ANNUAL REPORT

Report of the Wage Record Interchange System Confidentiality Reviews, March 2010

Conducted for the Employment and Training Administration, U.S. Department of Labor
by DTI Associates, Inc. – a Kratos Company

ANNUAL REPORT

Report of the Wage Record Interchange System Confidentiality Reviews, March 2010

Conducted for the Employment and Training Administration,
U.S. Department of Labor by DTI Associates, Inc. – a Kratos Company

EMPLOYMENT AND TRAINING ADMINISTRATION
UNITED STATES DEPARTMENT OF LABOR

Introduction

The WRIS Data Sharing Agreement (DSA) 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 WRIS DSA continues: 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.

To ensure the integrity of the information processed through the WRIS, the DSA describes a third-party review process referred to as Confidentiality Compliance Reviews. These on-site reviews are noted under Section VI.C.2 of the DSA where ETA's responsibilities are described. Among other requirements, ETA is charged with contracting an outside party to conduct Confidentiality Reviews to monitor the parties' compliance with the confidentiality requirements of the DSA. For the purpose of this report, these reviews are referred to as Confidentiality Reviews. As directed by ETA, the Confidentiality Reviews are being conducted with states to learn about their approach to data security, observe how states are meeting their obligations under the DSA and provide technical assistance where requested. The Confidentiality Reviews are also intended to highlight innovative policies and practices that might be of interest to WRIS member states. This report summarizes the observations from 15 on-site Confidentiality Reviews conducted in 2009 and the first quarter of 2010.

The Employment and Training Administration would like to thank the participating states for their cooperation and support of the WRIS Confidentiality Reviews. The states are presented below in the order the Confidentiality Reviews occurred:

Montana, Delaware, Oklahoma, North Dakota, Illinois, West Virginia, Idaho, Washington, Arkansas, Maryland, California, Florida, Kansas, New Mexico and Arizona

Site Review Process

The Confidentiality Reviews were conducted in accordance with the provisions of the DSA. The goals of each review were to understand how each state is complying 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. Each Confidentiality Review was divided into six areas of examination:

1. Structure of WRIS administration
2. WRIS user education and awareness
3. Administration and oversight processes
4. Data transmission
5. Physical security of WRIS data
6. Roles of contractors (if any)

The Confidentiality Reviews were conducted over one or two days at the location of each state's SUIA and PACIA agencies. Additional conference calls were held with a few states to interview interested parties who were not available or accessible at the time of the Confidentiality Review. The reviewers developed a series of interview protocols tied 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 also examined agency policies and procedures that pertained specifically to WRIS. Where available, the reviewers obtained 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 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.

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 to secure 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

Throughout the Confidentiality Review interview process, the reviewers found that each participating state had developed its own customized approach to serve the information management needs of its respective workforce systems. Included in this approach are each state's policies, procedures and systems associated with obtaining wage data through the WRIS Clearinghouse. A number of these policies and processes were considered by the reviewers to be innovative practices that could be shared and possibly replicated in states looking to strengthen their approach to data security. Key findings from the Confidentiality Reviews are briefly described below with a more comprehensive summary of observations presented in the following section.

I. ROBUST INFORMATION SECURITY

When it comes to ensuring the security and integrity of wage data, participating WRIS states have adopted a number of effective practices. For example, it was evident to the reviewers that the process of limiting the number of authorized staff who are directly involved in data transmission is an efficient method to safeguard sensitive information. This approach is also encouraged by the DSA, which requires states to have personnel involved with WRIS acknowledge their understanding of the confidential nature of the WRIS data and provide executed Access Acknowledgement documents to ETA.

Additionally, a number of states have instituted practices requiring the encryption of all sensitive data. This extends to data files transmitted within state agencies and to and from the WRIS Clearinghouse. Coupled with this are states' policies that require all portable media (flash drives, laptops, CDs, etc.) use encryption software. Several states also require that any e-mail containing sensitive data be encrypted. Additional examples include:

• Limiting Access to WRIS Data

Many state agencies either restrict access to WRIS data to a small number of staff members or, by employing an automated SUIA response, minimize human interaction with the system. Developed by the states' IT divisions in collaboration with the WRIS Operator, Affiliated Computer Services, Inc. (ACS), the SUIA response systems remove the operators from the process of responding to incoming WRIS wage data inquiries, minimizing the potential for an accidental breach. These systems are jointly governed by the states' extensive data security policies and those described in the DSA.

