# ANNUAL REPORT

*Wage Record Interchange System*
*Confidentiality Reviews, May 2011*

Conducted for the Employment and Training Administration, U.S. Department of Labor
by Command Decisions Systems and Solutions, Inc. (CDS$^2$)

# ANNUAL REPORT

## *Wage Record Interchange System Confidentiality Reviews, May 2011*

Conducted for the Employment and Training Administration,
U.S. Department of Labor by Command Decisions Systems and Solutions, Inc. (CDS$^2$)

**EMPLOYMENT AND TRAINING ADMINISTRATION**
UNITED STATES DEPARTMENT OF LABOR

# Introduction

In accordance with the Wage Record Interchange System (WRIS) Data Sharing Agreement, the U.S. Department of Labor's Employment and Training Administration (ETA) sponsored an independent observer to review seven member states' participation in the system.  The approach proposed by the ETA and implemented by Command Decisions Systems & Solutions, Inc. (CDS$^2$), the third-party organization engaged to conduct the reviews, was to examine each state's approach to implementing data security in accordance with the Data Sharing Agreement.  To that extent, the review team followed the process described below to confirm the states' understanding of their obligations and that appropriate policies, processes and systems are in place to secure wage data provided through the WRIS.  Additionally, they sought to identify innovations and best practices that member states may find of interest while also providing technical assistance to states regarding new amendments to the Data Sharing Agreement, coordination with the WRIS Clearinghouse, or policies for the secure interstate exchange of wage data.

Site visits were conducted between October 2010 and March 2011 with the following WRIS members: the District of Columbia, Georgia, Missouri, Nevada, Pennsylvania, South Carolina and Wyoming.  This Annual Report provides background information on WRIS, the organization of each confidentiality review, a summary of best practices and innovative approaches, and a compilation of observations from the states organized by the six areas of interest.

## BACKGROUND

The WRIS confidentiality reviews are governed by the Data Sharing Agreement (DSA), which was recently amended on February 17, 2011.  The Agreement states:

> The Wage Record Interchange System (WRIS) has been developed to facilitate the interstate exchange of wage data between participating states for the purpose of assessing and reporting on state and local performance for programs authorized under the Workforce Investment Act of 1998 (WIA), under other statutory provisions authorizing programs identified as One-Stop partners in the WIA, and for other purposes allowed under law. More specifically, the WRIS: 1) assists states in assessing the performance of individual training providers and state employment and training programs; 2) supports states in preparing and submitting reports to the United States Department of Labor (USDOL) regarding the performance of workforce investment programs and activities authorized under the WIA, or under other statutory provisions that are referenced in the WIA as authorizing programs identified as One-Stop partners; and 3) supports research and evaluation efforts authorized under the terms of this Agreement.

The document addresses the federal and state entities charged with administering the guidelines as follows:

> The purpose of this Agreement is to establish and implement the operating conditions and procedures that will govern the participation of the state agencies holding wage data (referred to as SUIAs), the state Performance Accountability and Customer Information Agencies (PACIAs) and the USDOL - Employment and Training Administration (ETA) in the WRIS

> and to establish certain conditions and procedures, consistent with 20 CFR Part 603, that are intended to protect the confidentiality of information disclosed among the participating parties through the WRIS.

The DSA, in Section VI.C.2, also describes the confidentiality review process that authorizes the site visits conducted by CDS[2] and described in this report:

> To further ensure the confidentiality of the Wage Data exchanged through the WRIS, ETA shall contract for an outside party to conduct Confidentiality Compliance Reviews to monitor the parties' compliance with the confidentiality requirements of the Agreement and to provide feedback and findings to the subject party on how its processes can be improved to better safeguard the Wage Data as required.

The DSA provides the foundation for WRIS and guides all operations and activities.  The confidentiality reviews and the process described in the following section were designed to examine how each state engages with the system and ensures the security of the wage and personal information exchanged between members.

These reviews could not have been completed efficiently without the cooperation and assistance of the staff members in the participating states: the District of Columbia, Georgia, Missouri, Nevada, Pennsylvania, South Carolina and Wyoming.  The U.S. Department of Labor extends its sincere gratitude for the investment of time and effort in support of this process.

# SITE REVIEW PROCESS

The on-site reviews were conducted in accordance with the provisions of the DSA. The goals of each review were to understand how each state complies with the DSA, to identify and discuss any areas of concern regarding the DSA requirements, and to capture policies and practices that might prove valuable to other members of the WRIS community. The reviews also served as an opportunity to identify evolving trends, particularly in light of the recession, that influence PACIA and SUIA approaches to WRIS.

Each confidentiality review was divided into six areas of examination:

1. **Structure of WRIS administration.** In this area, the review team sought to identify and interview all state employees directly or indirectly engaged in WRIS. Of particular interest were the organizational lines of responsibility.

2. **WRIS user education and awareness.** During this element, the reviewers examined each state's approach to training and orienting staff and contractors to the importance of data security, and the specific steps taken to ensure staff granted access to WRIS understood their responsibilities under the DSA.

3. **Administration and oversight processes.** Here, the review focused on the documentation of operating policies and procedures as well as staff familiarity with these resources and where they are archived.

4. **Data transmission.** At the heart of each review, the observers walked through the process each PACIA and SUIA follows to request, retrieve, and supply wage data through the WRIS Clearinghouse.

5. **Physical security of WRIS data.** This area focused on two aspects of data security: the policies, practices, and systems in place to secure data; and where and how long wage data obtained from the WRIS Clearinghouse are archived.

6. **Roles of contractors (if any).** A number of states have engaged contractor support ranging from case management systems to basic options such as reporting tools and supplemental staffing. The reviews examined contractor relationships to determine if wage data supplied through WRIS are exposed, and if the proper security controls are in place.

