AU/ACSC/STUDENT #2873/2008-09

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

IDENTITY THEFT & PROTECTING SERVICE MEMBER'S SOCIAL SECURITY NUMBERS

By

Todd A. Bean, Major, USAF

A Research Report Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements

Advisor: Lt Col James E. Parco, Ph.D.

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **APR 2009**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Identity Theft and Protecting Service Member’s Social Security Numbers**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Command And Staff College Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

The original document contains color images.

14. ABSTRACT

The Social Security Act of 1935 created social security numbers as a part of the New Deal Social Security Program. They were created to guarantee American workers received the proper proceeds for income rerouted into the social security program and limited purpose of tracking social security benefits. Over time, technology advancements and computers allowed government and business to become more efficient. Laws became more relaxed in reference to the use of social security numbers and agencies began to track, account, and pay each individual based on name and social security number. Organizations began using social security numbers as the primary source of personal identification. Today, your personal identity (name) and social security number is directly linked to your credit. Criminals only need your social security number and address or phone number to steal your identity, ruin your credit, or gain access to financial accounts. With advances in computer technology and expanded use of database resources which store personal information, identity theft has become one of the nation&#8223;s fastest growing crimes. Service members are required to have a military identification card on which the full social security number is prominently displayed. Additionally, almost every personnel or medical transaction begins with providing your social security number to an agent of the government. Service member were required to provide their social security number for activities not related to finance. The common use of the social security number became an efficient means to process any activity for each service member. A creep set in which social security numbers was used as an identification number, and unintentionally exposed service members to the risk of identity theft. During each deployment or permanent change of station service members printed orders contain full social security number and must be distributed and presented to multiple parties throughout the process. The Department of Defense is responsible for providing safeguards and protection of service member&#8223;s identity, to include the social security number. This research paper will investigate these policies and if they protect service members&#8223; social security numbers and personnel information from identity theft. Finally, a summary of recommendations for changes to policies, procedures, and training will be made, if it is required.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **SAR**	18. NUMBER OF PAGES **40**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

DISCLAIMER ii

LIST OF TABLES……………………………………………………………………………iii

ABSTRACT..v

BACKGROUND & HISTORY 7
Social Security Number (Initial Purpose)..7
Military Service Number 9
Identity Theft 12

SECURITY BREACH & THE LAWS 14
Veterans Affairs…………………………………………………………………15
Privacy Act of 1974 18

SAFEGUARDS & PROTECTION ....**Error! Bookmark not defined.**1
Identity Theft Task Force ....**Error! Bookmark not defined.**2
Defense Information Management Human Resource System**Error! Bookmark not defined.**4

CONCLUSION………………………………………………………………………….26

RECOMMENDATION…..……......……………..…………………………………28

APPENDIX A: 33

APPENDIX B: ……………………………………………………………………….35

BIBLIOGRAPHY 36

CITATIONS AND ENDNOTES………………………………………………………39

List of Tables

Table 1: Reports of Data Breaches 2006-2008……………………………………………………25

Abstract

The Social Security Act of 1935 created social security numbers as a part of the New Deal Social Security Program. They were created to guarantee American workers received the proper proceeds for income rerouted into the social security program and limited purpose of tracking social security benefits. Over time, technology advancements and computers allowed government and business to become more efficient. Laws became more relaxed in reference to the use of social security numbers and agencies began to track, account, and pay each individual based on name and social security number. Organizations began using social security numbers as the primary source of personal identification. Today, your personal identity (name) and social security number is directly linked to your credit. Criminals only need your social security number and address or phone number to steal your identity, ruin your credit, or gain access to financial accounts. With advances in computer technology and expanded use of database resources which store personal information, identity theft has become one of the nation's fastest growing crimes.

Service members are required to have a military identification card on which the full social security number is prominently displayed. Additionally, almost every personnel or medical transaction begins with providing your social security number to an agent of the government. Service member were required to provide their social security number for activities not related to finance. The common use of the social security number became an efficient means to process any activity for each service member. A creep set in which social security numbers was used as an identification number, and unintentionally exposed service members to the risk of identity theft. During each deployment or permanent change of station service members printed orders contain full social security number and must be distributed and presented to multiple parties throughout the process.

The Department of Defense is responsible for providing safeguards and protection of service member’s identity, to include the social security number. This research paper will investigate these policies and if they protect service members’ social security numbers and personnel information from identity theft. Finally, a summary of recommendations for changes to policies, procedures, and training will be made, if it is required.

METHODOLOGY

The problem-solution method was used and applied during this research. This method offers the best route to answer this question as it relates to the Department of Defense policy. The problem-solution methodology enables a seamless integration of resource evaluation and research recommendation in a logical manner. In order to answer the research question, a historical review of the social security number must be accomplished. This research paper will investigate if these policies protect service members' social security numbers and personnel information from identity theft.

BACKGROUND & HISTORY

Social Security Number

Social Security Numbers originated in the New Deal Social Security program, which began in 1936. The Social Security Administration assigned the social security numbers whose original intent was to identify separate retirement accounts for millions of citizens ensuring that each person received their proper pension. The numbering scheme was developed to prevent mistaken identities between persons having identical names and to accommodate population growth.

According to the social security number history, the number set is composed of nine numbers, which is assigned based on where one resided upon application for the number. The first three numbers are assigned according to state and are called area numbers. Area numbers are assigned to locations across the United States, increasing from east to west. Predominately, they‘ve been assigned according to state boundaries. Since 1972, this number has related to the applicant home address. Once the initial series of area numbers were exhausted, the assignments were expanded.

The middle two numbers are called group numbers and indicate when the social security number was assigned. The group number is associated with the order social security numbers are issued for a specific region. Prior to 1965 only half the group numbers were used. For an unidentified reason, presumably for security purposes, the social security administration 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 last four numbers are assigned sequentially as a particular area and group number combination, and referred to as the serial number.[1] An illustration of the social security card and a matrix of the social security numbering system are provided in Appendix A.

Within the bounds of the original purpose of the Social Security Number, employers could request this number from employees so payroll deductions for Social Security could be credited to their account. However, it was never intended to be a national identification number. John Newman emphasizes the deliberate limitations the Social Security Administration originally prescribed for Social Security Number in his article “How to Escape the Tyranny of the Social Security Number.” He wrote, “There was so much concern that the Social Security numbers and cards would be turned into national identity documents when the system was created, that all Social Security cards bore a disclaimer on the bottom that said, ‘not for identification’.”[2] This very specific disclaimer remained printed on cards up until the early 1980s. Cards issued since that time have not carried that caveat. “This fear of Social Security numbers being used as identity documents is also why the cards carry only a name on them, and no other identity data, such as birthdates or personal descriptions.”[3] Over time, the use of the social security number has mushroomed. Many companies maintained social security numbers as employee numbers for each employee. The Department of Defense assigned military identification numbers and tracked social security numbers for each service member. As technology grew, database systems developed and companies became more efficient, employers began to track employees by one number: the social security number.

