2007-03

An analysis of the use of the Social Security Number as Veteran Identification as it relates to identity theft : a cost benefit analysis of transitioning the Department of Defense and Veterans Administration to a Military Identification Number

Maraska, Donald G.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN ANALYSIS OF THE USE OF THE SOCIAL SECURITY NUMBER AS VETERAN IDENTIFICATION AS IT RELATES TO IDENTITY THEFT; A COST BENEFIT ANALYSIS OF TRANSITIONING THE DEPARTMENT OF DEFENSE AND VETERANS ADMINISTRATION TO A MILITARY IDENTIFICATION NUMBER

by

George R. Opria
and
Donald G. Maraska

March 2007

Thesis Co-Advisors: William Gates
Bill Hatch

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2007	Master's Thesis

4. TITLE AND SUBTITLE An Analysis of the Use of the Social Security Number as Veteran Identification as it Relates to Identity Theft; A Cost Benefit Analysis of Transitioning the Department of Defense and Veterans Administration to a Military Identification Number	5. FUNDING NUMBERS
6. AUTHOR(S) George R. Opria and Donald G. Maraska	
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	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200 words)

Identity theft has become one of the fastest growing crimes in America and stems from the widespread and growing reliance of organizations across the nation to use Social Security Numbers (SSN) as a primary personal identifier. Originally intended for the very limited purpose of tracking social security benefits, the value of the SSN as a unique identifier was quickly recognized, and its use rapidly grew. This "functionality creep" has led to the SSN becoming an almost *de facto* national ID number. Employers, universities, credit agencies and financial institutions began using the SSN as a unique personal identifier. The military started to use the SSN as a personal identifier in 1969 in place of the Military Serial Number. Today, the SSN is used pervasively throughout the military, from personnel rosters to medical records, from administrative records to operational orders.

This thesis analyzes the elimination of the SSN as the primary personal identifier within the Department of Defense and the Veterans' Administration, replacing it with a Military Identification Number (MIN). The elimination of the SSN at all but one critical location (pay related matters at the Defense Finance and Accounting System), would render all lost or stolen data useless to an identity thief. A Cost/Benefit Analysis of the transition from SSN to MIN using six methods of analysis; payback period method, discounted payback period, benefit cost ratio, net present value, internal rate of return, and a probabilistic NPV were examined. Each method's benefits and drawbacks are discussed and the findings are summarized. The CBA shows that the transition to a MIN is a cost effective solution with a Net Present Value that falls between $701 million and $554 million over a 10 year period.

14. SUBJECT TERMS Military Serial Numbers, Military Identification Numbers, SSN, Identity Theft, Primary Personal Identifier	15. NUMBER OF PAGES 94
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN ANALYSIS OF THE USE OF THE SOCIAL SECURITY NUMBER AS VETERAN IDENTIFICATION AS IT RELATES TO IDENTITY THEFT; A COST BENEFIT ANALYSIS OF TRANSITIONING THE DEPARTMENT OF DEFENSE AND VETERANS ADMINISTRATION TO A MILITARY IDENTIFICATION NUMBER

George R. Opria
Major, United States Marine Corps
B.S., Aviation, The Ohio State University, 1992

Donald G. Maraska
Major, United States Marine Corps
B.S., Economics, University of Idaho, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2007

Authors: George R. Opria

Donald G. Maraska

Approved by: William D. Hatch II, CDR, USN, Ret.
Thesis Co-Advisor

William Gates
Thesis Co-Advisor

Robert N. Beck
Dean, Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Identity theft has become one of the fastest growing crimes in America and stems from the widespread and growing reliance of organizations across the nation to use Social Security Numbers (SSN) as a primary personal identifier. Originally intended for the very limited purpose of tracking social security benefits, the value of the SSN as a unique identifier was quickly recognized, and its use rapidly grew. This "functionality creep" has led to the SSN becoming an almost *de facto* national ID number. Employers, universities, credit agencies and financial institutions began using the SSN as a unique personal identifier. The military started to use the SSN as a personal identifier in 1969 in place of the Military Serial Number. Today, the SSN is used pervasively throughout the military, from personnel rosters to medical records, from administrative records to operational orders.

This thesis analyzes the elimination of the SSN as the primary personal identifier within the Department of Defense and the Veterans' Administration, replacing it with a Military Identification Number (MIN). The elimination of the SSN at all but one critical location (pay related matters at the Defense Finance and Accounting System), would render all lost or stolen data useless to an identity thief. A Cost/Benefit Analysis of the transition from SSN to MIN using six methods of analysis; payback period method, discounted payback period, benefit cost ratio, net present value, internal rate of return, and a probabilistic NPV were examined. Each method's benefits and drawbacks are discussed and the findings are summarized. The CBA shows that the transition to a MIN is a cost effective solution with a Net Present Value that falls between $701 million and $554 million over a 10 year period.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Identity theft has become the fastest growing crime in America, affecting both the public as well as the private sector. Organizations' widespread and growing reliance on SSNs as identifiers has turned identity theft into a major crisis. The recent theft of a Department of Veterans' Administration (VA) computer containing a detailed database, the loss of detailed identification level data by a graduate school student, as well as instances of cracked databases including the theft of a LexisNexis database in 2005 all highlight the issue of protecting Americans from the identity theft. (Congressman Sam Farr)

The crisis with identity theft stems from the widespread and growing reliance by organizations across the nation on Social Security Numbers (SSN). After passage of the New Deal Social Security Program in 1936, the Social Security Administration started to assign the SSN. Originally designed for the very limited scope of providing social security benefits, the value of the number as a unique personal identifier was quickly recognized and its use started to grow. This "functionality creep" has led to the SSN becoming an almost *de facto* national ID number. Employers, universities, credit agencies and financial institutions all started using the SSN as a unique personal identifier. Even the military started to use the SSN as a personal identifier in 1969, replacing the Military Serial Number that had been previously used. It was from this "functionality creep" that the seeds were sewn from which identity theft grew.

Focusing on Government usage of the SSN, it is clear that reliance on this identifier is pervasive and the privacy safeguards that have been implemented to protect it are not making the "grade." A recent report by the House Government Reform Committee graded government agencies' information security procedures. It found that eight government agencies received an "F" and four received "D" grades. Included in those agencies receiving the failing grade were the Department of Defense (DoD) and the Department of Veterans Affairs (VA) (Committee on Government Reform 2006).

Still considered a relatively new phenomenon, a complete and universal definition of identity theft is not yet clear. While clarity and understanding of the identity theft problem are still being developed, the sheer magnitude of the potential cost to society requires that the crisis be addressed.

The DoD has reacted to the aforementioned incidents of data loss, and the resulting public and political pressure, by embarking on a path of increased security measures that run the gamut from encryption technologies to more restricted access and usage policies designed to reduce the possibility of personnel privacy data loss or theft. All of these measures, however, come with significant costs - both the real costs of the new technologies as well as productivity losses resulting from the more restricted usage policies. However, despite all of these efforts, data losses continue to occur at a great cost to society.

B. PURPOSE OF THE STUDY

The purpose of this thesis is to analyze identity theft in the military that results from lost or stolen personal data, identify a primary solution for analysis, and then conduct a detailed Cost Benefit Analysis. This study will follow a modified policy analysis format in order to more accurately identify the problem, as well as explore alternatives. The thesis will then depart slightly from a true policy analysis in that only the primary alternative will be analyzed.

C. RESEARCH QUESTIONS

This thesis seeks to answer several primary research questions as well as two secondary questions. The multiple research questions are required to properly cover the breadth of this subject within one comprehensive thesis. It is the comprehensive nature of the thesis that is unique to this study and is expected to provide the most value to the reader.

The primary research questions are as follows:

1. Do SSNs remain a viable DoD personal identifier?
2. How pervasive is the use of SSNs throughout DoD?
3. What is the historic role of Military Identification Numbers (MINs)?

The secondary research questions are as follows:

1. What are the costs and benefits (both direct and indirect) associated with transitioning to a MIN?
2. What spillover effects would be associated with transitioning to a MIN?

D. BENEFITS OF THE STUDY

The current political attention given to identity theft and particularly data losses from DoD and Government sources, has brought using the social security number as a personal identifier to the forefront of the nation's consciousness. Since individual branches of the military do not have the authority to issue their own identification number, this study will identify and evaluate the feasibility of a DoD wide policy change. Such a change would eliminate the use of the SSN as the primary personal identifier in favor of a military identification number. This thesis is intended to aid policy makers in their decision process to evaluate the alternatives and make an informed decision regarding the primary personal identifier within the DoD.

E. SCOPE OF THE THESIS

This thesis will consist of an extensive policy analysis including the following:

- A literature review
- A legal and historical review of the laws governing the creation and use of the SSN
- Development of alternatives, and
- A cost benefit analysis.

It is evident that there could be an infinite number of alternatives available for evaluation if the alternatives are based on varying degrees of security procedures and technological security measures (encryption, firewalls, etc.). Therefore, the authors have chosen to base this thesis around two distinct alternatives, either the status quo, which includes the aforementioned technological and use restrictions or the replacement of the social security number with a Military Identification Number (MIN) as the primary personal identifier within the DoD and the Department of Veterans Affairs (VA).

F. ORGANIZATION OF THE STUDY

The thesis will be organized into six main chapters, including this introduction chapter, Chapter I. Chapters II and III will include a literature review and will more completely identify the problem and its pervasiveness within DoD. Chapter IV will then

look at alternatives to address the identity problem and fully develop the primary alternative. Chapter V is the main focus of the thesis, which is a cost benefit analysis of the primary alternative. Finally, Chapter VI will summarize our findings and make recommendations.

II. LITERATURE REVIEW

A. FEDERAL GOVERNMENT SPONSORED STUDIES ON IDENTITY THEFT

1. Study by Javelin Strategy and Research

In 2006, the Better Business Bureau (BBB) and Javelin Strategy and Research co-released a study entitled *2006 Identity Fraud Survey Report* as a longitudinal update to the Javelin *2005 Identity Fraud Survey Report* and the Federal Trade Commission's *2003 Identity Theft Survey Report.* The 2006 report found that the number of identity fraud cases declined for the second year in a row, from 10.1 in 2003 to 8.9 million identity fraud victims in 2006. (See Figure 1) While the number of cases has declined, the dollar amount per case has risen to $6,383, a 21.6% increase since 2003. (BBB 2006) Given the inverse relationship between cases and costs, the annual dollar cost of identity fraud has held at statistically the same level, $56.6 billion, since 2003. (BBB 2006) The BBB report also showed the sources of identity theft (See Figure 2) and the average time spent by an identity theft victim seeking resolution increased from 33 hours in 2003 to 40 hours in 2006. (BBB 2006)

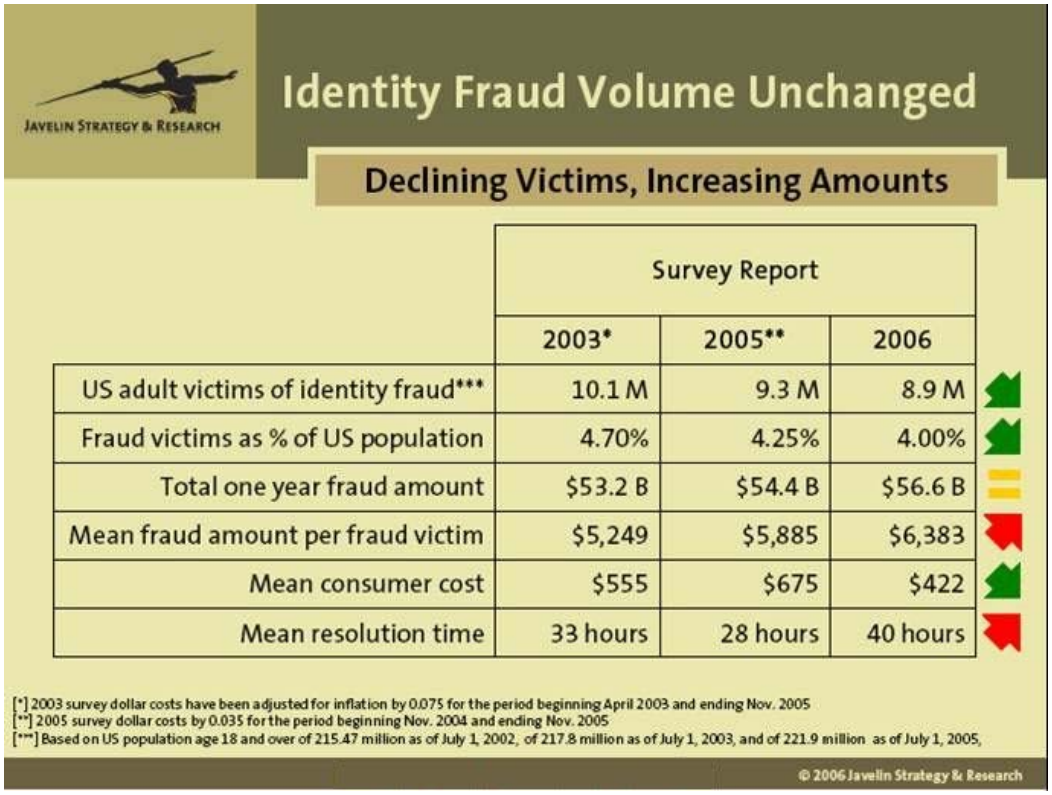

Figure 1. Identity Fraud Volume (From: Javelin Strategy and Research)

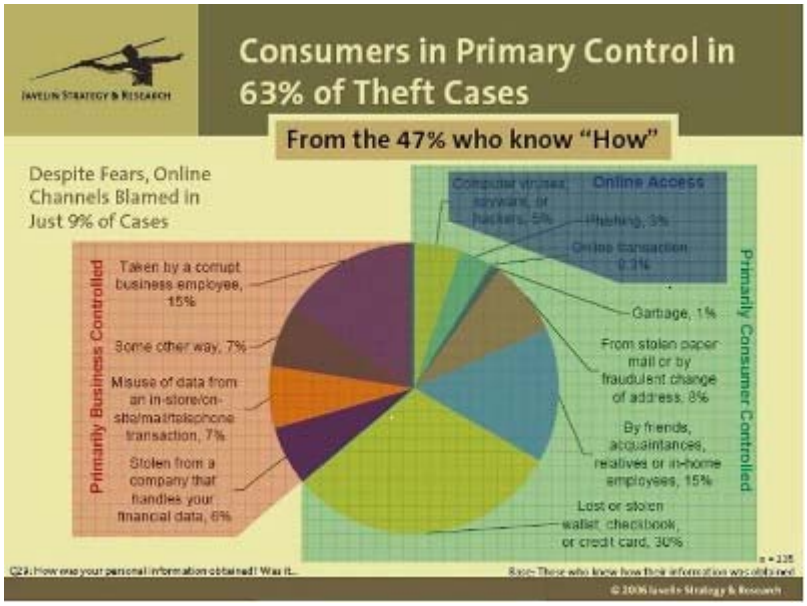

Figure 2. Identity Fraud Volume (From: Javelin Strategy and Research)

2. Identity Theft Literature Review by Graeme R Newman and Megan M. McNally for the U.S. Department of Justice

The study by Newman and McNally was funded by the U.S. Department of Justice and presented at the National Institute of Justice Focus Group Meeting held in January of 2005. After defining the types of identity theft, Newman and McNally broke true identity theft into three distinct stages:

- ***Stage 1: Acquisition of the identity***. During this stage the identity thief actually acquires the identity information, through whatever means necessary, to later use the identity information for subsequent gain.
- ***Stage 2: Use of the identity information.*** This stage includes accessing existing accounts, but can go much farther than that. Identity thieves can open new credit accounts, commit insurance or tax fraud, or use the stolen identity in many other illegal ways. This stage can take a long time to reach, as the identity thief carefully builds numerous credit accounts before ever tapping into them. The thief then "cashes out" all at once before the crimes are discovered by the victim or the credit issuing agencies.
- ***Stage 3: Discovery of the crime.*** This stage can take a long time to reach as well, particularly by the victim of the identity theft. Since the crime was probably conducted with new accounts established by the thief, the victim may not know about the crime until years later, particularly if the victim has not checked his credit report or has not recently applied for credit or a loan.

