OREA | Offices of Research and Education Accountability
Tennessee Comptroller of the Treasury, John G. Morgan

Safeguarding Social Security Numbers in Tennessee Government Records

October 2008

STATE OF TENNESSEE

John G. Morgan

Comptroller

COMPTROLLER OF THE TREASURY

STATE CAPITOL

NASHVILLE, TENNESSEE 37243-0264

PHONE (615) 741-2501

October 20, 2008

The Honorable Ron Ramsey
Speaker of the Senate
The Honorable Jimmy Naifeh
Speaker of the House of Representatives
and
Members of the General Assembly
State Capitol
Nashville, Tennessee 37243

Ladies and Gentlemen:

Public Chapter 170 (2007) directs the Comptroller of the Treasury to review state and local government policies and practices as they relate to protecting Social Security numbers from disclosure to the public. For the purposes of this report, the Offices of Research and Education Accountability reviewed literature and surveyed state and local government officials to determine how state and local governments' records security policies and practices compare with best practices. This report identifies the federal and state restrictions on Social Security number use and collection by government entities, details some current records management practices of government agencies in Tennessee, and suggests recommendations for improvement. The report provides information that may be useful to policymakers in considering ways to safeguard Social Security numbers in Tennessee government records.

Sincerely,

John G. Morgan
Comptroller of the Treasury

Safeguarding Social Security Numbers in Tennessee Government Records

Susan Mattson
Senior Legislative Research Analyst

Patrick Hultman
Associate Legislative Research Analyst

Phillip Doss, Director
Douglas Wright, Assistant Director
Offices of Research and Education Accountability
505 Deaderick St., Suite 1700
Nashville, TN 37243
615/401-7911
www.comptroller.state.tn.us/cpdivorea.htm

John G. Morgan
Comptroller of the Treasury

October 2008

Comptroller of the Treasury, Office of Research. Authorization Number 307361, 150 copies, October 2008. This public document was promulgated at a cost of $2.58 per copy.

EXECUTIVE SUMMARY

Federal and state laws authorizing or requiring Social Security number (SSN) collection by public and private entities, the utility of using the SSN as a records management tool, and the lack of other unique personal identifiers have led to widespread adoption of the SSN as a primary identifier. Increased SSN collection and use concerns both policy makers and consumer advocates because of its potential misuse by identity thieves. The growth in electronic records systems may leave more individuals at risk due to the vast number of records that can be accessed on one computer or through a single electronic server via the Internet.

Public Chapter 170 of 2007 directs the Comptroller of the Treasury to review current state and local government policies and practices as they relate to protecting SSNs from disclosure to the public and provide appropriate recommendations to the General Assembly.

The information presented in this report is based on a survey of and interviews with state and local government officials. Most of the conclusions on state and local policies and practices are based on information as self-reported by the agencies; the Comptroller's Offices of Research and Education Accountability (OREA) did not conduct a full review of or verify agency practices and policies.

Use and Protection of SSN by Governments

Tennessee state and local governments collect and maintain a large number of SSNs in their records, but in most instances, federal or state laws restrict their public access and release. The SSN is useful to government agencies as a unique identifier to distinguish among individuals' records and to allow agencies to share information relevant to multiple programs. Government agencies are responsible for establishing policies and practices to safeguard individuals' SSNs.

Identity Theft

The SSN is one piece of information used to commit identity theft. A survey conducted for the Federal Trade Commission in 2006 estimated that 3.7 percent of the adult U.S. population (or 8.3 million individuals) fell victim to some sort of identity theft in 2005; 22 percent of victims' cases involved the opening of new accounts and other fraud, which are more likely to involve the use of another's SSN. While identity theft can be a serious financial and emotional problem for its victims, studies suggest that more than half of identity theft victims suffer no monetary loss.

Security Breaches

In recent years, laws have required public and private entities to report to consumers the loss or theft of personal information. The required reporting of security breaches may contribute to widespread public concern over the ability of public and private entities to keep personal data out of the hands of identity thieves. However, research indicates that most security breaches do not result in identity theft. There have been several data breaches of state and local governmental entities in Tennessee, but no agencies have reported known links to actual identity theft.

Nevertheless, the potential for identity theft is increasing with the growth in electronic records. Continued review and safeguards by governmental entities to limit and protect personal information, within reasonable costs, could help to control the risk of identity theft and alleviate public concern.

Conclusions

The following conclusions are based on a comparison of Tennessee state and local policies and practices to best practices recommended by several national organizations for protecting the unintended disclosure of individuals' SSNs. The

best practices focus on decreasing the unnecessary use and collection of SSNs, increasing the security of electronic records systems, implementing management controls over records, and eliminating opportunities for public disclosure of SSNs.

Tennessee government agencies have reduced SSN use, but further reduction may be possible. State and local government survey responses indicated that few, if any, agencies maintain a list of files or records, paper or electronic, that include personal information such as SSNs. About half of state agencies and very few local agencies surveyed inform the public of the reason for collecting SSNs on all forms and how the information is protected. These practices can help agency staff identify areas where SSN collection may not be necessary or where a substitute identifier would suffice. (See page 11.)

Some agencies lack sufficient policies to protect SSNs. Most local agencies responding to the OREA survey indicated that they do not have written policies to protect SSNs from unauthorized release. Most state and local government agencies lack sufficient departmental policies or procedures to safeguard confidential information, such as SSNs, stored on portable electronic data storage devices and computer workstations. The state's Enterprise Information Security (EIS) policies – set by the Information Systems Council and implemented by the Office for Information Resources (OIR) – require confidential data authorized for mobile or workstation use to be encrypted when stored on mobile or workstation computing platforms. However, state agencies are responsible for developing their own procedures to support the EIS policies. Many state and local agencies also lack specific policies on the reporting of security breaches to ensure all breaches are reported and dealt with consistently and appropriately. (See page 12.)

Use of safeguards and management controls to protect SSNs in electronic and paper records varies. Local offices reviewed by OREA varied in security practices to protect SSNs. Most agencies surveyed did not identify any safeguards to protect the exposure of the documents transmitted between governmental or other authorized agencies. Although most state agencies transmit SSNs over secure computer systems, many indicated they do not encrypt the SSN. Few local offices indicated they encrypt SSNs transmitted electronically. (See page 14.)

Tennessee law does not clearly direct local government record custodians on the treatment of SSNs in agency records. Survey responses suggest some variation among local government offices regarding the treatment of SSNs in agency records. Several local government agencies with similar types of records indicated that they redacted SSNs prior to releasing records to the public while others did not do so. (See page 15.)

State information security policies meet best practices, but agency compliance is unclear. The EIS policies include several provisions to protect SSNs in the state's electronic information systems. These policies meet most of the information security and records management best practices identified. However, state government has not specifically evaluated state agency compliance with EIS policies. OIR established an information security internal audit and assessment program in October 2007 to audit the EIS policies. Currently, the audit team is focused on the Department of Finance and Administration but plans to expand its scope to other departments as time and staffing permit. The Comptroller's Division of State Audit conducts general reviews of state agencies' information security practices, but does not specifically test compliance with the EIS policies. (See page 16.)

State government provides limited oversight of local personal information protection practices. Local agencies are not regularly and completely evaluated to determine potential risks of disclosure and compliance with security and management controls for personal information, such as SSNs**.** The Comptroller's Division of County Audit provides limited oversight of information security at the local level, but these audits focus more on risks to financial systems and do not specifically look at the protection of personal information. No state entity conducts formal reviews of municipalities' personal information protection policies and practices. (See page 17.)

State law does not designate an agency to receive security breach notifications. Without such a requirement, law enforcement and consumer protection agencies may be unprepared to assist consumers affected by a security breach. The lack of an agency notification requirement also leaves the state without data needed to guide the review of and implement changes to information security policies. (See page 17.)

Recommendations

See pages 18-20 for a full discussion of the report's recommendations.

Legislative

The General Assembly may wish to appoint state and local government study committees to review government use and transmission of the SSN, the feasibility of further reductions of SSNs in government records, and confidential records statutes.

The General Assembly may wish to require local governments to develop specific written policies on the protection of personal or confidential information, including SSNs, in all paper and electronic records.

The General Assembly may wish to prohibit local government entities from publicly disclosing SSNs.

The General Assembly may wish to amend the security breach law to require that government agencies notify a specific entity of security breaches.

The General Assembly may wish to require additional records management assistance and training resources for local government officials.

The General Assembly may wish to require additional oversight to ensure that state and local agencies have developed and implemented information about security policies and practices to protect confidential information, including SSNs, maintained in their records.

Administrative

State and local government agencies should continue to implement policies and practices to restrict the storage of SSNs and other personal information on portable electronic data storage devices and computer work stations.

The Information Systems Council should consider requiring state agencies to report electronic data security breaches to the Office for Information Resources.

Local governments should develop written security breach procedures.

Table of Contents

INTRODUCTION

Federal and state laws authorizing or requiring Social Security number (SSN) collection by public and private entities, the utility of using the SSN as a records management tool, and the lack of other unique personal identifiers have led to widespread adoption of the SSN as a primary identifier. Increased SSN collection and use concerns both policy makers and consumer advocates because of its potential misuse by identity thieves. The growth in electronic records systems may leave many more individuals at risk due to the vast number of records that can be accessed on one computer or through a single electronic server via the Internet.

Directive and Scope

Public Chapter 170 of 2007 directs the Comptroller's Office to review current state and local government policies and practices relating to protecting SSNs from disclosure to the public. The legislation also requires businesses that collect SSNs to observe certain practices designed to prevent disclosure to the public.

This report provides a general overview of potential vulnerabilities within state and local government records systems. This report attempts to answer the following questions:

1. How prevalent is the SSN in state and local government records in Tennessee and what is it used for?
2. What kind of requirements and restrictions on the use and collection of SSNs are contained in state and federal law?
3. How do state and local records security policies and practices compare with best practices?

Survey Methodology and Limitations

The Comptroller's Offices of Research and Education Accountability (OREA) conducted a survey of state agencies and a sample of local government offices to determine agencies' policies and practices for protecting SSNs from public disclosure. The survey's purpose was to determine the extent of SSNs maintained by state agencies and local offices and whether state and local agencies have records handling practices and departmental policies that address "recommended or best practices" identified through OREA research to provide for SSN protection.

