U. S. Department of Commerce
National Oceanic and Atmospheric Administration

OCIO Boulder
Technical Administrative Support Branch (TASB)
Local Area Network (LAN)
NOAA1005

PRIVACY IMPACT ASSESSMENT

June 2009

Prepared by: Steve Hauwert, TASB Boulder

Reviewed by: Sarah D. Brabson, NOAA Office of the Chief Information Officer

Project: OCIO Boulder Technical Administrative Support Branch (TASB) Local Area Network (LAN)

Unique Project Identifier: 006-00-02-00-01-0511-00-404-139

IT Security System: NOAA1005

Project Description:

The OCIO Boulder TASB Local Area Network (LAN) (NOAA1005) is a general support system managed and operated by NOAA's Office of Chief Information Officer, System Support Division. It consists primarily of Windows based workstations and file servers. There are two locally developed databases on the NOAA1005 system that contain personally identifiable information (PII). These systems are the "Relocation Payment System (RPS)" and the "Year End Solutions" (YES) system.

The RPS is used by the Mountain Finance Branch to collect tax information pertaining to permanent change of station moves. RPS system has been replaced by the Integrated Travel Manager Relocation (ITMR) system, but RPS and the PII information it contains is still being retained for tax purposes.

The YES system is used by the Mountain Finance Branch to produce the Internal Revenue Services Form (IRS) W-2, Wage and Tax Statement, for transferred employees, and to send the W-2s to the Social Security Administration (SSA) and IRS.

The Mountain Finance Branch, which processes the W-2 information for all NOAA's relocation moves. It acquired the YES system to produce the W-2s for the travelers, and to create and transmit a consolidated file to IRS.

This PIA has been developed to comply with the requirement in Section 208 of the E-Government Act of 2002 (44 U.S.C. 36) and the Department of Commerce IT Privacy Policy.

1. What information is collected (e.g., nature and source)?

The fields used by RPS and YES include name of employee, Social Security Number (SSN), home address, federal income tax withheld, and other reimbursements, deductions, and withholdings that must be reported to IRS and SSA.

The employee makes a permanent change of station move and the paperwork is completed upon entry of duty. The employee completes a form CD-150, Request for Authorization of Travel and Moving Expenses, and this information was entered into the RPS before it was retired and is now entered into the ITMR system. Information from RPS and ITMR provides the source data for the YES system. Information from form CD-370, Travel Voucher, is another source of input to RPS and YES. The data from the Travel Voucher is used to calculate the withholding taxes.

2. Why is the information being collected (e.g., to determine eligibility)?

The information is being collected to determine employee and employer tax liability for the relocation expenses and reimbursements.

3. What is the intended use of the information (e.g., to verify existing data)?

RPS was used to determine the amount of monthly tax payment for the employer and determines the amount of the transfer employee's yearly tax liability. The RPS data was used to create the consolidated file for transmittal to IRS and SSA. RPS has been replaced by the ITMR system.

The YES system creates the W-2s that are sent to the transferred employees and creates the wage reporting electronic transmission file for the IRS and SSA. There are checks and balances in the RPS and YES systems to prevent duplication of information. Errors found are reported back to appropriate staff for corrective action.

The RPS and YES data are not used to assist users in identifying previously unknown areas of note, concern, or pattern. (This practice is sometimes referred to as data mining.)

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

The information is shared only with the IRS and SSA. The transferred employee receives a copy of the W-2 with the information. RPS and YES information is only shared with the transferee and the IRS via the SSA. The data is not shared by other individuals or systems other than individuals directly responsible to report this information.

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how may individuals grant consent?

Information for the RPS system comes from the CD-150, Request for Authorization of Travel and Moving Expenses; CD-29, Travel Order: and CD-370, Travel Voucher. These are completed by the employee as a precondition for authorization to travel and receive reimbursement for travel and relocation.

6. How will the information be secured (e.g., administrative and technological controls)?

Management Controls:

TASB Boulder performs daily scans for network vulnerabilities and performs security updates as required.

The Mountain Finance Branch staff with authorized access to request information from the database is limited. Requests from serviced organizations must be from authorized staff and processed through official channels. Any request received from outside official channels is investigated to determine if it is an attempt to fraudulently obtain data. If it is a legitimate request, the requestor is directed to submit the request through official channels and in writing.