The expanded use of social security numbers for personal identification continued despite concerns from citizens. Notwithstanding, the federal government further compounded the problem. In 1943, President Roosevelt signed Executive Order 9397 requiring federal agencies to use the social security number 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[4]. In 1961, Congress authorized the Internal Revenue Service to use social security numbers as taxpayer identification numbers.

Military Service Number

Originally, Service numbers were issued by the Armed Forces as a means of identifying individual members. These were also known as military serial numbers or, by the Coast Guard, as signal numbers. The Air Force and Army discontinued using service numbers in July of 1969, the Navy and Marine Corps in July of 1972, the Coast Guard on Guard in October of 1974 and social security numbers were used in place of service numbers.[5]

Cross referencing a social security number with a military serial number was difficult because they were entirely unrelated numbers assigned by different government agencies. The military soon became enticed by the benefit of using only one number for the purpose of the identification of its personnel, tracking pay, and medical benefits. The turning point in the Pentagon's decision to transition from military service numbers to social security numbers arose in 1966 after the example of the Veterans Administration. The Veterans Administration began using the social security number for hospital admissions to identify patients, patient records and other accounting purposes. The Pentagon followed suit and began the switch from military serial numbers to the social security number as identification reference numbers for all military personnel.

In 1972, the United States Department of Health, Education, and Welfare produced a report titled "Records, Computers, and the Rights of Citizens." This report recommended that the social security numbers not be used as an identifier. According to the Health, Education and Welfare committee, "the federal government itself has been in the forefront of expanding the use of the social security number"[6]. In addition to legislation, such as Executive Order 9397, authorizing, and even mandating, agencies to use the social security number as a personal identifier, as well as growing use in the private sector, law further expanding its utilization continued to roll off of the congressional presses. The Bank Secrecy Act of 1970, 31 U.S. Code 1051, required banks and other financial institutions to record social security numbers for all their customers.[7] Many institutions required the individual's social security number be displayed on their checks.

From 1936 to 1996, the use of social security number was completely unidentifiable from its original purpose. This number and its widespread application would soon become so interconnected that one could track pay benefits, employment, and credit to an individual. This creep of expanded use and the lack of sensitivity to its ubiquitous use turned the social security number into the unofficial national identification number, which is directly linked to its owner's credit. This gradual change has increasingly exposed citizens and service members to the risk of identity theft.

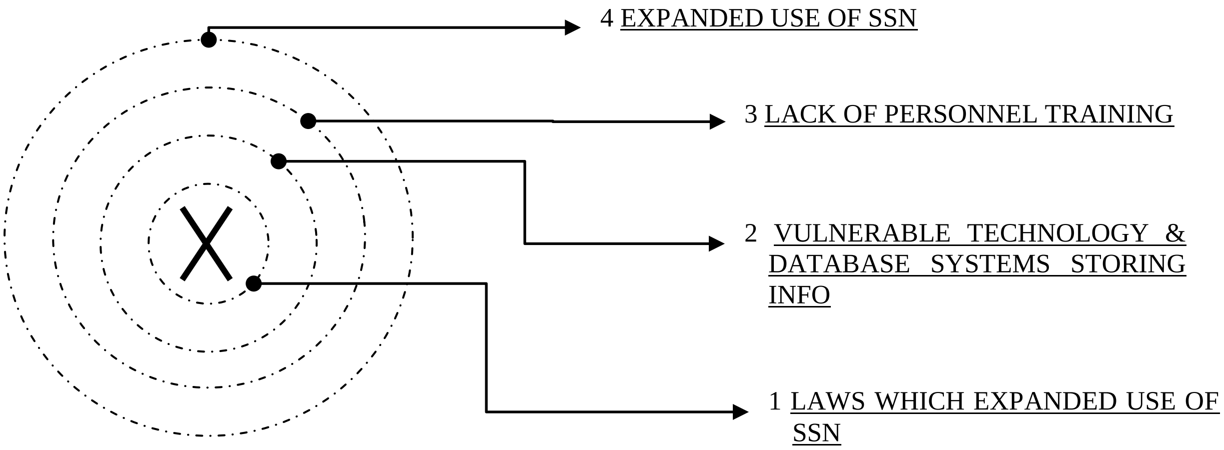
Consider the social security number and personal information as the center of gravity or a bull's eye of a target, which must be protected from identity theft. The layers or rings of the bull's eye illustrate the layers of vulnerability to the center. Laws are the first ring which allows the center or bull's eye (social security number and personal information) to become vulnerable. During this period (1936-1996) laws were passed to enable the increased or expanded use of social security numbers. The Tax Reform Act of 1976 authorized state or local tax, welfare, driver's license and motor vehicle registration office to use the social security number in order to establish identities.[8] In 1981, use of the social security numbers as the primary identifier was proliferated even further with the passage of the Department of Defense Authorization Act (P.L. 97-86) which required the use of social security numbers by the Selective Service System.[9] Laws such as these diminish the first layer of protection and make the target at risk because more widespread use across organizations creates more opportunities for the social security number to be found and linked to an individual's personally identifiable information.

The second layer of vulnerability is characterized by the financial and personnel database systems which store, process, and track employees' pay and benefits. During this period these systems were developed and widely used due to their efficiency and accounting as they related to employee benefits and pay. Additionally, the advancements in technology and the expanded use of personal computers compounded the risk of identity theft via criminals on the internet or "hacking". Companies had mainframes and resident experts, but the technological advances, internet, and personal computers increased efficiencies while exposing vulnerabilities due to the fact that hundreds of thousands of employees' information was being stored in one place.

The third layer of vulnerability is training and education of specialists who process the sensitive data of social security numbers and personal information. This training must include the risks of identity theft and how to properly store, secure, handle, and destroy the personal information of vulnerable customers. During these earlier years, however, personnel were not adequately trained and vigilant because the repercussions of identity theft were not yet prevalent and, therefore did not drive the requirement for rigorous training and handling processes.

The fourth layer of vulnerability is the extent of the use of social security numbers, which, in this case, is extremely widespread and common. If social security numbers are used more frequently for non-financial related matters, the exposure is increased which results in an increased risk to Identity Theft. The below picture depicts the social security number and personal information as the center of gravity for the period of 1936-1996. The dotted circles are fractured rings of vulnerability which have allowed the center of gravity (service member personal information) to become increasingly exposed to risk and ultimately identity theft.