The reviews were conducted at the location of each state's SUIA and PACIA agencies. When interested parties were not available or accessible at the time of the on-site meetings, follow-up conference call interviews were held. The reviewers followed a protocol linked to each of the six areas listed above and observed how states organized their resources to capture, analyze, and store wage data provided through the WRIS. The reviewers discussed with each state's designated WRIS representatives how the state generally trains its employees in topics such as information technology (IT) systems, data security, and ethics. They then examined agency policies and procedures that pertained specifically to WRIS. When available, the reviewers were provided copies of training and policy guides and organizational charts illustrating lines of communication and responsibilities.

Significant time was invested in understanding how each state handles the transmission and receipt of wage data obtained through the WRIS Clearinghouse and how that information is stored. Additionally, data retention and destruction policies were also discussed. A core element of each confidentiality review was a physical inspection of the work areas where wage data are handled. The reviewers also captured information on each state's approach to ensuring the security of personally identifiable information (PII).

The last element of each review dealt with the role of contractors in developing and maintaining information management systems. Presently, there are several options available to states interested in securing outside assistance for case management, data analysis and labor market information. The reviewers examined the relationships between the states and contractors to understand how they operated under the DSA.

# OBSERVATIONS AND HIGHLIGHTS

The seven states visited in 2010 and 2011 all demonstrated well-established data security policies, practices, and systems. Through the meetings, the reviewers noted several trends that all improve the security of wage data exchanged by member states through the WRIS Clearinghouse. The majority of states visited limit the number of employees who have access to WRIS-related information. In a few states, there were only two individuals in the PACIA organization who initiate the request and utilize the data for performance reporting. While this improves controls on data access, continuity of operations may suffer if a key individual becomes unavailable. It should be noted that all of the seven SUIA organizations reviewed maintain fully automated systems where no staff members come in direct contact with incoming wage data requests. This is a positive reflection on the reliable systems employed by the WRIS Clearinghouse.

Another significant development was the guides and manuals that states had prepared for their WRIS employees. Most of these printed and electronic resources describe all related policies, procedures, training, systems, software, and contact information. The reviewers found these documents to be a valuable asset for each state and extremely helpful in conducting the on-site confidentiality reviews.

The third significant trend is the designation of a dedicated information security officer. Increasingly, states are demonstrating their commitment to data security by assigning an individual to work independently on improving and implementing more robust information security measures. Often these individuals operate outside the operational chain of command to allow them to work independently and avoid any conflict of interest. All of the security officers interviewed described proactive approaches to data security through increased testing, staff training, and continuous improvement of procedures.

These and other trends observed during the reporting period are highlighted in this section.

## I. ROBUST INFORMATION SECURITY

### • Limiting Access to WRIS Data

States reviewed during this period have all implemented policies and systems that control access to sensitive data. Similar to past reviews, these states all limit network and file access only to those for whom such access is essential.

### • No Printed Materials

Several states examined do not print any materials that contain wage data obtained through the WRIS Clearinghouse. There were no examples of printed materials tied to performance reporting; the few examples observed of printed materials were all connected to data validation. Several states have developed data validation procedures where wage verification is conducted electronically with no printed materials added to the agency's archives. In these cases, wage verification is completed from a central office or remotely via phone links with an operator working in the central office.

## • Automated Programs that Identify Sensitive Data Such as SSNs

A number of states have added software utilities that actively scan e-mails and electronic files for Social Security Numbers (SSNs). Most states have established policies that prohibit the transmission of SSNs in an e-mail. These utilities automatically block any message that may contain a SSN. Two states have employed expert systems that monitor employee network usage to highlight unusual activity. These systems model employee behavior and usage and note non-uniform actions or attempts to access network drives or files which the employee is not authorized to view.

## • Protecting SSNs and Personally Identifiable Information

Several of the case management systems reviewed replace SSNs with unique identifying numbers to further protect sensitive data. States also employ encryption protocols that protect the transmission of data within the state agency. Under the DSA, all data transmissions to and from the WRIS Clearinghouse must be encrypted. Several states have taken that requirement a step further and encrypt data files that are transferred within the agency from one server or network to another.

## • Dedicated Security Officers

Described in the Observations and Highlights section above, a number of states are assigning independent and dedicated information security officers. All of these individuals described proactive and ambitious programs to further improve data security.

## • Third Party Data Security Reviews

Several states engage the services of a third-party contractor to review and test data security policies, practices and systems. These reviews typically involve internal and external tests with an emphasis on Internet-based attempts to access agency networks.

## • Annual Review of Data Security Policies and Procedures

All of the states visited described plans or practices tied to an annual review of policies and procedures. These reviews are intended to ensure policies, practices, and associated training reflect all state and federal regulations as well as the ever-changing nature of data security threats. A number of states include in these reviews the reauthorization and acknowledgement of employee data security agreements to remind staff of their obligations and to identify anyone who may no longer require access.

## II. AUTOMATED RESPONSE TO INCOMING SUIA WAGE DATA REQUESTS

All of the states visited have fully automated response systems to supply wage data in response to queries from the WRIS Clearinghouse. Of interest to the reviewers were the various approaches to incomplete or failed transmissions.  Typically these daily queries are fulfilled within an hour or two of receipt on a batch basis.  States have implemented confirmation processes that include an e-mail message to the operator or similar network report that describes the outcome.  Should a transmission fail, states have all included a reporting process to alert the operator to re-run the transmission program. In all cases, the incoming files are not observed and are over-written or deleted from the system within 24 hours.  No archive files containing SSNs are maintained by any of the SUIA agencies visited this period.

## III. COMPREHENSIVE TRAINING AND ACCOUNTABILITY

Many of the dedicated information security officers have expanded data security training.  The states visited all have standardized training for employees regarding state and federal policies and regulations. Specific to WRIS are annual reviews of the DSA and participation in ETA-sponsored training conference calls and Webinars.  All training outcomes are recorded, and continued network and WRIS access are predicated on successful completion.  To facilitate this expanded training and data security awareness, states are turning to automated on-line programs to deliver content.

## IV. ENRICHED PROCESS IMPROVEMENTS

Several states have continuous process improvement strategies in place regarding data quality and security. All states employ a mechanism that verifies data entered into their case management systems and ensures that SSNs conform to standards.  Where case files are entered or reviewed by front-line staff, procedures are in place to verify personal data.  In reference to data security, several states' information security officers described plans to conduct top-to-bottom reviews of policies and procedures to further improve systems with an emphasis on protecting against evolving threats.