OREA surveyed all state agencies, county offices in nine counties, and offices in the largest city in each county.[1] Offices included court clerks, trustees, school boards, sheriffs, utilities, registers of deeds, election administrators, human resources directors, mayors, clerks, and recorders. Survey responses were supplemented with interviews with several local officials and representatives of professional associations.

OREA received responses from 50 of 55 state agencies surveyed, a 91 percent response rate. Local government response to the survey was fairly limited: only 34 of the 78 (44 percent) county officials surveyed and 15 of 46 (33 percent) city officials surveyed responded. Survey information is self-reported by the agencies; Comptroller staff did not verify the survey information. Conclusions and recommendations are based on a comparison between policies and practices of state and local government officials and a list of current best practices.

Time did not allow a statistically representative sample of local government offices to identify all documents with SSNs, to project the number of records with SSNs, or to determine whether all local government offices have sufficient policies and practices to protect SSNs. The limited sample and limited responses may not be representative of

all local offices, but should provide a general indication of some of the vulnerabilities and issues involved in protecting SSNs in local records.

Some state agencies sent a consolidated response for the entire agency, while others sent separate responses from subparts of the agency. If any subpart of an agency indicated they had the policy or practice, OREA recorded a positive response on that question for the entire agency. Most agencies did not provide copies or references to specific policies for review, but instead described their practices or general state policies or laws. The responses are presented as reported by the agencies without further review of the specific policies or observation of their practices.

Background

Use of SSNs

SSN use has expanded beyond its original purpose as a record-keeping tool for administering a single government program. Government use of the SSN as a primary identifier multiplied in response to numerous federal laws requiring its collection to administer a broad range of government activities and programs.[2] Private sector use expanded in response to expanded government use. The use of the SSN as an identifier in both the public and private sectors has endured in part because other items that could be used as personal identifiers such as addresses, telephone numbers, or state-issued driver license numbers change over time.

Exclusive use of the SSN as an identifier in new federal government records systems was ordered by President Roosevelt in 1943. However, the catalyst behind expanded use of the SSN occurred in 1961 when the Internal Revenue Service began using it as an official taxpayer identification number.[3] Use of the SSN to identify individual taxpayers brought new government mandates to monitor financial transactions, facilitating expanded use and collection of the SSN by public and private sector entities.[4]

The Balanced Budget Act of 1997 contained provisions that furthered the growth of SSNs in government records. The Act required states to collect the SSNs of any applicant for a professional license, driver license, occupational license, recreational license, or marriage license. In addition, states were required to adopt procedures to include the SSN in divorce or child support pleadings and on death certificates.[5] Agencies in Tennessee that administer these licenses are required by law to furnish license holder and applicant data to child support enforcement agencies.[6] Federal law also requires all businesses to submit new employee data, including the SSN, to a state administered directory that is used to locate and sanction those who owe child support.[7]

The SSN is used by credit bureaus and business entities that access credit records in conjunction with certain commercial transactions. The SSN is used as an identifier to locate individual credit histories, and as an authenticator to verify the identity of individuals requesting access to sensitive information like that contained in bank account information or medical records. Private businesses such as auto insurance companies, cell phone providers, and utility companies routinely collect this information to identify customers who have a history of not paying bills on time or to report delinquent accounts to credit bureaus.

Government Use of SSNs

Federal, state, and local government agencies collect the SSN from citizens to determine benefit

eligibility, administer programs, or conduct research. The SSN is useful to government agencies as a unique identifier to distinguish among individuals' records and to allow agencies to share information relevant to multiple programs.

State and local agencies responding to the OREA survey cited identification, personnel functions, and records management as the most common reasons for collecting SSNs. Just over half of state agency respondents indicated that the SSN is required by federal and state law or policy for many personnel related functions, such as tax and benefit reporting. Agencies administering entitlement and benefit programs use the SSN as an identifier to verify information contained in other government databases and to ensure that benefits and services are restricted to those who are eligible. State and local agencies also use the number in law enforcement and court documents to verify the identity of criminal suspects or people involved in court cases. Many federal programs require state agencies to collect SSNs from participants in Federal Housing Administration programs, Medicaid, food stamps, and unemployment insurance.[8]

Prevalence of SSNs in Tennessee Government Records

State and local government agencies maintain a large number of records that include SSNs. State agencies responding to the OREA survey maintain at least 20 million individual SSNs in paper and electronic records.[9] Most agencies estimated between one and five percent annual growth in records with SSNs, or at least three million SSNs per year. While the small number of local government survey responses is insufficient to produce an estimate, sample results suggest that the SSN is widespread in local government records. The 49 local government respondents in eight counties and eight cities maintain at least four million SSNs in agency records with most estimating an annual growth rate between one and five percent.

Exhibit 1 identifies some common government records systems in Tennessee along with specific records that contain SSNs. Although a complete list of specific documents and records is not available, survey responses were sufficient to list general types of records. Personnel records are the most prevalent location for SSNs in both state and local government records. The SSN is also common in educational records, court and law enforcement records, and the client files of various entitlement and benefit programs.

Restrictions on Use and Disclosure of SSNs

Although most government records are considered open to public inspection, numerous state and federal laws restrict the use, collection, and disclosure of SSNs. Government agencies are responsible for establishing policies and practices to safeguard individuals' SSNs.

Federal Law Restrictions

Federal law prohibits the release of SSNs contained in motor vehicle records, records of healthcare providers and public health plans, and educational records. (See Exhibit 2.) The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects the privacy of identifying health information retained by public and private health plans, health care clearinghouses, and health care providers. Schools receiving federal funding are prohibited from publicly disclosing identifying information contained in student records under the Federal Educational Rights and Privacy Act of 1974 (FERPA). The Drivers Privacy Protection Act of 1994 prohibits a state's Department of Motor Vehicles from disclosing the SSN contained in individual motor vehicle records.

Agencies in Tennessee with records covered by these statutes include the Bureau of TennCare (HIPAA), the Tennessee Department of Education (FERPA), and the Tennessee Department of Safety (Drivers Privacy Protection Act) – all of which report maintaining over one million individual SSNs in their records.

Tennessee State Law Restrictions

Tennessee provides citizens the right to inspect state and local government records unless state or federal law indicates otherwise. Passed in 1957, the Tennessee Public Records Act provides the basis for the public's right of access to government records, while listing many of the requirements and exemptions for government records custodians. The public records chapter contains an additional part that provides an extensive list of government records considered confidential and not open for public inspection. This part includes many records likely to contain SSNs, including medical and educational records, many of which are already made confidential by federal laws such as HIPAA and FERPA. It also makes SSNs confidential when appearing in specific records including motor vehicle records, personnel files of all public employees, the records of a public utility, and records of all government entities in the state concerning a person with a restraining order or other order of protection.[10]

An exception to the Public Records Act, *Tennessee Code Annotated* 4-4-125 prohibits state agencies and subcontractors acting on their behalf from publicly disclosing the SSN of any citizen without permission. This provision restricts public access to SSNs in state records, but does not require any specific records security measures. (See Exhibit 3.)

Exhibit 1: Common Records Containing SSNs in Tennessee State and Local Government Offices

Personnel Records	Employment applications, benefits administration, payroll, tax withholding forms, employment eligibility documents
Education Records	*K-12*: Student records, federal school nutrition program documents, teaching licenses *Postsecondary*: Applications, transcripts, financial aid and scholarship documents, standardized test scores
Law Enforcement Records	Offender files, criminal history and fingerprint databases, criminal complaints and investigations, handgun permit applications
Court Records	*Criminal*: Judgments, law enforcement records, traffic cases *Civil*: Divorce and child support filings, orders of protection, adoption records, judicial hospitalizations
Vital Records	Birth and death records, marriage and divorce certificates and applications
Motor Vehicle Records	Driver license applications and driving records
Benefit and Entitlement Program Records	*Client Files*: Unemployment, TennCare, county health departments, Families First, food stamps, housing authorities
Voter Registration Records	Voter registration applications
Miscellaneous License Applications	Marriage license, business license, notary license, recreational license, U.S. Passports, real estate license, contractor license, health care professional license
Other Records	Tax filings and records, military records, state contracts, audit working papers, public utility customer records

Source: OREA survey of Tennessee state and local government agencies, February 2008.

Exhibit 2: Federal Laws Restricting the Use and Disclosure of SSNs

Privacy Act of 1974
Requires federal, state, or local government agencies requesting a Social Security account number to state whether disclosure is mandatory or voluntary, the statutory authority for requesting the SSN, and the manner in which it will be used
Family Educational Rights and Privacy Act of 1974
Prohibits all schools receiving federal funding from releasing educational records or personally identifying information (including SSN) of students without permission
Health Insurance Portability and Accountability Act of 1996
Protects the privacy of individually identifying health information retained by public and private health plans, health care clearinghouses, and health care providers
The Drivers Privacy Protection Act of 1994
Prohibits a state's Department of Motor Vehicles from knowingly disclosing certain personal information, including the SSN, contained in individual motor vehicle records
Social Security Act Amendments of 1990
Prohibits the willful disclosure of SSNs obtained or maintained by authorized employees or agents of federal, state, and local governments pursuant to any laws enacted after October 1, 1990
Fair and Accurate Credit Transaction Act of 2003
Requires public and private entities to take appropriate measures to dispose of sensitive information derived from consumer reports from credit reporting agencies
Intelligence Reform and Terrorism Prevention Act of 2004
Prohibits federal, state, and local governments from displaying SSNs, or any derivative thereof, on driver licenses, motor vehicle registrations, or other identification documents issued by state departments of motor vehicles

Source: United States Code.