• No Printed Materials

All states reviewed have designated data security as their highest priority. Available resources have been allocated to ensure the protection of sensitive information in all states observed. Data security policies were observed at every step of the transmission process, including the use of encrypted files, compartmentalized access to data, removal or masking of Social Security numbers (SSNs),

labeling of WRIS-supplied wage data, and the ability to isolate or remove WRIS-specific data from system files. A number of states had eliminated all printed materials containing wage data supplied through the WRIS. This precludes the need to store or destroy hard copy materials, therefore minimizing the risk of disclosure.

• Automated Programs that Identify Sensitive Data Such as SSNs

In addition to encrypting data as a security measure, several states use automated systems to safeguard sensitive data. For example, the practice implemented by one interviewed state involves incorporating an automated system that can block the transmission of SSNs identified in e-mails. Another state employs a system that automatically downloads encryption software to flash drives to protect any sensitive data stored on the devices.

• Protecting SSNs and Personally Identifiable Information

A number of visited states employ the practice of removing or masking SSNs from their case management systems and replacing them with unique identifiers to increase wage data security. Additionally, some states use software utilities that identify and control who has access to computer files, drives and systems. These programs also track user activity to deter unauthorized access and expedite failure analysis in the event of a security breach.

• Scanning Participant Case Files

One state has begun scanning hard copy case files at the local level and is storing this information electronically on the state's case management system. This investment will ensure controlled access to the participant information and also allow for validation of wage data received through the WRIS to be conducted within the state offices. The process eliminates the need to take WRIS-related data into the field, which could compromise the integrity of wage data.

• Dedicated Security Officers

Several states have assigned personnel to serve as dedicated security officers to ensure controlled access to sensitive employer and participant data. These individuals assist with policy reviews, process audits, clearance processes and training.

• Third Party Data Security Reviews

When resources were available, the interviewers found that some states engage outside consulting firms to evaluate and identify any security weaknesses. These audits test for vulnerabilities in electronic systems as well as weaknesses in policies and procedures. While this cost is not insignificant (between $30,000 to $50,000 for a small state), it does provide a high level of confidence that state data security practices are in place to protect sensitive information.

- **Annual Review of Data Security Policies and Procedures**

  Many states have a process to evaluate and review their data security policies and procedures. For example, one of the interviewed states re-examines their security procedures annually and provides a formal report of the results to a designated state official. This approach prompts a comprehensive review to ensure all policies are current.

II. AUTOMATED RESPONSE TO INCOMING SUIA WAGE DATA REQUESTS

The SUIA agencies in many states have implemented an automated process for responding to incoming requests from the WRIS Clearinghouse for state wage data. These states have developed these systems in concert with the WRIS Operator. An automated approach eliminates direct access to incoming data files and further reduces the opportunity for a breach. Most of these systems include an automated deletion function that erases the incoming data file after the response has been transmitted. As a result, there are no WRIS-related wage data stored or archived on the mainframe computers longer than is needed to complete each response. Additionally, most of these responses are completed immediately upon receipt of the request.

III. COMPREHENSIVE TRAINING AND ACCOUNTABILITY

A number of states have made investments in strengthening training procedures for staff to ensure the security of wage data. Examples include requiring all employees to complete recurring "refresher" courses on data security that are delivered and verified electronically. All states interviewed make data security resource materials and policies readily available online. Some states have developed standard operating procedures and/or operations guides and manuals for all employees who access wage data obtained through the WRIS. One state conducts desk audits to review the operating requirements and has created a checklist for employees to guide this review. Several states have produced detailed flowcharts that illustrate the agencies' processes for requesting and retrieving wage data through the Clearinghouse. At least one state has developed an orientation presentation to highlight the unique requirements tied to handling wage data obtained through the WRIS. An employee must complete this orientation before being permitted to access the WRIS information. Another state has adopted data security training developed by the Bureau of Labor Statistics and supplemented this with its own ethics and IT procedures training. This training is completed annually by all employees. Finally, a number of state SUIA agencies have incorporated Internal Revenue Service data security regulations into their training, policies and procedures for handling sensitive information.

