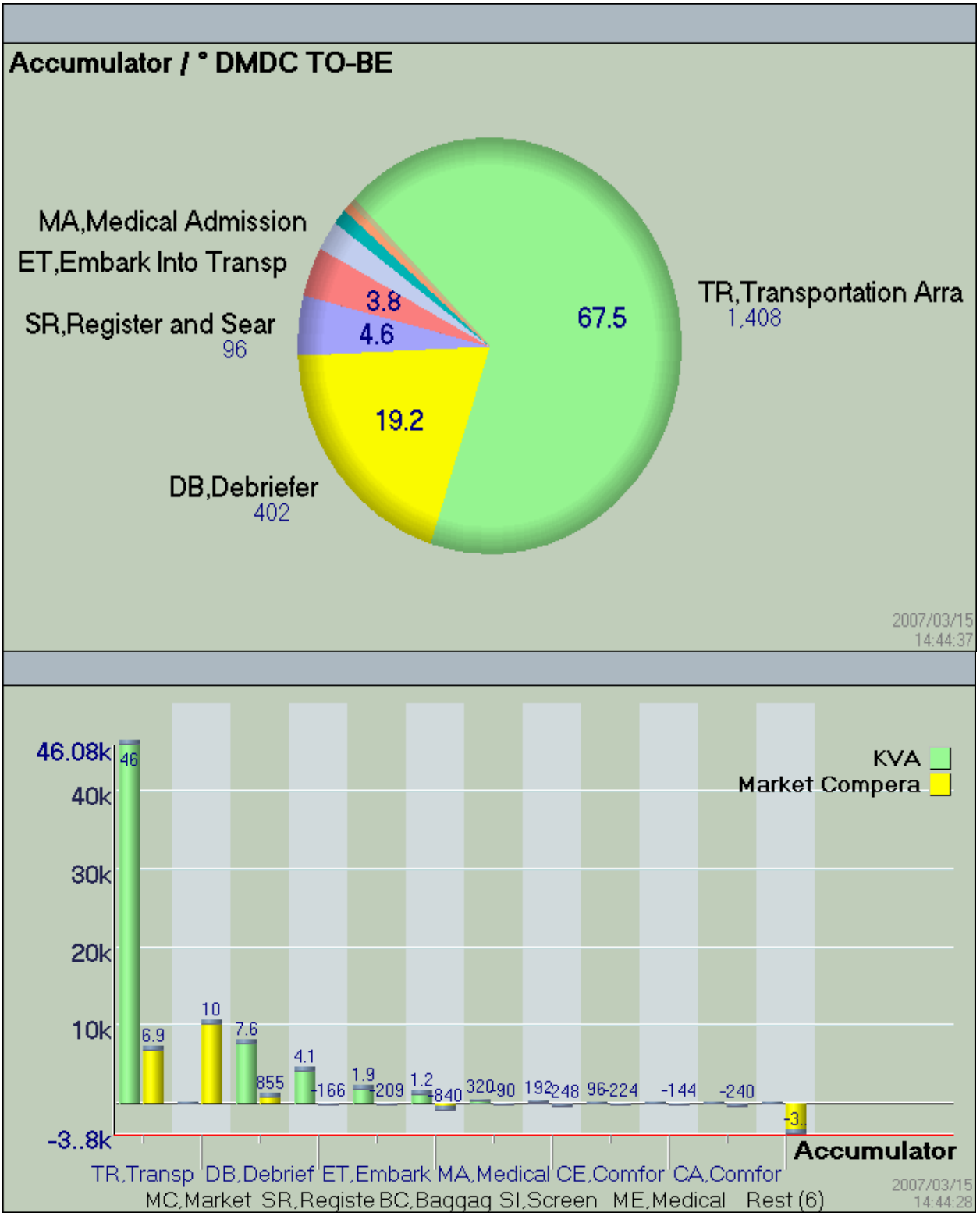


Figure 18. I-Gauss Views

LIST OF REFERENCES

[1] P. Sankar, "White Paper on Global Stabilization and Security, Identity Management: A First Step," Naval Postgraduate School, October 2006.

[2] A. Smith, " National Identification Cards: Legal Issues," The Congressional Research Service - The Library of Congress, CRS Web Order Code RS21137, January 2003.