The authors of the study point out the poor reporting record of identity theft victims. Reported identity thefts vary significantly according to the demographics of the victim. Older victims as well as lower income victims are less likely to report the crime at all. On average, it is estimated that 38 percent of identity theft crimes go unreported. Furthermore, there is no central tracking system within the criminal justice system to catalog identity theft. The Federal Trade Commission's statistics on the number and extent of identity theft is based on consumer complaints and surveys that they have conducted, not on actual crime data from the Justice Department. (Newman, McNally 2005) This type of data is characterized by non-response bias since it is survey data. The survey data also suffers from the victims' memories, their understanding of the crime and even their comprehension of the survey questions themselves. Victims may also be reluctant to fully answer the survey questions due to the private nature of the questions being asked. Privacy crime victims are understandably reluctant to share private

information in survey answers. Even the nature of randomly selected survey participants may be problematic, since identity theft victims may go to great lengths to remain "unseen" - keeping unlisted numbers, e-mail addresses, etc., which may prevent them from even being randomly selected to participate in the survey. (Newman, McNally 2005)

The Newman/McNally study further suggests that future identity theft research should concentrate on the specific components of identity theft and the opportunity structure of each of those components. (Newman, McNally 2005) The study suggests that this research will lead to effective techniques to prevent identity theft; however, they also acknowledge that this approach simply leads to "something like an arms race," where technology and other preventative measures work only until the thieves develop more sophisticated means to counter these preventative measures. (Newman, McNally 2005)

This study categorizes the various types of victims as well as the types of identity theft crimes outlined above. One particularly interesting category, especially for this thesis, is titled "institutional victims." The authors point out that certain groups of people may be more susceptible to identity theft crimes because of the group to which they belong to or their profession. Specifically mentioned are students and members of the military due to the frequent use of their SSN for purposes other than those associated with the Social Security Administration. Regarding military members, the following excerpt from the 2002 GAO study is offered:

> Members of the armed services may [also] be more susceptible than the general public to identity theft. Given their mobility, service members may have bank, credit, and other types of accounts in more than one state and even overseas. At times, service members may be deployed to locations far away from family members, which can increase their dependence on credit cards, automatic teller machines, and other remote-access financial services (GAO 2002)

3. Study by Federal Trade Commission

In September 2003, the Federal Trade Commission released a report entitled *Identity Theft Survey Report.* This survey was conducted by Synovate and can be considered the primary, definitive source of identity theft information within the United

States, particularly in regard to the victims of identity theft. The objectives of the study were to estimate the incidence of identity theft victimization, measure the impact of identity theft on the victims, identify actions taken by the victims and explore measures that may help future victims of identity theft. The study was conducted through telephone interviews of a random sample of US adults. (FTC 2003)

The study looked at incidents of identity theft and found that almost 10 million Americans had been the victims of identity theft within the previous year. (FTC 2003) The total percentage of all types of identity theft victims within the previous five years amounted to 12.7% or 27.6 million people.

This study breaks down identity theft into the following categories or types:

- new accounts and other fraud
- misuse of existing non-credit card account
- misuse of existing credit card accounts

The average cost of new accounts and other fraud associated with ID theft is estimated to be $10,200. This equates to a $33 billion loss for this category of ID theft in the year prior to the study. (FTC 2003)

The financial costs identified above are born by society as a whole; however, there are costs that the individual must directly bear. For example, the average ID theft victim spends $500 correcting the resulting problems. (FTC 2003) Victims of "New Accounts and Other Frauds" crimes face average costs that are considerably higher at $1,200 each. For cases in the U.S., this totals $3.8 billion. The resulting total cost to individuals in America amounts to $5.0 billion. (FTC 2003)

From a time lost perspective, the study showed that victims reported spending an average of about 30 hours to overcome the problems resulting from the identity theft and subsequent misuse of their personal information. (FTC 2003) Victims of "New Accounts and Other Frauds" spent considerably more time correcting the problems, averaging 60 hours each. The median time spent correcting problems was substantially less, at 2 to 9 hours. When aggregated, Americans spent over 300 million hours trying to correct problems resulting from ID theft. (FTC 2003)

4. Report by the Office of Management and Budget

On March 1, 2006, OMB issued a report entitled the *FY2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*. The Federal Information Security Management Act (FISMA) was enacted in 2002 to, among other things, develop a comprehensive framework to protect the government's information, operations and assets. FISMA requires that all federal departments conduct annual reviews of the agency's information security program and report the results of those reviews to OMB. OMB then prepares an annual report to Congress. In FY 2005, Federal agencies spent $5.0 billion securing the government's information technology. OMB's 2005 report graded a number of Federal departments with a rating of "poor." The Department of Defense was among agencies with the "poor" rating.

5. Congressman Neil Abercrombie Press Release

On May 25, 2006, Congressman Neil Abercrombie issued a press release concerning a bill he cosponsored: The "Veterans' Identity Protection Act of 2006" (*H.R. 5455*). The legislation aimed at helping veterans whose personal data was stolen from the home of a Veterans Affairs (VA) employee. Representative Abercrombie stated that the "legislation will protect veterans from identity theft by calling the VA to (1) provide veterans with one year of free credit monitoring—to alert them of changes in their credit in order to stop the theft before it gets out of control, and (2) provide veterans with one free credit report each year for two years after the end of credit monitoring, in addition to the free credit report available under the Fair Credit Reporting Act." Additionally, the Bill called for $1.25 billion in emergency funds for the first year of implementation to protect the approximately 26.5 million veterans.

6. H.R. 5835: Veterans Identity and Credit Security Act of 2006

As ordered by the House Committee on Veterans' Affairs *H.R. 5835* would require the VA to notify affected individuals when sensitive, personal information is lost, stolen, or otherwise compromised. Additionally, if the Secretary of the VA determines there is a risk that the compromised information could be used in a criminal manner, the VA would be required to provide services to alleviate any loss those individuals might suffer.

The Congressional Budget Office (CBO) estimates that implementing *H.R. 5835* will cost $5 million in 2007 and about $50 million over the 2007-2011 period. However, if the VA were to experience another data breach similar to the recent incident involving 17 million individuals, the cost could be as much as $1 billion. The estimates were based on projected spending for credit-protection services for affected veterans. All of these services would be provided at no cost to those individuals. The VA would be required to:

- Inform individuals of the steps being taken to remedy the problem,
- Explain to each individual the advantages and disadvantages of requesting a fraud alert and a credit security freeze from the major credit-reporting agencies, and
- Contract with the credit-reporting agencies to implement a security freeze of the file of each affected individual who requests it - to include credit reports every three months, rehabilitation services, and identity theft insurance up to $30,000.

CBO estimates that the VA could be expected to experience an average of three incidents a year in which sensitive, personal information is compromised in some manner. Excluding the recent incident, the average number of people affected by a data breach has been about 50,000. The expected cost of notification for a group this size would be approximately $500,000 a year. CBO estimates that 10-15% of those whose information is compromised will experience a loss on the order of about $450. Thus, CBO estimates that the cost to the VA would be, on average, about $10 million a year.

7. Identity Theft and Social Security Numbers Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce Washington, D.C., September 28, 2004

In 2003, the Federal Trade Commission (FTC) commissioned a survey to gain a better picture of the incidents of identity theft and the impact of the crime on its victims. The data showed that within the preceding 12 months, 3.23 million persons discovered that an identity thief opened new accounts in the victims' names. An additional 6.6 million consumers learned of misuse of an existing account. Overall, nearly 10 million people (4.6 percent of the adult population) discovered that they were victims of some form of identity theft. These numbers translate into nearly $48 billion in losses to businesses, nearly $5 billion in losses to individuals, and almost 300 million hours spent

by victims trying to resolve their problems. Social Security Numbers (SSNs) play a pivotal role in identity theft since they are used to match consumers to their credit and other financial information.

B. PRIVATE SECTOR AND PUBLIC ORGANIZATION SPONSORED STUDIES ON IDENTITY THEFT

1. Electronic Privacy Information Center (EPIC)

EPIC, a public interest research center established in 1994 to focus public attention on emerging civil liberties issues, has been involved in congressional testimony and various legal cases related to privacy issues. A summary of the history of the SSN and current SSN issues can be found on EPIC's web site. EPIC shows the "functionality creeps" that has occurred regarding usage of the SSN. Created in 1936 for the express purpose of administering the Social Security Laws, the use of the SSN has steadily expanded, despite privacy concerns of citizens and legislators. In 1961, a significant step was made in the "functionality creep" of the SSN when Congress authorized the Internal Revenue Service to use SSNs as taxpayer identification numbers. (EPIC)

As the "functionality creep" continued, the risk grew that the SSN would become a "de facto" national identifier. The government's concern for citizens' privacy resulted in the Privacy Act of 1974. By enacting this act, Congress recognized the dangers of widely using the SSN as a personal identifier, and was, in fact, rejecting calls by some for creating a national identification number and identification system. The Privacy Act of 1974 attempted to limit the use of the SSN to only those instances where there was clear legal authority to use it. (EPIC)

With the rise of identity theft resulting from widespread use of the SSN, several states have taken steps to limit or eliminate the use of the SSN. Arizona universities are no longer allowed to use the SSN as a student identifier. Similarly, public and private post secondary institutions in Colorado had to discontinue using the SSN as primary student identifier. (EPIC) All public and private schools in New York and West Virginia are restricted from using the SSN. In Kentucky, students have the ability to opt-out of using the SSN.

Additionally, laws have been passed by several states in response to the identity theft epidemic. Arizona now prohibits the disclosure of the SSN to the general public, nor can it be printed on government or private sector identification cards. Arizona also requires a minimum level of protection for online use and transmission of the SSN. (EPIC)

California passed a law that gives individuals the ability to request that a "security alert" be placed on their credit record as well as to request a "security freeze" which prevents credit agencies from releasing personal information from an individual's credit report. (EPIC) California also prohibits posting the SSN in a public domain or printing the SSN on an identification card. Additionally, businesses that use the SSN to identify customers are not allowed to print the SSN on invoices or bills that are sent through the mail. California also requires companies to notify individuals when a security breach is experienced. (EPIC)

Colorado has laws that limit collecting and using the SSN as well as regulations that govern the proper destruction of documents containing the SSN. Insurance companies are required to remove the SSN from their customers' identification cards. Georgia also requires businesses to safely dispose of records that contain any personal identifiers. (EPIC)

Case Law:

Greidinger v. Davis - When the state of VA passed a statute to compel voters to disclose their SSN, which would then be subsequently published in the public voting record, a Federal Appeals Court declared that the law was unconstitutional. The court declared that to the extent the Virginia voting laws "permit the public disclosure of Greidinger's SSN as a condition of his right to vote, it creates an intolerable burden on that right as protected by the First and Fourteenth Amendments." (EPIC)

Beacon Journal v. City of Akron - The Ohio Supreme Court ruled that the state could not disclose the SSNs of state employees under a state open record law. The source of the Court's reasoning was from the U.S. Constitution. The Court stated that

their ruling was "…intended to preserve one of the fundamental principles of American constitutional law – ours is a government of limited power. We conclude that the United States Constitution forbids disclosure under the circumstances of this case."

2. Discussion Paper by Julia S. Cheney for the Federal Reserve Bank of Philadelphia

This paper is the follow on to a workshop that was conducted on October 3, 2003 by the Payment Cards Center of the Federal Reserve Bank of Philadelphia. The paper defines identity theft and the need to narrow the definitions to better understand the associated crimes and, subsequently, take corrective actions. The more prevalent crime often characterized as "identity theft" can better be defined as payment fraud. This crime typically involves stolen credit cards or credit card numbers and fraudulent charges to those credit accounts. This crime, while more prevalent, is easily detected, stopped and corrected. (Cheney 2003)

True "identity theft," however, is much more complicated. "Fraud losses associated with identity theft can be significant, involve multiple accounts, remain undetected for much longer period, and ultimately result in costly and time-consuming efforts to re-establish the victim's credit standing." (Cheney 2003) True "identity theft" involves the thief using personal information of the victim to establish new accounts under the victim's name, but with different contact information (address and phone number) to hide the criminal activity from the victim.

To perpetrate this type of crime, the criminal requires detailed personal identification information about the victim to establish the new accounts. The thief acquires this personal information through a variety of sources, including low-tech methods such as stealing mail, raiding garbage cans, stealing wallets, etc. However, there is a growing component of technologically advanced criminals who are stealing personal identification data through the Internet by hacking into information stored on servers. (Cheney 2003)

Once someone's identity has been stolen and the thief has established credit card accounts, the thief then can use those accounts for financial gain. With the increased

prevalence of Internet and online sales, identity thieves have an easier route to perpetrate the crime. Internet sales grew 25 percent in 2002 to $43.5 billion and credit card payment fraud was estimated at 1.7 percent of those sales. (Cheney 2003)

3. Article by Hal Berghel for Communications of the ACM February 2003/Vol. 43, No. 2

Mr. Berghel explores the widespread use of the Social Security Number and the resulting dangers. President Roosevelt signed Executive Order 9397 and this began the "functionality creep" of the SSN. This Executive Order was signed in 1943 and authorized other government databases to use the SSN as the primary personal identifier. This and subsequent expansions using the SSN ignited a national privacy debate that eventually prompted Congress to pass the Privacy Act of 1974. However, this act proved too little, too late (Berghel 2003) The Privacy Act did require certain disclosures from federal agencies that requested SSNs from individuals, but it relaxed disclosure rules for state and local governments, and provided no prohibitions or penalties for the use of SSNs in business and commerce. (Berghel 2003) By enacting disclosure requirements, the Privacy Act actually legitimized the government's widespread use of the SSN as a primary personal identifier. Furthermore, in 1976, The Tax Reform Act authorized state and local authorities to use the SSN. (Berghel 2003) While the majority of the "functionally creep" of the SSN occurred in the early years, after establishing the Social Security Administration and it's now infamous SSN, the real damage was to come years later.

Berghel calls the SSN the "holy grail" of all the pieces of identity that an identity thief needs to obtain to perpetrate a crime. With the advent of the internet, coupled with the widespread, almost unchecked use of the SSN as a personal identifier, a new form of crime has sprouted up which has become the fastest growing crime in the U.S. (Berghel 2003)

4. Research Report by Neal Walters of the AARP Public Policy Institute, Protecting Social Security Numbers from Identity Theft

In her testimony before the U. S. House of Representatives Committee on Ways and Means, Subcommittee on Social Security on June 15, 2004, the director of Education, Workforce, and Income Security Issues for the Government Accountability Office, Barbara D. Bovbjerg, pointed out that approximately 227 million individuals

currently have Social Security Numbers (SSNs) and that, due to the SSN's uniqueness, it has become the "de facto" national identifier. This status of "de facto" national identifier makes SSNs sought after by those who wish to perpetrate fraud. The director of the Bureau of Consumer Protection, Federal Trade Commission, J. Howard Beales III, said in his testimony that an estimated 10 million individuals were victimized by identity theft every year.

A number of policy options have been proposed at both the state and federal levels to strengthen SSN protections.

- *Limiting Display*: S. 1332 and S. 29 by the 109th Congress propose prohibiting SSN use on identification or eligibility cards provided by employers, educational institutions or on state driver's licenses.
- *Limiting Sale and Purchase of SSNs*: Laws and regulations are being passed to limit the sale and purchase of SSNs so there must be a permissible purpose without affirmative consent. Such permissible purposes, as defined under the Fair Credit Reporting Act (FCRA), include establishing a consumer's eligibility for credit, insurance, rental housing, and employment through background checks in certain circumstances.
- *Increasing Security:* Other laws seek to Increase Security for legally collected SSNs and enhance penalties for illegal disclosure. They also require enhanced encryption, limited access, and adequate internal policies. To deter violations, increased penalties for misuse are being implemented, reflecting the seriousness of such crimes.
- *Increasing Awareness*: While increasing awareness of identity theft has positively reduced the occurrences of the crime, it has also had some undesirable secondary effects. Increased public concern for security of individual identity has negatively affected purchasing decisions, especially when it comes to online transactions.

5. Statement of the Military Officers Association of America (MMOA) on "The Veterans' Identity an Credit Protection Act of 2006" before the House Veterans' Affairs Committee, July 18, 2006 Presented by Col. Robert F. Norton, USA (Ret.)

In response to the recent theft of a VA laptop, Col. Norton reported that the MMOA's position concerning Social Security Account Number access was that they "support the objective to curtail routine use of and access to veterans' SSNs. The MMOA believes all government agencies that use the SSAN as a record identifier should, like the state of Virginia, begin now to develop alternative identifiers that pose less risk of identity theft." (Norton 2006)

6. CRS Report for Congress: Intelligence Reform and Terrorism Prevention Act of 2004: National Standards for Drivers' Licenses, Social Security Cards, and Birth Certificates by Todd B. Tatelman, January 6, 2005

Today SSNs are used as representations of individual identity, as secure passwords, and as keys for linking multiple records. The problem is that these uses are incompatible. The widespread use of the SSN as an identifier, resulting in its appearance on mailing labels, ID cards and badges, and various publicly displayed documents, makes it unfit to be a secure password providing access to financial and other personal information. The broad use and public exposure of SSNs has been a major contributor to the tremendous growth in identity theft and other forms of credit fraud.

These issues, as well as threats to national security, were briefly addressed in the comprehensive report to the nation, *The National Commission on Terrorist Attacks Upon the United States (9/11 Commission)*. The report recommended that the federal government set national standards for issuing identification documents, including drivers' licenses, social security cards and birth certificates. Final legislation, that was signed by President Bush on December 17, 2004, contained many of the provisions set forth by the report. Of particular interest to this study was language and provisions concerning the display and use of SSNs as identifiers. "The law amends the Social Security Act to expressly prohibit the states or their political subdivisions from displaying, electronically or otherwise, a social security number, (or any derivative of such number) on any driver's license or motor vehicle registration, or on any other document issued by states to an individual for identification." (CRS 2005)

7. Quantifying the Financial Impact of IT Security Breaches, Ash Garg, Jeffrey Curtis, Hilary Halper, 2003

This study, due to the conflicting incentives inherent in self-reported data, uses an event study methodology to measure the losses to publicly owned companies resulting from breaches in IT security. In doing so it "offers an alternative approach and more rigorous evaluation of breaches in IT security." (Garg 2003) The authors focus on the impact of breaches on the stock price of the affected companies. Given the Efficient Market Hypothesis (EMH), "if the markets are efficient (i.e., they react to all publicly

available information) then all present and future effects of a publicly reported security breach are captured in the stock price." (Garg 2003) This study illustrates, from a different perspective, the excessive costs associated with incidents of this kind.