## V. ENHANCED JOB SEARCH TECHNIQUES

All of the states visited maintain Web-based resources for job seekers to research labor market trends and job openings.  The reviewers noted that states are in the process of moving more resources to Web-based systems to allow them to concentrate limited staff resources on priority areas, including the hard-to-serve population.

## VI. IMPROVED STAFFING MEASURES

A common theme observed in this year's visits was "doing more with less."  Between staff cuts and other demands, it appeared to the reviewers that the number of staff involved with WRIS was lower than previously observed.  This may be a reflection of budget cuts, streamlined performance reporting, automated systems, unique state policies, or a combination of all these factors.  One advantage of having fewer staff with direct access to wage data supplied via the WRIS Clearinghouse is better control and security of the data. A potential downside is that concentrating operational knowledge increases the risk of operations disruption should a key person suddenly leave the position. With that in mind, the reviewers concentrated on confirming each state has a designated and trained back-up for key roles and that these individuals were familiar with their WRIS obligations.

## VII. AUTOMATED TRAINING PROGRAMS

As noted above, more states are utilizing on-line and automated data security training programs that are tracked and linked to performance evaluations. Several states have also incorporated an annual acknowledgement of the confidentiality provisions of the DSA into their security training. These programs are typically delivered via e-mail and can be tracked automatically with network and system access approvals tied to successful completion.

## VIII. SOFTWARE UTILITIES THAT TRACK USER ACTIVITY

Also referenced above are the increasingly sophisticated software utilities that track user activities to detect unusual behavior. These programs, developed internally or purchased as off-the-shelf software, monitor user activity to establish a baseline then highlight – and in some cases predict – user actions outside the norm.

## IX. USE OF INTERNAL SECURE FILE TRANSFER AND ENCRYPTION

All of the interactions with the WRIS Clearinghouse are encrypted. Further, the reviewers noted several states use encryption for internal data file sharing and transfers. This added layer of security further ensures that any data files that might be improperly accessed are protected. The reviewers also noted that all data transmissions to contractors operating case management systems are encrypted and that SSNs are masked and/or replaced by unique identifiers to protect personally identifiable information.

## X. WRIS DOCUMENTATION

The reviewers noted and acknowledge the extensive investment in WRIS documentation as well as data security resources. All of the states visited provided comprehensive resource guides compiling federal, state and WRIS-specific information on policies, processes, training materials, IT systems, and management information. The reviewers found that states used these materials for training and orientation as well as for continuity of operations. The guides were also extremely helpful in conducting the confidentiality reviews by aligning resource documents to the six areas of interest. While the materials were available in printed copy, several states have established controlled access portals on Intranets or collaborative work spaces where authorized individuals have ready access. The reviewers examined these documents to ensure state procedures adhere to the requirements of the DSA, including clearly defined procedures describing a response to a data breach.

# SUMMARY OF SIX FUNCTIONAL AREAS

Each confidentiality review entails the examination of six functional areas that pertain to specific requirements of the DSA applicable to all WRIS members. This section of the report summarizes the reviewers' observations as they examined how participating states ensure the security of wage data obtained from the WRIS Clearinghouse and the policies and procedures in place to protect this information. The state-specific reports all confirm that each Performance Accountability and Customer Information Agency (PACIA) and State Unemployment Insurance Agency (SUIA) visited during this reporting period has implemented robust procedures to securely process and handle wage data provided through WRIS.

## AREA 1: STRUCTURE OF WRIS ADMINISTRATION

The initial area of observation for each confidentiality review involves a review of WRIS administration in each state's PACIA and SUIA organizations. This aspect of the review identifies entities within the state that use, or have access to, wage data obtained through the WRIS system. This includes identifying and examining agreements among entities performing WRIS activities, confirming that there are provisions for monitoring other agencies that may share any WRIS responsibility with the SUIA or the PACIA, and examining any interconnected data management system or systems shared by WRIS-responsible agencies with other agencies, including network boundaries, monitoring use of data transferred to interconnected system, controls for access to WRIS data, and ensuring disposal of data.

During this element, the reviewers examined the agency or state government organizational chart to pinpoint where WRIS-related activities are conducted. The process was facilitated by the states' preparation of materials describing their respective approaches to each of the six areas of interest. The reviewers, through the site visit interviews and supporting documentation, confirmed in each case that clear lines of control and responsibility are in place to secure wage data provided through WRIS.

The structure in the majority of reviewed states is that both the PACIA and SUIA organizations are now housed within the same state department. In addition, one state is in the process of consolidation, based on 2011 legislation to reorganize two state agencies into one. This structure simplifies coordination of policies and procedures and narrows the span of management control. While not always the case, this situation is typically found in smaller states. Conversely, the reviewers visited a larger state where three separate state agencies had a role in administering WRIS: a workforce agency representing the PACIA; a tax or dedicated employment security entity serving as the SUIA; and a third dedicated IT organization that supports both the PACIA and the SUIA. Regardless of the number of state agencies engaged in WRIS activities, the reviewers confirmed that management controls were in place to coordinate the transfer, handling, and disposal of wage data supplied through the WRIS Clearinghouse.

A trend observed during the reporting period was the tight control over the number of staff engaged in WRIS. It was not clear if this was a result of tighter state budgets or tighter control over access to sensitive data, but some states had just two analysts assigned to processing and analyzing wage data obtained through WRIS. While this simplifies data security monitoring, it potentially raises the issue of concentrating organizational expertise. With this in mind, the reviewers examined how each state assigns and trains back-up staff. The process guides that the states have developed describing internal procedures, lines of communication, management responsibilities, applicable state and federal regulations, and links to training resources aid in back-up training. In all cases, the states visited during this reporting period clearly defined and restricted which of their employees could access wage data provided through the WRIS.

