



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

Does the Government Adequately Protect Personal Citizenry Information?

Clayton Holland

Missing Link Security

**This white paper is made available by Missing Link Security...We find
your weakest links.**



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

Abstract

The federal government of the United States collects, processes, stores and transmits copious amounts of sensitive, personal information associated with its constituency. Grievous breaches in control of this information continue to be reported in the media begging the public to wonder whether their personal data is safe in the hands of the Government. Legislation, national policy and associated doctrine governing federal control of the citizenry's personal information continues to develop and mature, today reaching every corner of the federal government and every information system that processes, stores or transmits Personally Identifiable Information (PII).

In depth audits of the government's control of PII shows continued control improvement and that privacy protection is becoming recognized as a cornerstone of the government's obligation to the public. Senior public officials are establishing organizational PII protection policies and employee training programs yet breaches continue at the least rungs of management's ladder. PII protection practices and a creed of adherence to privacy policy is slowly trickling down to information system administrators, mail clerks, property managers and sub-contractors, but is the slowing flood of sensitive, personal information from appropriate federal control sufficient? The White House Office of Management and Budget reports to Congress that it is, leaving the

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

public to wonder whether federal agency Inspector General Auditors receive phone calls from their banks asking to confirm suspicious charges to their personal credit accounts.

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

Does the Government Adequately Protect Personal Citizenry Information?

The government leverages enormous amounts of its constituency's personal information for many of its principal functions but how safe is this information from abuse and are the controls in place to safeguard the information working? The Internal Revenue Service collects, relies upon and processes social security numbers, full names, dates of birth, addresses, financial details, dependent information and many other facts concerning taxpayers in the performance of its mission. Consider government social programs that provide medical services to their constituencies; such programs must by definition of their mission collect names, addresses, telephone numbers, sex, age, income information, medical history, medical providers' information and many more details of the citizenry's personal lives (Harper, 2004).

What makes the collection and use of personal information by the government exceptionally significant is the opportunity for abuse available to the government in ways that are not shared with private organizations. Should the government abuse this information, the public has little recourse to prevent and recover damages that may result. Perversely, this may be especially true in the government's efforts to protect its constituency through law enforcement. State, local and federal law enforcement collects information about its constituency's travel, associations, statements, (including internet postings), possessions, purchases and even thoughts expressed and inferred. The people

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

rely upon government to leverage personal information to investigate both crime and potential crime to safeguard the innocent – but the public also has a right to privacy. Weighing privacy rights on one side of the fulcrum against empowering government with the information it needs to serve the public on the other side is a fiercely contested balancing act.

Breaches

The Identity Theft Resource Center reports that government security breaches involving compromise of personal information has slightly decreased since earlier years, but remains at disturbing levels (ITRC, 2009). In the first 10 months of 2009, 74 individual breaches were reported involving the compromise of 79,141,050 records. Some of the most noteworthy recent breaches include exposure of up to 1,000 personal records of Katrina hurricane victim's personal information records when a FEMA subcontractor accidentally mailed aid applications to the wrong parties. FEMA compounded their mismanagement of personally identifiable information by posting 16,857 names, Social Security and telephone numbers along with other private information of evacuated Katrina victims to 2 web sites.

The National Archives lost a hard drive containing more than 100,000 names, Social Security numbers and home addresses of people who visited or worked at the White House. The hard drive also contained White House Secret Service security

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

procedures, event logs, social gathering logs, political records and other information from the Clinton administration. The naval Hospital Pensacola reported the loss of a laptop computer containing 38,000 names, Social Security numbers and dates of birth of its pharmacy customers. An official of the New York Police Department pension fund has been charged with stealing backup tapes from a Staten Island storage facility containing names, Social Security numbers and direct deposit information including bank account numbers of 80,000 NYPD pensioners. And as of October, 2009, the National Archives Inspector General was investigating the loss of 76,000,000 personal records of military veterans including Social Security numbers that occurred when a defective hard drive containing data from an Oracle database was returned to a vendor with this sensitive information still on it.

These are just a few examples of compromise by the government of citizenry personal information. There are many more and they continue to happen - but how? What controls how the government safeguards personal information?

Controls

The Fourth Amendment to the Constitution of the United States reads, “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

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

place to be searched, and the persons or things to be seized.” The “right of the people to be secure in their persons” is widely recognized as inferring a constitutional right of citizenry to privacy. In the Supreme Court Case of *Olmstead v. The United States* (1928), Justice Brandeis' opinion included the assertion that that the language of the Constitution guarantees everyone basic rights to liberty and privacy which are inherent in, even if not expressed by, the actual words of the Constitution (Cline, 2009).