Exhibit 3: State Laws Restricting the Use and Disclosure of SSNs

Prohibits state entities from publicly disclosing the SSN of any citizen without permission unless otherwise permitted by state or federal law - T.C.A. 4-4-125(a)(b)
County Registrar and Commissioner of Elections required to remove SSNs from voter registration records, both paper and electronic, prior to release to anyone other than the holder - T.C.A. 2-2-127(a)
SSNs maintained by a governmental entity concerning a person with a valid order of protection may be treated as confidential and not open for inspection by the public - T.C.A. 10-7-504(a)(16)(B)
SSNs held by public utilities shall be treated as confidential and not open for inspection by the public - T.C.A. 10-7-504(a)(20)(B)
SSNs contained in personnel records of any state, county, municipal, or other public employee shall be treated as confidential and not open for public inspection - T.C.A. 10-7-504(f)(1)(C)
Persons are prohibited from placing the SSN on any document to be filed with the county register of deeds except for a power of attorney - T.C.A. 10-7-515
SSNs contained in court filings of divorce, legal separation, and paternity filings shall be placed in a separate envelope and made available only to the Department of Human Services and other agencies permitted by law - T.C.A. 36-4-106(b)(1); T.C.A. 36-5-101(c)(2)(B)(i)
SSNs contained in motor vehicle records may not be disclosed. This includes motor vehicle records maintained by the Department of Safety, Department of Treasury, and the offices of county clerk. SSNs may not be included in records sold by the Department of Safety - T.C.A. 55-25-104; T.C.A. 55-50-204(C)(2)
SSNs contained in motor vehicle records shall be treated as confidential and not open for public inspection - T.C.A. 10-7-504(a)(12)

Source: *Tennessee Code Annotated*.

Tennessee Agency Policies and Oversight

State Government

State agencies are subject to general directives within the law, as well as overall state and federal policies on protecting personal information, such as SSNs. Individual state agencies are primarily responsible for implementing policies and practices to protect SSNs included in their records.

Related state agency policies include:

- Department of Human Resources (DHR) Policy 99-026 limits access to personnel records and details procedures to protect the SSNs from public disclosure. The policies include procedures to redact SSN from records prior to public release, and shredding or destruction of records prior to disposal to protect confidential information.[11]

- Information Systems Council's (ISC) Enterprise Information Security (EIS) Policies establish the minimum requirements needed to protect the state's technology resources and ensure they remain available for use and include several policies protecting the confidentiality of personal information in government electronic records.[12] Made up of top officials from all three branches of state government, the ISC is responsible for developing policies for the overall management of the state's information systems, including security policies.[13] The ISC authorized the Office for Information Resources (OIR) in the Department of Finance and Administration to provide agencies with access to the state computer network and enforce the EIS policies. The EIS policies "envision maximum voluntary compliance" with the state agency-wide policies. OIR communicates policies to agencies, and agencies are responsible for developing computer network access and use procedures that support state policies. End users are responsible for following the policies and reporting potential security problems.

The Comptroller's Division of State Audit generally reviews information security as part of its financial and compliance audits but does not specifically look at adherence to specific state agency policies.[14]

Local Government

Local agencies have some information security direction from state and federal law, but few agencies surveyed indicated they had adopted specific policies related to the protection of personal information. County audits contain some general review of information security, but municipal audits contain no such review or oversight.

Additional Safeguards and Policies Required

Public Chapter 688, effective July 1, 2008, requires state agencies, municipalities, and counties to create safeguards and procedures for ensuring secure protection of citizens' confidential information on all laptops, computers, and other removable storage devices. The act allows citizens to sue governmental agencies whose failure to provide safeguards results in identity theft. This alters more recent identity theft deterrence laws, which exempted governmental agencies from civil damages resulting from the release of personal consumer information.[15]

Threat of Identity Theft

Identity Theft Defined

According to the definition within the Fair and Accurate Credit Transactions Act of 2003, identity theft means "…fraud committed or attempted using the identifying information of another person without authority."[16] While the SSN is only one piece of information used to commit identity theft, it is of particular value because it permits the opening of new financial accounts and allows access to some existing accounts. The SSN can also be used to obtain driver licenses and green cards granting immigration status, and to complete employment documents such as the W-4 and I-9 forms.

Problems Measuring Identity Theft

Measuring the prevalence of identity theft is complicated by underreporting or lack of legal action by many victims. Criminal statistics may not include identity thieves charged under fraud statutes or reflect the number of victims interested only in correcting information in credit reports or seeking reimbursement of expenses resulting from fraudulent activity.[17]

The U.S. Congress made identity theft a stand-alone crime when it passed the Identity Theft and Deterrence Act of 1998. At the time, only eight states had laws specifically addressing identity theft, the first of which was enacted in 1996.[18] The Tennessee General Assembly passed legislation in 1999 and 2004 specifying 'identity theft' and 'identity theft trafficking' as distinct felony crimes.[19] In 2007, 324 persons were convicted of identity theft in Tennessee compared to 179 persons in 2003.[20]

The Federal Trade Commission (FTC) established the Identity Theft Data Clearinghouse to gather data from consumers wishing to file identity theft complaints. Of the nearly 240,000 identity theft victims who contacted the FTC in 2004, 39 percent also contacted local law enforcement.[21] State consumer protection agencies and the FTC routinely assist identity theft victims, but there are no estimates regarding the overall prevalence of identity theft based on the number of complaints filed with these agencies. Because of the lack of available data, the FTC contracted for 2003 and 2006 general public survey studies to determine the identity theft victimization prevalence and the impact of identity theft.

Identity Theft Prevalence and Impact

While identity theft can be a serious financial and emotional problem for its victims, studies suggest that more than half of identity theft victims suffer no monetary loss. Most cases of identity theft do not involve the opening of new accounts or other fraud, which are more likely to involve the use of a SSN.

A 2006 FTC survey estimated that 8.3 million people in the United States fell victim to some sort of identity theft in 2005.[22] (See Exhibit 4.) The opening of new accounts and other fraud, which are more likely to involve the use of another's SSN,

Exhibit 4: Estimated Prevalence of Identity Theft in the U.S. in 2005 by Category of Misuse

	Percent of Adult Population	Number of Persons (millions)
New Accounts and Other Fraud	0.8%	1.8
Misuse of Existing non-Credit Card Account	1.5%	3.3
Misuse of Existing Credit Card	1.4%	3.2
Total Victims in 2005	3.7%	8.3

Source: Synovate and U.S. Federal Trade Commission, *Federal Trade Commission 2006 Identity Theft Survey Report*.

Note: Estimate based on a random telephone survey of 4,917 U.S. adults.

affected about 1.8 million adults, or 0.8 percent of the population, about 22 percent of the estimated identity theft victims. Most cases (78 percent) result from the use of existing credit card or other accounts, which do not usually require the misuse of SSNs.[23]

The FTC survey also collected data about the cost of identity theft among those victimized between 2001 and 2006. Although a small portion of this group reported significant expenses, most victims incurred no out-of-pocket expenses. Reported financial losses and time required to resolve identity theft were higher for identity theft involving new accounts. (See Exhibit 5.) The survey found:

- The median value of goods and services reported obtained by identity thieves was $500; however, five percent of victims reported values over $13,000. Most of these costs are borne by businesses rather than directly by victims; however, such losses can affect overall consumer prices as businesses pass on these costs to consumers.
- In over half of identity thefts, victims incurred no out-of-pocket expenses; however, 10 percent of victims reported expenses over $1,200 and five percent had expenses over $2,000.
- The median number of hours spent resolving the various problems that result from identity theft by victims was four hours. However, 10 percent of victims spent at least 55 hours and the top five percent spent at least 130 hours.

A similar national survey estimated that identity theft claimed 8.4 million victims in the United States in 2006, costing business and consumers $49.3 billion. Echoing findings from the FTC study, fewer than half of identity theft victims surveyed suffered monetary losses as a result. This study also found a decline in the instances of identity theft involving the opening of new accounts, a finding that may result from increased emphasis on privacy protection and consumer monitoring of financial accounts through the Internet.[24]

Exhibit 5: Cost of Identity Theft Discovered Since 2001 by Category of Misuse

		New Accounts and Other Fraud	Existing Non-Credit Card Accounts	Existing Credit Cards Only	All ID Theft
Value of Goods and Services Obtained by Identity Thieves	Median	$1,350	$457	$350	$500
	95th Percentile	$30,000	$6,000	$7,000	$13,000
Victims' Out-of-Pocket Expenses	Median	$40	$0	$0	$0
	95th Percentile	$5,000	$1,200	$400	$2,000
Hours Victims Spent Resolving Their Problems	Median	10	4	2	4
	95th Percentile	1,200	96	60	130

Source: Synovate and U.S. Federal Trade Commission, *Federal Trade Commission 2006 Identity Theft Survey Report*.

Note: Based on responses from 559 individuals who said their personal information was misused between 2001 and the date of the interview in 2006.

Security Breaches

In recent years, laws have required public and private entities to report to consumers the loss or theft of personal information. The required reporting of high profile security breaches may have contributed to widespread public concern over the ability of public and private entities to keep personal data out of the hands of identity thieves. An overwhelming majority of respondents (91 percent) to a 2007 Zogby International survey indicated that they are concerned about their identity being stolen.[25] However, evidence suggests that the risk of identity theft from security breaches is low, although the continued growth of and reliance on electronic records without sufficient safeguards could put more people at risk of identity theft.

As defined in *Tennessee Code Annotated*, security breaches are the unauthorized acquisition of unencrypted computer data, compromising the security, confidentiality, or integrity of personal information, including SSNs.[26] Security breaches may result from lost or stolen computers or data storage devices, websites with inadequate or missing security, or compromised passwords.

As of May 2008, 43 states, including Tennessee, have laws that require business and/or government entities to notify consumers of a breach in the security of unencrypted, computerized personal information.[27] The most stringent state laws include requirements that government and business entities notify credit reporting agencies and provide for civil damages through either private or public rights of action. Many states exclude breaches involving records that are considered public, or breaches that are not expected to expose persons to identity theft. Several states have an oversight component, requiring agencies or businesses that have experienced a security breach to provide reports and/or corrective action plans to the legislature or Attorney General.[28]

The national, nonprofit Identity Theft Resource Center (ITRC) reported 446 paper and electronic publicized breaches involving 127 million records including personal data in 2007. About half of these breaches and seven percent of the records were from government agencies or educational institutions.[29] The ITRC-reported number of publicized breaches has increased significantly over the last few years.[30] The federal Office of Management and Budget (OMB) found the number of federal agency incidents in which sensitive information on computer systems may have been compromised more than doubled in 2007.[31] However, an OMB official attributed part of the increase to better agency reporting.[32]

A U.S. Government Accountability Office (GAO) review of security breaches suggested that most reported breaches do not result in identity theft. Investigators found that of the 24 largest security breaches reported between 2000 and 2005, they could confirm only four that resulted in identity theft.[33]

Reported Security Breaches in Tennessee

Few state or local agencies or offices surveyed by OREA reported security breaches since 2000. Agency respondents reported no cases of known identity theft resulting from security breaches. Only 11 state agencies indicated any instances of theft or unintentional public release of SSNs from their agencies since 2000. Of the instances reported, the most common were stolen or lost laptops or storage devices (five agencies) that potentially included SSNs. Seven instances were reported as a result of programming errors involving electronic records, e.g., a listing including SSNs was inadvertently put in a file accessible by unauthorized or unintended users. These instances involved a larger number of affected individuals who were notified of the breach and advised to check their credit reports. Other instances reported included the loss or theft of paper documents that

included SSNs, the erroneous disclosure of an individual SSN, and publishing several documents including a SSN in a report.