Vulnerability of Personal Information and Social Security Numbers 1936-1996


X
4 EXPANDED USE OF SSN
3 LACK OF PERSONNEL TRAINING
2 VULNERABLE TECHNOLOGY & DATABASE SYSTEMS STORING INFO
1 LAWS WHICH EXPANDED USE OF SSN

What would eventually become prevalent in the minds of consumers and known as “identity theft” dramatically increased. Most dangerous and financially ominous is that each individual social security number is directly linked to identity and credit. This connection provides the basic susceptibility to identity theft.

Identity Theft

"Identity theft occurs when someone uses your personally identifying information, like your name, social security number, or credit card number, without your permission, to commit fraud or other crimes"[10]. Due to the fact that this information is interconnected, a thief only needs one piece, such as a credit card number, to find out more and dig further into one's personal records. The personal information belonging to hundreds of people can be accessed all at once by stealing records contained in large databases. Using this information, criminals can assume an unknowing victim's identity and make fraudulent withdrawals from bank accounts, open credit card accounts and run up vast debts, rent an apartment, or establish a telephone account.

The Federal Trade Commission estimates that as many as nine million Americans have their identities stolen each year.[11] It is quite possible that you or someone you know may have experienced some form of identity theft. This crime and the people behind it take on many guises. An identity theft victim may not find out about the breach until they review their credit report or a credit card statement and notice grave errors or they are contacted by a debt collector.

Identity theft and its aftermath are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. In addition to the financial losses incurred from an identity theft, there are significant costs associated with correcting erroneous information for which the criminal was responsible. Restoring one's reputation in the community is also a major factor after an identity theft. Consumers victimized by identity theft may lose job opportunities, or denied loans for education, housing or automobile purchase as a result of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit. If a service member were to experience any of these problems and they go unresolved, it could lead to judicial punishments, fines, loss of security clearance and, ultimately, discharged from service.

When the social security number was created, not only did its originators not anticipate its use as essentially a universal personal identifier, computers, laptops, massive database systems and the like, were not in their purview. Therefore, the "security measures" integrated into the number proving unsuitable in today's applications, were appropriate for a much more limited use. Minimal research is required to make deriving a valid social security number at random quite easy. These randomly formulated social security numbers belong to actual individuals who soon thereafter become unknowing victims of identity theft as bank accounts, credit cards, loans, etc. are opened in their name. Other common ways an identity thief may access your information include "shoulder surfing" by which a perpetrator watches from a nearby location or watches as you punch in a credit card number or listens as you tell someone the number over the phone. Many criminals engage in dumpster diving to find copies of checks, bank or credit card statements, or preapproved credit cards. The Internet has also become a common place where criminals are able to obtain identifying data. Additionally, social security numbers are sold and purchased by a wide variety of businesses making them even more accessible to thieves.[12] The fact that identity theft has become so prevalent and requires minimal effort on the part of the criminal compounds the military member's concern about their social security number prominently printed on his identification card as well as those of his dependents. Military personnel run the risk of unauthorized persons gaining access to their social security number every time they are required to show their identification card at the gate of a military installation or base exchange/commissary. Essentially every piece of paper containing any record of a military member includes her social security number, not to mention the numerous computer database records in which military personnel are listed. While a civilian can take proactive steps to safeguarding his social security number, a member of the military has no control over the universal use of social security numbers, nor can he opt out of being identified with the number. It has taken a rise in identity theft to result in legislation that works to help protect the consumer. Database breaches in the military have warranted the same type of notice and have encouraged leadership in the Department of Defense to take steps to better protect the social security numbers of military personnel.

SECURITY BREACH & THE LAWS

Since the late 1960's, the Department of Defense has expanded the use of social security. Social Security numbers have been displayed on items such as dog tags, chow line rosters, temporary duty orders, and promotion lists. A more daunting utilization of the social security number in the military is its application in the personnel, house hold goods shipments, financial/pay and medical systems. These systems have created cumulative databases which serve as a repository of service members' social security numbers and personal information. Simple disclosure of the social security number can link a member to databases containing medical, financial, educational, and credit information, all of which are contrary to the number's original intent. Todd Davis, CEO of the identity theft detection firm Lifelock states, "Data thieves and con artists have begun to increasingly target military personnel data, and thieves know [the military's use of social security numbers in everything] is the Achilles' Heel of the system"[13]

Veterans Affairs Security Breach

The Veterans' Affairs have experienced several data system thefts which are listed below. All of these systems contained the personal information of active duty, reserve, and guard members.

- May 3, 2006 (Washington): Laptop, external hard drive with data for 26.5 million retired, active and reserve military personnel
- Aug 3, 2006 (Reston, Va): Computer with data for 38,000 VA patients
- Nov 2, 2006 (New York): Computer with data for 1,600 VA patients
- Feb 2, 2007 (Birmingham, AL): hard drive with data for 2 million VA patients and doctors

The stolen computers and hard drives from these VA offices contained sensitive data for nearly 30 million active and retired service members. That's a significant portion of the more than 100 million personal records reported lost or stolen in the USA since 2006, based on a USA TODAY analysis of data compiled by the Privacy Rights Clearinghouse.[14] The breach in August 2006 put in jeopardy the personal information of nearly 80 percent of the active-duty force. This VA breach, in particular, was a case of routine carelessness with information that should be considered just as sensitive as classified information. Research has shown that it is a normal operating procedure for government employees to take home laptops that contain personal identifying information. "Statistics on financial fraud as a result of these breaches are hard to pin down, but defense officials acknowledge the rising risk. The Defense Department has made it a priority to tighten data-handling agencies and has increased training on theft prevention, department spokesman Maj. Stewart Upton said in an email interview. Because of the heavy reliance on the social security number, 'The cost to remove or replace its use will potentially be very high,' Upton said."[15] Not only is identity theft a financial concern for the individual military member, but there are also issues as they relate to national security and force protection. Stolen information could potentially be used to find out where military personnel live. In light of the fact that there is a global black market for this sort of information, there is worry that the data "could reach foreign governments and their intelligence services or other hostile forces, allowing them to target service members and their families."[16]

As a significant step in the right direction, a phased approach to eliminating the social security number from the military identification card, as will be discussed later, has been put in place by the Department of Defense (DoD), but will take a few years to accomplish. However, identification cards are only one piece in a bigger problem of the DoD's overuse of the social security number. Database security, proper handling of personally identifiable information and the universal use of the social security number along with the centralization of information systems all pose great risk to keeping personal information safe from identity theft. The eternal quest for efficiency through technology can create problems and present risks.