IV. ENRICHED PROCESS IMPROVEMENTS

Many states described practices that improve the processes they use to manage and transmit wage data. These procedures are intended to secure sensitive data by removing or restricting access and replacing data elements where possible. As mentioned previously, several states block SSNs from case management files and replace them with unique identifiers. Even if data files are exposed, SSNs and

other personally identifiable information are not compromised. Additional improvements were noted in how sensitive data are stored and ultimately destroyed. Most SUIA agencies delete incoming data files immediately after a response is provided. Wage data obtained through the WRIS Clearinghouse is stored in compartmentalized server folders or, in some cases, on dedicated drives to limit and control access. These wage data files are then deleted after the minimum retention period.

The reviewers noted two other practices that might be of interest to participants in the WRIS system. While not specific to data security, these practices helped to improve the quality of services provided to job seekers.

V. ENHANCED JOB SEARCH TECHNIQUES

During the interview process, some states described innovative services targeted to job seekers. At least one state is using the micro-blogging service Twitter. This particular state posts new job listings on its Twitter feed to permit job seekers to receive immediate notification. This state also employs a practice in which a registration for unemployment insurance (UI) triggers an auto-registration with the state's employment services.

Several states make their Web site for workforce services accessible to non-English-speaking job seekers through flag icons that, once clicked, can change the language of the entire site. The sites are understandable and easier to navigate for speakers of more than a dozen languages.

VI. IMPROVED STAFFING MEASURES

The current recession has had the dual effect of increasing workload at the same time states are reducing staffing levels to address budget constraints. A number of states mentioned challenges they are addressing to meet operating requirements in this environment. To support processing of the quarterly "rush" of employer wage reports, at least one of the participating states routinely engages a part-time cadre of retired state employees with UI knowledge and expertise in data security to augment full-time staff. This practice minimizes the risk of a procedural error by engaging experienced personnel who are familiar with state data security guidelines and practices.

Summary of Six Functional Areas

The standards and objectives included in the following six functional areas pertain to specific requirements of the DSA for all WRIS-participating states and account holders. This section provides a compilation of how the WRIS-participating states interviewed during the Confidentiality Review site visits both ensure the integrity of wage data received through the WRIS process and protect sensitive information. In all cases, it was observed that data security is accomplished through well-established policies and procedures developed by each state, in accordance with the provisions of the DSA and individual states' laws.

AREA 1: STRUCTURE OF WRIS ADMINISTRATION

The reviewers found that states are deeply committed to ensuring WRIS wage data confidentiality, limiting the number of staff who have access to the WRIS system or WRIS data. However, the organizational structure used by each state to ensure this limited access varies. In some participating WRIS states, the organizational structure is based on only one agency having access to wage data supplied through the WRIS system. In all cases, these states clearly defined and restricted which state employees could access wage data provided through the WRIS. PACIA and SUIA functions include transmitting the SSNs of individuals for inclusion in the Distributed Database Index (a SUIA function) and presenting requests for wage data that are allowable under the terms of the DSA (a PACIA function).

In other states, multiple agencies and their operational units share WRIS responsibility. In these instances, states employ interconnected 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. For example, the parties specified in the DSA for one of the interviewed states include two PACIAs in addition to the SUIA, and all three are situated in separate operational units within the state government. The state also operates and maintains a central database that contains all participant data and offers controlled, password protected access to approved personnel in the three state agencies.

Some states use case management systems and/or labor market exchanges developed or operated by contractors. These systems include a reporting feature to facilitate performance analysis. It was noted that states that work with contractors carefully control and define what information the contractors may access. In these states, this access is driven by state-wide and/or agency regulations that protect personally identifiable information.

Despite the differences in organizational structure, participating WRIS states are successfully employing various methods to control access to WRIS data. Additionally, states have been extremely conscientious about ensuring that individuals who are approved to work on WRIS have reviewed and acknowledged the appropriate data confidentiality agreements. These procedures ensure that confidential WRIS information is only accessed by approved entities.

AREA 2: WRIS USER EDUCATION AND AWARENESS

Representatives from the participating states described in detail their methods for training agency employees and specific training for employees who work with the WRIS. These training programs are conducted to ensure employees' understanding of the confidential nature of wage data and proper use of the technology systems used to facilitate the exchange of wage data information between participating states.