The growing regularity of security incidents is spurring increases in corporate investment in IT security spending. Information security continues to be a large and increasing concern for companies, organizations, and government agencies, with no end in sight. Driven by the expanding use of databases, electronic storage of records, and globalization, the need for Internet enabled file sharing is accelerating rapidly. A major concern, as illustrated by the authors' statement, is "the growing use of on-line technology and the spread of Internet connectivity around the world, driven by globalization, has made cyber attacks much easier today. Particularly concerning is the growing level of terrorist and criminal activity directed at communications networks and computer systems." (Garg 2003)

The event-study methodology used in this study is based on the Efficient Markets Hypothesis (Fama et al., 1969). The EMH maintains that as soon as new information is available it is analyzed by investors and incorporated into share prices. So, theoretically, the change in a stock's price reflects the impact of events and information on both short and long-term company performance (See Figure 3).

The study focused on twenty-two events that occurred between 1996 and 2002 that met their criteria. The authors separate the types of security incidents to estimate the economic impact reflected in the share price (market capitalization) over the three-day period following the news of the event. The authors classified security incidents into four major types. Of interest to this thesis are thefts of customer information and credit card information. This category is most similar to the type of breach applicable to this study and is distinct due to the fact that the loss of personal information has great potential to trigger legal liability to the organization.

The study found that in the event of the loss of credit card information (personal information) the one day drop in market value was 9.3% and it increased to a 14.9% three day negative reaction in stock price. The authors also point out that, "the market

perceives a direct correlation between the number of credit card numbers pilfered from a company and the appropriate marketplace punishment to the share price as larger thefts were penalized more." (Garg 2003)

Of the four categories delineated in the study, all realized a negative abnormal return. Of the most interest to our research, the market reacted most severely to personal information theft (between 9 and 15%) likely indicating third party liability (See Figure 4). (Garg 2003)

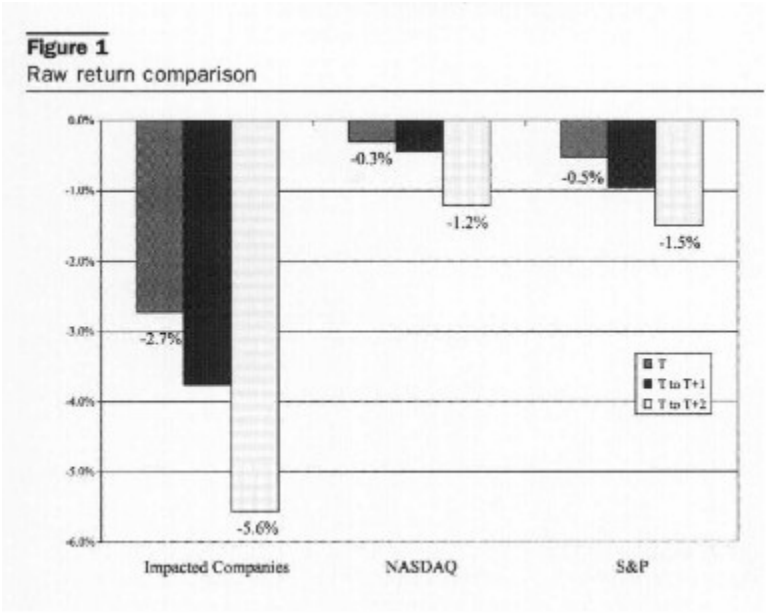

Figure 3. Raw Return Comparison (From Garg, Curtis and Harper, 2003)

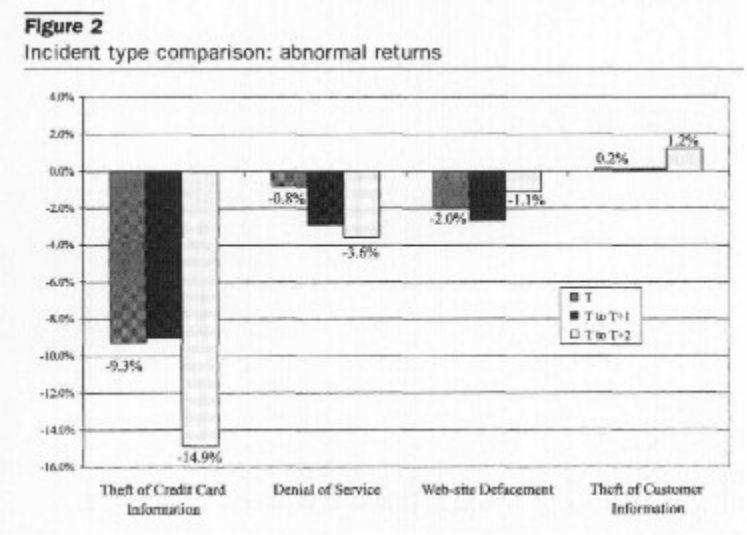

Figure 4. Incident Type Comparison (From Garg, Curtis and Harper, 2003)

THIS PAGE INTENTIONALLY LEFT BLANK

III. OVERVIEW OF PERSONNEL IDENTIFICATION AND THE NATURE OF THE CURRENT PROBLEM

To better understand the current use of the SSN as well as proposed alternatives and their associated costs, an understanding of the original use of the Military Serial Number must be addressed.

A. ORIGINAL USE OF MILITARY SERIAL NUMBERS

1. Background

Originally, the Armed Forces issued service numbers as a method of identifying individual members. These were referred to as Signal Numbers (SN) by the Coast Guard and as Military Service Numbers (MSN) by the Army, Navy, Air Force and Marine Corps. (National Archives 2007)

Military Service Numbers were unique identifiers, which differed by area and mode of entry into the Armed Forces. These numbers represented the region from which the person entered and whether they were drafted or volunteered for service (See Table 1). It was not possible to derive a Social Security Number from a Military Serial Number or visa versa because they were entirely unrelated numbers assigned by different government agencies. (Vietnam Research by Veterans 2007)

The first two numbers, as shown in the table below, correspond to the first two digits of serial numbers issued between the years 1940-1969.

(1) Regular and Reserve Air Force and Army

(2) Draftees between 1940-1946 (30-39 million)

(3) Draftees between 1948-1969 (50-57 million)

STATE	(1)	(2)	(3)
Alabama	18	38	54
Alaska	18	38	54
Arizona	18	38	54
Arkansas	18	38	54
California	19	39	56
Colorado	17	37	55
Connecticut	11	31	51
Delaware	12	32	51
Florida	14	34	53
Georgia	14	34	56
Hawaii	10	30	50
Idaho	19	39	56
Illinois	16	36	55
Indiana	15	35	52
Iowa	17	37	55
Kansas	17	37	55
Kentucky	15	35	52
Louisiana	18	38	54
Maine	11	31	51
Maryland	13	33	52
Massachusetts	11	31	51
Michigan	16	36	55
Minnesota	17	37	55

STATE	(1)	(2)	(3)
Mississippi	14	34	53
Missouri	17	37	55
Montana	19	39	56
Nebraska	17	37	55
Nevada	19	39	56
New Hampshire	11	31	51
New Jersey	12	32	51
New Mexico	18	38	54
New York	12	32	51
North Carolina	14	34	53
North Dakota	17	37	55
Ohio	15	35	52
Oklahoma	18	38	54
Oregon	19	39	56
Pennsylvania	13	33	52
Rhode Island	11	31	51
South Carolina	14	34	53
South Dakota	17	37	55
Tennessee	14	34	53
Texas	18	38	54
Utah	19	39	56

STATE	(1)	(2)	(3)
Vermont	11	31	51
Virginia	13	33	52
West Virginia	15	35	52
Washington	19	39	56
Wisconsin	16	36	55
Wyoming	17	37	55
Panama	10	30	50
Puerto Rico	10	30	50

Table 1. Military Serial Number Mode and Location Code (From: Vietnam Research by Veterans 2007)

The Air Force and Army ended the use of service numbers on July 1, 1969, the Navy and Marine Corps on January 1, 1972, and the Coast Guard followed suit on October 1, 1974, in favor of using the Social Security Number (SSN). (The National Archives 2007)

B. ADVENT OF SOCIAL SECURITY NUMBERS

1. Use by Civilians

The Social Security Act of 1935 created Social Security Numbers (SSN). They were intended for the social security program to guarantee American workers received the proper proceeds for income rerouted into the new program. The first SSNs were issued the following year. "The new pension system marked the first time in the United States that a government agency would be required to collect and use personal information from most of the population." (Smith 2002)

Figure 5. Picture of the Social Security Card (From: www.ssa.gov, Retrieved March 2007)

The SSN consists of nine digits, commonly written as three fields separated by hyphens: AAA-GG-SSSS. The first three-digit field is called the "area number." The central, two-digit field is called the "group number." The final, four-digit field is called the "serial number." (Social Security Online 2007)

a. Area Numbers

Area numbers are assigned to geographical locations, increasing from east to west across the continental United States (See Table 2). Where appropriate, they were assigned according to state (or territorial) boundaries. Since 1972 this number has related to the home address provided by the applicant at the time of application for the SSN.

If the initial series of area numbers were exhausted, the assignments were expanded as required. The following table illustrates the initial method of assignment. Currently the Social Security Administration acknowledges area numbers as high as 768.

SSN BY STATE		
001-003 NH	400-407 KY	530 NV
004-007 ME	408-415 TN	531-539 WA
008-009 VT	416-424 AL	540-544 OR
010-034 MA	425-428 MS	545-573 CA

SSN BY STATE		
035-039 RI	429-432 AR	574 AK
040-049 CT	433-439 LA	575-576 HI
050-134 NY	440-448 OK	577-579 DC
135-158 NJ	449-467 TX	580 VI Virgin Islands
159-211 PA	468-477 MN	581-584 PR Puerto Rico
212-220 MD	478-485 IA	585 NM
221-222 DE	486-500 MO	586 PI Pacific Islands*
223-231 VA	501-502 ND	587-588 MS
232-236 WV	503-504 SD	589-595 FL
237-246 NC	505-508 NE	596-599 PR Puerto Rico
247-251 SC	509-515 KS	600-601 AZ
252-260 GA	516-517 MT	602-626 CA
261-267 FL	518-519 ID	627-645 TX
268-302 OH	520 WY	646-647 UT
303-317 IN	521-524 CO	648-649 NM
318-361 IL	525 NM	650-699 unassigned, for future use
362-386 MI	526-527 AZ	700-728 Railroad workers through 1963, then discontinued
387-399 WI	528-529 UT	769-799 unassigned, for future use.

Table 2. SSN Area Numbers Showing Corresponding States

b. Group Numbers

The group number is associated with the order SSNs are issued for a specific region. Prior to 1965 only half the group numbers were used. For an unidentified reason, the SSA used odd numbers below 10 and even numbers above 9. The system was later modified to allow assignment of low even numbers and high odd numbers. The current process assigns group numbers for each area number in the following order:

- Odd numbers, 01 to 09
- Even numbers, 10 to 98
- Even numbers, 02 to 08
- Odd numbers, 11 to 99
- Group codes of “00” aren't assigned

All possible area numbers are assigned with each group number before using the next group number to maintain a chronological ordering of SSNs within the region.

c. Serial Numbers

Serial numbers are allocated in sequential order within each area and group number as the applications are processed. Serial number “0000” is never used. (CPSR 2001)

Initially the Social Security card had “NOT FOR IDENTIFICATION” printed on its face, giving the sense of confidentiality. However, as time passed, because of its characteristics, both the federal government and civilian institutions began using it for numerous purposes not related to its original intent.

In 1943, Roosevelt signed *Executive Order (EO) 9397* requiring federal agencies to use the SSN when creating new record-keeping systems. The order directed the Social Society Board to designate this number to all individuals required by a federal agency to have one. (Roosevelt 1943)

In 1962, the Internal Revenue Service began using the SSN as the taxpayer identification number. (Social Security Online, History 2007) This appeared to be the first time the number was recognized for its ease at linking records. In 1964, SSNs

were issued to high school students. The 1960's Social Security Administration manual stated that one of its reasons for such action was "to use the SSN for both automated data processing and control purposes, so the progress of students could be traced throughout their school lives across district, county and state lines." (Social Security Online, Administration Claims Manual 2007)

Many more organizations recognized the benefit of using this unique identifier to link, track and recall information. In a short period of time colleges, Medicare, state Medicaid, elderly programs, and Indian health programs followed suit, just to name a few.

Of particular interest is the 1966 decision by the Veterans' Administration (VA) to adopt the number for its use. The VA began using the SSN for hospital admissions and other accounting purposes. Given this the Pentagon began to switch from the MSN to the SSN as the service number for all military personnel. (Social Security Online, History 2007)

The Bank Secrecy Act (BSA) of 1970, 31 U.S. Code 1051, required banks and other financial institutions to record SSNs for all their customers. (Bank Secrecy Act 1970) Many institutions, for ease of operations, required the individual's SSN be displayed on the face of their checks. What would eventually become know as "identity theft" dramatically increased.

This single, convenient, and widely used number made the merging of records, especially large data systems, easy and manageable. In 1972, the United States Department of Health, Education, and Welfare (HEW) produced a report: *Records, Computers, and the Rights of Citizens*. This report recommended that the SSN not be used as an identifier. According to the HEW committee "the federal government itself has been in the forefront of expanding the use of the SSN." (HEW 1973, p. 121)

This report became the foundation for the Federal Privacy Act of 1974, which attempted to limit the abuse of the SSN. The Privacy Act of 1974 required authorization for government agencies to use SSNs in their data bases and required

disclosures when government agenciess requested the number. Agencies which were already using the SSN as an identifier before January 1, 1975 were allowed to continue using it.

The Act requires that any federal agency that requests an individual's Social Security Number has to disclose the following:

- The authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
- The principal purposes for which the information is intended to be used;
- The routine uses which may be made of the information, as published annually in the Federal Register, and
- The effects on a person for not providing all or any part of the requested information.

The Act requires state and local agencies which request the SSN to inform the individual of only three things:

- Whether the disclosure is mandatory or voluntary
- By what statutory or other authority the SSN is solicited
- What uses will be made of the number ((PRIVACY ACT OF 1974)

A weakness of the Privacy Act is that it does not carry any penalties.

The SSNs usage again expanded with The Tax Reform Act of 1976. This Act granted authority to state or local tax, welfare, driver's license, or motor vehicle registration authorities to use the number in order to establish identities. Meanwhile, the use of the number continued to expand in the private sector. SSNs were being asked for to rent an apartment, get a fishing license, begin telephone service, donate blood and get medical treatment. The SSN became essential in the establishment of credit. (Social Security Online Tax Reform Act of 1976)

2. Use by Military

The military's use of the SSN actually began as a result of actions of the VA. Beginning in 1966, the VA started using it as their hospital admissions number and designed their entire patient records' system around it. Shortly thereafter, in 1969 the DoD adopted the SSN and did away with the military service number that had previously been used. (The National Archives 2007)

Identity theft and the financial implications that accompany it were not even fathomable at the time that this transition took place. Computers and data base systems, of course, did not exist, so the transition was a fairly straightforward one. Forms were simply re-printed to reflect a block for the SSN instead of a service number.

In 1981, use of the SSN as the primary identifier was strengthened even further with the passage of the Department of Defense Authorization Act (P.L. 97-86), which required the use of SSNs, by the Selective Service System.

C. CONSTITUTIONAL/LEGAL ISSUES

1. Constitutional Review

While the U.S. Constitution does not directly address privacy, The Supreme Court has held that a right to privacy does, in fact, exist in the Constitution. It has been the basis behind Roe v Wade and host of other Court decisions and has been considered a "core value" behind the entire Bill of Rights. In Griswold v. Connecticut the Supreme Court found that there was an independent right of privacy. This right of privacy was not found in any one provision of the Constitution, but rather from the intent of the entire Bill of Rights, with particular attention given to the 4th Amendment.

The 4th Amendment states: "'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." While this amendment does not directly address privacy, it has been used as the basis for many Court decisions regarding privacy rights.

2. Legal Review

Amicus Curiae is a Latin phrase for "friend of the court." The American legal system allows a person, or organization, who is not a party to litigation to provide testimony at the invitation of the court to advise it on a matter of law directly affecting the litigation.

This legal review follows and includes excerpts, as they apply to this thesis, from an "Interests of AMICUS" brief written by Marc Rotenberg and David L. Sobel from the organization Computer Professionals for Social Responsibility (CPSR). The brief advises the court on issues related to the case of Greidinger v. Davis. (CPSR 1993)

The Privacy Act of 1974 clearly acknowledged the threat to privacy that disclosure of the SSN presents. Once acquired, it links an individual to databases holding financial, medical, educational, and credit information, all of which are unrelated to the number's original use.