Laws

The government has been long aware of the danger in widespread use of the social security number as a personal identifier which exposes citizens to abuse. In 1973, the United States Department of Health, Education, and Welfare expressed these concerns in its report: Records, Computers, and the Rights of Citizens. According to the Health, Education and Welfare committee, "the federal government itself has been in the forefront of expanding the use of the social security number"[17]. The report concluded with a recommendation that social security numbers not be used as a *de facto* universal identifier and its use be "limited to Federal programs that have a specific Federal legislative mandate to use the SSN, and that new legislation be enacted to give an individual the right to refuse to disclose his SSN under all other circumstances. Furthermore, any organization or person required by federal law to obtain and record the SSN of any individual for some federal program purpose must be prohibited from making any other use or disclosure of that number without the individual's informed consent"[18]. Congress's concern with potential abuses due to the government's increasing use of computers to store and retrieve personal data by means of a universal identifier as well as the report published by the Health, Education and Welfare committee became the foundation for the Federal Privacy Act of 1974, which attempted to limit the abuse of the social security number.

The Privacy Act of 1974

The Privacy Act of 1974 stipulated that authorization is required for government agencies that wish to use social security numbers in their databases and requires disclosures to the individual when government agencies request the number. Agencies already using social security numbers as personal identifiers before January 1, 1975 were allowed to continue using it. This law also requires agencies to follow "fair information practices" when gathering and handling personal data and places restrictions on how agencies can share and individual's data with other people and agencies.[19]

The law also gives individuals the right to request and review any record pertaining to them and to find out if those records have been disclosed. If an agency is found by an individual to have violated the provisions in The Privacy Act of 1974, it can be sued by that individual. The Act is limited, however, because it allows for many exclusions and room for loopholes. It only applies to the records of every individual held by certain federal agencies. Therefore, the records held by courts, executive components or non-agency government entities are not subject to the provisions of the Privacy Act. Additionally, state and local governments are not covered by the Privacy Act. Law enforcement agencies may also omit themselves from the Act's rules and there exists a "routine use" clause in the Act by which many agencies have circumvented its provisions. Military departments are covered by the Act[20].

The Department of Defense has laid out its enforcement of the Privacy Act through a series of directives, regulations, and policy memos under the direction of the Office of Management and Budget. The most recent regulatory document, DoD Directive 5400.11 "DoD Privacy Program" was issued in May 2007. These rules set forth by the Department of Defense set guidelines for collecting, safeguarding, maintaining, using, accessing, amending and disseminating personal information kept in systems of records to comply with the Privacy Act.

Further steps made by the government to protect the social security number come in the form of another piece of legislation proposed by the Committee on Ways and Means called The Social Security Number Privacy and Identity Theft Prevention Act of 2007. Leading up to this act, many hearings in front of the Committee on Ways and Means revealed continued concern will go far in remedying these vulnerabilities. The legislation will reduce the widespread availability of social security numbers by prohibiting government and businesses from displaying social security numbers on the Internet, on checks, on employee identification or benefit cars, on student identification cards, on patient cards, including Medicare cards, and on any other card used to access goods, services or benefits. In addition, this bill imposes new obligations on business and government to safeguard the social security numbers left in their care. Appropriately, the legislation leaves in place stronger state laws protecting social security number privacy and leaves open future opportunities for states to enhance privacy protections[21].

When the GAO was commissioned to investigate the laws in place to protect personally identifiable information, they reported in GAO-08-343 that there exist several other laws that serve to guard individuals from identity theft. The E-Government Act of 2002 provides regulatory and privacy requirements in order to improve the efficiency and effectiveness in the way government information is handled in the electronic arena such as in web-based Internet applications or other information technology. The E-Government Act accomplishes this through privacy impact assessments to analyze "how personal information is collected, stored, shared, and managed in a federal system."[22] This analysis ensures the way information handled is in compliance with legal, regulatory, and policy requirements. This law also established a new agency within the Office of Management and Budget called the Office of Electronic Government. The security of information held by the federal government is addressed by the Federal Information Security Management Act of 2002 (FISMA). FISMA requires agencies to develop and implement risk-based programs that provide security for personally identifiable information and the systems in which it is stored. This law "requires an agency, among other things, to categorize its information and systems according to the potential impact to the agency should the information be jeopardized."[23]

Agency-specific laws have also passed to add an additional layer of protection of personally identifiable information. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 require the Secretary of Health and Human Services to adopt standards for the electronic exchange, privacy, and security of health information. HIPAA protects the privacy of individually identifiable health information, and is enforced by the Office for Civil Rights. The

Department of Veterans Affairs (VA) is held legally responsible for protecting personal information via the Veterans Benefits, Healthcare and Information Technology Act of 2006. Under this law the VA must follow security requirements laid out in the law and must have established procedures for detecting and immediately reporting any security breaches. Congress must be notified of significant security incidents and the VA must provide credit protection services to anyone whose information had been compromised.

It is clear that the federal government is taking steps to ensure good stewardship of personally identifiable information on paper, but in a General Accounting Office after-inspection report to Congress titled, "Protecting Personally Identifiable Information," the following recommendations:

> These security breaches highlight the importance of federal agencies having effective information security controls in place to protect personally identifiable information—that is, information that can be used to locate or identify and individual, such as names, aliases, social security numbers, biometric records, and other personal information that is linked or linkable to an individual. Loss of such information may lead to identity theft or other fraudulent use of the information, resulting in substantial harm, embarrassment, and inconvenience to individuals.[24]

Previously, the General Accounting Office requested the Department of Defense Inspector General report on controls over the use and protection of social security numbers within the Department of Defense. The resulting report, D-2003-066, "revealed that three of the agencies made disclosures of personally identifiable information for legal purposes; however, their Privacy Programs needed improvements in policy administration, oversight, periodic reviews, physical security, and training. After notification of finding officials at the Department of Defense agencies (Defense Manpower Data Center, Army & Air Force Exchange Service, Defense Security Service) concurred and agreed to take the necessary remedial actions to mitigate the risk of improper disclosure of Social Security numbers."[25] If there is one thing that can be learned from a data breach such as that in the VA as well as the GAO report, it is that individuals must be vigilant in protecting their information. Knowing the laws that are put in place in order to recognize violations is a key part of keeping that layer of protection intact.

SAFEGUARDS & PROTECTION

The growth of technology and increased use of computers and database systems that house personal information has simplified many processes and has decreased waste and redundancy. However, defragmentation and centralization of information has led to the increased risk to individual privacy. Ease of use and technology allowed for efficiency but it also exposed a significant risk. The large and essentially universal use of social security numbers within the Department of Defense has exposed or service members to risk of financial harm. Fortunately, the reaction to these vulnerabilities and this self-induced predicament has the attention over our congressional leaders as well as the Executive Branch. In light of the attack on personal information and social security numbers by criminal elements, initiatives have been established to counter the illegal activities. Some of these initiatives include the President's Identity Theft Task Force for all citizens and few Department of Defense reactive tools to protect and support service members.