All of the interviewed states require their employees, including those with a role in the WRIS, to complete a state-specific form of data security and IT systems training. In many cases, employees are required to complete several online training courses. After completing the initial training, employees often must complete annual "refresher" courses or other regular training updates.

In several states, individuals with WRIS access receive training based on their responsibilities in the organization. This basic training is supplemented with ETA-sponsored training sessions, webinars and manuals. Several states also require employees to complete ethics training on a regular basis to reinforce the importance of protecting personal and sensitive information. Additionally, it was noted that all states make their training resource materials and policies readily available on their Internet and Intranet portals or through some other digital platform.

All of the states visited acknowledged the support that they receive from the WRIS Operator, Affiliated Computer Services, Inc., or ACS. Working with ETA, ACS has developed a WRIS Clearinghouse-specific manual that provides step-by-step instructions on requesting and receiving data via the WRIS. ACS provides similar support for the SUIA agencies that respond to incoming requests for wage data. In conjunction with ETA, ACS has supported training and informational sessions and webinars on WRIS.

In addition to online training, training sessions and webinars, a few WRIS states take a more personal approach to WRIS training. In one state where a small group of employees has access to WRIS wage data, a supervisor, who has a thorough understanding of the WRIS DSA and was one of the originators of the state exchange system, provides training and supervision to his subordinates. The employees also receive a copy of the DSA and a WRIS user manual. In another state, training is provided through mentoring and instructions provided to the state when it first entered the WRIS.

In all cases, training is not complete until individuals sign various acknowledgement documents. As required by provisions of the DSA, all participating WRIS states have their employees who access wage data sign the 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.

The reviewers noted that all states clearly understand the importance of properly managing confidential wage data and have a full range of training courses in place to ensure its security. Participating states recognize that providing

rigorous training on WRIS procedures, data security and IT systems will help eliminate the possibility of security breaches. In turn, this enhances employee knowledge about the WRIS system and its role in helping states assess the performance of training programs authorized under WIA and other authorized programs.

AREA 3: ADMINISTRATION AND OVERSIGHT PROCESSES

The reviewers saw firsthand the steps participating WRIS states are taking to ensure compliance with the DSA with regard to WRIS administration and oversight processes. All participating states have systems in place to track and monitor employee access and use of WRIS wage data, as well as procedures to respond to a security breach, should one occur. Representatives from participating WRIS states also described to the reviewers the challenges encountered related to the retention and destruction of data.

Some WRIS states 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. Using security features that track and monitor employee access to systems storing WRIS data is another method used by participating states. Some states have dedicated security officers to ensure controlled access to all electronic files, servers and systems. Other states even produce logs that track how long individuals are in the system and note if they produce any printed output. Several states have established procedures that eliminate the need to print any WRIS-related information. This removes the need to establish procedures for storing or disposing of WRIS-related printed materials. Additionally, password-protected log-in procedures are used as an added security layer to ensure that only authorized users are allowed access to sensitive WRIS wage data. These and other security steps are designed to discourage the misuse of the WRIS system or accidental disclosure of WRIS data.

Additionally, while some states do not include WRIS functions specifically in individual employee evaluations, they do have procedures that require regular reviews and participation in ETA-sponsored trainings and webinars. Participation in these activities, along with state-mandated training, is documented in the employees' performance evaluations.

All participating WRIS states have established processes for responding to a security breach. Representatives from participating WRIS states told the reviewers that standard procedures begin with internal notification followed immediately by advising ETA and the WRIS Operator. Several states noted that there are comprehensive forms and questionnaires that are required by state law that fully disclose the nature and extent of the incident. In some states, based on the severity of the breach and the state notification policy, information would be forwarded to the governor's office. As mentioned earlier, all states have some ability to track user access to IT systems and data records, including WRIS wage data stored on agency networks. These systems allow IT personnel to determine or trace who accessed the system in the event of a breach.

In conducting their interviews, the reviewers found that data retention and destruction practices varied among the participating WRIS

states. Data retention policies were typically divided into PACIA and SUIA approaches. PACIA agencies typically hold WRIS information long enough to support their performance reporting obligations. For example, in one state, data are retained for the federally mandated minimum of three years while another state maintains data records containing wage data obtained through the WRIS for a period of no longer than six years before qualifying electronic records are deleted. SUIA agencies tend to hold incoming data requests containing SSNs for short periods that are sometimes measured in hours and typically last no longer than one calendar quarter before being deleted. PACIA files are deleted manually, while most SUIA-related data are deleted automatically. There is a common interest among all states in discussing data retention and destruction policies further through the WRIS Advisory Group.