Health, Education and Welfare Secretary Elliot Richardson acknowledged in his 1971 testimony before Congress that "there would certainly be an enormous convenience in having a single identifier for each individual ... [making] more efficient the acquisition, storage, and use of data .... It is the very ease of assembling complete records, of course, which raises the specter of invasion of privacy." (HEW 1971)

The HEW report that followed recommended wide-ranging legal safeguards for federal record systems. The committee highlighted the hazards inherent in using the SSN as a personal identifier when they stated that "(it) would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems ..." (HEW 1971, p. 122)

The committee recommended enacting the following restrictions on the disclosure and dissemination of the SSN:

- Uses of the SSN should be limited to only those purposes required by the federal government.
- Federal agencies should not require the use of the SSN absent statutory authority.
- Congress should evaluate any proposed use of the SSN.
- Individuals have the right to refuse to provide their SSNs and should suffer no harm for exercising this right.

Organizations required by Federal law to obtain the SSN use the number solely for the purpose for which it was obtained and not make any secondary use of, or disclose the SSN without the informed consent of the individual. (HEW 1971, pp. 124-25)

Congress agreed the following year when these recommendations became the basis of the Privacy Act.

The growing number of computerized public and private sector databases has increased the frequency of abuse of the SSN. In 1991, the Subcommittee on Social Security of the House Committee on Ways and Means noted, "[t]he extensive use of computers has resulted in the wide-spread private sector use of the social security number as an identifier… The ability of the private sector to gather information, such as credit history, grocery store purchases, medical records (including pre-natal information), family medical histories and genetic makeup has raised fears that in the near future unregulated companies will serve as national identity bureaus collecting and dispersing an individual's most private information." (Subcommittee on Social Security of the House Committee on Ways and Means 1991)

Gwendolyn S. King, Commissioner of Social Security, testifying before the subcommittee stated that, "concerns in this country that [SSN might become a universal identifier], center on questions of individual privacy and the increased possibility of the invasion of privacy if all records pertaining to an individual could be accessed under one number...The need for a unique number for individual records in computer systems means that use of the SSN is likely to continue to expand in the years ahead… we (SSA) have a deep concern that individuals not be harmed through carelessness in the use of the SSN." (Subcommittee on Social Security of the House Committee on Ways and Means 1991, p. 25)

It is clear that possession of such a powerful number would afford all in its possession easy access to a large amount of sensitive information about an individual. Forty years ago, Congressman Frank Horton pointed out that "one of the most practical of our present safeguards of privacy is the fragmented nature of personal information. It is scattered in little bits across the geography and years of our life. Retrieval is impractical and often impossible. A central data bank removes completely this safeguard." (Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations 1966).

Use of the SSN, for reasons unrelated to the Social Security Administration significantly decrease the "fragmented nature of personal information," as Congressman Horton highlighted and Congress addressed in the Privacy Act of 1974. (Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations 1966).

This concern is not exclusive to the United States. In Canada, "the abuse of the Social Insurance Number is the only privacy issue that has regularly commanded the attention of members of the House of Commons in the last twenty years." (Flaherty 1989, p. 281)

Indeed, Canadian lawmakers have taken action to check the movement of the Social Insurance Number (SIN) toward becoming a universal personal identifier. Canadian Forces have instituted a Canadian Forces military service number (CF) to replace the SIN as the identifier and a separate employee identifier is being introduced for federal employees.

In addition, France has made efforts to restrict the use of similar national numbers. In 1980, France's National Commission on Informatics and Freedom denied the establishment of international identity cards and personal identification numbers. The French chose to assign the identification number to the card instead of the individual. By taking this approach, any card loss or breach in personal data would result in a new card and number being assigned to the individual. (Flaherty 1989, p. 227)

Still other countries have taken measure to protect citizens' privacy. Portugal's constitution, Article 35 (1-6), prohibits the routine interconnection of files and has made it clear that "citizens shall not be given all purpose national identification numbers." Greece uses a system containing national identity numbers for specified public sector data files, but has legislated that their linkage is forbidden. The Australian Privacy Act of 1988 addresses the use of their tax file number. The Act bars its use as a national identification system by "whatever means." (Spencer 1990, p. 60)

U.S. Federal Courts have acknowledged the gravity of the disclosure of SSNs. The courts, by looking toward Congressional intent embodied in the Federal Privacy Act of 1974, recognize that employees have a strong privacy interest in their SSNs.

Congress, in passage of the Privacy Act, acknowledged this interest by making unlawful any denial of a right, benefit, or privilege by a government agency because of an individual's refusal to disclose his SSN. In the Congressional Report, which followed passage of the Privacy Act, the Committee stated that the extensive use of Social Security Numbers as universal identifiers in both the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation." (House Committee on Government Operations 1974)

This admitted recognition provides persuasive policy arguments against the practice this thesis addresses. The potential for injury, whether financial, private, or from a national security standpoint, is not hypothetical. Occurrences of identity theft, fraud, and invasion of privacy, have increased as nonessential uses of the SSN have mushroomed.

D. STAKE HOLDERS

Use of the SSN a personal identifier has become so pervasive, that almost every organization within the DoD can be considered a "stake holder" or interested party should the DoD decide to transition to a MIN.

1. Unit Level

Every unit, down to the company or even platoon level uses the SSN to track and identify personnel. Unit rosters are produced daily, sometimes hourly as a unit prepares for a deployment or exercise and personnel are changed, moved around, added or deleted. When you consider the simple case that there might be 4 John Smiths in a 160-man company, the SSN quickly and easily makes a positive identification. Until very recently, the SSN was even required to be written on the outside of mail envelopes to ensure the letter was delivered to the correct individual.

2. Headquarters Level

As you go up in an organization, the number of persons and administrative functions increase dramatically. Service headquarters (HQs) are responsible for pay, orders, promotions, awards, etc. The SSN is currently used to identify individuals in each of these, and many more functions. The SSN truly has become the "de-facto" universal identifier, particularly within the DoD where the SSN is used for everything from membership in the club systems to your ID card.

3. Data Warehouses

Each Service, the VA, and DoD have their respective database systems and data warehousing capabilities. The Marine Corps' data warehousing system is the Total Force Data Warehouse (TFDW). This system "extracts" or receives data from over 30 different sources and holds over 13 years worth of personnel data. This data is combined and compiled based on the SSN.

The Defense Manpower Data Center (DMDC) is a comprehensive repository of personnel, manpower, training and financial data. The DMDC data and programs encompass the military personnel life cycle from accession to retirement, reserve components, families and dependents of Service Members, and civilian employees of the DoD. The DMDC data is combined and cross-referenced by SSN and as such, would certainly be considered one of the main "stake holders" for any transition to a MIN as the primary DoD personal identifier.

E. RECENT IDENTITY THEFT AND LOST DATA EVENTS

1. Data Purposefully Stolen or Hacked

In 1997, a major breach of high ranking military officers occurred when identity thieves obtained the SSN's of over 40 officers in the U.S. Marine Corps and Navy. The thieves used the SSN's to create fraudulent credit card accounts. This case brought a lot of attention to the military regarding identity theft, because a privacy advocate, Glen L Roberts had obtained the names and SSN's of over 4500 military officers from the publicly available congressional record and posted them on the internet. Of course, it was never clear if the thieves obtained the numbers from Roberts' posting or from the congressional record. (WebTV Addict 1999)

In 2003, the State of California experienced a loss of the personal data of 265,000 employees (including the Governor) when a hacker breached a secure database. The database was run by an outside storage company that failed to report the breach for 3 weeks. Consequently, the California Legislature hastily passed legislation that requires companies to inform customers of a breach involving personal data. However, throughout the nation, most companies remain quiet regarding lost or stolen data. The FBI and Computer Security Institute found 60% of companies studied had a computer security breach in the year studied and yet only 33% reported it. (Pelgrin 2003)

In August 2003, the Navy experienced a breach when a hacker broke into the Navy's purchase card program issued by Citibank. Citibank and the Navy were forced to cancel all of the cards to ensure the accounts were not used fraudulently. The breach affected approximately 22,000 card holders. (Pelgrin 2003)

2. Data Lost or Misplaced

Laptop computers and flash memory thumb drives have ushered in a new age of computer portability and worker productivity, but their small size has increased the likelihood of lost or misplaced storage devices. Considering laptops alone, there were 129 reported instances of lost laptops that contained personnel data. One of the largest losses of data involved a laptop lost by a Boeing employee on December 13, 2006, which included the names and SSNs of 382,000 employees. Ernst and Young lost a laptop on June 1, 2006, which included the credit information of 243,000 Hotels.com employees. Fidelity lost a laptop on April 4th of the same year, which included the retirement account information of 196,000 individuals. (Fortune January 22, 2007, Vol. 155 No. 1, publisher Time Inc., Telis Demos) So far, there have been no crimes resulting from any of these losses, but given the process that an identity thief has to go through before he can capitalize on the crime; it may be years before the 2006 losses result in crimes.

In 2006, a graduate student lost a thumb drive containing the SSNs of over 200,000 current and former Marines. In the same year the personal information of over 100,000 sailors and Marines was erroneously made available on the Naval Safety Center's Web site. (Hoellwarth 2006)

F. RESEARCH OBJECTIVES

The entering research assumption is that both the DOD and VA maintain the following personnel management system security objectives:

- Availability: the purpose of the system can be met, and the system is accessible to those who need to use it.
- Confidentiality: information is not made available or disclosed to unauthorized individuals.
- Integrity: the system performs its intended function in an unimpaired manner.

The use of a MIN as the primary personal identifier in all of these various personnel management systems would better meet the above objectives. The MIN would allow more people to have access to the systems because it would not jeopardize individual personal financial accounts. This increases the availability of the information and the eases the use of the systems involved. Since a MIN does not threaten the financial status of an individual, it also increases the confidentiality of the management systems. By lessening the impact of a potential loss, a MIN based system allows easier, more unrestricted use thereby increasing the Integrity of the system.

"Every organization has oceans of data and acres of information. However, only those organizations able to transform their disparate data streams into timely, relevant, and coherent information will ultimately achieve a real competitive edge. One of the organization's goals must be to improve the return on data by cascading information down through every level of the organization." (Read et al., 2003)

Given the demonstrated risks inherent in using the SSN as a personal identifier, as well as the frequency of the inadvertent dissemination of SSNs, continued use by the DoD and VA should only be sustained if it is shown to be absolutely necessary and if less intrusive alternatives do not exist. MINs are a viable alternative that would better serve DoD and the VA's interests in administering their systems of military/DOD identification. A single-purpose identifier may actually enhance personal privacy by restricting the extent of a person's identity that must be disclosed to interact with a large institution. Library cards and driver's licenses are examples of such limited purpose cards.

Service members and veterans are at an even greater risk than society as a whole due to the military's pervasive use of the SSN. This pervasive use demonstrates the utility of a personal identifier, but it may be that the SSN is the wrong number to use for this purpose. Policy changes that merely restrict usage of the SSN or technological measures such as encryption and passwords drastically reduce the utility of the SSN as a personal identifier and lower the productivity of those that have used it freely in the past.

A viable alternative to the SSN exists. By replacing the SSN with a MIN within DoD and the VA, all potential SSN losses are completely eliminated from all DoD sources. Given the above problem, this thesis will attempt to estimate the monetary costs and benefits of switching to using a Military Identification Number as the primary personal identifier, as well as conduct a cost benefit analysis of such a wholesale switch. The objective of the thesis is to determine if it is cost effective to society to conduct such a switch.

IV. ALTERNATIVE DEVELOPMENT

A. MILITARY IDENTIFICATION NUMBER

The main idea behind this thesis is the wholesale transition from the Social Security Number (SSN) to a Military Identification Number (MIN) as the primary identifier throughout the Departments of Defense (DoD) and Veterans' Administration (VA). By eliminating the SSN at all but one critical location, lost or stolen data becomes all but useless to the identity thief. The SSN would still need to be held at the Defense Finance and Accounting Service (DFAS) since they are responsible for withholding Social Security Tax and making direct deposits of pay and benefits to financial institutions. DFAS would be the sole location/system that held the match up between the MIN and the SSN. By limiting SSN use to one DFAS location, DoD could concentrate security measures on one system and location. All other computer systems and databases, even ID cards and paper records would only use the MIN. This design would minimize the data's worth to an identity thief, while increasing the usefulness of the system to its users. This increase would be dramatic since they will not have to implement cumbersome security measures.

1. Other Organizations that Have Already Made the Switch

Many public and private organizations are initiating similar transitions to the type this thesis is analyzing. Various states Department of Motor Vehicles are removing the SSN from driver's licenses in favor of unique, single purpose, state identification numbers. The same holds true for Colleges and Universities. Many have gone through the transition and are no longer using the SSN as a personal identifier.

B. TECHNOLOGY

Technology plays an ever increasing role in the proliferation of identity theft, but is also often viewed as the answer to thwart identity theft.

1. Proliferation of Identity Theft

The expansion of the Internet has made it increasingly easy to steal someone's identity and use it to open fraudulent accounts used for financial gain. This is primarily due to the fact that the Internet provides a degree of anonymity that did not exist 40 years ago when the "functionality creep" of the SSN began. (Cheney 2003)

Internet sales grow approximately 25 percent per year, and are the preferred environment for the identity thief to carry out his crime, the total dollar amount of identity theft has continued to increase in recent years, even while the total number of identity theft incidents has only declined slightly.

Increasingly adept identity thieves are using technology to crack databases and steal identity information. This is typically accomplished by hacking a database system through an Internet connection or accessing an encrypted database that was obtained by stealing a laptop or thumb-drive.

2. Tool to Prevent Identity Theft

Technology is the primary instrument being used to thwart identity theft. The increased incidence of user names and passwords is accompanied by the frustration of keeping track of them all. While this has no doubt reduced the occurrences of identity theft, it is far from a perfect solution. Plus, it continues to reduce the utility and productivity of using a universal personal identifier that drove the widespread use of the SSN in the first place. Once encryption or password technology is implemented, it is followed by security measures being cracked by identity thieves. Each cracked measure prompts a new counter-measure, which is eventually cracked once again. It is reasonable to assume that this pattern will continue. In fact, security software companies and virus protection companies count on this continued pattern for their very existence.

C. ACCESS RESTRICTIONS

Access restrictions and other policy changes are also part of the evolving "status quo." Such policy changes are driven by increased public identity theft awareness resulting from news coverage and even popular television commercials advertising a particular credit card's identity theft measures. Policy changes sometimes take the form of actual law, driven by state or federal statues, or simply procedural changes executed by public and private organizations.

V. COST/BENEFIT ANALYSIS

A. REQUIREMENTS AND METHODOLOGY

1. Office of Management and Budget (OMB) Requirements

Since the conversion from using the Social Security Number (SSN) as the primary personal identifier to the use of a Military Identification Number (MIN) would be implemented primarily through the Information Technology Systems, OMB Circular A-130 and OMB Circular A-94 are applicable. OMB Circular A-130 requires a benefit-cost analysis for each information system and OMB Circular A-94 provides the necessary guidelines and discount rates for the benefit-cost analysis.

2. Methodology

The public focus on the efficient use of tax dollars has intensified hand-in-hand with increased demand for better accountability. To make better, more informed decisions, policy makers need solid analysis of the costs and benefits associated with the available choices. The variables can be economic or intangible, but must be relevant and fit with the organization's mission and objectives.

Costs to implement a project include changing computer databases systems, training costs, materials (ID cards), administrative costs, and additional labor costs. These are fairly straightforward and apparent. Benefits, however, are not quite as easy to quantify.

Data collection needs to focus on both tangible and intangible benefits (to include public trust, morale, etc.). Intangible benefits may be difficult to convert into a monetary figure; however, they should not be disregarded when comparing the benefits of a project. Soft data, such as improved communication, increased job satisfaction, enhanced moral, policy changes, are a few examples of these intangible benefits.

The issue is that information security data is difficult to collect. Security risk is difficult to quantify and qualify. It is impossible to predict the time, methods, or frequency of future security incidents. It is acknowledged that costs of implementation

must be estimated and carefully checked with stakeholders; however, very few appear willing or able to give sound feedback. Consequently, assumptions must be made and existing data relied upon.

This thesis uses data that classifies misuse cases into categories of threats for which nationally surveyed risks and financial data are publicly available. The cost benefit analysis framework derives its figures from research, surveys, and actual misuse cases found in our literature review.

These cost assumptions are reasonable with regard to expected probabilities and costs associated with such misuses and breaches. For example, OMB, through annual national surveys shows that over the period of a year there are average probabilities of occurrence and ranges of financial impact due to exposure to these breaches.

Cost avoidance is used as the primary tangible benefit; however, if intangible benefits can be monetized, they should be included as well. If not they should be addressed and acknowledged.