Identity Theft Task Force

In 2005, President George W. Bush addressed this new information era and the fight against identity theft by issuing an executive order establishing the Identity Theft Task Force. The executive order charged fifteen federal agencies to put forth a plan to implement a comprehensive national strategy to combat more effectively this widespread and destructive crime, which afflicts millions of Americans each year. In April of 2007, the Task Force submitted its Strategic Plan to the President. The plan was focused in four key areas with 31 recommendations ranging from small, incremental steps to broad policy changes (including legislative proposals to fill in the gaps in current laws). The four areas on which the Task Force focused included:

-Increased data protection to keep consumer data out of the hands of criminals

-Eliminate the misuse of data, which will make it harder for criminals to access and exploit personal information.

-Make victim detection and recovery from identity theft easier through victim assistance.

-Improve the effectiveness of criminal prosecutions and punishment to increase deterrence of identity theft.[26]

The military can be viewed as a reflection or microcosm of the larger American society. If identity theft is occurring against civilians, there is identity theft within the military. Military members are not necessarily more protected than civilians from identity theft. There are many cases in which the military will benchmark and mirror solutions from corporate America. Just as the President provided strategic guidance in tackling identity theft throughout the private sector, Congress has imposed legislation within the Department of Defense to reduce the widespread use of social security numbers.

Recognizing that social security numbers prominently displayed on military identification cards is a significant leak point for the military member, The Department of Defense has taken the next step to phase out full social security numbers on all ID cards. As old cards expire, new cards will be replaced with just the last four digits of the social security number in lieu of the full number being printed on the card. Combining the last four digits of the social security number with other identifying information is sufficient to verify one's identity and is common practice in the private sector. The Department of Defense has described this action as a part of a larger phased approach to improving the protection of service members' personal information. In addition to the elimination of the full social security number the DoD has improved security over military databases and removed social security numbers from Tricare health system ID cards.

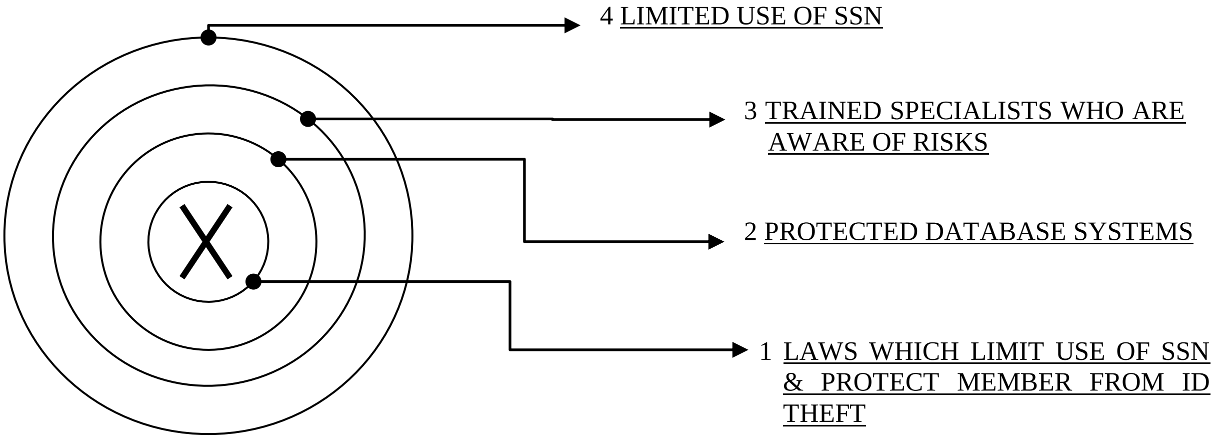
Defense Integrated Military Human Resources System (DIMHRS)

Implementing the new ID card with the truncated social security number is key in the transition to a Department of Defense joint personnel data base system. The Congressionally-mandated Defense Integrated Military Human Resources System (DIMHRS) is a "comprehensive, web-base solution that will integrate many existing personnel and pay processes into one self-service system."[27] This new system will support the military's Total Force across all services and components (Active or Regular Component, Reserve, and National Guard). This fundamental change in human resources support represents the Department of Defense's commitment to modernizing business practices and delivering timely and accurate pay and benefits. DIHMRS solves the problem of disconnect between personnel and finance computer systems, which in the past could not communicate with each other. This upgrade creates the "largest, integrated human resource information management system in the world."[28]

In the event someone becomes victim to identity theft or fraud, the Federal Trade Commission provides tools to help service members and consumers. Military Sentinel is a web-based tool put in place by the Federal Trade Commission and the Department of Defense to identify and target consumer protection issues that affect members of the United States Armed Forces and their families. Military Sentinel allows members of the Untied States Armed Forces to enter consumer complaints directly into a database that is immediately accessible by over 500 law enforcement organizations throughout the United States, Canada, and Australia. This tool will help prosecute criminals and assist those who have been exposed identity theft.[29]

Due to new initiatives and laws, the period of 1997 to 2009 has revealed a slightly fortified picture of protecting the service member's social security number and personal information from identity theft. This improved protection can be further illustrated via the center of gravity where the bulls-eye remains the social security number and personal information. The first ring of protection is reinforced with new laws which limit the use of social security number and distribution of personal information. The second ring includes improved database systems, which store personal information and financial documents such as the new Defense Information Management Resource System (DIMRS). These database systems include firewall protection, encryption codes, and restricted access to only authorized individuals. The third ring of protection entails training of employees and specialists who administer and use personnel, medical and financial data base systems. The guidance for this training is covered in the Department of Defense Regulation 5400. This also includes those who process documents which include social security numbers and personal information. The fourth and outermost ring of protection is provided through the reduction of requiring social security numbers for non personnel, medical or financial purposes. If the social security number is required, use of the last four digits plus full name can suffice in most cases. A memorandum from the Under Secretary of Defense dated 28 Jan 2009 states, "The office of Management and Budget has issued requirements for the protection of Personally Identifiable Information. These requirements include direction to all Federal Agencies to eliminate, when feasible, their use of the Social Security Numbers. The Department has developed the DoD SSN Reduction Plan, part of which will eliminate the use of visible SSNs on identification cards."[30] The solid rings along with the slight change in terms depict a still vulnerable center of gravity with more protection.

Protection of Personal Information and Social Security Numbers 1997-2009


4 LIMITED USE OF SSN
3 TRAINED SPECIALISTS WHO ARE AWARE OF RISKS
2 PROTECTED DATABASE SYSTEMS
1 LAWS WHICH LIMIT USE OF SSN & PROTECT MEMBER FROM ID THEFT
X

CONCLUSION

The Department of Defense has recognized and reacted to the risk of identity theft by committing to reducing the exposure of service member's social security numbers and increased protection of personal information.