In other states, multiple agencies and their operational units share WRIS responsibility. In these instances, states employ interconnected data management systems to protect the confidentiality of wage data while facilitating the exchange of information needed to fulfill WRIS data requests and prepare performance reports. As indicated previously, one of the interviewed states has three separate agencies within the state government engaged in WRIS. The reviewers examined the processes and controls in place that insure the security of wage data obtained via the WRIS Clearinghouse. Each agency maintains and coordinates access authorization and all employees supporting WRIS have reviewed and acknowledged the confidentiality provisions of the DSA. A central point of contact (often the PACIA representative to the WRIS Advisory Group) tracks employee acknowledgements and monitors compliance for the WRIS operator and back-up.

Several of the states reviewed use case management systems and/or labor market exchanges developed or operated by contractors. The contracted products and services range from systems that manage participant files and develop workforce system performance reports to focused selections where states engage the services of contractors to assist with various aspects of WRIS. A common feature is a reporting tool used to facilitate performance analysis. It was noted that states that work with contractors carefully control and define what information the contractors may access. The reviewers observed several examples of how data are accessed and stored and the agreements in place controlling these processes. Agreements between the states and contractors involving wage data obtained from the WRIS Clearinghouse all conformed to the requirements of the DSA.

Data disposal procedures and controls were also confirmed in each WRIS visit. The states reviewed during this period all limited the amount of data files and only printed wage data in support of data validation – even then only when necessary. None of the states retained any wage data associated with incoming data requests to the SUIA. Each state has defined procedures on how long data are to be archived by the PACIA in accordance with the guidelines of the state and the DSA. Data disposal procedures are defined by state regulations which the reviewers found typically to be influenced by federal guidelines issued by the Internal Revenue Service, Social Security Administration or the National Institute of Standards and Technology (NIST). Limiting access to a small number of analysts and tightly controlling or prohibiting the number of both electronic and printed archive files minimizes the potential for a breach.

The confidentiality reviews completed during this period confirmed that participating WRIS states successfully employ a range of methods to control access to WRIS data. The emerging trend of limiting access further protects sensitive data.  Additionally, all states clearly demonstrated that their staff who engage in WRIS activities have reviewed and acknowledged the appropriate data confidentiality agreements.  Together, this consistent approach ensures that only approved individuals and state organizations have access to confidential information exchanged through WRIS.

## AREA 2:  WRIS USER EDUCATION AND AWARENESS

Throughout the course of the site visits, the reviewers observed a growing trend in the states to employ automated training and orientation courses to educate employees regarding data security policies, procedures, and responsibilities.  These programs are frequently Web based, allowing states to accurately track who has completed this training.  Several states visited during this term also compiled federal, state, and WRIS-specific documentation made available to staff in both printed and electronic formats.  The reviewers found these training resources vital to ensuring employees' understanding of the confidential nature of wage data and proper use of the technology systems used to facilitate the exchange of wage data between participating states.

Each examination of the states' education and training programs began with a review of WRIS users' and managers' awareness of confidentiality principles.  This included a review of state policies and procedures as applied to data security, use of IT systems, and in a growing number of states, ethics training and acknowledgement.  The reviewers compared these state standards to the requirements of the DSA to ensure that they met or exceeded the WRIS standards, which they did in all cases.  Further, each on-site review included an overview of the DSA to confirm that WRIS users understand the guidelines and that all staff with access to this wage data have acknowledged the confidentiality provisions of the Agreement.

A continuing priority during this series of site reviews was the identification of best practices in WRIS training and education. All of the states observed have a general requirement that those employees with a role in or access to WRIS must complete a state-specific form of data security and IT systems training.  These trainings varied from a formal classroom setting to the completion of an on-line tutorial with intermittent questions to confirm comprehension.  One state has developed an extensive multi-part test that addresses data security, ethics, proper use of IT systems and Internet access. Each element is completed separately and contains a challenging examination of the student's understanding of the subject matter.  Another state has added data security elements from federal agencies such as NIST and the Bureau of Labor Statistics to enhance the content of the training.  Most states have also instituted annual "refresher" courses or other regular training updates to remind employees of their personal responsibility.

As noted earlier, many of these programs are now delivered electronically with e-mail notification, secure registration via the Internet, and confirmation of satisfactory completion. The results are then recorded by the information security officers and, in one state, included as an element of each employee's annual evaluation. Several states predicate continued network access on completion of security training with an automated suspension of privileges if the course or acknowledgement is not accomplished in the prescribed timeframe. In all cases, training is not complete until individuals sign various acknowledgement documents. As required by provisions of the DSA, all participating states have their employees who access wage data sign the WRIS Access Acknowledgement document. After completing data security and IT systems training, employees usually sign data security and IT usage policy agreements. Some states also require employees to sign state-specific acknowledgement documents that cover procedures for handling sensitive data. In one state, employees handling sensitive information also are required to review and acknowledge the Bureau of Labor Statistics data security access agreement.

The availability of program and processing documentation is crucial to keep WRIS functioning properly. All of the states provided copies of process manuals and instructions describing the steps required to request and retrieve wage data from the WRIS Clearinghouse. These reference materials were incorporated into the training materials and ready access was facilitated through dedicated network folders or assigned space on agency Intranets or collaborative work spaces. The reviewers noted that in each state the WRIS operators and back-up staff were all familiar with the location of these materials as well as how to contact WRIS Clearinghouse staff for assistance. The reviewers also reminded each state of the availability of WRIS program information on ETA's WRIS Web site, the Advisory Group's password-protected Collaborative Work Space, and WRIS Clearinghouse Web site.

The reviewers discussed with each state its interaction with the WRIS Clearinghouse operator, ACS. Each state illustrated how its in-house training programs combine with the training materials and resource documents developed by ETA. This includes the step-by-step instructions for requesting and receiving wage data results via the WRIS in support of PACIA reporting requirements, as well as the SUIA requirement to supply quarterly wage data to populate the Distributed Database Index (DDBI).

Each state acknowledged the integration of ETA-sponsored training and informational sessions. In most states, participation in these phone and virtual exchanges is encouraged. Several states noted that staff members attend ETA conference calls and Webinars in groups to ensure that all those engaged in WRIS receive consistent information.

