Wage Record Interchange System (WRIS)
Data Sharing Agreement Amendment Proposal

Proposal Number: 11

Proposal Title:

Prohibiting Wage Data Storage on Devices That Can Be Compromised

Reference: *Section VIII. Confidentiality/Restrictions on Use of Information, Subsection A, Paragraph 6, Subsection B, Paragraph 9, and Subsection C, Paragraph 8*

Date Submitted: September 23, 2009

Sponsoring Entity Information:

Contact Person: Karen Staha

Agency/Organization: Employment and Training Administration (ETA)

Phone: (202) 693-2917

E-mail: staha.karen@dol.gov

Statement of Issue:

The WRIS Agreement recognizes that wage data is confidential and measures must be taken to ensure the confidentiality and security of the data. Sections VIII. A.6., VIII. B.9., and VIII. C.8. provide that wage data shall be processed in such a way that unauthorized persons cannot retrieve such records by means of computer, remote terminal, or any other means. The proposed language addresses the concern that more specificity is needed in this description.

Discussion of Issue:

The proposed amendments add specificity to the above requirement by prohibiting the wage data from being maintained on any type of mobile or portable device that can be compromised and listing examples of such devices. The list of examples is not intended to be exclusive in order to accommodate advances in technology.

Statement of Proposed Change/Proposal:

Reference: Section VIII. Confidentiality/Restrictions on Use of Information, Subsection A, Paragraph 6

Original Provision:

6. The Queries obtained through the WRIS shall be processed in a manner that will protect the confidentiality of the records, and in such a way that unauthorized persons cannot retrieve such records by means of computer, remote terminal, or any other means.

Proposed Replacement Provision:

6. *The Queries obtained through the WRIS shall be processed in a manner that will protect the confidentiality of the records, and in such a way that unauthorized persons cannot retrieve such records by means of computer, remote terminal, or any other means. Such Queries may never be downloaded to or maintained on mobile or portable devices, such as laptop computers, BlackBerries, USB flash drives, iPods, CD-ROMs, DVDs, floppy disks or the equivalent of any of these devices. In addition, Queries may never be accessed from a non-secure location, such as airports, hotels, public Wi-Fi, or Local Area Networks (LANs).*

Reference: Section VIII. Confidentiality/Restrictions on Use of Information, Subsection B, Paragraph 9

Original Provision:

9. The Wage Data obtained through the WRIS Clearinghouse shall be processed so as to protect the confidentiality of the data, and in such a way that unauthorized persons cannot retrieve such records by means of computer, remote terminal, or any other means.

Proposed Replacement Provision:

9. The Wage Data obtained through the WRIS Clearinghouse shall be processed in a manner that will protect the confidentiality of the records, and in such a way that unauthorized persons cannot retrieve such records by means of computer, remote terminal, or any other means. Such wage data may never be downloaded to or maintained on mobile or portable devices, such as laptop computers, BlackBerries, USB flash drives, iPods, CD-ROMs, DVDs, floppy disks or the equivalent of any of these devices. In addition, wage data may never be accessed from non-secure locations, such as airports, hotels, public Wi-Fi, or Local Area Networks (LANs).

Reference: Section VIII. Confidentiality/Restrictions on Use of Information, Subsection C, Paragraph 8

Original Provision:

8. The Wage Data obtained by ETA through the WRIS shall be processed in a manner that will protect the confidentiality of the records, and in such a way that unauthorized persons cannot retrieve such data by means of computer, remote terminal, or any other means.

Proposed Replacement Provision:

8. The Wage Data obtained by ETA through the WRIS shall be processed in a manner that will protect the confidentiality of the records, and in such a way that unauthorized persons cannot retrieve such records by means of computer, remote terminal, or any other means. Such wage data may never be downloaded to or maintained on mobile or portable devices, such as laptop computers, BlackBerries, USB flash drives, iPods, CD-ROMs, DVDs, floppy disks or the equivalent of any of these devices. In addition, wage data may never be accessed from a non-secure location, such as airports, hotels, public Wi-Fi, or Local Area Networks (LANs).