Identity Theft is a risk faced by both civilian citizens and service members. Terrorism is also a risk faced by civilian citizens and service members. Acts of terrorism expose vulnerabilities to which the DoD reacts by changing force protection policies and procedures. In the same way, identity theft has revealed the lack of safeguards in place to protect service members' identities. The wide use of social security numbers compounded by the prevalence of database systems that house personal information culminate in vulnerabilities which expose everyone to identity theft. Identity theft cannot be eliminated in its current context of the widespread use of the social security number, but it can be mitigated and the risk significantly reduced. As service members take the oath to service and prepare to make the ultimate sacrifice, it is not unreasonable to expect the Department of Defense and service components to protect social security numbers and prevent identity theft, particularly if government personnel policies, procedures and data base systems increase the risk of identity theft. Unfortunately criminal activity has forced changes in the handling of social security numbers and personal information. In-depth training on how to handle social security numbers, improvements in database security/systems and increased awareness of identity theft has helped to change policy and educate service members. Notable improvement was noted in the Identity Theft Resource Center tabulated data base system breach totals from 2006 to 2008. From 2006 to 2008 government database breaches decreased by 50%.

Table 1: Reports of Data Breaches 2006-2008

	2008 - # of Breaches	*2008*	*2007*	*2006*
Business	240	36.6%	28.9%	21%
Educational	131	20%	24.8%	28%
Government/Military	110	16.8%	24.6%	30%
Health/Medical	97	14.8%	14.6%	13%
Financial/Credit	78	11.9%	7%	8%

Source: Identity Theft Resource Center

Although the improvements capture the progress made in preventing database breaches, this is one of many needed steps to protect service members' social security numbers and personally identifiable information. The Department of Defense's reaction to these vulnerabilities was certainly the force behind better protection, but much needed proactive measures will strengthen weak areas and halt the next or new vulnerable area.

A desire for ease and efficiency drove the Department of Defense to use the social security number in a variety of applications, which ultimately exposed service members to identity theft. The use and application of any advanced technological system which improved efficiency should be tested against potential risks or undesired effects. Process improvements along with technology system advancements can produce efficiency but increased risk, and ultimately reduced the effectiveness of protecting service members' social security numbers and personal information. This unintended consequence can be mitigated if system efficiency improvements is continuously balanced and/or measured against undesired effects or vulnerabilities. This will require leaders to more closely consider efficiency and effects when applying new process improvements and technological solutions.

RECOMMENDATIONS

The Department of Defense policy, procedures, and strategic guidance is adequate in providing the direction of protecting service member personal information and social security numbers. The DoD has reacted by correcting the flawed policies and lack of procedures, which expose service members to the risk of identity theft. Additionally, Congress has corrected some of the laws which exacerbated the problem associated with securing personal information and social security numbers. The recommendations in this section are center around the tactical execution of the policy, procedures and guidance. There is a delay between establishing strategic guidance and tactical execution at the base level. The Social Security Number Reduction plan is sound guidance, but there is a delayed implementation of the plan and slow marketing of how it applies to each service member. These recommendations are meant to help bridge this delay from strategic guidance to tactical execution and are directed at three areas: future data base systems, training, and educating service members. The education includes awareness of vulnerabilities, risks, and as well as resources which may help if they encounter identity theft.

The first recommendation is related to future database systems. The Defense Integrated Military Human Resource System is definitely a positive step in improving the efficiency of the Department of Defense personnel database system. The system implementation also includes new military identification cards with the truncated social security number, but it has challenges. How will DIMHRS interface with the current legacy systems of personnel and finance for a smooth data transfer between each service component? Since the Army is the lead component for DIMHRS will the other services have the ability to successfully apply transition lessons before a system crash or security breach? Finally, what are the reactive and proactive countermeasures within the system to prevent data base breach/hackers and can it successfully defend against new and innovative network attacks? A quote worth citing twice is: "DIMHRS will be the largest, fully integrated human resources information management system in the world."[31] This web based system will integrate all pay and personnel services. On the surface this appears efficient and convenient but what are the risks? This is essentially all the information one would ever need to know in one place. The system would demand a robust infrastructure with a reliable mainframe to reduce system single point of failure and security risk from cyber attacks. The efficiency of the system must be continuously measured against its effectiveness to secure personal information and prevent security breach or identity theft.

Fortunately, DIMHRS has had an aggressive Enterprise and Risk Assessment in November of 2008, at the direction of the Deputy Secretary of Defense. "The outcome highlighted a number of governance, program management, and requirements-related challenges associated with an effort as large and complex as DIMHRS." [32] A source within the MAJCOM A1communtity, who prefers to remain anonymous, expects the program and system implementation will slip pass fiscal year 2011. Although this is a delay in implementation, it is welcomed considering all the concerns and dynamic challenges of implementing such a revolutionary integrated database system.

Although training of individuals, employees, and contractors who work with service members' social security numbers and personnel information is covered in Department of Defense Regulation 5400.11-R, enforcement of this training must always remain as a priority and adapt to system security threats and vulnerabilities. Everyone must understand the repercussions of exposing personnel to fraud or those with criminal intentions. People are aware of identity theft, but tend to have an indifferent attitude about the risks unless they have been exposed to identity theft or personally know someone who has become a victim. This is similar to when a tire company selling flawed SUV tires and we have numerous SUV rollover accidents across the nation. The news may advertise the safety risk and the tire company may send out a recall of the tires, but some people will continue to drive on the flawed tires (and remain at risk) because the accident has not happened to them. The brunt of the responsibility falls on the specialist who is processing, storing, or transporting the sensitive personal information and the service member. Each member needs to be aware of the risk and vulnerabilities, and determine if the use of the social security number is absolutely necessary by asking questions about how or why is the social security number required for the particular transaction.

Marketing to and educating service members about the various risks and exposures identity theft should be significantly increased. A basic trifold or flyer can cover the definition, risks, preventive measures and what to do if exposed to identity theft. This could be part of the Defense Integrated Military Human Resources website once it is employed in the field. Otherwise it should be included on the current website pages of each service component and veteran affairs website. The trifold should also be produced/printed out and made available at each personnel center, financial offices, medical facilities, and veterans administration facilities. The trifold should be on the website and in the available for distribution at any location that requires social security number or personal information in order to make any transaction. An excellent example of this type of trifold exists and can be found on the Federal Trade Commission website. It is titled, "Military Personnel & Families Fighting Back Against Identity Theft, and can be found in Appendix B. If this is important enough for our government to create laws and the President to create a Task Force, it is important enough to properly market and educate and protect our service members.