The Privacy Act of 1974, 5 U.S.C. 552a, protects personally identifiable information pertaining to individuals held by federal agencies by prohibiting the disclosure of records contained in a federal (or federal contractor) “system of records” without the written consent of the individual to whom the record pertains. The Act includes some exceptions. In addition disclosures explicitly permitted in the statute, the Privacy Act also permits “routine use” disclosures if the disclosure is consistent with the purpose for which the information was collected and notice of the disclosure is published in the Federal Register. The Act is enforced by civil action, and by criminal penalty. An agency official (or contractor) who willfully discloses information in violation of the Privacy Act may be found guilty of a misdemeanor and may be fined up to \$5000 (Zalud, 2009).

The Freedom of Information Act (FOIA), 5 U.S.C. 552, allows the public to receive copies of records in the possession of the agencies of the U.S. Government.. In

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

general, documents must be released to a person requesting the document, unless the document falls into one of the release exemptions set forth in FOIA. Disclosure of personal data is exempt from FOIA. Personal data is defined by the Act as data which relates to a living person who may be identified from the data, or from the data along with other information which may be in the possession of the data controller. Access to one's own personal data held by a federal agency is also exempt from FOIA; such requests are handled through other channels (Harper, 2004).

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.) includes a requirement for the Information and Regulatory Affairs within the White House Office of Management and Budget to provide centralized coordination and oversight of information management within federal agencies – including those covered by the Privacy Act, FOIA and the Computer Security Act.

The Computer Security Act of 1987 requires federal agencies to safeguard sensitive information and defines sensitive information so as to include information covered by the Privacy Act.

Presidential Decision Directive 63 (PDD-63, Critical Infrastructure Protection) was signed by President Clinton on May 22, 1998 and defines U.S. federal government policies on critical infrastructure protection. PDD-63 is the foundation document for the creation of the National Infrastructure Protection Center (NIPC), the United States

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

Computer Emergency Readiness Team (US-CERT) and other organizations devoted to protecting the nation's crucial industrial and financial base. PDD-63 cites as one of 10 guidelines, "Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably."

The E-Government Act (Public Law 107-347) passed by the one hundred and seventh Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title II and III of the E-Government Act requires that agencies assess the impact on privacy for information systems that collect personally identifiable information (PII) through a privacy impact assessment (PIA). Federal agencies are required by the Act to make PIAs publicly available. Many agencies also conduct preliminary Privacy Threshold Analysis's (PTA), which is little more than a non-releasable abbreviated form of a PIA to determine whether a public-releasable PIA is required under the E-Government Act.

Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) was preceded by the Government Information Security Reform Act and retained the bulk of the original language. Its purpose is to place responsibility for ensuring the security of federal information on the head of the federal agency and the agency CIO. It requires that the CIO or his delegated representative

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

explicitly authorize IT systems to operate with assessed risk as the basis for the decision. FISMA mandates an agency-wide, full life-cycle program to ensure the security of federal data and systems that process, store or transmit federal data. This means that federal agencies must also ensure the security of commercial systems that process, store or transmit federal data operated under contract at non federal installations. FISMA is intended to ensure that agencies mature their information assurance capabilities from being an attribute of individuals within the organization to an attribute of the organization. FISMA directs the national Institute of Standards and Technology (NIST) within the Department of Commerce to establish minimal acceptable standards for safeguarding federal information and associated systems. Toward this end, NIST published Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations. NIST SP 800-53 details 205 control requirements in 18 families of operational, managerial and technical controls designed to safeguard sensitive information. The publication's title is misleading. Although originally published as recommendations, Federal Information Processing Standards Publication number 200, Minimum Security Requirements for Federal Information and Information Systems (FIPS 200) published in March of 2006, made NIST SP 800-53 control recommendations mandatory.

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

Among the mandatory control requirements all federal agencies must follow related to protection of PII, NIST SP 800-53 requires that all federal information systems conduct a privacy impact assessment prior to operational use of the system. The document specifically defines sensitive information so as to specifically include Privacy Act-protected information, and privacy concerns are cited in a great many of the mandatory control requirements. Together, FIPS 200 and NIST SP800-53 represent unprecedented privacy protection doctrine affecting every federal and federal contractor IT system throughout the government. The doctrine also requires that each control requirement be tested annually and certified independently every three years. Agencies are required to submit reports of system security certification results to OMB annually; these reports directly affect agency and program budget allocations by OMB.

Effectiveness

Each year, the Office of Management and Budget (OMB) reports to Congress on the previous year's implementation of security and privacy controls throughout the federal government based on agency Inspector General reporting associated with the Federal Information Security Management Act of 2002. The most recent report to Congress, for fiscal year 2008, indicates continued, steady improvement. As previously mentioned, management for every federal information system as well as all systems that process federally-owned data or that process data on behalf of the federal government is

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
 A Veteran Owned Small Business
 123 S Fayette Street
 Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

required to conduct Privacy Impact Assessments (PIAs) and post a System Of Records Notice (SORN).