The most visible Tennessee local government breach was the theft of two laptop computers from the Davidson County Election Commission in December 2007 containing the SSNs of over 300,000 registered voters. The computers were recovered by the police and there was no evidence that the SSN information had been accessed. All voters were notified and offered credit monitoring service paid by the metropolitan government for a year.[34] The Division of County Audit released a limited review of information system controls for the Election Commission in May 2008, which the Administrator of Elections and the Director of Information Technology Services are addressing.[35] Internal auditors and a systems security firm are also reviewing Metro Nashville's policies and practices for protecting personal information.[36]

ITRC reported eight publicized data breaches by Tennessee governments or educational institutions in 2007 involving 413,800 records. Most of these records (80 percent) were from the Davidson County Election Commission theft where the data was recovered with no evidence of access by the thieves.[37] As of July 22, 2008, ITRC has reported six publicized data breaches by Tennessee educational institutions in 2008 involving 26,619 records. Most of the records (17,000) involved Williamson County Schools student records. The system confirmed that 5,300 student SSNs were accidentally posted on the Internet for less than 30 days.[38] No actual identity theft from the breach has been confirmed. ITRC did not report any publicized data breaches in 2008 involving non-educational government records.[39]

Best Practices to Protect Against the Disclosure of SSNs

Best practices to protect SSNs from disclosure include reducing the unnecessary use and collection of SSNs, securing electronic records systems, using management controls, and reducing or protecting the transmission of records containing SSNs. (See Exhibit 6.) OREA analysts used these practices to assess general areas of risk for state and local governments in Tennessee.

Exhibit 6: Summary of Best Practices to Protect SSNs from Disclosure

1. Decrease the unnecessary use and collection of SSNs
    a. Review agency use and collection of SSNs and provide justification for collection to designated records authority
    b. Limit the collection of SSNs to those instances where it is required by law or necessary for agency function
    c. Develop a substitute for SSNs where a unique identifier is needed
    d. Inform citizens of the purpose for SSN collection, the intended use, the legal justification for collecting the SSN, and the consequences for refusing to provide the number
    e. Inform citizens of the steps taken by the agency to ensure the confidentiality of the SSN
2. Increase the security of electronic records systems
    a. Store data containing SSNs on secure servers
    b. Do not unnecessarily save data containing SSNs to laptops or other portable data storage devices
    c. Use technological controls such as encryption, password protections, and secure Internet connections to store or transmit files containing SSNs
    d. Inventory and track the location of files containing SSNs
3. Implement management controls for records containing SSNs
    a. Classify records according to the level of sensitivity or confidentiality of the information they contain
    b. Develop and implement written security policies detailing procedures for storage, transmission, disposal, and disclosure procedures for records containing SSNs
    c. Restrict access to records containing SSNs to those employees who need the numbers for the performance of their job duties
    d. Conduct regular trainings and audits or reviews to ensure compliance with records security policies
4. Eliminate opportunities for public disclosure of SSNs
    a. Reduce or protect the transmission of SSNs in paper and electronic records

Sources: U.S. President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, (Washington, D.C., 2007); California Department of Consumer Affairs, Office of Privacy Protection, *Recommended Practices on Protecting the Confidentiality of Social Security Numbers*, (2008); U.S. Federal Trade Commission, *Privacy Online: A Report to Congress*, "Fair Information Practice Principles," (Washington, D.C., 1998); National Association of State Chief Information Officers, *Keeping Citizen Trust: What Can a State CIO Do to Protect Privacy?*, (Lexington, KY, 2006).

CONCLUSIONS

Tennessee government agencies have reduced SSN use, but further reduction may be possible.

Although Tennessee state and local governments have reduced or eliminated SSNs from many government records in recent years, many government agencies have not systematically reviewed their use of SSNs as suggested by best practices. Best practices not followed by most agencies include 1) to compile, review, and maintain a list of all records and computers that include SSNs and determine legal confidentiality requirements or whether a substitute identifying number would suffice and 2) to inform consumers why the SSN is needed. Such a review could help agencies identify possible areas to further reduce SSN use and the risk of security breaches, and potential identity theft from government records. If SSNs are not unnecessarily included in records and reports, they cannot be stolen or inadvertently released.

The collection of SSNs has been reduced or eliminated in several local records over the last few years. As of June 2003, SSNs are prohibited on property deeds or mortgage documents filed with county registers of deeds.[40] As of May 2007, elementary and secondary schools may no longer require the use of the SSN as a personal identification number to track students or to print on class rolls.[41] Laws changed in 2007 require the SSN and other personal information of persons involved in divorce and child support cases to be filed in a separate sealed envelope in the court records and limit its access to the clerks and certain government agencies.[42]

The State of Tennessee is currently implementing Project Edison, an integrated software system that performs administrative business functions such as financials and accounting, procurement, payroll, benefits, and personnel administration. According to system consultants, Edison will greatly reduce the usage of SSNs in state computer systems and also on forms, reports, and communications. Instead of using SSNs as a key identifier for employee records, a randomly-generated employee ID number will be used.[43]

In 2004, the University of Tennessee at Knoxville began issuing unique student identification numbers to replace the SSN in student records systems, a practice that expanded to all University of Tennessee campuses by 2006.[44] By fall 2008, all 19 Board of Regents institutions had switched to a new system that replaces SSNs with a student identification number.[45] While student records are confidential under federal law, the use of an alternate identifier in records systems reduces opportunities to misuse personal information if records are lost or compromised.

Efforts by other states to reduce the use of SSNs include the use of task forces to study SSN use, requiring agency review of SSNs, and limiting SSN collection unless it is authorized by law or otherwise necessary for agency function. Virginia passed legislation this year requiring state agencies and municipalities to review collection and use of citizens' SSNs and explain why it is required or needed for agency function.[46] Three states have recently created task forces charged with identifying ways to reduce government collection and use of SSNs or replacing the SSN with another identifier.[47] Virginia, North Carolina, South Carolina, and Florida prohibit state and local government agencies from use and/or collection of citizens' SSNs unless permitted by law or required to carry out agency duties.[48]

Responses to the OREA survey of Tennessee state and local governments suggest that many agencies do not follow best practices for reducing SSN use. Few, if any, agencies had a list of all files or records, paper or electronic, that include personal information such as SSNs. Several state agencies (43 percent) indicated that in some cases, the SSN is used primarily for records management, e.g., to organize and locate specific records, indicating use of another identifier may be possible. About half of state agencies and few local agencies surveyed by OREA indicated that they inform a person of the reason for collecting SSNs on all forms and how the information is protected. Reviewing SSN use and providing personal information collection and privacy statements when collecting SSN may help government agencies identify areas to further reduce SSN use and instill public confidence that personal information is protected.

Some agencies lack sufficient policies to protect SSNs.

While most government agencies in Tennessee take measures to protect SSNs, some lack written policies or procedures directing staff on appropriate and consistent safeguards for SSNs in

their records. Based on responses to the survey, this is more often true for local government agencies.

Local governments lack written security and management control policies regarding SSNs. Most local offices responding to the OREA survey indicated that they do not have or follow written policies that address**:**

- the release of public records with SSNs,
- the protection of SSNs from unauthorized disclosure,
- confidentiality agreements from employees dealing with personal information,
- the disposal of records containing SSNs, or
- action to take when a SSN security breach is discovered.

Specific requirements in *Tennessee Code Annotated* regarding security breach notifications and the disposal of records defined as confidential records apply to all public entities in the state.[49] Without written policies addressing these requirements, government records custodians may lack specific guidance on how to comply with legal requirements.

Many local government agencies do not have dedicated staff to manage records. Securing confidential or sensitive information contained in records is an essential records management task governed by complex laws. Agencies that manage records governed by broad federal privacy statutes such as FERPA or HIPAA may have detailed policies for handling confidential information. Some local government agencies are large enough to have dedicated staff to manage records, while record keeping may be an incidental duty for staff in smaller agencies.

Most state and local government agencies lack sufficient departmental policies and procedures to safeguard confidential information, such as SSNs, stored on portable electronic data storage devices and computer workstations. The state's Enterprise Information Security (EIS) policies – set by the Information Systems Council and implemented by the Office for Information Resources (OIR) – require confidential data authorized for mobile or workstation use to be encrypted when stored on mobile or workstation computing platforms.[50] Most state agencies responding to the OREA survey (61 percent) did not have specific agency level policies requiring the encryption of electronic data containing SSNs. Many agencies indicated in the survey that they were looking into encryption policies and purchasing software.

Few local governments surveyed by OREA have written policies addressing the confidentiality and protection of SSNs in their records. Of the few local agencies indicating the use of laptops, safeguards focused more on preventing laptop theft than protecting confidentiality of data.

Most state agencies (83 percent) responding to the OREA survey indicated that their agencies stored information containing SSNs on computer workstations in their offices. Over half of state agencies (57 percent) stored SSNs on laptop computers or other portable data devices. Only a few local offices surveyed indicated data storage on laptops or portable devices; however, over half indicated SSNs were stored on office computer work stations. Several state agencies indicated in the OREA survey that they were not aware whether lost or stolen laptops contained personal information.