A common observation across all states visited is the relatively small number of employees engaged in WRIS activities. This has encouraged those with more experience to mentor colleagues and offer guidance on policies and procedures. A potential risk in concentrating operational experience in a handful of staff is continuity in the event of an illness, retirement or employment separation. With this in mind, the reviewers discussed with each state their continuity plans should back-up staff have to assume a lead role. PACIA operations were well documented in all cases and designated back-up staff were knowledgeable. SUIA operations are fully automated in all states visited. The lead programmers were interviewed in each state and confirmed that protocols are in place to ensure continued operation.

The reviewers noted that all states clearly understand the importance of properly managing confidential wage data and have implemented training courses to ensure its security. Several states demonstrated plans to proactively update course materials and engage employees to ensure all are current regarding their responsibilities. Reviewed states all understand the importance of providing rigorous training on WRIS procedures, data security, and IT systems to minimize the possibility of a data breach. WRIS operations benefit from this focus on data security training since it results in more knowledgeable staff and more secure systems upon which wage data are processed and archived.

## AREA 3: ADMINISTRATION AND OVERSIGHT PROCESSES

Area Three of each site review focuses on the agency's documentation of data security procedures and confirms that adequate controls are in place. The reviewers examined how each organization documents PACIA and SUIA policies or standard operating procedures (SOPs) governing employee access to WRIS. This includes: confirming that procedures are established for employees' individual utilization of WRIS data; determining if there is an automated system in place to track access to sensitive information; reviewing how state policies and regulations are applied and how these are consolidated with the WRIS DSA; examining how each state agency responds to a data breach or misuse of sensitive information; establishing how compliance is tracked and if data security is an aspect of employees' annual evaluation; and, should a breach occur, confirming that states have documented procedures for notifying both ETA and the WRIS Clearinghouse.

The reviewers were uniformly impressed with the approach all the states have taken to develop and maintain printed and electronic copies of WRIS program materials. In each review conducted during this period the states provided copies of their respective WRIS guides that highlighted responsible organizations, described the training requirements, featured the relevant federal and state regulations and policies, specifically detailed the data transmission and handling procedures, identified federal, state, as well as WRIS-specific security policies, and in the case of those states who engage the services of a contractor, how the contractor relationship is managed and controlled. The reviewers found these comprehensive guides to be extremely helpful in conducting the reviews and also noted their value to each state as an orientation and reference resource as employees are introduced to WRIS.

A trend observed during this reporting period is how states are limiting access to WRIS-related data. As noted above, the states observed control access to wage data and limit the amount of personally identifiable information that is potentially accessible by restricting wage data access to a minimal number of employees. Several states employ sophisticated automated security features on their IT networks that track and monitor employee access to systems storing WRIS data. A growing number of states assign dedicated information security officers to ensure controlled access to all electronic files, servers and systems. Limits are placed on printed WRIS-related information, and in two states it was observed that an SOP does not permit materials to be printed or archived that contain wage data obtained from the WRIS Clearinghouse. All states visited have either instituted, or are in the process of strengthening, password-protected log-in procedures and are more closely monitoring network access and approvals. Access to WRIS-related information in all cases is controlled at the network drive level where only authorized staff may view sensitive data. These and other security steps are designed to control access and minimize the opportunity for an accidental disclosure of WRIS data.

The reviewers inquired in each confidentiality review about whether states have specific WRIS functions included in individual employee evaluations. Generally, this has not been the case, but many states reported that their guidelines require regular data security reviews and participation in state and federal training. This includes the WRIS conference calls and Webinars sponsored by ETA. One aspect of performance reviews, noted in several states, is an access clearance. That is, employees' continued access to state IT systems and clearance to handle sensitive data is predicated on satisfactory job performance. A poor performance report may lead to the rescission of network access. All states confirmed they have documented policies regarding improper use or access of sensitive information, that if confirmed, lead to disciplinary action up to and including termination.

All WRIS states visited provided guidelines for responding to a security breach. Representatives from the participating states told the reviewers that standard procedures begin with internal notification to line management followed by instructions established by each state. Of particular interest to the reviewers is the requirement of the states to immediately advise ETA and the WRIS operator about any security issues related to wage data supplied from the WRIS Clearinghouse. Following the confidentiality review, several states amended, or clarified, WRIS guides and resource materials to emphasize the notification requirement. On this subject, all the states visited confirmed that their IT systems have the capability to track user access so that, in the event of a breach, they can pinpoint the source and establish the extent of information released.

The final topic of interest in this area regards the states' data retention policies. Under the DSA, each state may retain the wage data received through WRIS only for the period of time required to utilize it for assessment and reporting purposes, or to satisfy applicable federal records retention requirements. The reviewers have observed that archived materials generally reside in two areas, electronic files used to support performance reporting and printed wage data used in data validation. All states described policies that require them to hold data for periods longer than three years. PACIA agencies typically hold WRIS information long enough to support their performance-reporting obligations. Periods observed have ranged to as long as eight years and potentially longer depending on federal requirements. All of the SUIA agencies observed retain incoming queries from the WRIS Clearinghouse only for as long as needed to develop their response. Typically these data are deleted immediately or overwritten the following day by the next incoming request. No state archives these incoming data queries consisting solely of SSNs. The reviewers noted that there is a continued interest to discuss data retention and destruction policies further through the WRIS Advisory Group.

## AREA 4: DATA TRANSMISSION

The reviewers observed that all seven states visited during the reporting period have well-established secure data transmission procedures for both the PACIA and SUIA organizations. A common observation was that states are making a conscious effort to limit the number of state employees authorized to execute data transmissions for the PACIA organizations. Similarly, in all cases SUIA transmissions were observed to be fully automated and monitored by a small group of state employees and, in one instance, by a contractor. Limiting the number of individuals with access to wage data supplied by the WRIS Clearinghouse improves data security. While a few states have their PACIA and SUIA data transmissions handled by separate entities, for the majority of states observed during this period a single state agency controlled data transmission. All states observed have instituted safeguards to ensure that the risk of a data breach is minimal. If a data breach were to occur, all states now have protocols in place to inform state authorities as well as ETA and the WRIS Clearinghouse operator, ACS.