WRIS participating states have developed a variety of systems and procedures for guarding against improper access and misuse of WRIS wage data and personally identifiable information. In the event of a security breach, states have developed processes for notifying the appropriate parties and pinpointing the cause of the breach by tracking user access. Additionally, WRIS members recognize the importance of proper data retention and destruction practices as it relates to overall wage data security, and are continuously evaluating ways to enhance their procedures.

AREA 4: DATA TRANSMISSION

All the interviewed states demonstrated that the secure transmission and validation of WRIS data was their highest priority. Most states reported an efficient process for transmitting and receiving data via the WRIS, and all states reviewed were pleased with the responsiveness of the WRIS Operator and the support received from ETA.

Wage data obtained via the WRIS is used to augment performance data obtained from state wage records to complete the states' workforce program reporting requirements. Generally, WRIS state administrators employ several actions to access the WRIS wage data. A few states have their data transmission handled by separate entities for the PACIA and SUIA, while most smaller states work within one state entity. Several safeguards are in place to ensure that the risk of a data breach is minimal, and if a data breach does occur, all states have a specific protocol in place to inform authorities.

Each state designates state employees as the operators who are responsible for data transmission to and from the WRIS Clearinghouse. This applies to both the PACIA and SUIA agencies. These individuals are familiar with WRIS procedures and maintain a close rapport with the support staff of the WRIS Operator. States assign and train backup operators in the event that the primary person responsible is absent. These state operators all follow the very clear and concise instructions developed by the WRIS Operator. Each state's PACIA has an established process for retrieving wage data supplied by the WRIS and storing it on a secure network or dedicated workstation.

This information is then used to augment the state's performance reports for WIA, Wagner-Peyser, Trade Adjustment Assistance and Veterans' Employment and Training Service programs. The SUIA agencies have all worked with the WRIS Operator to establish a secure

link to provide data to the Distributed Database Index of wage earner SSNs and to respond to incoming requests for state wage information. In the majority of cases, the SUIA agencies have implemented fully automated programs to provide wage data to the WRIS.

The PACIA process involves direct access to, and handling of, wage data supplied through the WRIS Clearinghouse. Given the extremely sensitive nature of this information, all states restrict access to this information and control where it is stored and how long it is saved. Conversely, the SUIA process is almost entirely automated with no direct access to, or handling of, incoming requests consisting of SSNs supplied through the WRIS Clearinghouse. SUIA operations involve state wage and employer data which are housed in secure facilities with controlled access.

Data received from the WRIS Clearinghouse is stored on a secure server for a period of time determined by state policies and laws. As noted above, the PACIA retains this information for a period of time required to fulfill performance reporting requirements. The SUIA retains this information only as long as it is needed to respond to the request, often deleting the data file immediately after completing the transmission. In addition to the data stored on secure network drives, several states create an archive copy of the data and store it on an optical compact disk or removable hard drive. These portable media were observed to be stored in locked cabinets in secure access-controlled facilities, and were not accessed or used outside of these controlled spaces. In a limited number of instances, printed materials were produced that contain wage data obtained through the WRIS Clearinghouse. This information was used to support validation of ETA-related performance data. The reviewers observed the locked cabinets where this information was stored and reviewed the procedures regarding how this information was controlled, archived and destroyed. In each case the reviewers confirmed that the handling of this information conformed to state rules and regulations regarding protecting personal information.

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. These requests typically yield a small increase in absolute terms (~ 2 to 5 percent) for WIA participants and a slight (~ 1 percent) increase in absolute terms for Wagner-Peyser participant outcomes.

In approaching data transmission, a number of states have incorporated standards from other federal regulatory agencies such as the National Institute of Standards and Technology (NIST). NIST publishes standards regarding data transfer and storage. States have also reviewed federal statutes such as the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA) to understand all approaches to secure data transmission.