Storing unencrypted personal information on individual computer workstations, laptops, or other portable storage devices may heighten the risk of

security breach. Storing sensitive data on secure servers and the use of encryption software can mitigate the risk of security breaches in the event of loss, theft, or other unauthorized access. The use of electronic logs that record access to files containing sensitive information may heighten accountability and aid efforts to recover lost or compromised data. Recent state legislation requiring state and local governments to create safeguards and procedures to protect data containing citizens' confidential information may aid in the development of additional policies.[51]

Only about half of the state agencies (51 percent) and few local offices responding to the OREA survey indicated they have a policy on handling security breaches involving SSNs. Tennessee's security breach law requires businesses and government entities to provide notification of unauthorized access to unencrypted data containing personal information, including a person's name in combination with SSN.[52] The notification must be made to all affected consumers or citizens. When a data breach involves more than 1,000 persons, all nationwide consumer reporting agencies and credit bureaus must also be notified.

The number of breaches included in the survey responses is fairly small given the millions of SSNs maintained by state and local agencies. Few Tennessee local governments reported security breach instances as part of this study. The Chief Information Security Officer at OIR indicated that the agency has not been informed of any large scale data security breaches in state government in the last few years.[53] Other outside organizations reported a few data breaches involving Tennessee governmental entities.[54]

Use of safeguards and management controls to protect SSNs in electronic and paper records varies.

Local offices reviewed by OREA varied in security practices to protect SSNs. Almost all agencies responding to the OREA survey indicated they maintain paper copies of records with SSNs. Although most indicated that these documents are stored in a secure location, several indicated that they are not. Most, but not all, local government agencies indicated they followed a secure disposal procedure, primarily shredding, for paper documents with SSNs. Few local government agencies reported storing SSNs on laptops or other data storage devices.

Most agencies did not indicate any safeguards to protect the exposure of the documents transmitted between governmental or other authorized agencies. Almost all state and local agencies responded that they send or receive documents with SSNs within or outside their agencies during the course of business. Most agencies receive or send paper documents through the U.S. mail. A large number also transmit such documents by fax. Several agencies indicate that many of these documents are hand-delivered to other agencies or sent through messenger or inter-office mail. Some methods agencies reported to help secure this information included:

- marking a letter or fax "confidential"
- using sealed envelopes
- maintaining limited access to or secure location of fax machines
- confirming that a fax is sent and received

Although most state agencies use secure systems to transmit SSNs electronically, only about 38 percent of state agencies transmitting information electronically indicated they use an additional

safeguard to encrypt the SSN. One agency has software designed to detect SSNs for encryption. Other agencies indicated that the transmission was only between secure servers, over dedicated or secured networks, or between systems with multiple firewalls. Some agencies use a secure web application with user identification or send password protected files. Only a few agencies reported restricting the SSN information by assigning a different ID number or including only a portion of the SSN. Two agencies did not indicate the means of protection used.

About 76 percent of responding state agencies indicated that they send or receive SSNs over the Internet. Most of the agencies indicated the information was transmitted through e-mail, many indicating the secure state e-mail system or through the state secure computer network. OIR provides the means to conduct secure transfer of data among state users. Most agencies, but not all, take advantage of the services offered including: secure e-mail to transfer encrypted forms and documents among state agencies; secure file servers, many maintained at the State Data Center; and protected web sites that allow data entry.

Few local offices indicated they encrypted SSNs transmitted electronically. About half of the local agencies surveyed indicated that SSNs are sent electronically**,** primarily to secure state and federal agency computer networks. Two county offices indicated they had software that checks for potential SSNs to encrypt.

Some methods state and local agencies reported using to protect disclosure of SSNs from electronic records included:

- excluding SSNs from printed electronic documents
- assigning a non-SSN identification number to include on ID cards and printed statements
- including only a portion of the SSN on printed documents
- excluding SSNs from identification cards
- excluding SSNs from files on public access data terminals

Tennessee law does not clearly direct local government record custodians on the treatment of SSNs in agency records.

The Tennessee Public Records Act provides citizens the right to inspect government records unless state law provides otherwise.[55] Tennessee state law prohibits the public disclosure of SSNs by state entities and defines the SSN as confidential when appearing in specific types of government and business records. Public access to SSNs in state agency records is restricted by a single statute. However, access to SSNs in local government records is restricted by numerous statutes applying to specific records types.

Local government records custodians seeking guidance on the legal status of SSNs may be confounded by the changing list of records-specific exceptions to the public records act appearing throughout *Tennessee Code Annotated*. The records management guide for county government officials published by the University of Tennessee County Technical Assistance Service further illustrates the confusing legal status of the SSN:

> Social Security Numbers (SSNs) have been a cause of concern and difficulty for many local government records custodians. The difficulty with SSNs is that they are confidential when held by certain government officials for certain purposes, but may not be confidential when part of a different record or kept by a different office, or collected in a different manner… Sorting out when and how these records may be accessed by the public is, to say the least, confusing.[56]

Responses to the OREA survey of local government officials reflect variation in the treatment of records containing SSNs. Several local government agencies with similar types of records indicated that they redacted SSNs prior to releasing records to the public while others did not do so.

Exhibit 7: Tennessee's Information Security Policies that Address Best Practices

Requires agencies to classify data on the state network as "personal or confidential records" as designated by state and federal law and that such data be protected from unauthorized disclosure, use, modification, or destruction (Policy #5)
Requires all computer users with access to state's computer network to sign acceptable use policy; details responsibilities to protect confidential information, prevent unauthorized access to the network, and report security breaches and other suspicious activity (Policy #6)
Physical and logistical control policies that limit placement of computer equipment to secure areas and require password use and other protections (Policy #7)
Agency requirements to maintain standard security procedures and sanitize all data storage devices before disposal (Policy #8)
Requires encryption of confidential data stored on computer workstations, laptops, or other portable data storage devices; prohibits the storage of confidential data on workstations, laptops, or portable data storage devices unless absolutely necessary (Policy #9)
Limits user access to the data needed to perform individual job duties; requires termination of access when users leave state employment (Policy #9)
Agency requirements to follow procedures in T.C.A. 47-18-107(3)(A) to notify affected parties in the event of a security breach involving personal information (Policy #11)

Source: Tennessee Department of Finance and Administration, Office for Information Resources, "Enterprise Information Security Policies," Version 1.6, April 2008.

State information security policies meet best practices, but agency compliance is unclear.

State agency information security policies address most of the security and management control best practices identified in research. The Information Systems Council's Enterprise Information Security (EIS) policies include several provisions that meet best practices to protect SSNs in electronic information systems. (See Exhibit 7.)

State government has not specifically evaluated state agency compliance with EIS policies. The statewide EIS policies give OIR in the Department of Finance and Administration authority to audit any device attached to the State of Tennessee network. However, OIR's use of this authority to test state agency compliance with EIS policies is limited. OIR established an information security internal audit and assessment program in October 2007 to audit EIS policies. Currently, the audit team is focused on the Department of Finance and Administration but plans to expand its scope to other departments as time and staffing permit. The OIR officer indicated that agencies vary in how well they follow the standards. Larger agencies that deal with extensive federal regulations including information security requirements tend to adhere more closely to the policies.[57]

In the course of their regular audits of state agencies, the Comptroller's Division of State Audit reviews general electronic information security based on industry "best practices." The procedures do not specifically look at compliance with OIR's Enterprise Information Security policy, but address many of the same issues. Additional audit work is performed if potential weaknesses are identified. State Audit annually reviews OIR's security as it relates to security for financial systems used to produce the State's Comprehensive Annual Financial Report (CAFR).[58]

Most of State Audit's information security audit findings in 2006 and 2007 relate to access to information systems and failure to terminate access when employees leave. The audit procedures do not specifically address personal information such as SSNs, although a finding for one state agency identified the protection of SSNs in the system developed and maintained by an outside contractor as a risk. In most cases, specific security problems cannot be detailed in published reports to protect the systems and data under question.[59]

State government provides limited oversight of local personal information protection practices.

Local agencies are not regularly and completely evaluated to determine potential risks of disclosure and compliance with security and management controls for personal information, such as SSNs. The Comptroller's Division of County Audit provides limited oversight of information security at the local level, but these audits focus more on risks to financial systems and do not specifically look at the protection of personal information. Few local offices contacted indicated they had written information security policies related to the protection of sensitive information such as SSNs.

The Division of County Audit looks at computer and system security policies as part of their regular information security system reviews of county governments. Their audit work focuses on financial systems and identifies any security concerns they discover. Specific security related findings are usually not included in published audit reports because they could provide the means for others to access confidential or sensitive data.[60]

A 2006 County Audit publication identifies some high risk areas involving technology in county governments that could affect personal data security and makes recommendations to address the weaknesses.[61] Some potential risks to personal information include:

- Hard drives/other media not properly destroyed when no longer in use
- Logical access controls were inadequate; some systems not password protected
- Controls over physical access to computers were inadequate; computers located in areas that are easily accessible to unauthorized individuals
- No security for wireless networks
- No controls over web-based applications
- Lack of disaster recovery plans

Municipal government agencies receive no state level oversight of their information security practices. The Division of Municipal Audit does not require a review of information security practices, including SSNs, as part of their financial audits. According to the Director of Municipal Audit, their audit focus is limited to the fair presentation of cities' financial statements.[62]

State law does not designate an agency to receive security breach notifications.

Tennessee's security breach law does not require public or private entities to notify a government agency of unauthorized access to computerized data containing personal information.[63] Without such a requirement, law enforcement and consumer protection agencies may be unprepared to assist consumers affected by a security breach. The lack of an agency notification requirement also leaves the state without data needed to guide the review of and implement changes to information security policies.

Recommendations

Legislative

The General Assembly may wish to appoint state and local government study committees to review government use and transmission of the SSN, the feasibility of further reductions of SSNs in government records, and confidential records statutes. Addressing the complex legal framework regulating government records and potential reductions in SSN use by government entities is beyond the scope of this study. Records custodians and experts in records management and information technology are best equipped to determine where collection and use of the SSN is necessary to conduct government business and potential consequences of restricting its use. Persons knowledgeable about records management issues can assist with any proposed changes to records law, and help determine where restrictions on SSN disclosure are impractical or unnecessary. For instance, where government records are archived on microfilm or microfiche, broad requirements to redact SSNs could be difficult, costly, and less effective than other security measures. The study committees could also provide recommendations to further safeguard the transmission of paper and electronic documents with SSNs.