Once reasonable numbers are agreed upon, evaluation techniques will be applied to aid in the analysis. Popular evaluation techniques used in the private sector are:

- Payback period
- Discounted payback period
- Benefit Cost Ratio (BCR)
- Net present value (NPV)
- Internal rate of return (IRR)
- Probabilistic Net Present Value (PNPV)

3. Purpose

A cost to benefit analysis (CBA) best matches the approach of this research to provide the decision maker with an analysis of alternatives. The scope of this research precludes the CBA from analyzing all of the possible alternatives available and therefore, compares the following two primary options:

- The status quo of continued use of the SSN as the primary personal identifier, and
- The proposed alternative of eliminating the SSN and converting to a Military Identification Number.

While at first glance this may appear as a very limited view of the alternatives, closer consideration reveals otherwise. Other alternatives that come to mind, such as encryption technologies, policy changes, legal requirements, or criminal enforcement procedures designed to protect identity data and prevent identity theft, are captured within the status quo alternative. These types of options are already being implemented and expanded upon. The proposed alternative of eliminating the SSN and replacing it with an MIN is the only real differentiated option resulting in the decreased impact of breaches.

B. COST

Due to the difficulty in collecting accurate implementation estimates of such a conversion, this research requires a multi-directional approach. The intention is to arrive at a realistic and reasonable cost estimate to conduct a cost-benefit analysis. The first method is to use the Y2K event as a proxy. The second estimation methodology used is to apply a factor to existing IT Operation and Maintenance budgets. The theory of this multi-directional approach is to examine different processes that bring to the surface more issues and components of the overall expenditures than a single approach would. An additional advantage of the multiple approach process is that it compares and contrasts the final cost figures involved in such a project. Glaring differences in final figures act to provide a signal for the necessity of further exploration and deeper analysis of one or both of the approaches, as well as the inputs used in their computations.

Y2K is used because of the IT/data base similarities. The assumption is that the conversion from SSNs to a MIN will be most similarly related to such an effort, though smaller in magnitude with regard to the number of systems affected and scope of work per system.

The Budget Estimate method justifies costs by breaking out the main sub-processes required from start to finish, taking care to only count those costs not shared by both alternatives.

1. Y2K Proxy

The recent Y2K problem can be considered a proxy for estimating the cost of the SSN to MIN conversion. For the purpose of this thesis, the various aspects of fixing the Y2K problem are assumed similar in scope and cost as conversion to a MIN as the

primary personal identifier, relative to the total number of data systems. Y2K was undoubtedly more involved than the database conversions necessary for the SSN to MIN conversion, since the Y2K fix had to address each and every line of code in every software program where a two digit year was used. Given this, a range of factors from 10 to 25 percent of the Y2K costs has been assigned to the SSN/MIN conversion. While this assumption may not be wholly accurate, it is reasonable to expect that the cost be within this order of magnitude and adequate for this cost benefit analysis. While the Y2K problem affected almost every DoD computer system, including weapon systems, communication systems and manpower systems, the MIN conversion would only affect manpower systems that currently use the SSN as the primary personal identifier. It took approximately 6 years for the DoD to address the Y2K problem at a cost of $3.596 billion. This cost covered approximately 2,101 mission critical systems and 5,488 mission support systems and covers the entire correction process, including identifying the problem, fixing systems and conducting tests. Using the Consumer Price Index (CPI) inflator, this equates to $4.2 billion in 2007 dollars. The VA's Y2K costs add an additional $231.4 million. (Informed Budgeteer 2000) This equates to $310 million in 2007 dollars using the same CPI inflator.

No one actually knows the total number of manpower systems being used throughout the DoD. The Department of Defense has approximately 10,000 computer systems, of which about 2,500 are designated as mission critical. The estimated 10,000 systems cover everything from war fighting systems that have nothing to do with SSNs to the various manpower and logistics systems. The DOD requested approximately $19 billion for fiscal year 2004 to operate, maintain, and modernize its reported 2,274 business systems.

This estimate, however, almost certainly under-represents the true number of business systems in DoD. Since DoD does not centrally manage its computer systems, it does not have an accurate method of identifying and tracking these systems. DoD relies on what is commonly known as the "data call" to obtain this type of information. The "data call" goes out to each DoD department requesting certain information, in this case, the number of business systems in existence. However, each of the DoD's departments is currently refining their own inventory and, therefore, cannot give a truly accurate answer

back to DoD. For instance, the DoD logistics community currently reports 565 systems, which are included in the 2,274 business systems previously reported. However, the logistics community recently identified an additional 3,000 potential systems of which at least 1,900 were actual systems.

Of the 2,274 business systems reported within DoD, 665 are related to Human Resource Management. An additional 10 are under the Installations and Environment category, but related to personnel. Logistics systems account for an additional 565 systems and some portion of these deal with SSNs and personnel. Accounting and Finance make up 542 systems, of which some portion would undoubtedly pertain to personnel that use SSNs. (GAO-04-615 DOD Business Systems)

Using the previous research and accounting for its under reported number of systems, it is estimated that the number of systems that use the SSN and would, therefore, need to be converted to a MIN is in the order of 1,000 systems. This is approximately 10 percent of the total number of systems involved in the Y2K problem.

To account for the fewer systems involved, we take 10 percent of DoD's Y2K costs in 2007 dollars which is $420 million. Reducing this again by factors of 10 and 25 percent, acknowledges the difference between the scope of the Y2K problem and the SSN to MIN conversion and gives an estimated DoD wide conversion cost of between $42 million and $105 million.

Since the VA deals exclusively with personnel (veterans), it is assumed that 100 percent of the VA's Y2K costs dealt with manpower systems. Following the same logic applied above, the research concludes that the VA contributes an additional $31 to $69 million, in 2007 dollars to total costs.

Taking the low and high estimates for both the DoD and VA and adding them together results in a range of $73 to $174 million as the cost estimate for the SSN to MIN conversion. This methodology shows that the VA's costs are 65.7 percent the size of DoD's.

2. Budget Estimate Method

The second method of estimating the cost of the SSN to MIN Conversion is a budgeting method. This involves using the DoD's IT budget and applying a factor to

account for the additional costs to implement the SSN to MIN conversion. To get an idea of the size of the problem, a review of the sheer magnitude of DoD's IT budget is appropriate.

DoD's FY2004 IT budget was $28 billion. which includes $18.8 billion for the 2,274 business systems previously identified. Of the $18.8 billion, $4.8 billion was for development and modernization while the remaining $14 billion was for operations and maintenance. (2004 GAO Report, Business Systems Modernization) As previously explained in the Y2K cost estimate method, the 2,274 business systems can be further reduced to approximately 1000 systems that deal with SSNs, equating to 44 percent of the business systems. 44 percent of the $14 billion in operations and maintenance is $6.15 billion. This $6.15 billion, therefore, represents the amount of the IT operations and maintenance budget that goes to systems that deal with the SSN.

A reasonable cost estimate for the SSN to MIN conversion would be 2 to 3 percent of this $6.15 billion in operations and maintenance costs. This 2 to 3 percent factor was derived from a telephone interview with the Vice President of a major consulting firm that provides one of the industry's most comprehensive set of decision-support modeling tools to help managers and cost analysts plan and estimate critical projects. 2-3 % of the $6.15 billion gives a cost range of between $123 million and $184 million.

Additionally, the VA's total IT budget for 2007 was $1.26 billion. The operations and maintenance portion of this budget is $555 million. Using the same 2 to 3 percent factor as explained above for the DoD, provides a range of $11 million to $16.5 million for the VA to implement the same SSN to MIN conversion. Combining the DoD and VA figures brings the total conversion cost estimates to between $133 million and $200.5 million.

From the above cost estimation methods, the research has arrived at a low estimate of $73 million and a high estimate of $200.5 million for the costs of implementation. For further analysis, a theoretical cash flow is needed. To establish this cash flow, other IT projects were used as a basis for the major categories of implementing

a new IT system or conducting a major update to an existing system. The flow of money through these categories and over the 10-year time frame is an estimate to show relevant CBA metric comparisons (See Tables 3 and 4).

Year	*Startup*	*Acquisition*	*Development*	*Operation*	*Maintenance*	*Total*	*Present Value (7% discount)*
1	$2 M					$2 M	$2 M
2		$20 M	$10 M			$30 M	$28.0 M
3				$5 M	$1 M	$6 M	$5.24 M
4				$5.15 M	$1.03 M	$6.18 M	$5.04 M
5				$5.30 M	$1.06 M	$6.37 M	$4.86 M
6	$1.52 M				$1.09 M	$2.61 M	$1.87M
7		$15.23 M	$7.62 M		$1.12 M	$23.9 M	$15.9 M
8				$3.80 M	$1.76 M	$5.57 M	$3.46M
9				$3.92 M	$1.81 M	$5.74 M	$3.34 M
10				$4.04 M	$1.86 M	$5.91 M	$3.21 M
Total						$94.4 M	$73.0 M

Table 3. Low Estimate Cash Out-Flows (approx $73 million)

The following cash flow represents the high estimate. Instead of using of using the $200.5 million previously found, the following cash flow table was established by tripling the low estimate. This estimate is 10 percent higher than the $200.5 million high estimate found in the Budget Estimate method and provides a more conservative CBA.

Year	*Startup*	*Acquisition*	*Development*	*Operation*	*Maintenance*	*Total*	*Present Value (7% discount)*
1	$6 M					$6 M	$6 M
2		$60 M	$30 M			$90 M	$84.11 M
3				$15 M	$3 M	$18 M	$15.72 M
4				$15.45 M	$3.09 M	$18.54M	$15.13 M
5				$15.91 M	$3.18 M	$19.10M	$14.57 M
6	$4.57 M				$3.27 M	$7.85 M	$5.60 M
7		$45.69 M	$22.85 M		$3.38 M	$71.92M	$47.93 M
8				$11.42 M	$5.28 M	$16.71M	$10.40 M
9				$11.77 M	$5.44 M	$17.21M	$10.02 M
10				$12.12 M	$5.61 M	$17.73M	$9.64 M
Total						$283.0M	$219.1 M

Table 4. High Estimate Cash Out-Flows (approx $219 million)

3. Efficient Market Hypothesis Method

The Efficient Market Hypothesis, as developed by Professor Eugene Fame at the University of Chicago, Graduate School of Business, states the financial markets governing public companies quickly reflect all known information that can affect the company. This theory suggests that all of the financial losses to a company that experiences a data breach of privacy information will quickly be reflected in the stock price of the company. According to the hypothesis, even the probabilities of the resulting financial losses would be accounted for in the market capitalization of the company.

Several large, publicly traded financial companies have experienced major data breaches over the past several years. In the research paper, "Quantifying the financial impact of IT security breaches," Ashish Garg et al., show that the average market capitalization loss resulting from several theft events concerning credit card information was a -15% change in market cap. (Garg et al., 2003)

Using various aspects of the size of the DoD, such as its $1.1 trillion in assets, its 3.3 million military and civilian personnel and its $416 billion annual budget, (GAO, 2004) the potential value of a DoD data loss can be estimated. If you combine the VA and DoD budgets, they total approximately $490 billion. By using this as a proxy for the "market capitalization" of the DoD, a significant data loss from DoD or the VA would equate to approximately a societal loss of $73.5 billion. This efficient market hypothesis method shows that the cost estimate used in this research is actually a conservative one.

C. BENEFITS

Capital investment decisions are complex and often involve many non-quantitative or qualitative factors that are difficult to fully capture in analysis. Often an organization may go ahead with an investment because of political pressure or to accomplish social objectives that lie outside the profit motive. In making capital investment decisions, private producers only consider producer surplus. The Federal Government, on the other hand, is obligated to account for producers and consumers, the government and society as a whole.

1. Cost Avoidance

There are approximately 26.5 million veterans in the Veterans Administration system. From the literature review, CBO estimates that implementing H.R. 5835 would cost $5 million in 2007 and about $50 million over the 2007-2011 period ($10 million per year). However, if the VA were to experience another data breach similar to the recent incident involving 17 million individuals, the cost could be as much as $1 billion. The CBO estimated that the VA could be expected to experience an average of three incidents a year in which sensitive, personal information is compromised in some manner. Excluding the recent incident, the average number of people affected by a data breach has been about 50,000. The expected cost of notification for groups this size would be approximately $500,000 a year. CBO estimates that 10 to 15 percent of those whose information is compromised will experience a loss on the order of about $450. Thus, CBO estimates that the cost to the VA would be about $10 million a year on average. This estimate, however, is not complete.

a. Interpolation Method

Total societal financial loss estimates to business and individuals in 2006 that are directly related to identity theft are $55 billion and $5 billion per respectively, in the United States alone (FTC 28 September 2004). 10 million people per year discover they are victims of identity theft. This is 4.6 percent of the approximately 217,391,304 United States adult population. The DoD and VA combined account for 13.6 percent of the U.S. adult population. (29,565,231/217,391,304=.136). Researchers estimate that the amount of identity theft attributed to loss of records at work accounts for 3 percent of all identity thefts. (Identity Theft: The Aftermath 2004)

For this research the 3 percent estimate has been revised up to 5 percent for the DoD/VA population because "work" comprises a relatively larger portion of the DoD employees' life, i.e., health care, child care, Family Service Center, deployed mailing addresses, exchange, commissary, MWR, club systems, etc. which are all part of DoD/VA.

The potential benefits derived from this estimation method are illustrated in Table 5, below.

Benefit Category	***Benefit Elements***	***Value (Tangible or Intangible)***
Financial loss to society avoided	Individual and business financial loss	$60 Bil/yr * 13.6% * 5%= $408 mil yr
Financial loss to DoD and VA avoided	Direct gov't bailouts, ID theft Insurance, Credit check cost coverage	$10 M * 2 = $20 mil yr

Table 5. Interpolation Method Benefits

b. Second Estimation Method

The CBO estimated that the cost for Veterans' Affairs to meet the requirement to notify and provide credit watch for individuals due to information breach as stipulated in H.R. 5835, the Veterans' Identity and Credit Security Act of 2006, to be the following:

- $5 million for 2007
- $50 million 2007-2011 ($10 million a year)
- (However, if there were a breech similar to the most recent (17 million), the cost could be >$1 billion.)

In making theses estimates, the CBO assumes that the VA will experience three breaches a year. CBO estimates that the personal information of 50,000 people will be compromised per breech, and that 10-15% will experience a loss (become a victim of identity theft). The average estimated loss would be approximately $450. Using this data, the total individual loss per year is approximately $10,125,000, as shown below.

- 50,000 people*15% loss rate = 7,500 people/breach
- 7,500*3 breaches/yr = 22,500 people/yr
- 22,500*$450 personal loss/person = $10,125,000 total personal loss/yr

However, the analysis above DOES NOT account for losses to private businesses. Private business absorb the vast majority of the financial losses associated with identity theft, so using a conservative estimate of a 10 to 1 ratio for costs (business to individual) it is estimated that the following business losses are experienced:

- $10,125,000*10=$101,250,000 business loss/yr
- $101,250,000 + $10,125,000 personal/yr = $111,375,000 total/yr

This $111,375,000 figure represents the total annual losses attributable to identity theft associated with the VA alone. Presuming the DoD follows a similar pattern, the costs to society would be $222,750,000 per year.

Comparing this CBO based estimate with an estimate using 2004 figures from Identity Theft: The Aftermath 2004 (IT 2004), it is possible that the calculation may be on the low side. IT 2004 estimated the average cost to the individual as $2671 in

earnings and expenses, 5.9 times as large as the aforementioned $450. To ensure a conservative estimate, the lower 10% loss experience rate was applied resulting in the following:

- 50,000 people*10% loss rate = 5,000 people/breach
- 5,000*3 breaches/yr = 15,000 people/yr
- 15,000*$2,671 personal loss/person=$40,065,000 total personal loss/yr

Using the same conservative estimate of a 10 to 1 ratio for costs (business to individual) it is estimated:

- $40,065,000*10=$400,650,000 business loss/yr
- $400,650,000+ $40,065,000 personal/yr =$440,715,000 total/yr

These figures, represent the total annual losses associated with the VA alone. Assuming the DoD follows a similar pattern, $881,430,000 per year is the total cost to society.

The $408 million per year estimate, computed in the interpolation method, falls in the middle of this estimated range and appears reliable for use in the cost benefit analysis.

2. Benefit Schedule

Obviously the $408 million of annual indirect benefits (costs avoided) could not possibly be realized in the first year; therefore, an annual schedule of benefits must be calculated (See Table 6). Additionally, the total costs must be allocated appropriately to the two organizations involved, the DoD and the VA.

To estimate such a schedule, the $408 million is divided by the 29.5 million individuals comprising the DOD and VA system. The result is $13,830,508 in annual costs per million individuals. This figure is then multiplied by three to represent the total annual costs, $41,491,525, associated with the DoD. It is also multiplied by 26.5 to illustrate the portion of total costs, $366,508,475, for which the VA is responsible. In essence the total $408 million has been prorated across the two organizations.

It is assumed that implementation of the conversion will be staggered. For estimation purposes, calculations assume transition first at the DoD followed by the VA.

