The reviewers also continued to observe broad efforts to improve data quality. By instituting procedures to ensure that only the most accurate and complete data enter their respective case management and wage data systems, the states ultimately provide more valuable information to the WRIS members. An example of the proactive steps states have taken to enhance data quality is self-service registration that filters SSNs that don't conform to Social Security Administration (SSA) guidelines. State operators also review or "scrub" the SSNs that they provide to the WRIS Clearinghouse to eliminate any duplicate entries or obviously non-conforming numbers. The reviewers also noted that in states where participant files are established with the assistance of front-line staff, care is taken to verify personal information including SSNs.

Finally, the reviewers confirmed with IT administrators that the WRIS Web site is Secure Sockets Layer (SSL) encrypted and that the data transmitted to and from the state are Advanced Encryption Standard (AES) encrypted. Of the two, AES is the standard specified by the National Institute of Standards and Technology and employed by the WRIS Clearinghouse.

AREA 5: PHYSICAL SECURITY OF WRIS DATA

Each of the states visited during this period have established clearly defined and comprehensively implemented security policies and procedures. A trend observed was the number of dedicated information security officers that states have hired to oversee this critical role. States also are employing increasingly sophisticated software tools to protect against cyber attacks and to monitor employee actions to guard against accidental as well as intentional misuse of sensitive information. Physical security was noticeably strengthened with most facilities engaging guards at building entrances as well as electronic key card control at all critical internal access points.

Data security was also integrated into the WRIS data transmission process. All of the PACIA and SUIA organizations reviewed have instituted procedures that adhere to the DSA. Examples include the use of encrypted files, compartmentalized access to networks, drives, and, in some cases, specific files containing wage data obtained from the WRIS Clearinghouse. The majority of states – and if applicable their support contractors – remove, mask, or encrypt SSNs once they are stored in case management systems. All of the organizations visited maintain control over WRIS-supplied wage data such that they have the ability to isolate or remove WRIS-specific data from system files.

The reviewers focused on portable media since states have a wide range of rules and procedures dedicated to data security that can vary from organization to organization. Examples of portable media include laptop computers, thumb drives, CDs, back-up tape, and external hard drives. Practices include data encryption software on laptops, CDs, flash drives or removable hard drives, and virus and intrusion detection software on laptops. Without exception, none of the visits revealed portable media containing wage data obtained from the WRIS Clearinghouse that were removed from secure facilities; all portable media in use for WRIS purposes were encrypted.

A summary of state data and physical security measures is presented in the following paragraphs.

The growing threat of cyber attacks, coupled with the sensitive nature of information that is managed by PACIA and SUIA organizations, has led many state agencies to hire dedicated information security officers. All of the individuals interviewed who fill a dedicated data security role possessed extensive IT backgrounds and training. Without exception it was noted that these individuals either had instituted a review of data security policies and procedures or were in the process of doing so. Also evident to the reviewers was an emphasis on proactive approaches to remind staff of their data security responsibilities and ensure compliance. The security officers interviewed were all familiar with the many IT audits that SUIA organizations are subject to, such as the IRS or SSA reviews, and have incorporated third-party examinations or "stress tests" to confirm their systems and practices are robust enough to withstand a focused attack.

All of the individuals charged with ensuring data security emphasized employee awareness of state and WRIS-specific security guidelines. The reviewers found state employees who handle and control access to WRIS-related information to be well informed regarding data security. All state employees who have access to wage data obtained through the WRIS were confirmed to have reviewed and acknowledged the DSA. All the states reviewed maintain comprehensive procedures and regulations concerning data security and the handling of personal information. Copies of these documents were obtained from each state. The reviewers also reinforced the states' responsibility to immediately notify ETA and the WRIS Clearinghouse in the event of a data security breach.

The states reviewed during this period require new employees to undergo background checks and require employees to complete training in data security and acknowledge ethics guidelines and regulations. One state has instituted a dedicated ethics course for all managers that is reviewed annually. The states also require some level of annual training for all employees in data security and ethics with electronic updates to remind them of the importance of protecting personally identifiable information.

Another emerging trend observed was the use of ever more sophisticated software tools to monitor access to IT systems and data. These include intrusion detection software to guard against unauthorized access via the Internet and internal tools to ensure the proper handling of personally identifiable information (PII). All states visited compartmentalize wage data obtained via the WRIS Clearinghouse and tightly control access. The reviewers observed the documented procedures that each state follows to grant authorization to access this information. An emerging best practice observed in two states was the use of software tools that monitor access to sensitive drives and files that model user behavior to detect unauthorized or improper handling of data. This software can be calibrated to immediately freeze user access if it detects unauthorized actions. Similar tools scan e-mail transmissions to detect SSNs, which most states prohibit from being transmitted via e-mail.

The reviewers found that physical security in buildings, and particularly in data processing centers, was increasingly sophisticated. Most of the offices employed automated technologies employed to control access and all of the data processing centers use electronic key cards to monitor access. The majority of offices visited posted guards during business hours. Several of the buildings had controlled access to internal offices that require staff to unlock doors using key cards that record their arrival. In addition to these safeguards, all of the data processing centers had multiple points of controlled access that required visitors to sign in and out of each space and be escorted at all times.