Supporting Documentation:

Not applicable

Preliminary Decision on Disposition of Amendment Proposal: 03/02/2010

Disposition Discussion:

A comment was received from Kansas on this amendment proposal during the 60-day comment period requesting clarification on the definition of non-secure location as it relates to a Local Area Network, since Amendment 11interpreted to prevent download of WRIS files from ASC or the transfer of WRIS files to any network connected server or PC workstation without regard to the use of VPN connectivity, SSL connectivity or FTP connectivity. Kansas further requested clarification on the prohibition of the download to "laptop computers," noting that a "laptop computer" can be a more secure storage device than a file server or a PC workstation if proper procedures as established by NIST for FISMA implementation are followed.

A comment was received from New York on this amendment proposal during the 60-day comment period suggesting that, rather than brand names such as "BlackBerry" and "iPod," generic terms such as "wireless handheld devices" and "portable media players" be used for the portable devices listed in the amendment.

Comments were received from Texas and Maine on this amendment proposal during the 60-day comment period objecting to the total prohibition on downloading or maintaining WRIS data on a portable device. Texas noted that this amendment would impede the many states that only issue their employees laptops and instead recommended that the amendment require that portable devices used to store data be encrypted and protected with a strong password of at least eight numbers, non-alphanumeric characters, and

uppercase and lowercase letters.

A comment was received from Tennessee on this amendment proposal during the 60-day comment period observing that the amendment does not define adequately what "can be compromised" means; and specifying devices, absent the needed definition, will only confuse the matter. Tennessee expressed support for strong usernames and passwords.

A comment was received from North Carolina on this amendment proposal during the 60-day comment period saying that, while limiting the devices that the WRIS data can be downloaded/stored on does offer an additional level of protection, it is more important for states participating in WRIS to understand the confidentially requirements (and consequences), and act accordingly with security policies and practices, since technology is changing rapidly and restricting the download/storage location of the WRIS data on these devices doesn't address future technology or a host of other scenarios that demonstrate lax security policies and practices.

A comment was received from Washington State on this amendment proposal during the 60-day comment period stating that because Washington is a two-PACIA state in which the two agencies collaborate on federal reporting but do not share a common network, it remains prudent to have the option to transmit encrypted information via portable medium so the two PACIAs do not have to submit redundant requests to the WRIS.

Following review of the comments received during the 60-day comment period, the State of Massachusetts agreed to revise the language of its amendment proposal to address the issues raised. The preliminary decision on the disposition is to incorporate the revised language into the Agreement.

Proposed Dispositions:

Reference: Section VIII. Confidentiality/Restrictions on Use of Information, Subsection A, Paragraph 6

6. *The Queries obtained through the WRIS shall be processed in a manner that will protect the confidentiality of the records and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal, or any other means. Queries may be downloaded to, or maintained on, mobile or portable devices only if the queries are encrypted with a very strong password that, at minimum, meets the standards established by the National Institute of Standards and Technology (NIST). Queries may be accessed only from a secure location.*

Reference: Section VIII. Confidentiality/Restrictions on Use of Information, Subsection B, Paragraph 9

9. *The Wage Data obtained through the WRIS Clearinghouse shall be processed in a manner that will protect the confidentiality of the records and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal, or any other means. Wage Data may be downloaded to, or maintained on, mobile or portable devices only if the Wage Data are encrypted with a very strong password*

that, at minimum, meets the standards established by the National Institute of Standards and Technology (NIST). In addition, Wage Data may only be accessed from secure locations.

Reference: Section VIII. Confidentiality/Restrictions on Use of Information, Subsection C, Paragraph 8

8. *The Wage Data obtained by ETA through the WRIS shall be processed in a manner that will protect the confidentiality of the records and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal, or any other means. Wage Data may be downloaded to, or maintained on, mobile or portable devices only if the Wage Data are encrypted with a very strong password that, at minimum, meets the standards established by the National Institute of Standards and Technology (NIST). In addition, Wage Data may only be accessed from secure locations.*