



STATE OF TENNESSEE
DEPARTMENT OF LABOR AND WORKFORCE DEVELOPMENT
DIVISION OF WORKFORCE DEVELOPMENT
220 French Landing Drive
Nashville, TN 37243-1002
(615) 741-1031

January 20, 2012

Workforce Investment Act Memorandum Number 12-49

Topic: Information Security

Subject: Safeguarding Individual Information

Purpose: To notify staff of the procedures and operations processes needed to ensure the safeguard and management control of individual identifiers.

References: Privacy Act of 1974, P.L. 93-579; Freedom of Information Act of 1966, 5 U.S.C. § 552; Social Security Amendments of 1990, P.L.101-508; Workforce Investment Act of 1998, 29 U.S.C. § 2935; Policy for Collection and Use of Workforce System Participants' Social Security Numbers, TEGL 5-08; Acceptable Use, T.C.A. Dissemination of Social Security Numbers, T.C.A. § 4-4-125(a)(b); Confidential Records, T.C.A. §10-7-504; Identity Theft Deterrence, T.C.A. §10-7-5; Consumer Protection, T.C.A. § 47-18; Voter Registration Forms, T.C.A. § 2-2-127; SSN Redaction, T.C.A. § 10-7-515; Divorce & Annulment Forms, T.C.A. § 36-4-106; Alimony & Child Support Forms, T.C.A. § 36-5-101; Motor Vehicle Records, T.C.A. § 55-25-104; "Safeguarding Social Security Numbers in Tennessee Government Records," Tennessee Comptroller of the Treasury, October 2008; State of Tennessee, Office of Information Resources, Enterprise Information Security Policies, Document Version 1.5, January 8, 2008.

Background: Individual identifiers in local workforce development programs have been used as a means to track workers' earnings and eligibility since the inception of the Workforce Investment Act (WIA) of 1998. And over the years, the Social Security Number (SSN) has been the de facto identifier used by workforce agencies to comply with ETA's requirement that we use SSNs to match a program participant's records with that individual's quarterly wage record information. While the laws and regulations require the use of SSNs, they generally impose limitations on how they can be used. Some laws and regulations govern the disclosure and use of SSNs, while others establish information security programs that protect sensitive personal information; in both cases, however, there are limitations regarding the storage, sharing, and destruction of SSNs. For instance, Section 7(b) of the Privacy Act states that any federal, state or local

government agency that requests an individual to disclose an SSN shall inform that individual whether the disclosure is mandatory or voluntary, by what statutory or other authority such a number is solicited, and what uses will be made of it. Under WIA 1998, the disclosure of an SSN is voluntary; but when SSNs are provided and documented, Tennessee law prohibits the public disclosure of the SSNs without valid permission. Tennessee law then requires the establishment of safeguards and management controls for the storage, sharing, and destruction of SSNs in an organization's electronic and paper records. Local Workforce Investment Areas (LWIA), as well as associated contractors and vendors, need to review their safeguards and management controls in the light of this policy.

Instructions:

Controls and Safeguards for Paper Documents

LWIAs and their associated contractors and vendors collect SSNs in several areas of their work. Whether photocopied or original, SSNs are collected on standard service applications, eligibility certifications, various identity and employment eligibility forms, support service request forms, activity tracking forms, training application forms, assessment tests, partner agency screen shots, letters from employers and government agencies, among several others. In addition, the following table displays a list of common records in Tennessee which often do contain SSNs. This table is not exhaustive of all paper forms in Tennessee which may contain SSNs, and the content of this table is subject to change:

License Applications	Voter Registration	Benefit & Entitlement Forms	Motor Vehicle Records	Vital Records
Court Records	Law Enforcement Records	Education Records	Personnel Records	Military Records

One effective management control of these documents is to develop a written policy regarding how best to collect, store, and dispose of SSNs; and how best to safeguard and prevent unlawful disclosure of SSNs, in accordance with the law. The LWIAs, contractors and vendors are strongly encouraged to develop such policies, and conduct regular training for staff and audits regarding how to implement the policies in the workplace. The policy needs to identify specifically who oversees the controls and safeguards, how unlawful, accidental, unintentional, or related collections and disclosures of SSNs are to be reported, and have detailed corrective action steps. Overall, the policy needs to address the process of authorized release of public records with SSNs, actions to be taken when an SSN security breach is discovered, the protection of SSNs from unauthorized disclosure, confidentiality agreements with employees, and the disposal of records that contain SSNs.

An effective method of controlling and securing confidential information is to implement business practices that decrease the unnecessary use and collection of SSNs. To this end, organizations need to create and keep a list of all documents which contain sensitive and/or confidential identifiers; associate the documents

with the laws regarding confidentiality and lawful disclosure, and determine whether a substitute identifier will suffice. If so, then the procedure for using substitute identifiers can be described in the policy. Other methods of limiting the collection and disclosure of SSNs are to identify the laws governing collection and disclosure, and restrict collection and disclosure only to those documents required by law and necessary to the organization's functions. The items cited in the 'References' section of this policy should be helpful toward improving and establishing procedural safeguards over a wide range of documents containing SSNs and other sensitive individual identifiers. For example, Dissemination of Social Security Numbers, T.C.A. § 4-4-125(a)(b), prohibits posting or publicly displaying SSNs, printing an SSN on anything mailed to a customer unless required by law or the document is a form or application, storing of SSNs in unlocked cabinets, and posting voice mail messages containing SSNs.