There were very few instances of employees printing materials that contain WRIS-related information. Two of the states that were visited do not print any WRIS-related data. Several others print materials to support the data validation process, but then destroy records once the data validation requirements are met. The reviewers noted that in the cases where printed materials are produced, they are secured in locked file cabinets in guarded and/or access-controlled buildings. Unlike past reviews, none of the states visited during this reporting period stores WRIS-related data on portable media. All wage data captured by the PACIAs are archived on secure, access-controlled network drives. No wage data obtained from the WRIS Clearinghouse are archived or stored by SUIA agencies.

The reviewers personally observed all of the workspaces where individuals access or process WRIS-related information for PACIA reporting. Without exception, all of these work areas are located in access-controlled facilities. Most of the work areas were in limited-access offices or, with one exception, high-walled cubicles with limited sight lines. One WRIS member had recently converted to the use of low-walled cubicles throughout the agencies. The reviewers reminded all states of their obligation in the DSA to protect against unauthorized or accidental exposure of WRIS-related information by providing secure locations for their operators and analysts who handle wage data. The reviewers discussed these procedures and guidelines with all of the individuals who work with wage data obtained through the WRIS to confirm they are aware of their obligations under the DSA to safeguard sensitive information. Emphasis was placed on ensuring they take steps to avoid direct visual access to computer monitors, secure any printed materials in locked containers, employ timed password-protected screen savers, and follow state guidelines on protecting passwords and log-in codes. The workspaces examined, with one exception, were found to be secure with limited sight lines. In the case of the member that had converted to low-walled cubicles, it was suggested that PACIA staff work from alternate locations, with limited sight lines, during periods when accessing wage data from WRIS. All facilities visited provide well-marked document disposal shredders or bonded disposal bins for secure destruction of printed materials.

Where possible, the reviewers conducted a similar physical site review of SUIA operations. In most cases, these physical inspections involved data processing centers containing mainframe computers and network operations. These centers all employed extensive layered security where staff and visitors "key in" and "key out" to maintain accountability in secure areas. The reviewers found that most personnel who work in these data centers undergo more extensive clearance processes than their

colleagues given the nature of their work and the access they have to wage and personal information. The reviewers met with information security officers who outlined data security procedures and described the third-party reviews they undergo. Several states noted that they comply with NIST standards and regularly undergo IRS and/or SSA audits to ensure their systems and procedures meet these stringent guidelines. During the SUIA agency tours, the reviewers did not observe any printed materials containing wage data obtained through the WRIS. The reviewers also confirmed that none of the incoming queries from the WRIS Clearinghouse containing SSNs from other states is observed or archived by any of the SUIAs. These automated transmissions are completed on a daily basis with incoming data files securely deleted after the response action is complete.

The importance of data security has been clearly communicated to staff, particularly in those states that employ dedicated information security officers. State resources to accomplish this include the existence of multiple safeguards and assigned staff to monitor security procedures and take steps needed to minimize the possibility of a data breach. In several states, the governor and other state leaders emphasize data security, and have passed legislation protecting PII. Many states provide continuous monitoring, including the sophisticated software tools described above, to ensure security and minimize the potential for a data breach.

Data transmission to and from the WRIS Clearinghouse in all cases was observed to follow system guidelines including encrypted secure transfer. Details are described in Area Four of this report. Several states employ similar measures for data transfer within their respective agency. That is, files transferred from analyst to analyst are first encrypted then transmitted over a secure link within the same network. The reviewers also observed how data are handled between state agencies and contractors providing case management and analytical support. In each case there were documented procedures describing the steps to encrypt and securely transmit sensitive data to and from the contractor. As noted previously, many states mask or replace SSNs in case management systems to guard against accidental release.

Data files containing wage data obtained via the WRIS Clearinghouse are stored on secure network drives for all states visited during this reporting period. No cases of back-up disks were observed. The reviewers did, however, focus on how states handle portable media and reviewed their procedures and guidelines controlling use of these storage devices to ensure compliance with the provisions in the DSA. Most of the states visited have strict guidelines that control or prohibit the use of portable media such as thumb drives, CDs, or external drives to store PII. Laptops are similarly controlled with prescribed procedures for ensuring software, virus scanning and intrusion detection tools are in place and current. One state requires laptops to be connected to the network at least once every 30 days to ensure these software utilities are operating properly. Failure to complete this process results in loss of network access. Another state physically inventories all thumb drives and disks to ensure they employ a software utility that prevents the unauthorized copying of data files. All of the states visited have policies and procedures in place that recognize the potential for a data breach to occur through the loss or misuse of portable media. The observed practices address this concern and appear to minimize this risk.

Overall, the reviewers noted an expanded emphasis on data security including significant investments in staff dedicated to this purpose. All of the states visited have instituted comprehensive security measures and indoctrinated their employees to ensure that they comply with the requirements of the DSA.