The reviewers observed and discussed how each state has developed and documented its processes and systems tied to the WRIS data interchange process. Several states have dedicated security officers who regularly review these procedures to ensure their reliability, particularly in light of ever-evolving electronic security threats.

Data quality is a common interest in all states as it pertains to the request for, receipt of and supply of wage data. Most state workforce

agencies have a feature in their self-service case management systems that filter SSNs that don't conform to the Social Security Administration's guidelines. These describe what sequence and combination of numbers could represent an SSN. The reviewers observed that a number of states "scrub" or filter the SSNs that they provide to the WRIS Clearinghouse. Despite this effort, several states reported instances of non-conforming SSNs appearing in their data files with wage data attached. Another common issue reported by the states is an SSN returning reported wages from an improbably large and distributed number of states.

For every state PACIA, wage data requests and responses are transferred via a secure file transfer protocol (FTP) server hosted by the WRIS Operator. As indicated in the DSA, permission to log on to this system, referred to as the WRIS Clearinghouse, is restricted to approved individuals. All of the states reviewed have approved a limited number of employees who are directly involved in data transmission. They are identified by the state and ETA confirms their access clearance. The WRIS Operator then assigns an access password to each approved state operator. These passwords are automatically reset after 90 consecutive days if there are no log-in attempts. All individuals who access the WRIS Clearinghouse and/or wage data obtained through the WRIS have completed confidentiality acknowledgements as required under the DSA.

State SUIA agencies provide quarterly records from state wage records and respond to incoming WRIS requests using an automated and paperless 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 Operator to ensure complete data transmissions.

SUIAs in many states have an automated and well-tracked process to receive and respond to requests for wage data. States have a specified response time to address incoming requests. In numerous states, an automatically generated production report notes a successful WRIS response and provides additional information if there is a response failure. In the event this occurs, the program automatically issues an e-mail to the state IT operator and the WRIS Operator.

Several states reported that their SUIA data transmission procedures comply with Internal Revenue Service rules for handling personal information such as SSNs and are subject to an annual audit by state and/or federal examiners. During this transmission process, there are no printouts of data files. States reported that files containing SSNs (WRIS request) and files containing wage data (WRIS response) are stored temporarily on a secure server with controlled access. These files are deleted after the response data are loaded into the states' respective case management systems.

AREA 5: PHYSICAL SECURITY OF WRIS DATA

All interviewed states demonstrated robust data security measures to safeguard wage data obtained via the WRIS. All PACIA and SUIA data transmission and storage processes involved limited password-protected access. Data security was observed at every step of the transmission process including the use of encrypted files, compartmentalized access to data, removal or masking of SSNs, labeling of WRIS-supplied wage data, and the ability to isolate or remove WRIS-specific data from system files. A number of states employed data encryption software on any portable electronic storage device, including laptops, CDs, flash drives or removable hard drives.

Several states instituted software utilities in their case management systems that replace SSNs with unique identifiers. Others follow a similar approach by masking or removing direct access to SSNs and other personally identifiable information. Several states initiated policies and practices that preclude the printing of any WRIS-supplied wage data.

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 are required to review the DSA. All interviewed states maintain comprehensive procedures and regulations concerning data security and the handling of personal information. Each state also had defined procedures to notify state and federal agencies, including ETA, in the event of a data security breach.

Most of the states interviewed require new employees to undergo background checks, and require employees to complete training in data security and acknowledge ethics guidelines and regulations. 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.

The majority of data acquired via the WRIS for PACIA reporting are stored in secure drives tied to the states' case management systems. As noted previously, all of the interviewed SUIA agencies delete the incoming data request files containing SSNs after providing a response. The reviewers found that no state held data for more than one calendar quarter, and most deleted these files immediately after a response was provided.

There were a few instances of materials being printed that contain WRIS-related information. All of the examples observed by the reviewers were tied to the data validation process. The reviewers noted that printed materials are secured in locked file cabinets in guarded and/or access-controlled buildings. Several PACIAs create electronic backup copies of WRIS return data that are stored on optical disks or removable hard drives. In both cases, these portable media are locked in filing cabinets in access-controlled buildings.