Table 1

Excerpted results of IG assessments of 25 major agencies for fiscal year 2008

Agency	Quality of Certification and Accreditation Process	Quality of Privacy Impact Assessment Process
Agency for International Development	Excellent	Excellent +
Department of Agriculture	Poor	Satisfactory +
Department of Commerce	Satisfactory +	Good
Department of Defense	Failing	Failing
Department of Education	Satisfactory	Excellent +
Department of Energy	Satisfactory	Satisfactory
Environmental Protection Agency	Good +	Excellent +
General Services Administration	Satisfactory	Satisfactory
Department of Health and Human Services	Satisfactory -	Good -
Department of Homeland Security	Good +	Good

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
 A Veteran Owned Small Business
 123 S Fayette Street
 Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

Department of Housing and Urban Development	Satisfactory	Satisfactory -
Department of the Interior	Satisfactory +	Excellent +
Department of Justice	Good -	Excellent
Department of Labor	Satisfactory	Good
National Aeronautics and Space Administration	Excellent +	Good
National Science Foundation	Good	Excellent
Nuclear Regulatory Commission	Satisfactory +	Excellent
Office of Personnel Management	Satisfactory -	Excellent +
Small Business Administration	Satisfactory	Satisfactory
Smithsonian Institution	Satisfactory	Satisfactory -
Social Security Administration	Good -	Excellent +
Department of State	Good +	Good +
Department of Transportation	Satisfactory	Satisfactory -
Department of the Treasury	Satisfactory	Satisfactory
Department of Veterans Affairs	Satisfactory +	Satisfactory +

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

Note. Federal systems with a PIA increased from 84% in 2006 and 2007 up to 92% in 2008. Federal systems with a SORN increased from 83% in 2006 and 2007 to 92% in 2008.

+ Indicates improvement from preceding report

- Indicates downgrade from preceding report

The 2008 OMB report states that all federal agencies now have policies in place to ensure that all personnel are familiar with privacy requirements and that 84% report having targeted, job-specific privacy training in place. The report also shows progress within all agencies toward establishment of privacy breach notification plans, and that most agencies produced a demonstrated ability to provide formal, comprehensive breach notification plans. The report shows that across the federal government, plans are being produced to reduce unnecessary collection of Social Security Numbers and PII. Overall, OMB finds that senior agency officials have been sensitized to privacy risks associated with federal holding of Social Security Numbers and PII.

Summary

Appearances are that government controls associated with its holding of citizenry's personal information are appropriately designed, in place and operating - though not as effectively as they could be. Devastating breaches still occur, and the most common cause appears to be associated with apathy at low levels of government.

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

Contractors ignore policy concerning handling of PII, unencrypted laptops are stolen, reams of un-shredded, printed PII is thrown away in public trash bins, hard drives are unsecured or disposed of still containing sensitive information including PII, archived backup tapes of PII are not properly secured, and IT system owners do not adequately safeguard the systems that process PII on behalf of their constituency.

Senior public officials are establishing organizational PII protection policies and employee training programs - yet breaches continue at the least rungs of management's ladder. PII protection practices and a creed among civil servants of adherence to privacy policy is slowly trickling down to information system administrators, mail clerks, property managers and sub-contractors, but will it be enough to overcome lower pay-grade apathy so as to altogether prevent privacy breaches ? Of course not. At some point, the public will likely find consensus on the amount of PII loss and compromise by the government that is acceptable, but that level has not yet been reached and for now, remains somewhere over the horizon.

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

References

- Harper, J. (2004). Privacy and government. Retrieved October 31, 2009 from <http://www.privacilla.org/government.html>
- Identity Theft Resource Center. (2009). Data breaches. Retrieved November 2, 2009 from http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml
- Cline, A. (2009). Decision: Olmstead v. United States (1928). Retrieved November 2, 2009 from http://atheism.about.com/library/decisions/privacy/bldec_OlmsteadUS.htm
- Zalud, B. (2009). The private side of security. Retrieved November 2, 2009 from http://www.securitymagazine.com/Articles/Feature_Article/BNP_GUID_9-5-2006_A_1000000000000552069
- Federal Information Security Management Act of 2002, Pub. L. No. 107-347, Title III (2002).
- U.S. Department of Commerce. National Institute of Standards and Technology. (2007). *Recommended security controls for federal information systems* (Rev 3 ed.) (SP 800-53). Washington, DC: U.S. Government Printing Office. Retrieved August 15, 2009 from <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

U.S. Department of Commerce. National Institute of Science and Technology. (2006, March). *Minimum security requirements for federal information and information systems* (FIPS 200). Washington, DC: U.S. Government Printing Office.

Retrieved February 24, 2009 from <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>

Clinton, B. (1998). Presidential Decision Directive/NSC-63. Retrieved November 2, 2009 from <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>

Office of Management and Budget. (2009). *Fiscal year 2008 report to congress on implementation of The Federal Information Security Management Act of 2002.*

Retrieved November 4, 2009 from http://www.whitehouse.gov/omb/assets/reports/fy2008_fisma.pdf

This white paper is made available by Missing Link Security...We find your weakest links.