Study committees appointed for this purpose may also include the recently created Advisory Committee on Open Government. The Advisory Committee on Open Government, in conjunction with the Comptroller's Office of Open Records Counsel, is authorized by statute to provide comments on proposed legislation concerning open records or open meetings.[64] Staff from the Comptroller's Offices of Research and Education Accountability and the Office of Open Records Counsel could provide support to such study committees and respond to specific research or legal questions as they arise.

As part of this directive, the General Assembly may consider requiring state and local agencies to compile an inventory of all electronic and paper files that include personal information such as SSNs. Such a listing would provide a means for each agency or office to review the need for the SSN and consider substituting another number. Agencies could submit records inventories to the study committees to assist the development of new guidelines or recommendations for records management and SSN use. Virginia passed legislation in 2008 requiring state agencies and municipalities to review collection and use of citizens' SSNs and explain why it is required or needed for agency function.[65] Three states have recently created task forces charged with identifying ways to reduce government collection and use of SSN or replacing the SSN with another identifier.[66]

The General Assembly may wish to require local governments to develop specific written policies on the protection of personal or confidential information, including SSNs, in all paper and electronic records. The required policies should address the following records management practices:

- release of public records with SSNs
- protection of SSNs from unauthorized disclosure
- classification of personal information contained in records in accordance with state and federal laws
- linking access to records containing SSNs to employees requiring access to fulfill their job duties

- adoption of a clean desk/work area requiring employees to secure access to records containing SSNs
- confidentiality agreements from employees dealing with personal information
- disposal of records containing SSNs
- actions to take when a SSN security breach is discovered

An appointed study committee of records custodians and other experts (as in the previous recommendation) could develop minimum standards and suggested policies for local governments to consider.

The General Assembly may wish to prohibit local government entities from publicly disclosing SSNs. A broad restriction against releasing SSNs in local government records would provide clear guidance to local government officials. A prohibition applying to local governments could resemble *Tennessee Code Annotated* 4-4-125, a law prohibiting state agencies from publicly disclosing SSNs. This law provides clear direction for records custodians while also allowing for any disclosures permitted by law or needed for agency function.[67] Florida, Georgia, and North Carolina specifically exempt the SSN and other personal information in state and local government records from the disclosure requirements of their respective public records laws.[68]

The General Assembly may wish to amend the security breach law to require that government agencies notify a specific entity of security breaches. The Division of Consumer Affairs in the Department of Commerce and Insurance provides citizens with consumer protection information, and may be an appropriate agency to receive security breach notification. Identity theft victims wishing to bring private action against those responsible are required by law to contact the division.[69] Notifying the division of security breaches may help the agency to assist affected citizens concerned about the potential for identity theft. A notification requirement would also permit the collection of security breach data to better prevent future breaches and help inform any future data security requirements.

The General Assembly may wish to require additional records management assistance and training resources for local government officials. In general, local government agencies must observe many of the same records management and security requirements as larger state agencies, often with less staff and fewer resources. Additional technical assistance may help local government agencies to secure sensitive personal information in records by supporting policy development, clarifying legal requirements regarding the treatment of records containing SSNs, and providing records management consulting. The Municipal Technical Advisory Service (MTAS), the County Technical Assistance Service (CTAS), the State of Tennessee Library and Archives, and the Comptroller's Office of Open Records Counsel support local governments and may be best suited to provide additional records management assistance.[70]

The General Assembly may wish to require additional oversight to ensure that state and local agencies have developed and implemented information security policies and practices to protect confidential information, including SSNs, maintained in their records. Some alternatives to consider include:

- Requiring the Office for Information Resources to audit compliance with the statewide policies to protect personal information in state information systems and to assist agencies in correcting deficiencies.

- Encouraging the Comptroller of the Treasury, Department of Audit, to more specifically review the protection of personal information as part of the regular audits of state, county, and municipal governments.

Administrative

State and local government agencies should continue to implement policies and practices to restrict the storage of SSNs and other personal information on portable data storage devices and computer work stations. If such storage is necessary, policies are needed to ensure personal information is protected through encryption or other appropriate means as required by Public Chapter 688 of 2008.

The Information Systems Council should consider requiring state agencies to report electronic data security breaches to the Office for Information Resources. The Enterprise Security Policies repeat the directive in the security breach law, but do not require state agencies to report breaches to OIR. Adding this requirement would provide additional oversight and aid the development of future security policies. OIR could also provide technical assistance to address the reasons for the security breach.

Local governments should develop written security breach procedures. Without written policies, local government records custodians lack specific guidance to comply with Tennessee's security breach law.

ENDNOTES

[1] OREA surveyed officials in Fentress, Giles, Hamilton, Knox, Madison, Rutherford, Shelby, Sullivan, and Weakley Counties.

[2] U.S. General Accounting Office, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, (Washington, D.C., 2002) pp. 6-7.

[3] U.S. Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, "The Social Security Number as a Standard Universal Identifier," (Cambridge, MA: MIT Press, 1973) accessed December 15, 2007, http://aspe.hhs.gov.

[4] For more about private sector requirements to collect the SSN see U.S. Federal Trade Commission, Bureau of Consumer Protection, Division of Privacy and Identity Protection, *Staff Summary of Comments and Information Received Regarding the Private Sector's Use of Social Security Numbers*, "Appendix," (Washington, D.C., 2007) accessed August 29, 2008, http://www.ftc.gov.

[5] 42 U.S.C. § 666(a)(13).

[6] Tenn. Code Ann. § 36-5-711; Tenn. Code Ann. § 36-5-713.

[7] 42 U.S.C. § 653a(h); 42 U.S.C. § 653a(b)(1)(A).

[8] 24 C.F.R. § 5.210(a); 42 U.S.C § 1320b-7(a)(1).

[9] Limitations in the survey may have underestimated this number. Eighteen state agencies reported over one million SSNs in their records, the highest possible response category.

[10] Tenn. Code Ann. §§ 10-7-503–504.

[11] Telephone interview with Brenda Boatman, Records Officer, Tennessee Department of Human Resources, January 7, 2008.

[12] Tennessee Department of Finance and Administration, Office for Information Resources, "Enterprise Information Security Policies," Version 1.6, April 2008, accessed August 27, 2008, http://state.tn.us/finance/oir/security/.

[13] Tenn. Code Ann. §§ 4-3-5501 & 5502.

[14] Interview with Kandi Thomas, Assistant Director, Division of State Audit, Tennessee Comptroller of the Treasury, January 16, 2008.

[15] Tenn. Code Ann. § 47-18-2107(h).

[16] 16 C.F.R. § 603.2.

[17] U.S. General Accounting Office, *Identity Theft: Prevalence and Cost Appear to be Growing*, (Washington, D.C., 2002) accessed December 14, 2007, http://www.gao.gov.

[18] U.S. General Accounting Office, *Identity Theft: Greater Awareness and Use of Existing Data Are Needed*, (Washington, D.C., 2002) accessed April 1, 2008, http://www.gao.gov.

[19] Tenn. Code Ann. § 39-14-150(i).

[20] Tennessee Administrative Office of the Courts, special report produced for OREA from the "Felony Judgment Database," April 29, 2008.

[21] U.S. Federal Trade Commission, *National and State Trends in Fraud and Identity Theft*, (Washington, D.C., 2005) accessed December 18, 2007, http://www.consumer.gov.

[22] This figure may not include "synthetic ID theft" where someone creates a fictitious identity combining real and contrived information of one or more consumers rather than using the identity of a single individual.

[23] Synovate and U.S. Federal Trade Commission, *Federal Trade Commission 2006 Identity Theft Survey Report*, (McLean, VA, 2007) accessed April 25, 2008, http://www.ftc.gov.

[24] "U.S. Identity Theft Losses Fall: Study," Javelin Strategy Group, February 1, 2007, accessed June 19, 2008, http://www.javelinstrategy.com; "Identity Theft is Dropping According to New Research," Javelin Strategy Group, February 1, 2007, accessed June 19, 2008, http://www.javelinstrategy.com.

[25] "Zogby Poll: Most Americans Worried about Identity Theft," Zogby International, April 3, 2007, accessed April 16, 2008, http://www.zogby.com.

[26] Tenn. Code Ann. § 47-18-2107(a)(1).

[27] "State Security Breach Notification Laws," National Conference of State Legislatures, accessed May 7, 2008, http://www.ncsl.org.

[28] N.H. Rev. Stat. Ann. § 359-C19; S.C. Code Ann. § 1-11-490; Haw. Rev. Stat. § 487N-1; 815 Ill. Comp. Stat. 530; Va. Code Ann. § 18.2-186.6; W. Va.Code § 46A-2A-102; Conn. Gen. Stat. § 36a-701b; Ark. Code Ann. § 4-110-105.

[29] Identity Theft Resource Center, "2007 Data Breach Stats," February 26, 2008, accessed April 29, 2008, http://idtheftmostwanted.org.

[30] For trend data, see Identity Theft Resource Center previous years' Breach List and Breach Stats Reports, http://idtheftmostwanted.org.

[31] Office of Management and Budget, *Fiscal Year 2007 Report to Congress on Implementation of the Federal Information Security Management Act of 2002*, March 1, 2008, accessed September 17, 2008, http://www.whitehouse.gov/omb.

[32] Courtney Mabeus, "OMB Reports Big Increase in Data Breaches in 2007," Federaltimes.com, March 1, 2008, accessed March 5, 2008, http://federaltimes.com.

[33] U.S. Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, (Washington, D.C., 2007) accessed April 17, 2008, http://www.gao.gov.

[34] Charles Booth, "Disk Found in Stolen Laptop," *The Tennessean*, January 28, 2008.

[35] Tennessee Comptroller of the Treasury, Division of County Audit, "Limited Review of Information System Controls – The Election Commission of the Metropolitan Government of Nashville and Davidson County, Tennessee," May, 2008.

[36] Sandy Cole, "Metro Redesigning Information Data and Will Regain Voter Confidence," *The Tennessean*, January 15, 2008; Sheila Wissner, "Password on Stolen Laptop Had Been Changed," *The Tennessean*, January 15, 2008.

[37] Analysis of information from Identity Theft Resource Center 2007 Data Breach List accessed April 29, 2008, http://www.idtheftcenter.org.