The reviewers attempted to personally observe all 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 and staffed with cleared personnel. All of the individuals who work with wage data obtained through the WRIS are aware of their obligations under the DSA to shield exposure to sensitive

information. This includes taking steps to avoid direct visual access to computer monitors, securing any printed materials in locked containers, employing timed password-protected screen savers and following state guidelines on protecting passwords and log-in codes. The workspaces that were examined were found to be secure with limited sight lines, minimizing visual access to passersby. These facilities also provided well-marked document disposal shredders or bonded disposal bins.

The reviewers conducted a similar review of SUIA operations. In most cases, these physical inspections involved data processing centers containing mainframe computers. All of these centers employed extensive, layered security where staff and visitors "key in" and "key out" to maintain 100 percent accountability of who has entered the secure areas. The reviewers found that most personnel that work in these data centers undergo further extensive clearance processes, given the nature of their work and the access they have to wage and personal information. Several states incorporate Internal Revenue Service guidelines into their data security procedures. These include the proper way to delete electronic records, and specifications on limiting sight lines to computer monitors to preclude co-workers from observing or recording sensitive information. During the SUIA agency tours, the reviewers did not observe any printed materials containing wage data obtained through the WRIS.

The reviewers were not able to directly observe all of the data servers and mainframe computer systems that contain wage data supplied via the WRIS. Several states operate secure facilities that exclude visitors and severely limit access. These facilities have the latest data security features and employ state-of-the-art physical protection and disaster recovery backup methods.

The importance of data security has been clearly communicated to staff. State resources include the existence of multiple safeguards and assigned staff to monitor security procedures and take the necessary steps to minimize the possibility of a data breach. In several states, the governor and other state leaders emphasize data security, including legislation protecting personal data. Many states provide continuous monitoring to ensure security and minimize the occurrence of a data breach.

All interviewed states employ proactive security measures and policies to minimize the possibility of a data breach. One state uses an automated program to identify SSNs in outgoing e-mail messages. This program automatically scans every outgoing e-mail to ensure that SSNs are not included. This state also requires that electronic messages containing personally identifiable information be encrypted. This extends to flash drives which are automatically programmed with encryption software. Several states have an active scanning feature on their networks that track users to ensure compliance with state data security and IT system usage regulations. One state suspends user access to the network if an individual has not logged on during any 30-day period. If there is no account activity after 60 days, the account is closed.

One of the interviewed states conducts regular reviews of its IT security system and contracts with an outside vendor to test the system every three years. The review examines the security system by conducting internal and external attempts to penetrate the electronic defenses. The state also uses closed-circuit television cameras and employs biometric-controlled access to sensitive areas, including computing centers housed in the facility.

Several states employ dedicated security officers who monitor compliance with state and federal data security regulations. In addition to monitoring access, these security officers and their staff review state policies, update training, research government and commercial practices and compile findings to inform state leaders. These individuals play a critical role in how states would respond to data breaches by investigating and establishing the extent of a breach, should one occur.

The general assessment is that every state has instituted comprehensive security measures that meet or exceed the requirements of the DSA.

AREA 6: ROLE OF CONTRACTORS

Roughly half of the states visited noted that they have entered into an agreement with a contractor or consortium to either supply a data management system and/or to receive operational support. The two service providers observed were America's Job Link Alliance (AJLA) based in Topeka, Kansas, and Geographic Solutions, Inc., (GSI) based in Palm Harbor, Florida. The reviewers had the opportunity to visit both organizations and learn firsthand how they are providing data management and performance analysis support to WRIS member states.

All states that engage contractor support have included the requirements of the DSA into their contractual agreements. These agreements also clearly define what information the contractors are authorized to access and how it must be handled.

Contractors provide data management, analysis and reporting tools via Web-based platforms. These products and services are used by states for comprehensive case management, labor market information, job matching and performance reporting.

Both AJLA and GSI offer their clients server-hosting facilities but also can provide support to systems based in state computing centers. Both contractors work from access-controlled facilities that employ current security, fire suppression and disaster recovery systems.

The reviewers noted that states engaging contractors' support understood their obligations under the DSA and had established agreements that defined the specific role of their service provider.