Operational Controls:

Physical access to the computer that hosts NOAA1005 is protected by uniformed DOC police at the drive-in gate and main entrance. Video cameras cover all entryways. A random numeric keypad can be used to gain entry to the building. A random numeric keypad is also used to restrict access to the TASB Boulder ADP room located in the David Skaggs Research Center Building, GB503. The cable plant MDF and IDF rooms are also restricted access via random numeric keypad in this building. Daily backups are performed. Data access is restricted. Access is not available to the public and users must be authorized to have access to the applications.

The RPS system is direct data entry from the CD-150 and Travel Voucher. The electronic file generated from this system is input into the YES system along with ITMR electronic file produced from the travel manager system. These files all reside on the TASB Boulder network. The W-2s produced by the YES system are printed and delivered to the client via mail in envelopes. The envelopes are sealed and clearly stamped/marked with the notation "Privacy Act Materials". The electronic file containing Transferee W-2 information for all NOAA is forwarded directly to the IRS by the TASB Boulder using the SSA's Business Services Online Secure Web site. This can only be done by the person registered to access the Web site.

Technical Controls:

The RPS and YES systems are stored on the OCIO TSB LAN file servers and access is restricted to only those individuals who require the information to perform their job function. To obtain access, a written request must be submitted by a management level employee with responsibility for the data. A firewall protects the network and is configured to deny any traffic originating outside the LAN and an Intrusion Detection System (IDS) is in place on the campus network. Remote access to the information, when it is required, is accomplished via a Citrix server which is configured to eliminate any direct file transfer between the server and a connected computer. Thus the data is accessible, but never actually stored on the remote device.

Access controls are implemented on production systems through the use of system usernames and passwords as well as database (application) usernames and passwords. There are no automated access audit logs within either of the databases. Microsoft Windows access rights and audit logs are used to restrict and monitor access to the files which make up the databases. These audit logs are reviewed on a monthly basis or more often if the situation warrants it. Password length and duration of validity follow Department of Commerce

standards as outlined in the *IT Security Program Policy and Minimum Implementation Standards.*

A Security Certification and Accreditation (C&A) in accordance with the requirements of the Federal Information Security Act of 2002 (FISMA) is current and in force. The C&A process is an audit of policies, procedures, controls, and contingency planning, required to be completed for all federal government IT systems every three years.

Data Extract Log and Verify Requirement:

The applications, (RPS and YES) do not directly support a database extract by end-users. RPS and YES contain PII. There are only two instances for extracting data. The first instance is to produce a W-2. All transferees in the database for the prior calendar year will receive the W-2. The W-2 is placed in an envelope and stamped to indicate the content is 'Privacy Act' materials. The extraction data is not retained. The RPS system was a source for the W-2 Extraction in prior years but is no longer being used and is replaced by the ITMR system. The RPS database is still being retained for tax purposes. The second instance for extraction is to produce a file for the IRS. This extracted information will be kept longer than 90 days in accordance with the IRS regulations. The file is assigned a batch number and year. Only the Relocation Specialist has access to this information.

The RPS/ITMR systems produce the annual file extract of W-2 and IRS 941 related information. This data includes employees' SSN and income related information. As part of the IRS 941 and W-2 process, this information is generated from the application as a file and submitted to the IRS as part of NOAA's formal reporting procedures. This data is retained for four years in accord with IRS directions. Other than this, there is no data extract/reporting performed on the RPS and YES systems

While there are currently no extracts being retained other than for the purpose of IRS reporting, beginning in Q4-FY08, for any PII/BII extracts resulting from RPS, ITMR, or YES that have not been destroyed after 90 days, an e-mail is sent requiring e-mail confirmation that either the PII data has been destroyed or that the need continues for an additional 90 days. Data extracts sent to Treasury for disbursement of funds or for IRS reporting via W-2 or 941 processing are exempt from this tracking requirement since this data is required by law and these organizations must retain this information.

7. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

No. The existing Privacy Act system of records notice for DEPT-18 Employees Personnel Files Not Covered by Notices of Other Agencies, applies to the personal information in this system.

8. Are these records covered by an approved records control schedule?

The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the

Federal Government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. GRS 1, Civilian Personnel Records, and GRS 2, Payrolling and Pay Administration Records, apply to most of the underlying paper records in this system.

RPS contains six years of information in the system or approximately 300 transferees. This information is kept throughout the system lifecycle. This is a retired system. YES contains four years of information. The incoming data is for all of NOAA (from the Local RPS and ITMR) and contains approximately 500 records. Current and historical information from the RPS and YES are needed to conform to IRS regulations and maintain the ability to review internal processes for quality review or analysis.