Areas of Future Research

The areas of future research related to this topic would some key areas. The current system has always reacted to the vulnerabilities based off of failures or some service members dealing with identity theft as a result of exposure by the government. A more effective solution could involve proactive steps to prevent identity theft and the risk. Perhaps DIHMRS is this proactive solution, but a follow-up action would monitor, inspect, and evaluate DIMHRS once it is implemented and include the back-up system which supports the DIHMRS infrastructure. DIHMRS is a monolithic system which affords significant efficiency, but will it yield an undesirable effect and increase the risk of exposing service member's personal information or social security numbers to cyber crimenals? Accountability is another area which could decrease the gap between strategic guidance and tactical execution. The data is readily available in relation to the risk of identity theft and improvements in reducing the risk, but it is all governed by law. A Commander or Director must ensure the sensitive information is properly secured, stored, and handled. What happens to those units or organizations which fail to comply with the laws, regulation or guidance? A final area to consider is the results of Higher Head Quarter inspections for finance and personnel units, in relation to protection of service members' personal information and social security numbers. The government has a responsibility to protect the service members' social security number and prevent identity theft, just as the service member has the responsibility to support and defend.

Appendix A

SOCIAL SECURITY NUMBER ALLOCATIONS

Since 1973, social security numbers have been issued a central office. The first three (3) digits of a person's social security number are determined by the ZIP Code of the mailing address shown on the application for a social security number. Prior to 1973, field offices assigned social security numbers.

The chart below shows the first 3 digits of the social security numbers assigned throughout the United States and its possessions. See "Note" at bottom of page.

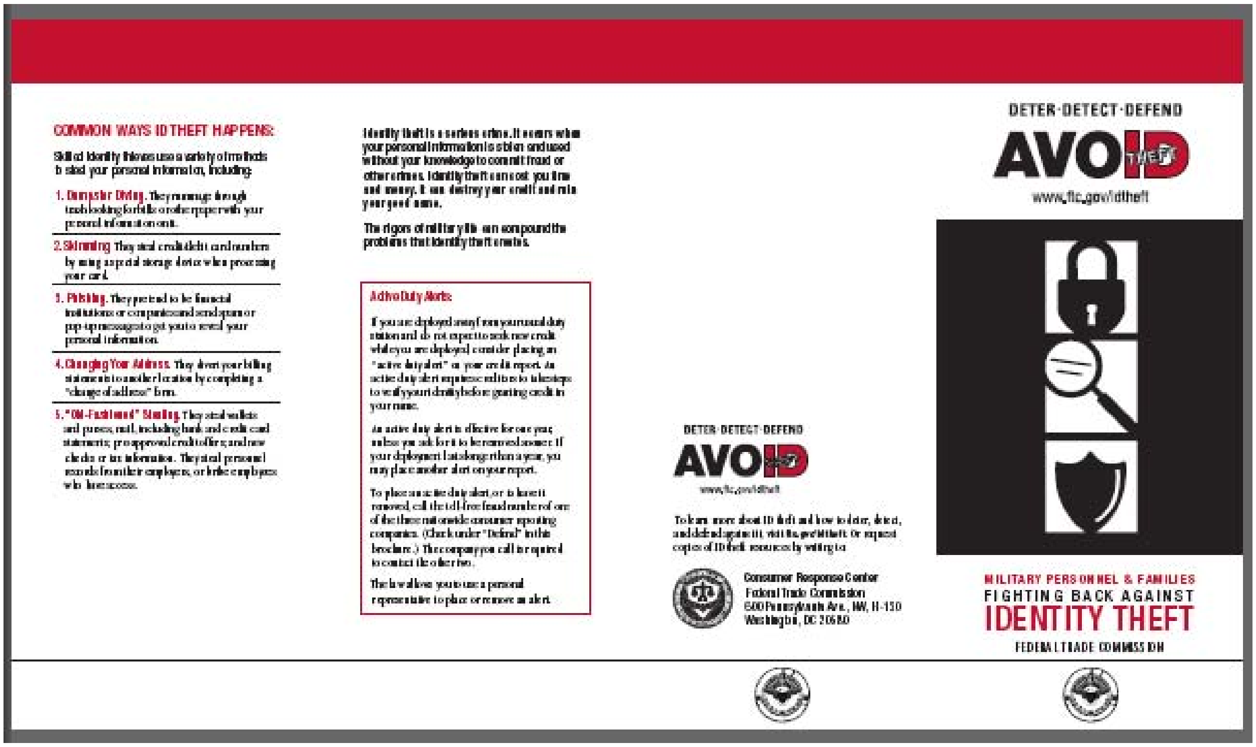
001-003	New Hampshire	261-267	Florida	449-467	Texas	530	Nevada
004-007	Maine	589-595		627-645		680	
008-009	Vermont	766-772		468-477	Minnesota	531-539	Washington
010-034	Massachusetts	268-302	Ohio	478-485	Iowa	540-544	Oregon
035-039	Rhode Island	303-317	Indiana	486-500	Missouri	545-573	California
040-049	Connecticut	318-361	Illinois	501-502	North Dakota	602-626	
050-134	New York	362-386	Michigan	503-504	South Dakota	574	Alaska
135-158	New Jersey	387-399	Wisconsin	505-508	Nebraska	575-576	Hawaii
159-211	Pennsylvania	400-407	Kentucky	509-515	Kansas	750	

212-220	Maryland	408-415	Tennessee	516-517	Montana	751	
221-222	Delaware	756-763		518-519	Idaho	577-579	District of Columbia
223-231	Virginia	416-424	Alabama	520	Wyoming	580	Virgin Islands
691-699		425-428	Mississippi	521-524	Colorado	580-584	Puerto Rico
232-236	West Virginia	587		650-653		596-599	
232	North Carolina	588		525,585	New Mexico	586	Guam
237-246		752-755		648-649		586	American Samoa
681-690		429-432	Arkansas	526-527	Arizona	586	Philippine Islands
247-251	South Carolina	676-679		600-601		700-728	Railroad Board**
654-658		433-439	Louisiana	764-765		729-733	Enumeration at Entry
252-260	Georgia	659-665		528-529	Utah		
667-675		440-448	Oklahoma	646-647			

NOTE: The same area, when shown more than once, means that certain numbers have been transferred from one State to another, or that an area has been divided for use among certain geographic locations.
Any number beginning with 000 will NEVER be a valid SSN.

** 700-728 Issuance of these numbers to railroad employees was discontinued July 1, 1963.

Appendix B



COMMON WAYS ID THEFT HAPPENS:

Skilled identity thieves use a variety of methods to steal your personal information, including:

1. Dumpster Diving. They rummage through trash looking for bills or other paper with your personal information on it.
2. Skimming. They steal credit/debit card numbers by using a special storage device when processing your card.
3. Phishing. They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. Changing Your Address. They divert your billing statements to another location by completing a "change of address" form.
5. "Old-Fashioned" Stealing. They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personal records from their employers, or bribe employees who have access.