[3] Wikipedia, "Identity Management," August 2007, http://en.wikipedia.org/wiki/Identity_management #Electronic_Identity_Management_.28IdM.29, accessed July 2007.

[4] Under Secretary of Defense Personnel and Readiness, "About P&R.," July 2006, http://www.dod.mil/prhome/about.html, accessed August 2007.

[5] United States of America, Department of Defense, "DMDC Profile, "Information and Technology for Better, Decision Making," 2004.

[6] Sun Microsystems, "Customer Success Story: The Defense Manpower Data Center, Department of Defense," March 2005, http://www.sun.com/sucess-servers.html, accessed September 2007.

[7] Magdi N. Kamel and Tara L. Lutman, "The Defense Manpower Data Center Pay Data Warehouse: Development and Lessons Learned," Proceedings of the 13th International Workshop on Database and Expert Systems Applications (DEXA'02) 1529-4188/02, IEEE Xplore 2.1, http://ieeexplore.ieee.org.libproxy.nps.navy.mil/, accessed September 2007.

[8] W. Inmon, "Building the Data Warehouse: Getting Started," December 2000, http://www.billinmon.com, accessed May 2007.

[9] SAS Success Story, "The Defense Manpower Data Center," February 2005, http://www.sas.com/sucess/dmdc.html/, accessed July 2007.

[10] Sun Microsystems, "Secure Identity Management at the U.S. Department of Defense White Paper," May 2003, http://www.sun.com/software, accessed September 2007.

[11] C. Krulak, Department of the Navy, Headquarters US Marine Corps, "*Operational Maneuver From the Sea*," Washington, D.C., January 1996.

[12] Expeditionary Strike Group Experimentation, Expeditionary Warfare School Distant Education Program, *Expeditionary Operations*, *Course Book and Readings*, Volume 1, 8656, p. 51.

[13] Privacy International, Interim Report, "Mistaken Identity; Exploring the Relationship Between National Identity Cards and the Prevention of Terrorism," April 2004, http://www.privacyinternational.org, accessed August 2007.

[14] "The Metrics of IT Business Value," *Intel Premier IT Magazine*, Winter 2007.

[15] D. Sward, "Measuring the Business Value of Information Technology," *IT Best Practices Series*, *Practical Strategies for IT and Business Managers*, June 2006.

[16] G. Graves, "The United States Navy Reserve Component's Account Management Challenge in a Navy Marine Corps Intranet Environment," M.S. Thesis, Naval Postgraduate School, Monterey, CA, September 2005.

[17] K. Kovats, "Assessing the Potential Value of Forcenet Technologies within the JFMCC Planning Process Using the VKA Methodology," M.S. Thesis, Naval Postgraduate School, Monterey, CA, June 2006

[18] J. Teng, V. Grover and K. Fiedler, “Business Process Re-Engineering: Charting a Strategic Path for the Information Age,” *California Management Review*, 1994.

[19] T. Davenport and J. Short, “The New Industrial Engineering: Information Technology and Business Process Redesign,” *Sloan Management Review*, Summer 1990.

[20] M. Hammer, “Reengineering Work: Don’t Automate, Obliterate,” *Harvard Business Review*, July-August 1990.

[21] M. Herrera, R. Simmons, B. Rideout, J. Housand, A. Peters, and A. Strickland, "Adapting 802.16 Technologies to Expeditionary Operations," power point presentation for CC 4221, Department of Information Sciences, Naval Postgraduate School, Monterey, CA, May 2007.

[22] G. Wells, "Tracking a Mass Evacuation," *Lessons Learned from Hurricane Rita*," October 2006, http://www.geoplace.com/ME2/dirmod.asp?sid=119CFE3ACE2A48319AA7DE6A39B80D66&nm=News&type=Publishing&mod=Publications%3A%3AArticle&mid=8F3A7027421841978F18BE895F87F791&tier=4&id=6DA6148F866A459C9FA0ACA3EF222800, accessed September 2007.

[23] J. Boyd, "Department of the Navy Identity Management Initiative," power point presentation, Department of Operations Research, Naval Postgraduate School, Monterey, CA, July 2007.

[24] I. Gorton, Essential *Software Architecture*, New York: Springer-Verlag Berlin Heidelberg, 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC,
   Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Head, Information Operations and Space Integration Branch, PLI/PP&O/HQMC, Washington, DC