[38] Williamson County Schools, "Q&A Regarding Notice of Security Breach," July 16, 2008, accessed July 29, 2008, http://www.wcs.edu.

[39] Analysis of information from Identity Theft Resource Center 2008 Data Breach List accessed July 28, 2008, http://www.idtheftcenter.org.

[40] Tenn. Code Ann. § 10-7-515.

[41] Tenn. Code Ann. § 49-6-5102; Tenn. Code Ann. § 49-6-5103.

[42] Tenn. Code Ann. § 36-4-106; Tenn. Code Ann. § 36-5-101(2)(B)(i)(b).

[43] Melissa Apple, Project Edison Consultant, Tennessee Department of Finance and Administration, ERP Division, "Edison SSN Reduction," E-mail to the author, April 11, 2008.

[44] The University of Tennessee, "Graduate School Policies," accessed June 20, 2008, http://gradschool.utk.edu; Colby Sledge, "Hand Scans Added to MTSU's ID System," *The Tennessean*, July 20, 2008.

[45] Telephone interviews with Tom Danford, Chief Information Officer, Tennessee Board of Regents, March 11, 2008 and September 17, 2008.

[46] VA Chapter 840 (2008). Some provisions not in effect until July 1, 2009.

[47] IL Public Act 95-0482 (2007) created the Social Security Task Force; CA Public Chapter 627 (2007) created a task force in the Office of Privacy Protection, Division of Consumer Affairs; HI Act 140 (2006) created the Identity Theft Task Force.

[48] Va. Code Ann. § 2.2-3808(A); N.C. Gen. Stat. § 132-1.10 (b)(1); S.C. Code Ann. 30-2-310 (a); Fla. Stat. Ann. § 119.071(5)(2)(a).

[49] Tenn. Code Ann § 10-7-504(b); Tenn. Code Ann. § 47-18-2107.

[50] Tennessee Department of Finance and Administration, Office for Information Resources, "Enterprise Information Security Policies," Version 1.6, April 2008, accessed August 27, 2008, http://www.state.tn.us/finance/oir/security.

[51] Public Chapter 688 (2008).

[52] Tenn. Code Ann. § 47-18-2107.

[53] Interview with Jason Gunnoe, Chief Information Security Officer, Office for Information Resources, Tennessee Department of Finance and Administration, January 9, 2008.

[54] Identity Theft Resource Center, "2007 Data Breach Stats," February 26, 2008, accessed April 29, 2008, http://idtheftmostwanted.org.

[55] Court decisions have affirmed this construction of the law, ruling that the act creates a "presumption of openness" with government records unless the law states otherwise. See *Memphis Publishing Co. v. City of Memphis*, 871 S.W.2d 681.

[56] University of Tennessee County Technical Assistance Service, "Records Management for County Governments," (Knoxville, TN, 2005), p. 28, accessed June 15, 2008, http://www.ctas.tennessee.edu.

[57] Interview with Jason Gunnoe, Chief Information Security Officer, Office for Information Resources, Tennessee Department of Finance and Administration, January 9, 2008.

[58] Interview with Kandi Thomas, Assistant Director, Division of State Audit, Tennessee Comptroller of the Treasury, January 16, 2008.

[59] Tenn. Code Ann. § 10-7-504(i); Interview with Kandi Thomas, Assistant Director, Division of State Audit, Tennessee Comptroller of the Treasury, January 16, 2008, and OREA review of 2007 Division of State Audit's financial and compliance audits with system findings.

[60] Interview with Penny Austin, Assistant Director, Division of County Audit, Tennessee Comptroller of the Treasury, April 16, 2008.

[61] Tennessee Comptroller of the Treasury, Division of County Audit, "High Risk Areas Involving Technology in County Government," accessed April 8, 2008, http://www.comptroller1.state.tn.us/RA_CA/ManualsGuidance.asp.

[62] Interview with Dennis Dycus, Director, Division of Municipal Audit, Tennessee Comptroller of the Treasury, April 24, 2008.

[63] Tenn. Code Ann. § 47-18-2107.

[64] Public Chapter 1179 (2008).

[65] VA Chapter 840 (2008).

[66] IL Public Act 95-0482 (2007) created the Social Security Task Force; CA Public Chapter 627 (2007) created a task force in the Office of Privacy Protection, Division of Consumer Affairs; HI Act 140 (2006) created the Identity Theft Task Force.

[67] Tenn. Code Ann. § 4-4-125.

[68] Fla. Stat. Ann. § 119.0721; Ga. Code Ann. § 50-18-72(a)(11.3)(A); N.C. Gen. Stat. § 132.1.10.

[69] Tenn. Code Ann. § 47-18-2104.

[70] Specific statutory responsibilities for these agencies are spread throughout *Tennessee Code Annotated*. Examples include Tenn. Code Ann. § 6-54-123 (MTAS); Tenn. Code Ann. § 10-7-404(b) (CTAS); Tenn. Code Ann. § 10-7-404(b) (Tennessee State Library and Archives); Public Chapter 1179 (2008) (Comptroller's Office of Open Records Counsel).

APPENDIX A: AUTHORIZING LEGISLATION

Public Acts, 2007
Public Chapter 170

SECTION 6.

(f) The comptroller of the treasury shall review current state and local government policies and practices as they relate to protecting social security numbers from disclosure to the public, and provide appropriate recommendations to the general assembly by February 1, 2008.

APPENDIX B: PERSONS CONTACTED

Melissa Apple, System Consultant
Enterprise Resource Planning
Tennessee Department of Finance and Administration

Penny Austin, Assistant Director
Information Systems
Division of County Audit
Tennessee Comptroller of the Treasury

Lily Barnes
Hardeman County Register of Deeds

Cindy Benefield
Lawrence County Trustee

Donna Bridges, Director
Records Management Division
Tennessee Department of General Services

Patricia Burke
Administration Support Assistant
UT County Technical Assistance Service

Mary Clement, Director
Division of Consumer Affairs, Tennessee Department of Commerce and Insurance

David Connor, Executive Director
Tennessee County Commissioners Association

David Davenport
Jefferson County Sheriff

Dennis Dycus, Director
Division of Municipal Audit
Tennessee Comptroller of the Treasury

Daphne Fagen
Marshall County Clerk

John Fergusson, System Consultant
Enterprise Resource Planning
Tennessee Department of Finance and Administration

Jason Gunnoe
Chief Information Security Officer
Office for Information Resources
Tennessee Department of Finance and Administration

Mahalia Hughes
Sumner County Circuit Court Clerk

Libby McCroskey
Senior Legal Consultant
UT County Technical Assistance Service

Dr. Wayne Moore, Director
Local Government Archives Development Program, Tennessee Library and Archives

Marie Murphy, Executive Director
County Officials Association of Tennessee

Beth Pendergrass, Manager
Information Systems, Division of State Audit,
Tennessee Comptroller of the Treasury

Beverly Rowe
Records Clerk, Dickson Police Department

Kandi Thomas, Assistant Director
Division of State Audit
Tennessee Comptroller of the Treasury

E. Ross White, Assistant Director
Division of Consumer Affairs, Tennessee Department of Commerce and Insurance

Karen Yacuzzo
Tennessee Administrative Office of the Courts

APPENDIX C: RESPONSE LETTER FROM THE OFFICE FOR INFORMATION RESOURCES

STATE OF TENNESSEE
DEPARTMENT OF FINANCE AND ADMINISTRATION
OFFICE FOR INFORMATION RESOURCES
312 ROSA L. PARKS AVENUE
SUITE 1600, TENNESSEE TOWER
NASHVILLE, TENNESSEE 37243-1102
(615) 741-3700
FAX (615) 532-0471

DAVE GOETZ
COMMISSIONER

MARK BENGEL
CHIEF INFORMATION OFFICER

MEMORANDUM

TO: Phillip Doss, Director

FROM: Mark Bengel, CIO

SUBJECT: "Safeguarding Social Security Numbers" report

DATE: October 1, 2008

Thank you for including the Office for Information Resources (OIR) in your study on "Safeguarding Social Security Numbers in Tennessee Government Records." We concur with the recommendations within the report. We take the protection of confidential State government data very seriously.

To that end, we would like to highlight some of the initiatives that are in place to protect confidential data such as citizens' social security numbers.

OIR has implemented an information security program to help address many of the issues this report identifies. This program has published policies that directly apply to the protection of social security numbers. The policies can be found on the State's web site:

http://www.state.tn.us/finance/oir/security/secpolicy.html

Beginning in October 2007, OIR began an internal audit and assessment program. The main goal of this program is to ensure the State's information resources are adequately protected through testing and inspection of internal controls.

Finally, the State also supports the education and awareness of information security risks using various media and training resources. Many agencies take advantage of these

efforts to promote information security safeguards, such as confidential data usage and protection, within the agency.

Safeguarding Tennessee state government records is a continuous process and is of utmost importance to our division.

cc: Jason Gunnoe
Chief Information Security Officer

Jamie Etheridge
Deputy Chief Information Officer

APPENDIX D: SURVEY TO STATE AGENCIES

Questionnaire Response For:		
Agency Name:	Division:	Date:
Contact Name:	Contact Telephone No.	Contact Email:

Questionnaire Completed for:
☐ Entire Agency
☐ Agency Subpart (other agency units completed separately)

1	**Inventory of Documents/Records Containing Social Security Numbers**
1a	What is the estimated number of individual Social Security numbers contained in records maintained by your agency? Note: This estimate should include the total number of non-redundant Social Security numbers contained in electronic and paper records maintained by your agency. ☐ None ☐ 1 – 100 ☐ 101 – 1,000 ☐ 1,001 – 10,000 ☐ 10,001 – 100,000 ☐ 100,001 – 500,000 ☐ 501,000 – 1,000,000 ☐ 1,000,001 or more
	If your answer to question 1a was "none," please stop here and return the survey.
1b	List all types of documents/records (paper and electronic) containing Social Security numbers (e.g. applications, medical records, employee/student/client files, licenses, tax, property, judicial/law enforcement, etc.) that are handled, processed, or maintained within your agency or department.
1c	What are the primary uses or purposes for including the Social Security number in each document or record listed above (e.g. benefit eligibility determinations, records management, research, law enforcement, program delivery, identification, etc.)?
1d	What is the estimated annual growth of individual Social Security numbers contained in agency records or documents? ☐ None ☐ 1% – 5% ☐ 6% – 10% ☐ 11% – 25% ☐ 26% – 50% ☐ 51% – 75% ☐ 76% – 100% ☐ 100% or more

	Questions	Yes	No	Comments
2	**Records Handling Practices**			
2a	Do any of your agency records or documents that are open for public inspection include individual Social Security numbers?			If "yes," please describe the circumstances. If "no," **skip to question 2c.**
2b	Does your agency remove or otherwise conceal individual Social Security numbers that are contained in records (electronic or paper) before making them available for public inspection?			If "yes," please describe the circumstance (record being released to public, etc.) and the methods used to remove or conceal Social Security numbers.
2c	When collecting Social Security numbers, does your agency notify individuals of the purpose for collecting the number, how the number will be used or shared, or the measures in place to protect the number from disclosure?			If "yes," please describe the information provided.