Identity theft is a serious crime. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name.

The rigors of military life can compound the problems that identity theft creates.

Active Duty Alerts:

If you are deployed away from your usual duty station and do not expect to seek new credit while you are deployed, consider placing an "active duty alert" on your credit report. An active duty alert requires creditors to take steps to verify your identity before granting credit in your name.

An active duty alert is effective for one year, unless you ask for it to be removed sooner. If your deployment lasts longer than a year, you may place another alert on your report.

To place an active duty alert, or to have it removed, call the toll-free fraud number of one of the three nationwide consumer reporting companies. (Check under "Defend" in this brochure.) The company you call is required to contact the other two.

The law allows you to use a personal representative to place or remove an alert.

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft

To learn more about ID theft and how to deter, detect, and defend against it, visit ftc.gov/idtheft. Or request copies of ID theft resources by writing to:

Consumer Response Center
Federal Trade Commission
600 Pennsylvania Ave., NW, H-130
Washington, DC 20580

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft

MILITARY PERSONNEL & FAMILIES

FIGHTING BACK AGAINST

IDENTITY THEFT

FEDERAL TRADE COMMISSION

Bibliography

Acohido, Byron, “Military personnel prime targets for ID theft”, USATODAY.com

AVOID (Identity Theft) Deter-Detect-Defend
www.ftc.gov/idtheft

Bank Secrecy Act, 1970, 31 USC 1051 et seq. Retrieved from http://www.uhuh.com/laws/31usc1051.htm/bank/secrecy/act

Defense Integrated Military Human Resources System (DIMHRS)
www.dimhrs.mil

Defense Privacy Office, Department of Defense Privacy Act Implementation
Department of Defense Directive 5400.11
Department of Defense Regulation 5400.11-R
www.defenselink.mil/privacy

Department of Defense 5200.1-R, Information Security Program
Department of Defense 5200.2-R, Personnel Security Program
Department of Defense 5220.22-M, National Industrial Security Manual
Department of Defense 5200.22-R, Industrial Security Regulation

Department of Defense Authorization Act, “Report to the Chairman, Subcommittee on Military Readiness, Committee on National Security, House of Representatives,” March 1997.

Dominguez, Michael L.“Business Practice Changes to Allow the Removal of Social Security Numbers from DoD Identification Cards”, Memo for Secretaries of the Military Departments, January 2009.

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.”www.epic.org.

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, “Information Security: Protecting Personally Identifiable Information,” GAO-08-343, January 2008.

General Accounting Office, “Controls over the use and protection of social security numbers within the Department of Defense,” GAO-2003-066, April 2006.

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.

https://afkm.wpafb.af.mil/AFDIMHRS - AF DIMHRS CoP, Tool Box Note
Deputy Secretary of Defense directed Business Transformation Agency to perform Enterprise Risk Assessment Model review of DIMHRS

Identity theft Resource Center; “Working to resolve identity theft, 2008 data breach totals” www.idtheftcenter.org

Maze, Rick, “Pentagon to Phase out SSNs on ID cards”, 3 Apr 2008. www.armytimes.com.news

Military Sentinel; www.consumer.gov/military

National Archives, National Personnel Records Center, St. Louis. www.archieves.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.
Newman, John Q, “How to escape the Tyranny of the social security number”, www.loompanics.com

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 from http://www.usdoj.gov/oip/privstat.htm.

Roosevelt, Franklin D.,”Executive Order 9397, Numbering System for Federal Accounting Relating to Individual Persons,” 8 Federal Register 16095, November 1943. Retrieved 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 Better Business Bureau., January 2006.

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

Social Security Administration Claims Manual. Retrieve from www.ssa.gov.

Social Security Online. Retrieved from www.socialsecurity.gov.

Social Security History. Retrieved from http://www.ssa.gov/histoy/ssn/ssnchron.html.

Subcommittee on Social Security of the House Committee on Ways and Means, “Use of Social Security Number as a National Identifies: Hearings Before the Subcommittee on Social Security of the House Committee on Ways and Means,”102d Cong., 1st Session, 1991.

Swendiman, Kathleen S., “CRS Report for Congress RL30318: The Social Security Number: Legal Developments Affecting its Collection, Disclosure, and Confidentiality”, February 2008. Retrieved from http://www.fas.org/sgp/crs/misc/RL30318.

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

Tax Reform Act of 1976, Public Law 94-455, sections 1211, retrieved from Social Security online /www.ssa.gov/OP_Home/rulings/oasi/33/SSR79-18-oasi-33.html

Tyson, Ann Scott, “Data theft affected most in military”, Washingtonpost, 7 Jun 2006, www.washingtonpost.com

Notes

[1] www.ssa.gov/history/ssn

[2] Newman, "Escape Tyranny of Social Security Number" p.2

[3] Newman, "Escape Tyranny of Social Security Number" p.2

[4] Roosevelt, "Executive order 9397 Numbering Systems"

[5] http://vietnamresearch.com/history

[6] Subcommittee on Social Security of the House Committee on Ways and Means, "Use of Social Security Number as a National Identifies: Hearings Before the Subcommittee on Social Security of the House Committee on Ways and Means,"102d Cong., p.21

[7] Bank Secrecy Act of 1970

[8] Tax Reform Act of 1976

[9] Swendiman, "CRS Report for Congress: RL30318"

[10] www.ftc.gov

[11] www.ftc.gov/idtheft

[12] www.ftc.gov/idtheft

[13] Acohido, "Military personnel prime targets for ID theft", USATODAY.com

[14] Acohido, "Military personnel prime targets for ID theft", USATODAY.com

[15] Acohido, "Military personnel prime targets for ID theft", USATODAY.com

[16] Tyson, "Data theft affected most in military", Washingtonpost, 7 Jun 2006, www.washingtonpost.com

[17] 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, p.121

[18] 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, p.121

[19] http://www.usdoj.gov/oip/privstrat.htm.

[20] Privacy Act of 1974

[21] The Social Security Number Privacy and Identity Theft Prevention Act of 2007

[22] General Accounting Office, "Information Security: Protecting Personally Identifiable Information, p.9

[23] General Accounting Office, "Information Security: Protecting Personally Identifiable Information, p.9

[24] General Accounting Office, "Information Security: Protecting Personally Identifiable Information,

[25] General Accounting Office, "Controls over the use and protection of social security numbers within the Department of Defense,"p.5-6

[26] www.ftc.gov/opa/2007/04/idtheft.shtm

[27] www.dihmrs.mil

Notes

[28] www.dihmrs.mil
[29] www.consumer.gov/military
[30] Dominguez, "Business Practice Changes to Allow removal of SSN"
[31] www.dihmrs.mil

[32] https://afkm.wpafb.af.mil/AFDIMHRS