This section has been organized to describe observations of both PACIA and SUIA data transmission processes. PACIA data transmissions are conducted primarily on a quarterly basis and are manual. An approved operator initiates the wage data request through the Clearinghouse, establishes a “need by” date for the results, and then stands by for the response. SUIA transmissions typically take place daily and, in all cases observed during this period, are fully automated. The reviewers’ observations for each are summarized in the following paragraphs.

## PACIA DATA TRANSMISSION

The processes followed by the states reviewed to request and supply wage data to the WRIS Clearinghouse are fairly consistent. The wage data obtained via the WRIS Clearinghouse are used to augment performance data obtained from state wage records to complete the states' workforce program reporting requirements for Workforce Investment Act (WIA), Wagner-Peyser, and other programs specifically permitted by the DSA. The reviewers noted that not every state tracks performance for all federal programs. At a minimum, the states visited during this period all measure WIA and Wagner-Peyser outcomes while some also examine the Trade Act programs (TAA), the Veterans Workforce Investment Program, and others.

Each member state designates at least one primary and one back-up state employee to serve as data transmission operators. These individuals are responsible for requests sent to, and data files retrieved from, the WRIS Clearinghouse. While primary operators are assigned for both the PACIA and SUIA agencies, only the PACIA operators directly handle wage data provided by the Clearinghouse.

The reviewers conducted extensive interviews with the primary PACIA operators in each of the states visited. These interviews aimed to understand the process each state follows and ensure that all requirements of the DSA are observed. This included understanding which staff members have approved access to the WRIS Clearinghouse, how these assignments were made, where the data are stored and for how long, and the process for deleting extraneous or outdated wage records. Where available, the reviewers also interviewed the back-up operators to confirm that these individuals are also familiar with WRIS Clearinghouse procedures and that their accounts are current so no disruption will occur in the event that the primary account holder is absent. The reviewers confirmed that the state operators all follow the very clear and concise instructions developed by the WRIS Clearinghouse to request and retrieve wage data. In all site confidentiality reviews conducted during the reporting period, the PACIA organizations have developed a written operations manual describing the state's approach to requesting, retrieving, and securely storing wage data supplied by the WRIS.

The PACIA process involves direct access to, and handling of, wage data supplied by the WRIS Clearinghouse. Given the extremely sensitive nature of this information, all states restrict access to it and control where it is stored and how long it is saved. As noted above, the reviewers observed that all states visited during this reporting period have established strict controls regarding the number of staff authorized to access WRIS-related data. Further, as part of the data transmission process, the reviewers confirmed that each state had one active primary account holder and at least one back-up. Records were reviewed to ensure that those staff members who were listed on the ETA database were consistent with the state employees executing the data requests.

For every state PACIA reviewed, wage data requests and responses are transferred via the secure Web site hosted by the WRIS Clearinghouse. These data requests consist of a list of SSNs tied to workforce service recipients who have received services from the state during the selected reporting period.
As indicated in the DSA, permission to log on to the WRIS Clearinghouse is restricted to approved individuals as described above. These approved individuals are identified by the state and their credentials are approved for access to the WRIS Clearinghouse by ETA. The WRIS Clearinghouse then

assigns an access password to each approved state operator.  These passwords become invalid if there are no log-ins to the system after 90 consecutive days.  The reviewers documented that all of the state employees who access the WRIS Clearinghouse and/or wage data obtained through the Clearinghouse have completed the confidentiality acknowledgements as required under the DSA.

The reviewers noted the various approaches the PACIAs take regarding their requests.  Most states request wage data for every workforce system program participant whether they have reported wages in the state or not.  Other states limit their requests to the WRIS Clearinghouse to those program participants who do not have reported wages in the state.  During this reporting period all seven of the states visited submit the SSNs of every workforce program participant to be certain any wages reported in other states are recorded.  Overall, states indicated that the absolute value of adding wage data from the WRIS Clearinghouse adds 2-10 %  to outcome measures.  The reviewers continued to observe that smaller states, and states that border larger states, tend to derive greater benefits from WRIS participation.

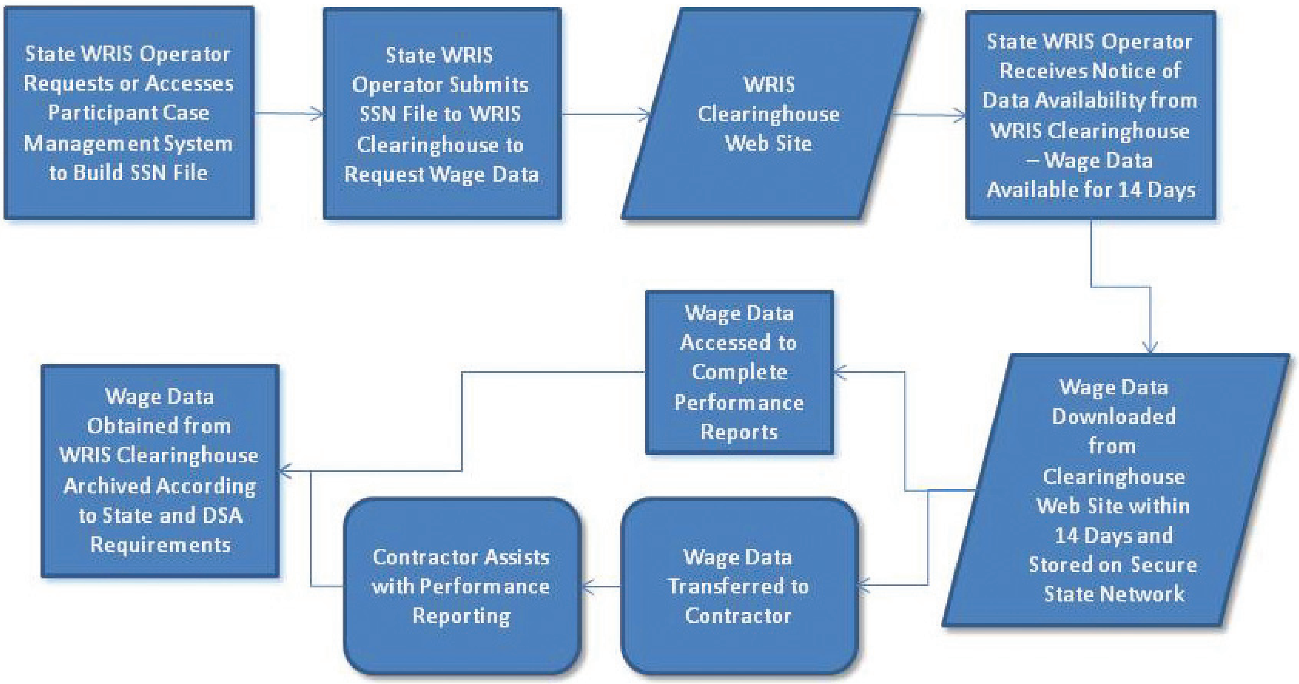
Wage data received from the WRIS Clearinghouse are retained for a period of time determined by each member state of the system.  In all instances observed, wage data received from the Clearinghouse are stored on a secure server.  As noted above, the PACIA retains this information for a period required to fulfill performance reporting requirements.  How long the information is retained is influenced by data validation, federal and state audits of workforce programs, and ongoing evaluations of the effectiveness of DSA-approved workforce services.  In all cases, the data are retained for at least three years.