Period (Yr)	DoD % Implemented	$ Benefits	VA % Implemented	$ Benefits	Total $ Benefits
1	0%	$0	0%	$0	$0
2	30%	$12,447,458	0%	$0	$12,447,458
3	60%	$24,894,915	0%	$0	$24,894,915
4	90%	$37,342,373	0%	$0	$37,342,373
5	99%	$41,076,610	0%	$0	$41,076,610
6	100%	$41,491,525	0%	$0	$41,491,525
7	100%	$41,491,525	25%	$91,627,119	$133,118,644
8	100%	$41,491,525	50%	$183,254,237	$224,745,763
9	100%	$41,491,525	75%	$274,881,356	$316,372,881
10	100%	$41,491,525	100%	$366,508,475	$408,000,000

Table 6. Theoretical Implementation Schedule (Indirect Benefits)

The direct benefits follow the same schedule, but are applied uniformly to the $20 million ($10 million for each department) as recommended in the CBO study. The combined cost and benefits (low and high estimates) are shown in Tables 7 and 8.

Yr	Costs	Direct Benefits	7% Disc Factors	PV Costs	PV Direct Benefits	Indirect Benefits	PV Indirect Benefits	PV Total Benefits	Difference PV Total Bene-Costs
1	2,000,000	0	1	2,000,000	0	0	0	0	-2,000,000
2	30,000,000	3,000,000	0.9346	28,037,383	2,803,738	12,447,458	11,633,138	14,436,876	-13,600,507
3	6,000,000	6,000,000	0.8734	5,240,632	5,240,632	24,894,915	21,744,183	26,984,815	21,744,183
4	6,180,000	9,000,000	0.8163	5,044,721	7,346,681	37,342,373	30,482,500	37,829,181	32,784,460
5	6,365,400	9,900,000	0.7629	4,856,133	7,552,663	41,076,610	31,337,149	38,889,812	34,033,679
6	2,616,013	10,000,000	0.7130	1,865,181	7,129,862	41,491,525	29,582,884	36,712,746	34,847,565
7	23,974,800	12,500,000	0.6663	15,975,422	8,329,278	133,118,644	88,702,573	97,031,851	81,056,430
8	5,569,858	15,000,000	0.6227	3,468,628	9,341,246	224,745,763	139,960,366	149,301,612	145,832,984
9	5,736,954	17,500,000	0.5820	3,338,959	10,185,159	316,372,881	184,131,897	194,317,057	190,978,097
10	5,909,063	20,000,000	0.5439	3,214,139	10,878,675	408,000,000	221,924,967	232,803,642	229,589,503
Total	**94,352,088**	**102,900,000**		**73,041,198**	**68,807,934**			**828,307,592**	**755,266,394**
Net Benefits					**-4,233,264**			**755,266,394**	

Table 7. Low Estimate

Yr	Costs	Direct Benefits	7% Disc Factors	PV Costs	PV Direct Benefits	Indirect Benefits	PV Indirect Benefits	PV Total Benefits	Difference PV Total Bene-Costs
1	6000000	0	1	6,000,000	0	0	0	0	-6,000,000
2	90000000	3,000,000	0.935	84,112,150	2,803,738	12,447,458	11,633,138	14,436,876	-69,675,273
3	18000000	6,000,000	0.873	15,721,897	5,240,632	24,894,915	21,744,183	26,984,815	11,262,918
4	18540000	9,000,000	0.816	15,134,163	7,346,681	37,342,373	30,482,500	37,829,181	22,695,018
5	19096200	9,900,000	0.763	14,568,400	7,552,663	41,076,610	31,337,149	38,889,812	24,321,412
6	7848000	10,000,000	0.713	5,595,516	7,129,862	41,491,525	29,582,884	36,712,746	31,117,230
7	71924400	12,500,000	0.666	47,926,265	8,329,278	133,118,644	88,702,573	97,031,851	49,105,586
8	16710000	15,000,000	0.623	10,406,148	9,341,246	224,745,763	139,960,366	149,301,612	138,895,464
9	17210000	17,500,000	0.582	10,016,377	10,185,159	316,372,881	184,131,897	194,317,057	184,300,680
10	17727000	20,000,000	0.544	9,642,313	10,878,675	408,000,000	221,924,967	232,803,642	223,161,328
Total	**283,055,600**	**102,900,000**		**219,123,227**	**68,807,934**			**828,307,592**	**609,184,364**
Net Benefits					**-150,315,293**				

Table 8. High Estimate

D. ANALYSIS

For an analysis of long-term investments a variety of evaluation techniques must be considered. The more popular of these include the following:

- Payback period
- Discounted payback period
- Benefit to Cost Ratio (BCR)
- Net present value (NPV)
- Internal rate of return (IRR)
- Probabilistic Net Present Value (PNPV)

These techniques provide the decision maker with the information to compare the proposed alternatives - maintaining the status quo versus implementing a conversion from SSN to MIN. Additionally, these metrics are useful when comparing other, future alternatives of varying costs, size, time for implementation, etc.

1. Payback Period

The payback period measures the length of time required to recover the amount of initial investment. Though it's simple to calculate, it disregards the time value of money. To quantify the payback period, the cumulative benefits are considered to identify the

instant that the cumulative cash flow breaks even. At this break-even point the initial investment is repaid. Table 9 shows the figures previously discussed to provide a payback period analysis.

Years	Out-Flow	In-Flow	Net Cash-Flow	Cumulative Cash-Flow	Cumulative Cash In-Flow
1	2	0.0000	-2	-2	-73.0412
2	30	15.4470	-14.553	-16.553	15.4470
3	6	30.8940	24.894	8.341	30.8940
4	6.18	46.3420	40.162	48.503	46.3420
5	6.3654	50.9760	44.6106	93.1136	50.9760
6	2.616013	51.4910	48.87499	141.9886	51.4910
7	23.9748	145.6180	121.6432	263.6318	145.6180
8	5.569858	239.7450	234.1751	497.8069	239.7450
9	5.736954	333.8720	328.135	825.942	333.8720
10	5.909063	428.0000	422.0909	1248.033	428.0000

Table 9. Payback Period Using Low Cost Estimates

Since the cash inflows are not equal, the payback period is discovered based on trial and error. Using $73.04 million as the total up front cost of the project and observing cash inflows, the following total break-even point is derived:

$73.04 M = 3 + ((73.04M- ($15.447M + $30.894M)) / $46.342M) = 3.57 yrs

Period	Out-Flow	In-Flow	Net Cash-Flow	Cumulative Cash-Flow	Cumulative
1	6	0.0000	-6	-6	-219.1236
2	90	15.4470	-74.553	-80.553	15.4470
3	18	30.8940	12.894	-67.659	30.8940
4	18.54	46.3420	27.802	-39.857	46.3420
5	19.0962	50.9760	31.8798	-7.9772	50.9760
6	7.848039	51.4910	43.64296	35.66576	51.4910
7	71.9244	145.6180	73.6936	109.3594	145.6180
8	16.70958	239.7450	223.0354	332.3948	239.7450
9	17.21086	333.8720	316.6611	649.0559	333.8720
10	17.72719	428.0000	410.2728	1059.329	428.0000

Table 10. Payback Period Using High Cost Estimates

Using the same logic with the higher cost estimate of $219M (See Table 10) the following total break-even point is determined:

$$\$219.1236\ M = 6 + (\$23.97M / \$145.618M) = 6.16\ yrs$$

When using payback period as an evaluative tool, the decision rule is to choose the project with the shorter payback period. The shorter the payback period the less risky the project, in part due to the greater liquidity afforded the organization.

The payback period method for evaluating an investment project is simple to compute and easy to understand. However, it does not recognize the time value of money and ignores the impact of continued returns after the payback period. These continued cost savings are exactly the returns the research is examining.

2. Discounted Payback Period

The discounted payback period takes into account the time value of money. Time value of money is a critical consideration in financial and investment decisions. Discounting is used to evaluate the future cash flows associated with capital budgeting projects to determine its present value (PV). PV is the present worth of future sums of money.

The discount rate, more commonly called the opportunity cost of capital, is the minimum rate of return required by the investor. The PV of a series of mixed payments (deferred costs) is the sum of the PV of each individual payment. The discounted payback period, therefore, is computed by adding the PV of each period's benefits until such benefits equal the initial investment.

Period	Discounted Out-Flow	Discounted In-Flow	DiscNet Cash-Flow	Cumulative
1	2	0.0000	-2	-2
2	28.03738	14.4370	-13.6004	-15.6004
3	5.240632	26.9850	21.74437	6.143984
4	5.044721	37.8290	32.78428	38.92826
5	4.856133	38.8890	34.03287	72.96113
6	1.865181	36.7130	34.84782	107.8089
7	15.97542	97.0320	81.05658	188.8655
8	3.468628	149.3010	145.8324	334.6979
9	3.33896	194.3170	190.978	525.6759
10	3.214139	232.8040	229.5899	755.2658

Table 11. Discounted Payback Period Using Low Cost Estimates

Since the discounted cash inflows are not equal, the payback period is discovered based on trial and error. Using $73.04M as the present value of the costs over the life of the project and observing discounted cumulative cash inflows (see Table 11) the following total break-even point is derived:

$73.04 M = 3 + (($73.04M-($14.437M + $26.985M)) / $37.829 M) = 3.836 yrs

Table 10 also illustrates that discounted cash flow becomes positive in year three, with a cumulative cash flow break even at 2.717 yrs.

2 + ($15.60 M / $21.7443 M) = 2.717 yrs

Period	Discounted Out-Flow	Discounted In-Flow	DiscNet Cash-Flow	Cumulative
1	6	0.0000	-6	-6
2	84.11215	14.4370	-69.6751	-75.6751
3	15.7219	26.9850	11.2631	-64.412
4	15.13416	37.8290	22.69484	-41.7172
5	14.5684	38.8890	24.3206	-17.3966
6	5.595544	36.7130	31.11746	13.72085
7	47.92627	97.0320	49.10573	62.82658
8	10.40588	149.3010	138.8951	201.7217
9	10.01688	194.3170	184.3001	386.0218
10	9.642416	232.8040	223.1616	609.1834

Table 12. Discounted Payback Period Using High Cost Estimates

Using the same logic with the higher cost estimate of $219M (See Table 12) yields the following total break-even point:

$219.1236 M = 6 + ($64.2706M / $97.03M) = 6.662 yrs

Again, discounted cash flow is positive in year three; however, discounted cumulative cash flow does not break even until 5.559 yrs.

5 + ($17.3966 M / $31.117 M) = 5.559 yrs

3. Benefit to Cost Ratio (BCR)

The BCR, also called the profitability index, is the ratio of the total PV of future cash inflows to the initial investment, (PV/I). This index ranks projects in descending order of attractiveness. If the BCR is greater than 1, then accept the project, for example, if the index equals 1.50, then this project generates $1.50 for each dollar invested, time

adjusted. The greatest advantage of the BCR is that it compares all projects on the same relative basis regardless of size. The index is widely used to rank projects that compete for limited funds.

As shown in Table 13, with a PV of benefits estimated at $828.307 million over the ten-year period, the profitability index is 11.34.

828.307 / 73.04 = 11.34

Similarly, Table 14 depicts an index of 3.78, over the same time period using the higher cost estimate.

828.307 / 219.1236 = 3.78

Year	PV Costs Cumulative	PV Benefits Cumulative	Incremental BCR
1	2,000,000	0	0.0000
2	30,037,383	14,436,876	0.4806
3	35,278,016	41,421,692	1.1742
4	40,322,736	79,250,872	1.9654
5	45,178,870	118,140,684	2.6150
6	47,044,051	154,853,430	3.2917
7	63,019,472	251,885,281	3.9969
8	66,488,100	401,186,893	6.0340
9	69,827,059	595,503,950	8.5283
10	73,041,198	828,307,592	11.3403

Table 13. BCR Using Low Cost Estimates

Year	PV Costs Cumulative	PV Benefits Cumulative	Incremental BCR
1	6,000,000	0	0.0000
2	90,112,150	14,436,876	0.1602
3	105,834,047	41,421,692	0.3914
4	120,968,209	79,250,872	0.6551
5	135,536,609	118,140,684	0.8717
6	141,132,124	154,853,430	1.0972
7	189,058,389	251,885,281	1.3323
8	199,464,537	401,186,893	2.0113
9	209,480,914	595,503,950	2.8428
10	219,123,227	828,307,592	3.7801

Table 14. BCR Using High Cost Estimates

Though this technique is straight-forward it does have a disadvantage in that it only considers the relative magnitude of net benefits. Therefore, the BCR may favor projects with lower costs and benefits over those with greater net benefits, depending on their relative magnitudes.

4. Net Present Value (NPV)

The NPV and the Internal Rate of Return (IRR) are called discounted cash flow (DCF) methods. Both consider the time value of money in addition to estimated future cash flows. Starting with a given amount invested today, NPV looks forward in time to determine the amount of future returns (costs avoided) needed to satisfy the cost-of-capital requirements of the organization. (OMB Circular 94 requires an ROE of 7 percent.) The present value of an investment is found by discounting such future returns. This figure is the most a business should be willing to invest in order to receive future returns from the investment.

The NPV is the excess of the PV of cash inflows (costs avoided) generated by the project less the initial investment - (I): NPV=PV-I.

The capital recovery portion of the cash return is very important to understand. NPV discounts all cash flows at the cost of capital, thus implicitly assuming that these cash flows can be reinvested at this rate. This allows for decision makers to plan ahead for the capital recovery from the project to ensure the 7 percent ROE is met.

Period	Out	In	Cumulative
1	2	0.0000	-73.0412
2	30	15.4470	15.4470
3	6	30.8940	30.8940
4	6.18	46.3420	46.3420
5	6.3654	50.9760	50.9760
6	2.616013	51.4910	51.4910
7	23.9748	145.6180	145.6180
8	5.569858	239.7450	239.7450
9	5.736954	333.8720	333.8720
10	5.909063	428.0000	428.0000

Table 15. NPV Using Low Cost Estimates

From the figures in Table 15 the NPV of the ten year period is $701.07M. Using the higher cost estimates of Table 16, the NPV is $554.99M over the same ten year period.

per	Out	in	Cumulative
1	6	0.0000	-219.1236
2	90	15.4470	15.4470
3	18	30.8940	30.8940
4	18.54	46.3420	46.3420
5	19.0962	50.9760	50.9760
6	7.848039	51.4910	51.4910
7	71.9244	145.6180	145.6180
8	16.70958	239.7450	239.7450
9	17.21086	333.8720	333.8720
10	17.72719	428.0000	428.0000

Table 16. NPV Using High Cost Estimates

The decision rule is that if NPV is positive, accept the project; otherwise reject it. Additionally, the NPV provides more accurate ranking of alternatives since the cost of capital is a more realistic reinvestment rate, an advantage it holds over the IRR.

5. Internal Rate of Return (IRR)

The IRR, also called the time-adjusted rate of return, is defined as the rate of interest that equates the investment (I) with the PV of future cash inflows. It is the precise discount rate that yields a zero NPV. Higher IRRs are preferable to lower IRRs assuming the IRR is higher than the hurdle rate.

Applying the formula to the figures in Table 15, the IRR over the ten-year period is 62%. Using the higher cost figures of Table 16, the IRR over the same ten-year period is 31%.

The decision rule here is to accept the project with the highest IRR that exceeds the cost of capital; otherwise reject it.

The advantage of using the IRR method is that it considers the time value of money; however, like the BCR, it fails to recognize the varying sizes of investment in competing projects. Its largest drawback is that it implies a reinvestment rate at IRR. Thus, the implied reinvestment rate will differ from project to project.

6. Probabilistic NPV

As stated earlier, the NPV is the excess of the PV of cash inflows (costs avoided) generated by the project less the initial investment. To consider the NPV in a more realistic fashion a probability spreadsheet was developed using the Crystal Ball software. Crystal Ball uses Monte Carlo simulation to assist in decision analysis. The software enables the analyst to define probability distributions on uncertain model variables and then use the simulation to generate random values from within the defined probability ranges. The outcome is a probability-based spreadsheet illustrating a more convincing Net Present Value (NPV).

For simulation purposes, the following variables were used: present value of the cash flow, implementation cost, and the discount rate. The probability distributions are referred to as "assumptions" and used to define the uncertainty. The assumptions are based on this research, intuition, and the desire to maintain conservative estimations.

Additionally, for this analysis, it is assumed that a triangular distribution best fits the present value of the benefits and costs associated with a conversion from the SSN to a MIN. Triangular distributions are ideal for describing basic situations where the minimum, likeliest, and maximum values are somewhat known.

To calculate the minimum PV of benefits, the low benefit figure taken from the CBO's figures of $222,750,000 was used by applying our benefit schedule. For the maximum and most likely PV of benefits the larger figure of $408,000,000 was run through the benefit schedule. For costs, the same triangular distribution principle was applied using $73,000,000 as a minimum and $219,000,000 as a maximum. However, a more conservative estimate of $200,000,000 was chosen as the most likely amount (See Table 17).