	Paper Records			
2d	Does your agency collect or maintain paper documents containing Social Security numbers for any reason?			If "no," please **skip to question 2h.**
2e	Are these documents located in a secure location?			If "yes," please describe the safeguards to protect the documents.
2f	Does your agency follow a disposal procedure for paper documents containing Social Security numbers?			If "yes," please describe the procedure.
2g	Does your agency send or receive any paper records or documents containing individual Social Security numbers within or outside your agency?			If "yes," please describe the means of transmission (fax, U.S. mail, inter office communications, etc.) and the safeguards to protect the privacy of the numbers.
	Electronic Records			
2h	Does your agency send or receive individual Social Security number(s) over the internet for any purpose?			If "yes," please describe the safeguards to protect the privacy of the numbers.
2i	Does your agency store information containing Social Security numbers on laptops or other portable data storage devices?			If "yes," please describe the circumstances and any safeguards in place.
2j	Does your agency store electronic data containing Social Security numbers on computer workstations located in the office?			If "yes," please describe the circumstances and any safeguards in place.
	Questions	**Yes**	**No**	**Comments**
3	**Agency Policies**			
3a	Are there agency policies or procedures about handling, maintenance, and disclosure of records or documents containing Social Security numbers?			If "yes," please reference or describe the policies or procedures.
3b	Are there agency policies or procedures requiring that documents or records containing Social Security numbers are maintained in a secure environment with specification on security measures required?			If "yes," please reference or describe the policies or procedures.
3c	Are there agency polices or procedures requiring the encryption of electronic data containing Social Security numbers?			If "yes," please describe or reference the policies or procedures.

3d	Are there policies requiring all employees to sign confidentiality agreements that apply to sensitive or personal information that they may use or disclose as part of their job?			If "yes," please reference or describe the policies or procedures.
3e	Are there agency policies or procedures limiting access to records or documents containing Social Security numbers to those employees whose duties require access to those records?			If "yes," please reference or describe the policies or procedures.
3f	Are there agency policies or procedures on training for employees on the appropriate use and disclosure of Social Security numbers?			If "yes," please reference or describe the policies or procedures.
3g	Are there agency policies or procedures limiting disclosure of records containing Social Security numbers to those instances where it is necessary for carrying out agency business?			If "yes," please reference or describe the policies or procedures.
3h	Are there agency policies or procedures that specify the methods for disposal of records or documents containing Social Security numbers?			If "yes," please reference or describe the policies or procedures.
	Questions	**Yes**	**No**	**Comments**
3i	Are there agency policies or procedures to ensure that employee access to documents or electronic data with Social Security numbers is terminated when an employee leaves the agency?			If "yes," please reference or describe the policies or procedures.
3j	Are there agency policies or procedures on handling security breaches involving Social Security numbers?			If "yes," please reference or describe the policies or procedures.
3k	Does your agency have any contracts/agreements for services with organizations that are given access to Social Security numbers collected by the agency?			If "yes," please reference or describe the contract specifications for the protections of social security numbers.
4	**Security Breaches**			
4a	Are you aware of any instances of theft or unintentional public release of Social Security numbers from your agency or contractors since 2000?			If "yes," please describe and indicate the action taken.

APPENDIX E: SURVEY TO LOCAL AGENCIES

Questionnaire Response For:		
Office:	City/County Name:	Contact Name:
Job Title:	Contact Telephone No.	Contact Email:

1	**Inventory of Documents/Records Containing Social Security Numbers**
1a	What is the estimated number of individual Social Security numbers contained in records maintained by your office? Note: This estimate should include the total number of individual Social Security numbers (SSN) contained in electronic and paper records maintained by your agency. The same SSN contained on multiple documents counts as one number. ☐ None ☐ 1 – 100 ☐ 101 – 1,000 ☐ 1,001 – 10,000 ☐ 10,001 – 100,000 ☐ 100,001 – 500,000 ☐ 501,000 – 1,000,000 ☐ 1,000,001 or more
	If your answer to question 1a was "none", please stop here and return the survey
1b	List all types of documents/records (paper and electronic) containing Social Security numbers (e.g. applications, medical records, employee/student/client files, licenses, tax, property, judicial/law enforcement, etc.) that are handled, processed, or maintained within your office.
1c	What are the primary uses or purposes for including the Social Security number in each document or record listed above (e.g. benefit eligibility determinations, records management, research, law enforcement, program delivery, identification, etc.)? For records unrelated to personnel and payroll management, please explain why the Social Security number is needed.
1e	What is the estimated annual growth of individual Social Security numbers contained in office records or documents? ☐ None ☐ 1% – 5% ☐ 6% – 10% ☐ 11% – 25% ☐ 26% – 50% ☐ 51% – 75% ☐ 76% – 100% ☐ 100% or more

	Questions	**Yes**	**No**	**Comments**
2	**Records Handling Practices**			
2a	Do any documents or records contained in your office open for public inspection include individual Social Security numbers?			If "yes," please describe the circumstances. If no, **skip to question 2c.**
2b	Does your office remove or otherwise conceal individual Social Security numbers that are contained in records (electronic or paper) before making them available for public inspection?			If "yes," please describe the circumstance (record being released to public, etc.) and the methods used to remove or conceal Social Security numbers.
2c	When collecting Social Security numbers, does your office notify individuals of the purpose for collecting the number, how the number will be used or shared, or the measures in place to protect the number from disclosure?			If "yes," please describe the information provided.

2d	Does your office send or receive any records or documents containing individual Social Security numbers within or outside your agency?			If "yes," please describe the means of transmission (fax, U.S. mail, inter office communications, etc.) and the safeguards to protect the privacy of the numbers.
	Paper Records			
2e	Does your agency collect or maintain paper documents containing Social Security numbers for any reason?			If "no," please **skip to question 2h.**
2f	Are these documents located in a secure location?			If "yes," please describe the safeguards to protect the documents.
2g	Does your office follow a disposal procedure for paper documents containing Social Security numbers?			If "yes," please describe the procedure.
	Electronic Records			
2h	Does your office transmit or receive individual Social Security number(s) over the internet for any purpose?			If "yes," please describe the safeguards to protect the privacy of the numbers.
2i	Does your office store information containing Social Security numbers on laptops or other portable data storage devices?			If "yes," please describe the circumstances and any safeguards in place.
2j	Does your office store electronic data containing Social Security numbers on computer workstations located in the office?			If "yes," please describe the circumstances and any safeguards in place.
Questions		**Yes**	**No**	**Comments**
3	**Office Policies**			
3a	Does your office have written policies regarding the release of records or documents containing Social Security numbers contained in public records?			If "yes," please attach the policies.
3b	Does your office have written policies to protect Social Security numbers contained in agency records systems from unauthorized public disclosure? Please include written policies pertaining to the security of paper and electronic records containing SSN.			If "yes," please attach the policies.

3c	Does your office have written policies requiring all employees to sign confidentiality agreements that apply to sensitive or personal information that they may use or disclose as part of their job?			If "yes," please attach a copy of the confidentiality agreement.
3d	Does your office have a written policy which specifies the methods for disposal of records or documents containing Social Security numbers?			If "yes," please attach the policies.
4	**Security Breaches**	**Yes**	**No**	**Comments**
4a	Does your office follow any written policy or law regarding security breaches involving Social Security numbers?			If "yes," please attach the policies and/or reference the law.
4b	Does your office have any contracts/agreements for services with organizations that are given access to Social Security numbers collected by the agency?			If "yes," please reference or describe the contract specifications for the protections of social security numbers.
4	**Security Breaches**			
4c	Are you aware of any instances of theft or unintentional public release of Social Security numbers from either your office or contractors providing services to your office since 2000?			If "yes," please describe and indicate the action taken.

Offices of Research and Education Accountability Staff

Director

♦Phillip Doss

Assistant Director
(Research)

♦Douglas Wright

Assistant Director
(Education Accountability)

Russell Moore

Principal Legislative Research Analysts

♦Erin Do
Jessica Gibson
♦Kim Potts

Senior Legislative Research Analysts

Katie Cour
♦Susan Mattson

Associate Legislative Research Analysts

Keith Boring
Nneka Gordon
♦Patrick Hultman
♦Cara Huwieler
♦Angela Mullin-Jackson
Regina Riley

Legislative Research Intern

Joseph Woodson

Executive Secretary

♦Sherrill Murrell

♦indicates staff who assisted with this project

To conserve natural and financial resources, we are producing fewer printed copies of our publications. Please consider accessing this and other OREA reports online at http://comptroller.state.tn.us/cpdivorea.htm.

The Offices of Research and Education Accountability provide non-partisan, objective analysis of policy issues for the Comptroller of the Treasury, the General Assembly, other state agencies, and the public.

The Office of Research provides the legislature with an independent means to evaluate state and local government issues. The office assists the Comptroller with preparation of fiscal note support forms for the Fiscal Review Committee, monitors legislation, and analyzes the budget.

The Office of Education Accountability monitors the performance of Tennessee's elementary and secondary school systems and provides the legislature with an independent means to evaluate the impact of state policy on the public education system.

Offices of Research and Education Accountability
Suite 1700, James K. Polk Building
505 Deaderick Street
Nashville, TN 37243-0268
615-401-7911
http://comptroller.state.tn.us/cpdivorea.htm