During this reporting period, the reviewers confirmed that all wage data supplied by the WRIS Clearinghouse are stored on secure network drives.  The reviewers, unlike past years, did not observe states producing archive copies of the data on optical compact disks or removable hard drives.  Further, the reviewers noted that all data requests to – and receipt of wage data from – the WRIS Clearinghouse were conducted inside secure state office buildings on state-operated information technology networks.

A general trend continued during this period is that states strictly limit the amount of printed information containing wage data supplied by the WRIS Clearinghouse.  All instances of printed WRIS-related information involved data validation.  Most states now destroy printed reference information containing wage data immediately after data validation is completed.  In those cases where wage data are archived, the reviewers observed the locked cabinets and confirmed that procedures were in place to control access.  The reviewers also revisited archiving and document destruction policies and procedures.  For each state visited, the reviewers noted that the handling of WRIS-related information conforms to state rules and regulations regarding PII as well as to the requirements of the DSA.

The following illustration outlines the general approach followed by each state to request supplemental wage data from the WRIS Clearinghouse and highlights the alternate approach followed by those states who engage the services of a contractor.  Several of the states visited during this period engage contractors to manage and house participant case files and assist with performance reporting.

## PACIA Data Transmission Process Diagram


State WRIS Operator Requests or Accesses Participant Case Management System to Build SSN File
State WRIS Operator Submits SSN File to WRIS Clearinghouse to Request Wage Data
WRIS Clearinghouse Web Site
State WRIS Operator Receives Notice of Data Availability from WRIS Clearinghouse – Wage Data Available for 14 Days
Wage Data Downloaded from Clearinghouse Web Site within 14 Days and Stored on Secure State Network
Wage Data Accessed to Complete Performance Reports
Wage Data Transferred to Contractor
Contractor Assists with Performance Reporting
Wage Data Obtained from WRIS Clearinghouse Archived According to State and DSA Requirements

PACIA data requests begin with the development of a data file containing the SSNs of all workforce services participants. This information is captured in states' case management systems or in systems developed and administered by contractors. The request is submitted to the WRIS Clearinghouse by the state employee holding an access account. Typically, a few days after the date file is loaded via the secure Web site, the account holder receives an e-mail notice that the wage data are available for retrieval. This information is collected via the secure Web site and in all cases observed, stored on a secure network drive with controlled access. In cases where the state manages its own systems, the approved analysts complete the performance reports. In instances where a contractor manages the system, the state's WRIS operator transfers the wage data using similarly secure Web-based connections to the contractor. The reviewers noted that the contractor systems encrypt all data and mask SSNs by replacing them with unique identifiers to further protect this information. State-administered systems employ similar data security strategies to prevent the accidental release or exposure of SSNs. Each state retains the wage data obtained from the WRIS Clearinghouse for at least three years or as long as is deemed necessary by the state.

## SUIA DATA TRANSMISSION

Unlike the manual process followed by the PACIA operators, the SUIA process is almost entirely automated with no direct access to, or handling of, incoming queries from the WRIS Clearinghouse. SUIA operations involve state wage and employer data which are housed in very secure facilities with state-of-the-art controlled access. SUIA operations observed during this reporting period were all housed on mainframe computer systems. The SUIAs interact with the WRIS Clearinghouse to provide two data files – the quarterly Distributed Database Index (DDBI) of all reported wages in the state as reported by employers and state wage data in response to daily queries issued by the WRIS Clearinghouse. In both cases, wages are tracked by individual SSNs, which form the cornerstone of the WRIS Clearinghouse.