Summary

In fulfillment of its responsibilities under the DSA at Section VI.C.2, ETA sponsored 15 Confidentiality Reviews during 2009 and the first quarter of 2010. The results of each Confidentiality Review will be shared with each state individually. This Annual Report serves as a compilation of the observations and records those policies and practices that may be valuable to other states in improving their data security systems. From these observations, it is clear 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 Confidentiality Reviews 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 be identified during the review, ETA, under DSA Section IX. D, has the responsibility to work with the state to resolve the issue immediately to avoid further action. None were observed. The reviews provided an opportunity for ETA's representatives to learn how states are addressing their obligations as members of the 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 prepared with resource documents, organizational charts and training materials, and made available the key individuals that support WRIS activities.

ETA plans to incorporate these observations in future training programs to meet the evolving needs of the WRIS community. It is generally understood that data security threats constantly change, requiring ETA and the participating states to continually review and update policies and procedures to avoid a breach in security. Subsequent on-site reviews will continue to focus on innovations that will keep sensitive information secure.

WRIS Acronyms and Definitions

Access Acknowledgement

Access Acknowledgement document, the document signed by individuals who have reviewed and agreed to the terms of the WRIS Data Sharing Agreement

ACS

Affiliated Computer Services, Inc., the WRIS Operations contractor

Aggregate Data

Data that has been stripped of any information that would identify the individual(s) to whom the data pertains, including but not limited to, name and Social Security number (SSN), and that have been aggregated into a group(s) containing no fewer than three records, provided however, that nothing herein shall prevent a PACIA from observing a more stringent aggregation policy with regard to its own use and reporting of data

AJLA

America's Job Link Alliance is a consortium of workforce agencies whose primary purpose is to maximize return on investment in workforce development information technology.

DDBI

Distributed Data Base Index, an index of all SSNs for which wages have been reported to participating states over a period of up to eight quarters. The DDBI contains three information items for each entry: SSN, quarter for which wages were reported, and the state that holds the wage record. Participating states continuously update the DDBI, in accordance with a schedule determined by the WRIS Advisory Group.

DOL, USDOL

United States Department of Labor

DSA

WRIS Data Sharing Agreement

ETA

Employment and Training Administration

FERPA

Family Educational Rights and Privacy Act (FERPA), 20 USC 1232g, a federal statute protecting an individual's right to privacy of his/her educational records

FIPS

Federal Information Processing Standard

FISMA

Federal Information Security Management Act

FTP

file transfer protocol, a standard network protocol used to exchange and manipulate files over a TCP/IP-based network, such as the Internet

HIPAA

The Health Insurance Portability and Accountability Act of 1996, which protects the privacy of individually identifiable health information

IT

Information Technology

LMI

Labor Market Information

NIST

National Institute of Standards and Technology

OIG

Office of the Inspector General

OMB

Office of Management and Budget

Operations Contractor

the entity responsible for the technical operation and maintenance of the WRIS Clearinghouse hardware and software, and for providing technical support to states participating in the WRIS

PACIA

the Performance Accountability and Customer Information Agency designated by the governor to be responsible for coordinating the state's program for assessing state and local program performance and evaluating training provider performance as required under the WIA

PII

personally identifiable information

Query

describes an inquiry seeking Wage Data sent from the WRIS Clearinghouse to the SUIA in a participating state

Reply

a response from a SUIA to a Query

Request

a request for Wage Data received by the WRIS

Result

describes the Wage Data transmitted from the WRIS Clearinghouse to a PACIA in response to a Request

State

includes all fifty states, as well as the District of Columbia, Puerto Rico and the Virgin Islands

SUIA

the state agency that holds wage data, whether or not such agency also administers the state's unemployment insurance program

Wage Data

individually identifiable information reported quarterly by employers as required by Section 1137(a)(3) of the Social Security Act including, but not limited to, employer names and employee names, SSNs and associated wages

Wagner-Peyser programs

programs authorized under the Wagner-Peyser Act, 29 USC 49 et seq

WIA

Workforce Investment Act

WIASRD

the standardized records on individual participants that states must submit to the Secretary of Labor for clients receiving services under the WIA, per Section 185(a)(3)

WRIS

Wage Record Interchange System, an automated system for facilitating the exchange of Wage Data between participating states for the purpose of assessing the performance of individual training providers and state employment and training programs; preparing and submitting reports to the 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; supporting research and evaluation efforts, and for other purposes allowed under law.

WRIS Clearinghouse

the location of the central processing operation through which WRIS Requests, Queries, Replies, and Results are processed. The WRIS Clearinghouse is operated by the Operations Contractor.