Restricting access to documents containing SSNs also is an effective control over specifically how SSNs may be shared. Local areas, contractors and vendors can limit access to these documents to only those employees who need the SSNs in their job duties. It is helpful to start this process by classifying the documents according to levels of confidentiality and sensitivity of the information they contain. This method also helps to safeguard that SSNs are shared only when necessary for work duties, and when vital to the organization's business. It also is vital that participants and staff should know the purpose of the SSN collection, what it is intended to be used for, the legal justification for the collection of SSNs, and the consequences of not providing the SSN.

Regarding the disposal of SSNs in documents no longer required to be kept, shredding is the preferred method. Further, LWIAs, contractors and vendors should note that all such documents containing personal identifiers, including SSNs, must be kept in a secure manner even when employees in custody are away from their work area. The preference is that the documents should be kept in locked cabinets or locked workspaces at all times, when not in use for the performance of job duties. The display of SSNs on desks and generally in workstations also should be restricted, and documents that contain SSNs used in the regular course of work should be shredded or locked in metal file cabinets, and not made available to the casual observation of individuals who may walk by or visit the work area.

Controls and Safeguards for Electronic Documents

In addition to the safeguards and controls for paper documents, information security policies at LWIAs, contractors and vendors, need also to cover automated and electronic records. Local areas, contractors and vendors need to establish in the policies administrative, technical, physical, and security safeguards for individual identifiers in automated environments.

The following table displays a list of common automated and electronic record types in Tennessee which often do contain SSNs. This table is not exhaustive of all automated and electronic records in Tennessee which may contain SSNs, and the content of this table is subject to change:

Input and Output Documents	Reports	Punched Cards	Magnetic Tapes
Disks	OnLine Computer Storage	Mobile Disks	PDA Hard Drives and PDA Cards

At a minimum, the safeguards must be sufficient to 1) prevent careless, accidental, or unintentional disclosure, modification, or destruction of SSNs; 2) minimize the risk that skilled technicians or knowledgeable persons could improperly obtain access to, modify, or destroy SSNs; 3) prevent casual entry by unskilled persons who have no official reason for access to SSNs; 4) minimize the risk of an unauthorized disclosure of SSNs during testing of computer programs; 5) control the flow of data into, through, and from the organization's computers; 6) protect against environmental hazards; 7) have adequate internal controls so that the disposal of automated files with SSNs is accomplished in such a manner as to make the SSNs unobtainable to unauthorized personnel. The state's Enterprise Information Security policies require confidential data authorized for mobile or workstation use to be encrypted, and Dissemination of Social Security Numbers, T.C.A. § 4-4-125(a)(b) prohibits the transmission of SSNs over the internet unless the connection is secure or the number encrypted, and the transmission of SSNs by email message or email message attachment unless the site is secured or the number encrypted.

One good method to implement these safeguards is to increase the security of electronic records systems by first storing the SSNs on secure servers, use advanced technical controls such as encryption, password protections, and secure internet connections to store, share, or transmit files containing SSNs. Effective ways to enhance these safeguards is to prohibit the unnecessary saving of SSNs on laptops or other mobile devices such as flash drives or personal digital assistants (PDA). Further, it is important to inventory and track electronic files containing SSNs, and classify electronic records according to levels of confidentiality and sensitivity of the information they contain, such as SSNs. The state's secure email system is an example of controls and safeguards for the transfer of individual identifiers through one of two, or more, secure email servers available to GroupWise account holders. The servers are available to account holders. The recipient can receive and view the messages in one of two ways. First, and so long as the recipient's email system has certain security functions enabled, the recipient receives the secure message in the recipient's own email client, and can view the message and attachments directly. If the recipient's email system does not have TLS or SSL enabled, the secure message is transferred through the second of the two secure servers, which then sends a text message and html link to the recipient's email client, with notification the secure message can be retrieved through the link. Provided the recipient has requested and received

proxy email credentials from information technology authorities, the text message then makes the link active, and the recipient can select the link and access the web based email system in the server, then view the secure email and attachments.

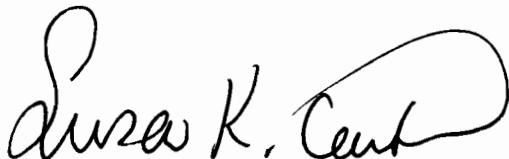
Another method to secure electronic files containing SSNs is to decrease the use of participant SSNs in online computer displays and archives. The state's DolceVita performance reporting system is an example of how security can be enhanced, by removing all SSNs from the display of WIA participant identifiers, and instead substituting equally effective individual identifiers. Our Case Management and Activity Tracking System (eCMATS) also has logical access controls which are password protected, and now housed on secure servers at the Office of Information Resources (OIR).

Additional steps need to be documented in policy and implemented regarding the disposal of electronic versions of files containing SSNs. Hard drives and other computer media products containing SSNs and other confidential data need to be disposed in a manner so that any confidential data possibly contained on the media, including SSNs, should be unobtainable to unauthorized personnel.

Contact: For questions regarding the WIA Title 1 program, please contact Dan Holton, WIA Program Manager, at 615-741-5326 or dan.holton@tn.gov.

Effective Date: January 20, 2012

Expiration Date: Indefinite

A handwritten signature in black ink, reading "Susan K. Cowden". The signature is fluid and cursive, with a large loop at the end of the last name.

Susan K. Cowden, Administrator
Division of Workforce Development