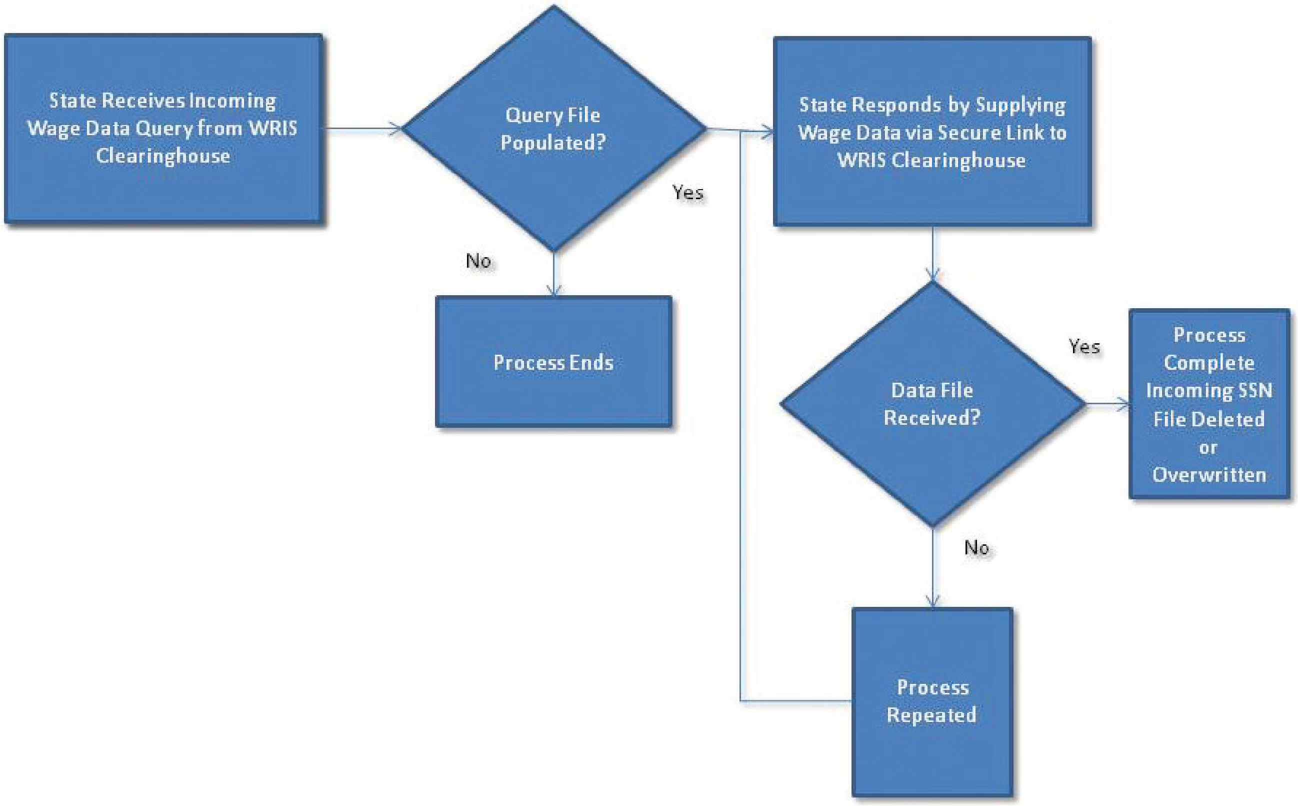
The SUIA agencies have all worked with the WRIS Clearinghouse to establish a secure link to provide wage data and respond to incoming queries. As required by the DSA, SUIAs submit, on a quarterly schedule, state wage records for the DDBI and respond to incoming WRIS queries for state wage data using an automated system. This information is transmitted over secure links, referred to as frame relays, which connect the state mainframe computers with the WRIS Clearinghouse. These links are monitored by the states and the WRIS Clearinghouse to ensure complete data transmissions.

The quarterly wage information forms the DDBI index, by which incoming requests for wage data from the WRIS members are matched to identify available wages over a period that spans eight calendar quarters. The reviewers noted that all of the states visited during the reporting period have an automated and well-established process to receive and respond to requests for wage data. States, according to the DSA, have a requirement to address incoming queries for wage data in a complete, timely, and accurate manner. All of the states visited during this period receive daily requests for wage data. The automated systems receive these WRIS Clearinghouse queries, data files containing SSNs representing workforce participants from other states, and promptly provide available wage data tied to matching SSNs. Each state has an established procedure to monitor the success or failure of these daily requests to confirm that the required data are transmitted. All states reported that this process is extremely reliable and any issues that have arisen were addressed quickly by ACS, the WRIS Clearinghouse operations contractor.

SUIA operations observed during the reporting period align with tax reporting. As such, the IT systems and mainframe computers that process this information are subject to numerous federal and state auditing agencies, among them the Internal Revenue Service (IRS), as well as federal standards maintained by the National Institute of Standards and Testing (NIST). The reviewers noted that these multiple levels of review help ensure that any data received by the SUIAs from the WRIS Clearinghouse will be handled securely and that SUIA operations do not involve any direct access or printing of wage data queries from the Clearinghouse. Further, all of the states visited this period have implemented procedures that overwrite or delete incoming request files containing SSNs within 24 hours, ensuring that no data reside on their systems. In essence, the SUIA entities observed retain this information only as long as it is needed to respond to the query from the Clearinghouse, often deleting the data file immediately after completing the transmission.

The following process flow chart illustrates how each of the states visited during the reporting period process incoming requests for wage data.

## SUIA Data Transmission Process Diagram


State Receives Incoming Wage Data Query from WRIS Clearinghouse
Query File Populated?
Yes
No
Process Ends
State Responds by Supplying Wage Data via Secure Link to WRIS Clearinghouse
Data File Received?
Yes
Process Complete Incoming SSN File Deleted or Overwritten
No
Process Repeated

The SUIA data transmission process begins with the state receiving a daily query for wage data from the WRIS Clearinghouse. These data queries occur at roughly the same time each day. The actual data query varies based on inquiries posted by other states and in some case may not include an actual query as illustrated in the diagram. The automated system receives the query over a secure and encrypted link to the WRIS Clearinghouse, and in most cases immediately begins assembling a response file containing wage and employer data, with North American Industry Classification System (NAICS) codes tied to each SSN. Once the systems confirm that the incoming queries have been successfully completed, the systems either delete the files immediately or overwrite the files with the next day's request. None of the states visited to date maintains an archive of incoming SSNs or print any materials containing data supplied by the WRIS Clearinghouse. All of the systems have a mechanism to notify the operator if a data response is incomplete. The reviewers confirmed the systems are extremely reliable with few examples of data queries going unfulfilled.

## GENERAL OBSERVATIONS

The reviewers were impressed with the comprehensive yet detailed approach taken by all states to document the data transmission procedures. These WRIS-specific guides provided both general terminology as well as technical instructions to provide the PACIA and SUIA agencies with back-up instructions. This information was used for general orientation as well as for specialized training on the systems.

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.