AREA 6: ROLE OF CONTRACTORS

Four of the seven states visited during the reporting period confirmed that they have entered into an agreement with a contractor to either supply a data management system and/or to receive analytical support for performance reporting. One state also engages the services of a contractor to assist with Unemployment Insurance (UI) operations including supplying wage data from the SUIA to the WRIS Clearinghouse. The contractors or service providers observed were Americas Job Link Alliance (AJLA), Future Works Systems, Inc., Geographic Solutions, Inc., and On Point Technology, Inc. In each case the reviewers discussed with the states whether wage data obtained from the WRIS Clearinghouse are shared with their contractors, and, if so, whether the appropriate safeguards and agreements are in place to ensure its security.

An important consideration included in the DSA is that any state that engages contractor support must include the requirements of the WRIS DSA in its contractual agreements. These agreements must clearly define what information the contractors are authorized to access and how it must be handled. This requirement was confirmed with each state. The reviewers also examined state documentation to identify contractor staff that support case management systems to ensure that each has personally reviewed and acknowledged the DSA.

With the exception of the one WRIS member that retains a contractor for SUIA support, systems contractors provide data management, analysis, and reporting tools via Web-based platforms. These products and services support comprehensive case management, labor market information, job matching, and performance reporting. To accomplish this, the contractors have instituted secure, encrypted platforms to transmit and receive participant data via the Internet. The states and contractors employ state-of-the-art platforms and software utilities to protect confidential data. These same systems have been audited independently by the states and in some cases by federal agencies and are regularly monitored by the respective state information security officers.

Where possible, the reviewers personally observed the process state analysts follow to transmit to and receive wage data from support contractors. This includes information obtained from the WRIS Clearinghouse. In each case, the data transmission processes involve the use of data encryption and transmission via a secure file transfer protocol. A review of data management procedures also confirmed that contractors handling participant data mask individual SSNs and replace them with unique identifiers. Contractors also review data files to identify duplicate entries and

non-conforming SSNs. In accordance with the DSA, all wage records obtained from the WRIS Clearinghouse are tracked and can be maintained separately from wage data collected by the state.

The SUIA support contractor supplies consulting staff that are co-located with state staff responsible for populating the DDBI and responding to daily inquiries for state wage data. These contractors confirmed they have reviewed and acknowledged the DSA and have participated in conference calls and on-line training as they pertain to the SUIA function.

Among the contractors engaged by states observed during this period, AJLA offers its member states information management and reporting tools that facilitate workforce system operations and performance reporting. Future Works develops and supports a Web-based application service to help states and local workforce agencies manage performance data, and Geographic Solutions offers its clients case management systems and reporting tools designed for the public workforce system. On Point Solutions supports state workforce agencies' UI systems with solutions that improve workflows, optimize organizational reporting efficiency, and protect against identity theft and organized fraud targeting Unemployment Insurance trust funds.

The reviewers noted that states engaging contractor support understood their obligations under the DSA and had established agreements that defined the specific role of their respective service provider. This was demonstrated to the reviewers in the WRIS guides and policy documents developed by each state. As noted previously, the requirements of the DSA have been incorporated into the contractors' agreements with the states.

SUMMARY

This report was intended to provide an overview of observations made during the conduct of the seven on-site confidentiality reviews completed between October 2010 and March 2011. ETA sponsored these reviews in fulfillment of its responsibilities under the DSA. Individual reports have been provided to each state that reflect the unique observations recorded. This Annual Report serves as a compilation of the observations with an emphasis on the general policies and practices that may be valuable to other member states in improving their data security systems. The reviewers noted that every state visited has made significant investments in establishing and maintaining their data security practices.

The reviewers were careful to inform each interviewed state that the purpose of the DCRs is to observe WRIS activities and provide feedback for process improvement. The on-site reviews are not audits and the contractors engaged to conduct these meetings have no authority to render determinations. Should an egregious state practice have been identified during the review, ETA, under the Data Sharing Agreement at Section IX.D, has the responsibility to work with the state to resolve the issue immediately to avoid further action. No such practices were observed during this period though the reviewers did discuss, and several states clarified, policies and procedures that may not have fully reflected the requirements of the DSA. The reviews provided an opportunity for ETA's representatives to learn how states are addressing their obligations as members of WRIS and to identify innovative practices that may be of value to other members of this system.

The reviewers were extremely impressed not only with the data security practices employed by the states, but also with the comprehensive approach taken to support the reviews. All of the PACIA and SUIA representatives were well prepared with resource documents, organizational charts, and training materials and made available the key individuals who support WRIS activities. The combination of well-documented procedures and the availability of key staff for interviews facilitated the on-site confidentiality review process.

Because of the ever-changing threats to data security, it is understood that ETA will review these observations and incorporate them into ongoing training and orientation activities and resources. Future on-site confidentiality reviews will continue to focus on the WRIS member states' policies, practices, and systems designed to improve data security.