Period	Minimum	Likeliest	Maximum	Mean in simulation
PV Period 1	0	0	0	0
PV Period 2	8.4400	15.4470	15.5000	13.1633
PV Period 3	16.8600	30.8940	30.9000	26.2770
PV Period 4	25.3000	46.3420	46.3500	39.4795
PV Period 5	27.8000	50.9760	50.9800	42.9744
PV Period 6	28.1100	51.4910	51.5000	43.6752
PV Period 7	79.5000	145.6180	145.6200	123.4649
PV Period 8	130.9000	239.7450	239.7500	203.2803
PV Period 9	182.2800	333.8720	333.8800	283.5487
PV Period 10	233.6000	428.0000	428.0100	362.8702
PV of Costs	73.00	200.00	219.00	164.41

Table 17. Assumptions for Low Estimate Method

(*Figures are in millions of dollars, assumes a 7% discount rate, and a triangular distribution for all benefit and cost figures)*

Crystal Ball software was then used to calculate the probable net present value (PNPV). A Monte Carlo simulation of two thousand trials was run, randomly selecting numbers from the assigned distribution. The resulting distribution is shown in Figure 6 below:

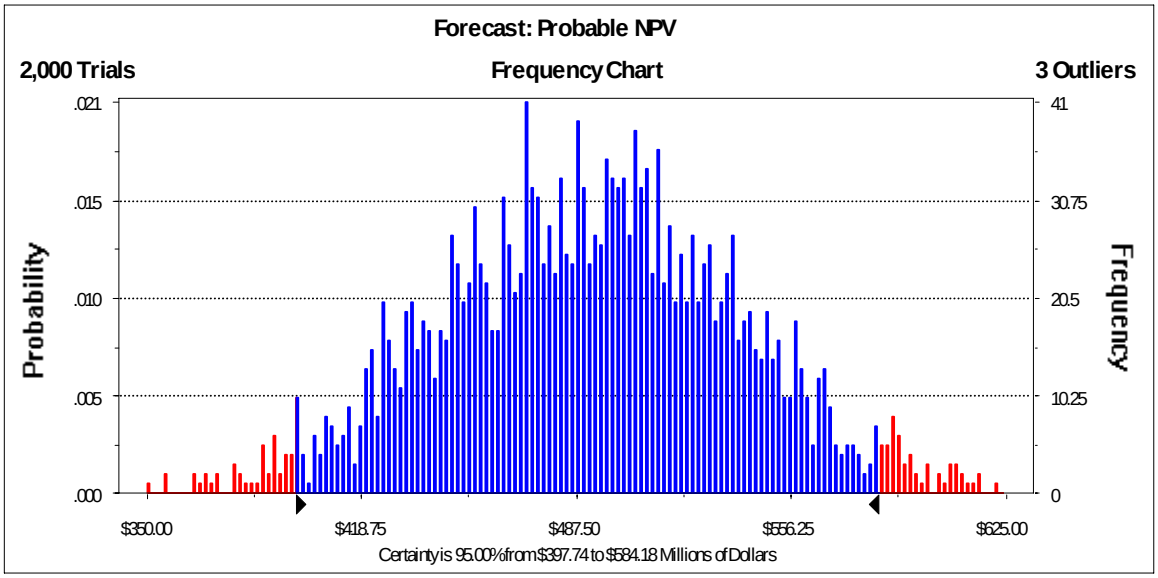

Figure 6. Probable NPV Distribution Low Estimate

Based upon these findings, there is a 95 percent degree of confidence that the true mean of the NPV population falls somewhere between $397.74 and $584.18 million dollars. Table 18 shows the summary statistics of the low estimate.

Statistic	Value
Trials	2,000
Mean	$492.29
Median	$492.86
Standard Deviation	$46.99
Variance	$2,207.69
Skewness	0.02
Kurtosis	2.84
Coeff. of Variability	0.10
Range Minimum	$351.47
Range Maximum	$647.14
Range Width	$295.66
Mean Std. Error	$1.05

Table 18. Summary Statistics Low Estimate

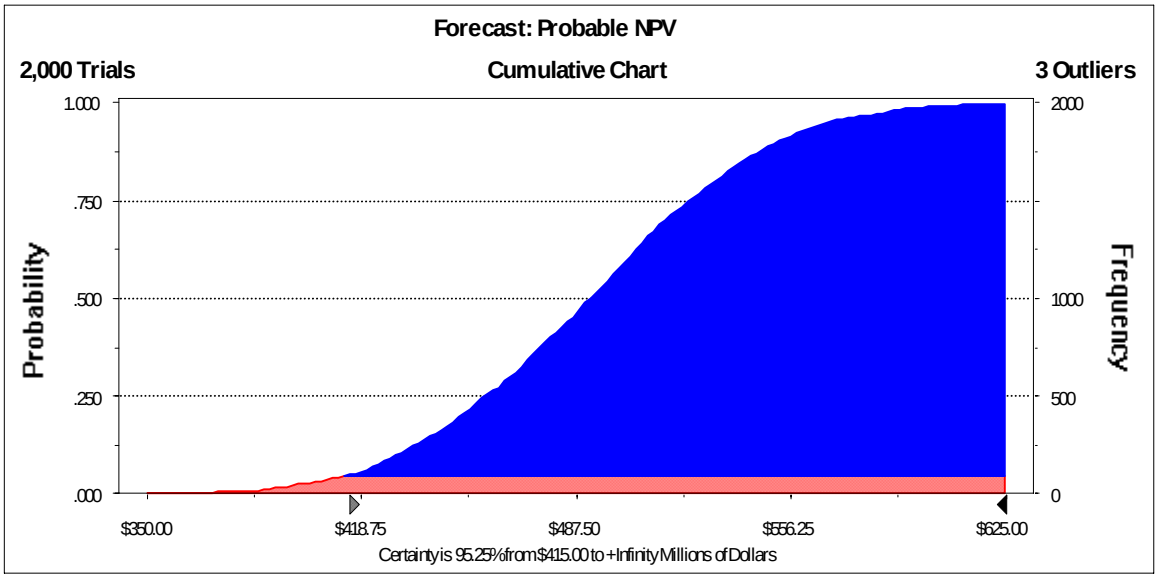

Figure 7. Cumulative Probable NPV, Low Estimate

Figure 7 above shows the simulation output indicates that 95.25 percent of the time, the NPV, with a 7 percent discount cash rate, varying implementation costs and cash flows, is above $415 million.

A second analysis was performed assuming triangular distributions centering on the total benefits from the benefit schedule. To calculate the minimum PV of benefits low benefit figure of $222,750,000 was used once again. For the maximum value the larger benefit figure of $881,430,000, taken from calculations using the 2004 figures from Identity Theft: The Aftermath 2004 (IT 2004), was applied. The benefit schedule based on the $408,000,000 figure was used for the most likely outcome.

Crystal Ball software was then used to calculate the probable net present value (PNPV). A Monte Carlo simulation of one thousand trials was run, randomly selecting numbers from the assigned distribution. The results are shown in Table 19 and Figures 8 thru 10:

Statistic	Value ($ in millions)
Trials	1,000
Mean	$804.79
Median	$799.48
Standard Deviation	$121.55
Variance	$14,774.94
Skewness	0.20
Kurtosis	2.81
Coeff. of Variability	0.15
Range Minimum	$441.53
Range Maximum	$1,158.39
Range Width	$716.86
Mean Std. Error	$3.84

Table 19. Summary Statistics, High Estimate

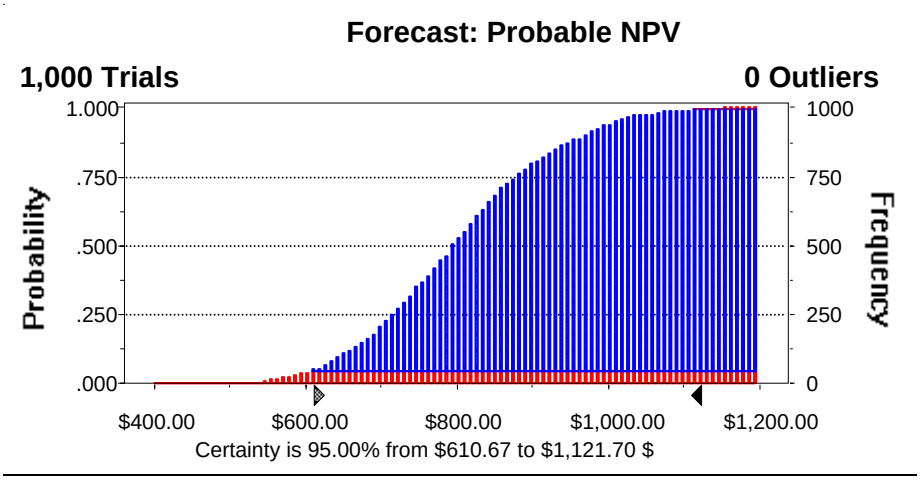

Figure 8. Cumulative Probable NPV, High Estimate

Based upon these findings there is a 95 percent degree of confidence that the true mean of the population falls somewhere between $610.67 and $1,121.70 million dollars.

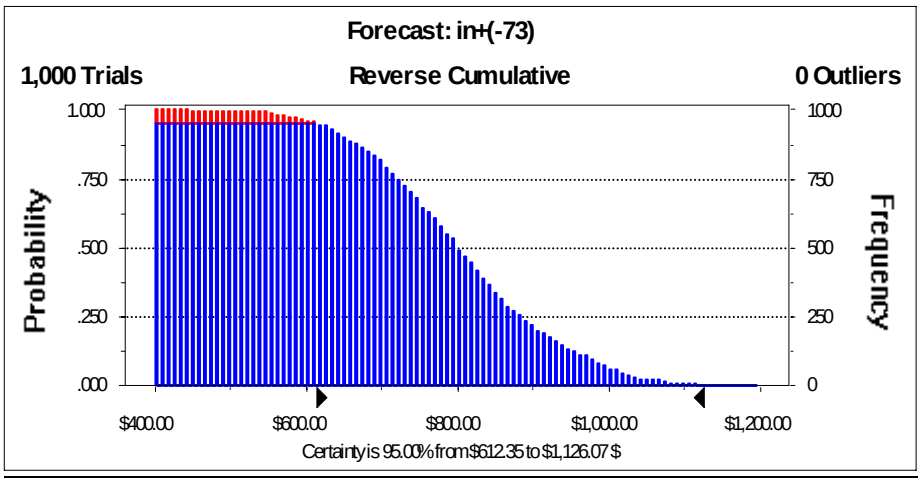

Figure 9. Reverse Cumulative Probable NPV, High Estimate

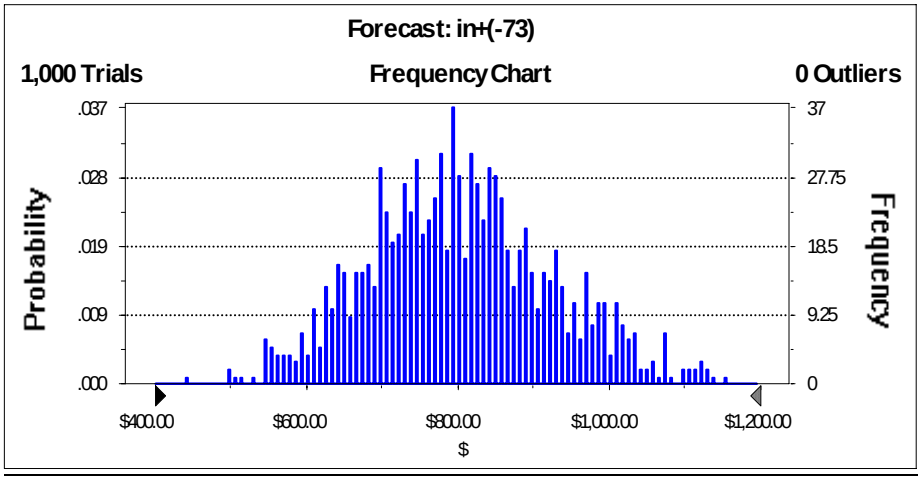

Figure 10. Probable NPV Distribution Low Estimate

By referencing Figures 8 through 10 and Table 19, the data shows that, for the low estimate, at the 95 percent confidence level the true mean of the NPV population falls between $397,740,000 and $584,180,000, with a mean of $492,290,000. Looking at the high estimate, at the 95 percent confidence level the true mean of the NPV population falls between $610,670,000 and $1,121,700,000, with a mean of $804,790,000.

E. SUMMARY OF OUTCOMES FOR ALL METHODS

SSN to MIN Conversion	Payback period	Discounted Payback period	Benefit to Cost Ratio (BCR)	Net present value (NPV)	Internal rate of return (IRR)	Probabilistic-Net Present Value (PNPV)
Low Cost	3.57 yrs	3.836 yrs	11.34	$701.07M	62%	$804.79 (High Benefit)
High Cost	6.16 yrs	6.662 yrs	3.78	$554.99M	31%	$492.29 (Low Benefit)

Table 20. CBA Summary Table

Table 20 is the compilation of the metrics from the previous section. It indicates that, given the assumptions made throughout the cost/benefit analysis, the following can be assumed about a conversion from SSN to a MIN:

- The Payback period figures show that the benefits will begin to exceed the costs somewhere between 3.57 and 6.16 years, and between 3.836 and 6.662 years when the benefits are discounted.
- For every dollar invested in the conversion the return will be between $3.78 and $11.34 over the ten year period considered.
- The internal rate of return lies in the 31 to 62 percent range.
- The NPV is between $554.99 and $701.07 million, or $492.29 and $804.79 million when risk adjusting probability distributions are applied.

These metrics provide the decision maker tools by which other alternatives can be measured and ranked.

The combined cost and benefit are graphically illustrated below in Figures 11 thru 14 below:

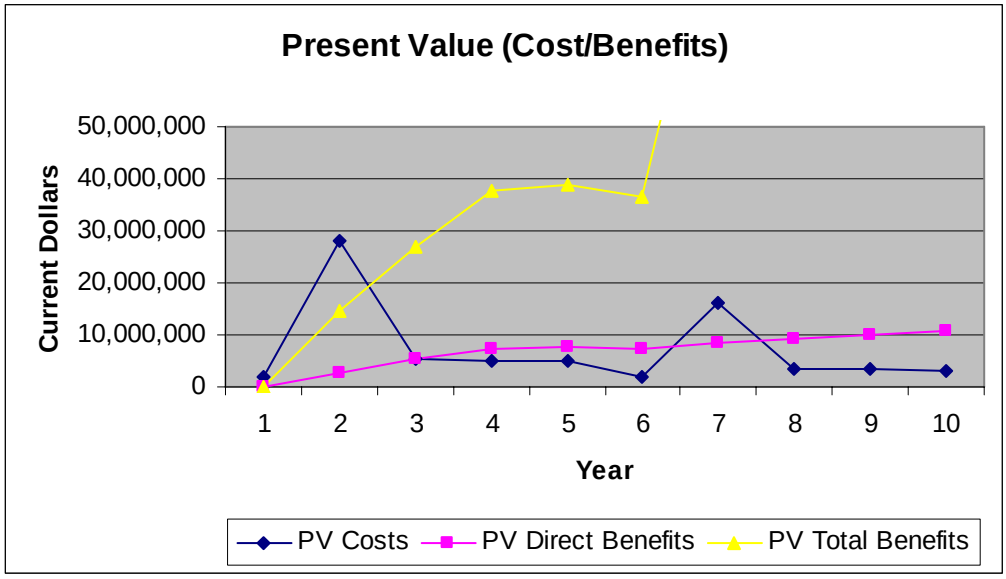

Figure 11. Present Value of Cost and Benefits, Low Cost Estimates

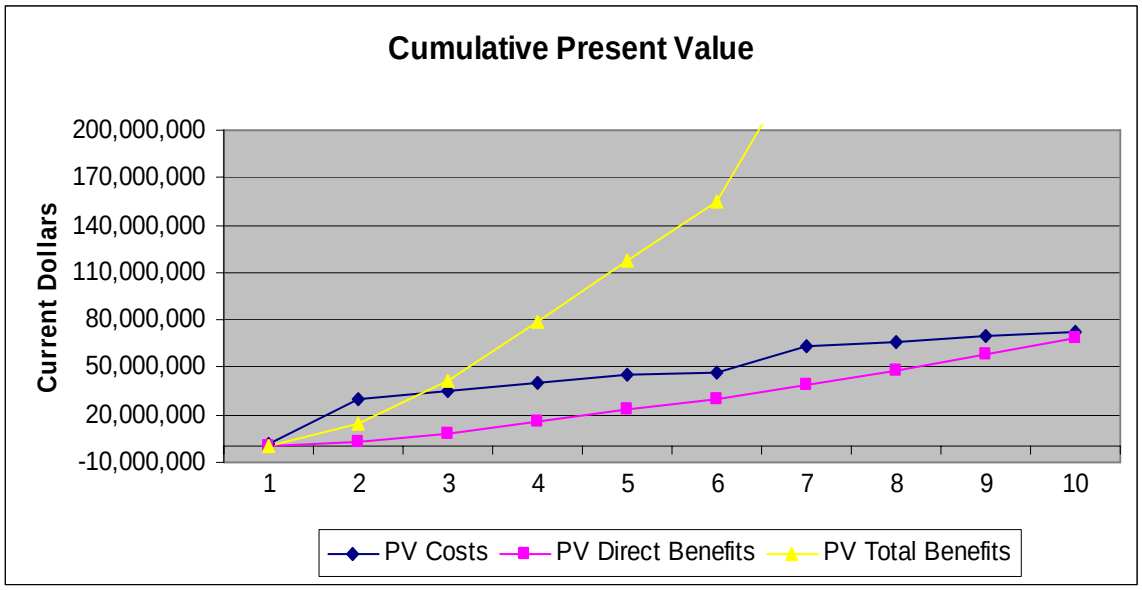

Figure 12. Cumulative Present Value of Cost and Benefits, Low Cost Estimates

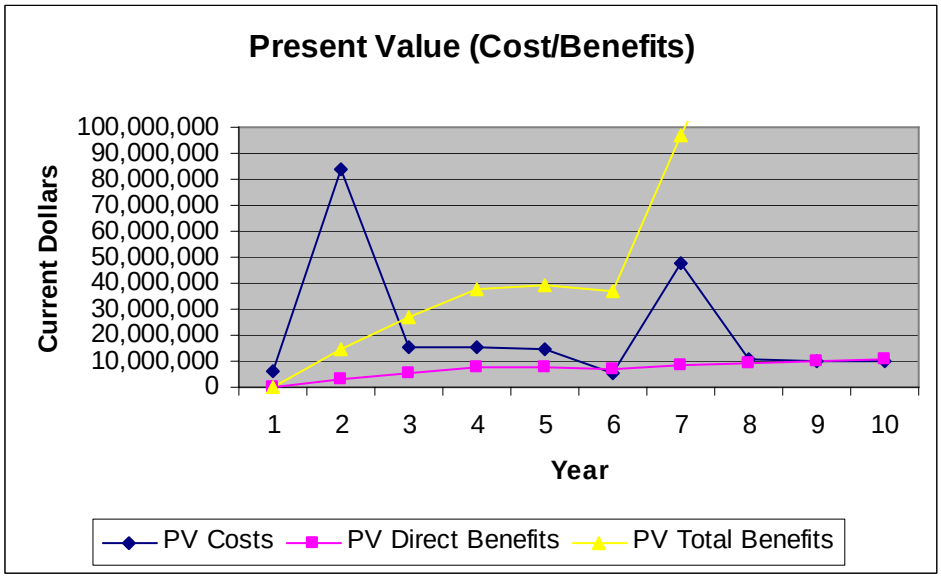

Figure 13. Present Value of Cost and Benefits, High Cost Estimates

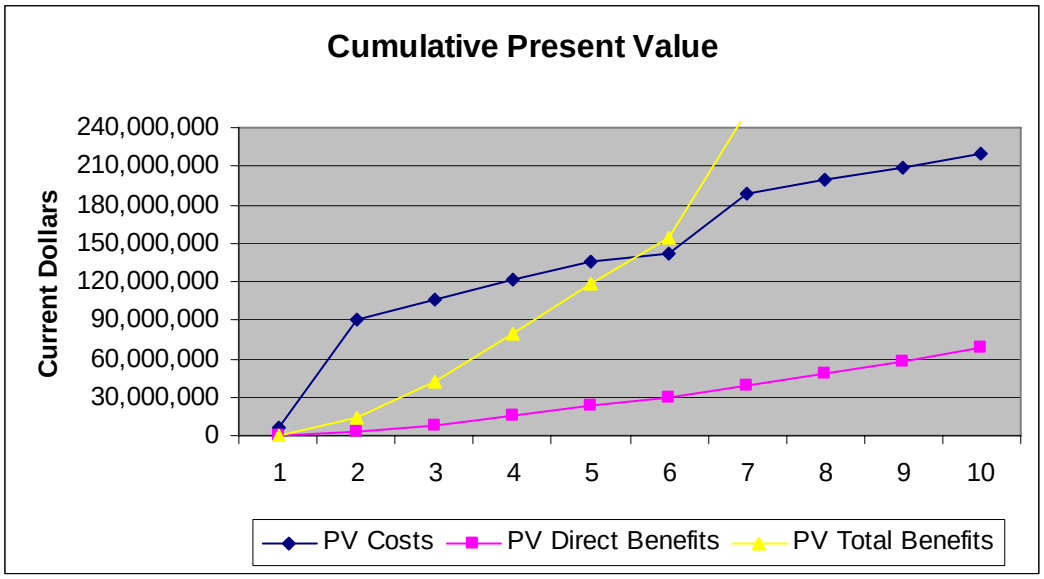

Figure 14. Cumulative Present Value of Cost and Benefits, High Cost Estimates

F. SECONDARY EFFECTS (INDIRECT BENEFITS)

The occurrences of identity theft that are averted by switching the DoD and VA over to a MIN will have spillover effects in productivity.

1. Morale Benefits

Identity theft is a valid concern to Department of Defense and Veterans' Administration employees. The SSN is used and disseminated far too frequently. For instance, every time a member undergoes a Permanent Change of Station, (PCS), copies of the PCS orders and Military ID cards are copied numerous times. The check-out and check-in procedures at the old and new commands require copies of both the PCS orders and ID cards. Each item clearly displays the employee/service member's SSN. The probability of becoming a victim of identity theft would be greatly reduced if the DoD employee (both military and civilian members) were assigned a MIN. These individuals would worry less about ID theft, thus increasing morale.

2. Time Savings

The average amount of time that a victim of identity theft spends, correcting records and dealing with the repercussions, is thirty hours. It is reasonable to assume that the majority of this time is spent during working hours. This lost time on the job is eliminated by switching to a MIN as the primary personal identifier within DoD and the VA.

3. Productivity Gains from Unrestricted Use of Identification Number

The SSN "functionality creep" is due to increased productivity inherent in having a widely accessible, unique personal identifier. As various technology security measures (such as encryption) and policy restrictions which limit the use and display of the SSN have been initiated, the usefulness of the identifier has diminished. Conversion to a MIN would increase productivity recently lost as these various measures to prevent identity theft have been implemented. Since a loss or breach of the MIN will have no value to an identity thief, the identification can be freely used without use restrictions, display restrictions, or technology security measures. Organizations could once again produce rosters with an identification number. Additionally, the MIN itself can hold meaning by assigning the numbers based on some unique sequence. Even researchers, such as the manpower students at the Naval Postgraduate School will be more productive since they would no longer have to deal with encrypted data files and restrictive usage policies.

VI. SUMMARY, AND RECOMMENDATIONS

A. IDENTITY THEFT IN THE U. S. AND U.S. MILITARY

Identity theft in the U.S. has quickly become one of the largest categories of crime in the U.S. and is a tremendous financial strain on the U.S. economy. The widespread and growing reliance on SSNs as an identifier is the primary cause for the increase in identity theft. Identity theft costs the U.S. economy approximately $56.6 billion per year and the average time spent by an identity theft victim seeking resolution increased to about 40 hours in 2006.

The military is more susceptible to identity theft than the U.S. public at large due to the prolific use of SSNs for purposes other than those associated with the Social Security Administration. Use of the SSN as a personal identifier has become so pervasive that nearly every organization within the DoD uses it. It is estimated that the SSN is used in approximately 1000 major computer systems and databases. In reality there are many more, smaller, independent systems that use SSNs that have not even been reported or tracked.

B. COST BENEFIT ANALYSIS OF A CONVERSION TO A MIN

By applying two methods - Y2K as a proxy and the Budget method - to determine the costs associated with converting the DoD and VA from use of the SSN as a personal identifier to use of the MIN, the total costs range from $73,000,000 to $200,500,000.

Using an interpolation of national figures then comparing them to figures provided by both the CBO and Identity Theft: The Aftermath 2004 (IT 2004), annual benefits after conversion range from $222,750,000 to $881,430,000. However, the figure most likely centers around $408,000,000.

The following methodologies were used as part of the analysis:

- Payback period
- Discounted payback period
- Benefit to Cost Ratio (BCR)
- Net present value (NPV)
- Internal rate of return (IRR)
- Probabilistic Net Present Value (PNPV)

SSN to MIN Conversion	Payback period	Discounted Payback period	Benefit to Cost Ratio (BCR)	Net present value (NPV)	Internal rate of return (IRR)	Probabilistic-Net Present Value (PNPV)
Low Cost	3.57 yrs	3.836 yrs	11.34	$701.07M	62%	$804.79 (High Benefit)
High Cost	6.16 yrs	6.662 yrs	3.78	$554.99M	31%	$492.29 (Low Benefit)

Table 21. CBA Summary Table

The results, summarized in Table 21, show the decision maker that, given the assumptions made throughout the cost/benefit analysis, the following exist:

- The Payback period figures show that the benefits will begin to exceed the costs somewhere between 3.57 and 6.16 years, and between 3.836 and 6.662 years when the benefits are discounted.
- Every dollar invested in the conversion will return between $3.78 and $11.34 over the ten year period considered.
- The internal rate of return lies in the 31 to 62 percent range.
- The NPV is between $554.99 and $701.07 million, or $492.29 and $804.79 million when risk adjusting probability distributions are applied.

C. RECOMMENDATIONS

It is recommended that further research be undertaken to identify and/or perform the following:

- Viable alternatives and solutions to secure military, civilian and veterans' personal identities.
- The Costs and benefits associated with these alternatives and solutions be reviewed.
- Conduct cost to benefit analysis to derive the same Cost/Benefit metrics found in this work for comparison.

Upon completion all research results should be compiled and provided to the appropriate decision makers. These metrics should provide the tools by which other alternatives can be measured, prioritized, and ranked.

LIST OF REFERENCES

Arkin, William M., "Name, Rank, E-Mail Address?," Retrieved October 14, 2006, from www.washingtonpost.com, 2000.

Bacon, Kenneth H., DoD News Briefing, December 8, 1998.

Bank Secrecy Act, 1970, 31 USC 1051 et seq. Retrieved January 4, 2007, from http://www.uhuh.com/laws/31usc1051.htm#Bank%20Secrecy%20Act.

Baum, Katrina, "Identity Theft, 2004," Bureau of Justice Statistics, April 2006.

Berghel, Hal, "Identity Theft, Social Security Numbers, and the Web," Communications of the ACM, February 2000/Vol. 43, No. 2.

Center for Information Technology, National Institutes of Health, "Cost-Benefit Analysis Guide for NIH IT Projects," 1998.

Cheney, Julia S., "Identity Theft: A pernicious and Costly Fraud," Federal Reserve Bank of Philadelphia, December 2003.

Computer Professionals For Social Responsibility (CPSR, 15 May 2001). Retrieved November 5, 2006, from http://www.cpsr.org/prevsite/cpsr/privacy/ssn/ssn.structure.html.

CPSR, "Computer Professionals for Social Responsibility, Interest of Amicus brief," 1993. Retrieved November 10, 2006, from www.eff.org/Privacy/ID_SSN_fingerprinting/gre idinger.brief.

Department of Defense Authorization Act (P.L. 97-86), "Report to the Chairman, Subcommittee on Military Readiness, Committee on National Security, House of Representatives," March 1997.

Department of Defense News Release, "Defense Issues Final Status Report on Y2K Preparations," December 16, 1999.

Electronic Privacy Information Center, "Social Security Numbers," January 17, 2006.
Electronic Privacy Information Center, "Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, before the Subcommittee on Social Security Committee on Ways and Means, U.S. House of Representatives." Retrieved November 12, 2006, from www.epic.org.

Flaherty, David H., "Protecting Privacy in Surveillance Societies," Chapel Hill: University of North Carolina Press, 1989.

Garamone, Jim, "Y2K Problem Will Be Nuisance, Not Crisis." American Forces Information Service, October 1998.

Garg, Ashish, et al.,., "Quantifying the Financial Impact of IT Security Breaches," Information Management and Computer Security, Volume 11 Number 2, 2003, pp. 74-83.

General Accounting Office, "DOD Business Systems Modernization: Billions Continue to be Invested with Inadequate Management Oversight and Accountability," GAO-04-615, May 2004.

General Accounting Office, "Year 2000 Computing Crisis: An Assessment Guide," GAO/AIMD-10.1.14, September 1997.

General Accounting Office, "Year 2000 Computing Crisis: Cost and Planning Use of Emergency Funds," GAO/AIMD-99-154, April 28, 1999.

HEW report, "Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems," U.S. Department of Health, Education and Welfare, The MIT Press, Cambridge, Massachusetts, 1973.

Lenard, Thomas M. and Rubin, Paul H., "an Economic Analysis of Notification Requirements for Data Security Breaches," Progress on Point, Release 12, 12 July 2005.

Lieberman, Robert J, "Statement of Robert J. Lieberman, Deputy Inspector General, Department of Defense, before the Senate Committee on Budget On Defense Management Issues," Report No. D-2001-050, February 12, 2001.

National Archives, National Personnel Records Center, St. Louis. Retrieved December 11, 2006, from www.archives.gov/st-louis/military-personnel/social-security-numbers.html.

Newman, Graeme R. and McNally, Megan M. "Identity Theft Literature Review," U.S. DOJ Doc No. 210459, July 2005.

Office of Management and Budget, "FY 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002," March 1, 2006.

Pletcher, Dale, "Identity Theft: The Aftermath 2003, A Comprehensive Study – to Understand the Impacts of Identity Theft on Known Victims as well as Recommendations for Reform," Identity Theft Resource Center, September 2003.

Privacy Act of 1974, "House Report 93-1416: House Committee on Government Operations. *Privacy Act of 1974,"* 93rd Congress, 2d Session, 1974.

Privacy Act of 1974, 5 U.S.C. § 552a, As Amended. Retrieved February 20, 2007, from http://www.usdoj.gov/oip/privstat.htm.

Read, Cederic, Scheuermann, Hans-Dieter and the my SAP Financials Team, "The CFO as Business Integrator," Published by John Wiley and Sons Ltd., The Atrium, Southern Gate, Chichester, West Sussex, England, 2003.

Roosevelt, Franklin D., "Executive Order 9397, Numbering System For Federal Accounts Relating To Individual Persons," 8 Federal Register 16095, November 1943. Retrieved February 18, 2007 from http://www.dod.mil/privacy/pdfdocs/EO_9397.pdf.

Rubina, Johannes, et al.,. "2006 Identity Fraud Survey Report," Javelin Strategy and Research for the B.B.B., January 2006.

Shim, Jae K. and Siegel, Joel G., and Sons, Inc. "The Vest Pocket CFO," second edition, John Wiley and Sons, Inc., Hoboken, New Jersey, 2005.

Smith, Robert Ellis, "Social Security Numbers: Uses and Abuses," ISBN 0-930072-18-9, Privacy Journal, 2002.

Social Security Administration Claims Manual. Retrieved December 15, 2006, from www.ssa.gov.

Social Security Online. Retrieved January 6, 2007, from www.socialsecurity.gov.

Social Security Online, History. Retrieved January 6, 2007, from http://www.ssa.gov/history/ssn/ssnchron.html.

Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations, "The Computer and the Invasion of Privacy: Hearings before the Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations," 89th Cong., 2d Session, 1966.

Spencer, Michael, "1992 And All That: Civil Liberties in the Balance," Privacy Laws and Business, February 1989.

Subcommittee on Social Security of the House Committee on Ways and Means, "Use of Social Security Number as a National Identifier: Hearings before the Subcommittee on Social Security of the House Committee on Ways and Means," 102d Cong., 1st Session, 1991.

Synovate, Prepared for Federal Trade Commission, "Identity Theft Survey Report," September 2003.

Syverson, Paul, "The Paradoxical Value of Privacy," Naval Research Laboratory, March 14, 2003.

Tax Reform Act of 1976, Public Law 94-455, sections 1211(a), (b), and (d). Retrieved February 21, 2007, from Social Security Online at http://www.ssa.gov/OP_Home/rulings/oasi/33/SSR79-18-oasi-33.html.

Vietnam Research by Veterans. Retrieved November 21, 2006, from http://vietnamresearch.com/history/milcart.html.

WebTV Addict, "Web Publicity No Joy for Military Officers," Retrieved January 18, 2007 from www.net4tv.com.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Bill Hatch, CDR, USN Ret.
   Naval Postgraduate School
   Monterey, California

4. Bill Gates, PHD
   Naval Postgraduate School
   Monterey, California

5. Steve Mehay, PHD
   Naval Postgraduate School
   Monterey, California

6. Bob Beck, Dean, School of Business and Public Policy
   Naval Postgraduate School
   Monterey, California

7. Mr. Robert J. Carey
   Chief Information Officer
   Department of the Navy
   Millington, Tennessee

8. The Honorable John G. Grimes
   Chief Information Officer
   Department of Defense
   Washington, D.C.

9. Mr. Vincent Lauter
   Defense Data Management Center
   Seaside, California

10. Mr. Wayne Wagner
    Navy Annex
    Arlington, Virginia

11. Ms. Nancy Dolan
Navy Annex
Arlington, Virginia

12. Marine Corps Representative
Naval Postgraduate School
Monterey, California

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

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

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

16. Kent Crawford
Monterey, California