

**U.S. Department of Commerce (DOC)
National Oceanic and Atmospheric Administration (NOAA)
Office of the Chief Information Officer (OCIO)**



**National Weather Service Eastern Region
ER LAN/WAN
Privacy Impact Assessment**

November 15, 2013

Prepared by: Shine Kang, NWS Eastern Region, ISSO

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

FOR OFFICIAL USE ONLY

NWS ER LAN/WAN

Name-of-System: NOAA8882

Unique Project Identifier: 006-000351104 00-48-02-00-02-00

Project Description: The NWS Eastern Region (ER) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees, contractors, volunteers, and other individuals who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of tracking job vacancies, developing statistical reports, and performing other related administrative tasks. Weather Forecast Offices (WFO)/River Forecast Centers (RFC) maintain local databases that contain information on volunteers who provide weather reports to them.

This PIA is prepared in accordance with NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010.

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

The NWS ER WAN/LAN system maintains information concerning each member of the ER workforce. This information is managed by the NWS Easter Region Headquarters (ERH) Administration Personnel.

The information maintained on these databases consists of:

- Name /Position /GS Level/Series/Service Computation Date/Date of Grade/ Date of separation
- Residential information (Address, phone number/s)
- Government email addresses
- Division/Organization Name
- Regional Office Location
- Optional text field with current/relevant personnel issues.

ERH administrative personnel do not require SSN or DOB on the following documents:

Time and Attendance
Leave Slips
Travel Vouchers
Employee Resumes
Performance Appraisals
Personnel Actions

FOR OFFICIAL USE ONLY

NWS ER LAN/WAN

In addition, Administrative personnel do not store or process sensitive PII data for any Admin, Human Resources, and/or Payroll processes. WAN/LAN does not process personnel actions.

Asset information in the form of Internet Protocol (IP) Addresses is maintained by the IT Staff and only those individuals have access to the IP information.

There are also local databases at the local WFO/RFC that maintain information on volunteers who provide them weather reports. The databases hold all of the following information on these volunteers:

- First and last name
- Mailing address
- County
- Phone (home/cell)
- Email address (personal email, not NOAA email)

All of this information collected on volunteers is provided voluntarily and most people who sign up do so during a community outreach training program, known as “spotter talks.” An ER staff is responsible for the maintenance of this database. This database information is accessible for viewing by all staff members in order to make calls for severe weather information.

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

The information is used by Eastern Region to supplement managing employee records, maintaining organizational readiness, and maintaining other administrative records.

IP addresses are collected by the IT staff to aid in locating computers and systems at the location.

The WFO/RFC database information is collected to contact volunteers when severe weather information is needed.

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

The ERH database information is used by ERH Administration Staff to supplement the management of employee records, provide statistical data, track volunteers and students, etc.

FOR OFFICIAL USE ONLY

NWS ER LAN/WAN

IP addresses are collected by the IT staff to aid in locating computers and systems at the location.

The WFO/RFC local databases are used to collect severe weather information from volunteers that may assist the public.

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

The information is not shared with any third party or other unauthorized personnel. The information is not available to the general public, other NWS regions, or other NOAA components.

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?

Prospective volunteers must provide their contact information in order to be selected as a volunteer; the information is necessary for effective performance of volunteer duties. The volunteers' information is sent to HR for record keeping purposes. Employees and contractors are required to provide their PII as a condition of employment; however, this information is not stored in ER. All the employee information is sent to Workforce Management Office in Norfolk, VA. To mitigate unnecessary risks to this personal information, only authorized ERH Administration staffs handle the data.

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

The information is secured in accordance with FISMA requirements. The most recent Assessment and Authorization was completed on June 7, 2013). The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a Moderate.

Management Controls

All employees and contractors undergo a national agency check with inquiries (NACI) security check when employed or contracted. This involves a check of Federal and local law enforcement records to help ensure the trustworthiness of the employee. Every year the IT system undergoes a thorough Continuous Monitoring for the Assessment and Authorization (A&A) process that is performed by a NWS Security Team. The A&A

FOR OFFICIAL USE ONLY

NWS ER LAN/WAN

process ensures that the security plan and operational, management, and technical controls meet Department of Commerce (DOC) guidelines for continued operation. All security controls are reviewed and approved by the system and database administrators, developers, and managers prior to implementation. Contractors that have access to the system are subject to information security provisions in their contracts required by DOC Policy.

Every year the IT system undergoes a thorough Continuous Monitoring for the Assessment and Authorization (A&A) process that is performed by a NWS Security Team. The A&A process ensures that the security plan and operational, management, and technical controls meet Department of Commerce (DOC) guidelines for continued operation. All security controls are reviewed and approved by the system and database administrators, developers, and managers prior to implementation.

The current Authorization to Operate (ATO) under the [Federal Information Security Management Act of 2002](#) (FISMA) was renewed on June 7, 2013.

Operational Controls

The information is maintained on systems that are located in a locked computer room located in NWS ER Headquarters in Bohemia, NY. Access to the computer room is limited to those with a demonstrated need for access and support personnel. Access to the computer room is monitored and access logs are maintained. All visitors are escorted by authorized personnel while in the computer room. Access to the server is controlled by a separate log-on process, which is also monitored for anomalous activities. The computer room has appropriate environmental security controls, including measures to mitigate damage to automated information system resources by fire, electricity, water, and inadequate climate controls.

Technical Controls

Access controls are used on the production equipment through the use of system usernames and passwords, as well as database usernames and passwords. With the HSPD-12/Common Access Card (CAC) deployment (Phase I and Phase II completion in 2012), all the Windows system users are mandated to use the CAC card for authentication through Active Directory. Access logs are maintained and reviewed for any improprieties. Password complexity and duration of validity adhere to established DOC IT security standards.

The databases are routinely updated, at least on a monthly basis, to reflect current information about ER employees. Records are deleted from this database once an employee is no longer employed in the region. The database is backed up on a regular basis.

FOR OFFICIAL USE ONLY

NWS ER LAN/WAN

Data Log Extract and Verify

Currently, the process for logging and monitoring data extracts is manual. Access to the database is limited to a few systems administrators and human resources personnel. Individuals with access are advised on the requirement to destroy all data extracts once they are no longer needed.

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 Notices ([SORNs](#)) for DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, and DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies, apply 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 Chapter 1300 National Weather Service Records Disposition Schedule and 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. The underlying paper records are covered by GRS 1, Civilian Personnel Records.

Chapter 1300 National Weather Service Records Disposition Schedule for Service Locations Data Networks states the following:

Records that provide information on specific service locations and areas, and data networks used in tracking hydrologic, hydroclimatic and meteorologic observations. This series contains electronic and hard copy documents relating to the establishment, modification, maintenance and administration of data reporting networks. Metadata that identifies the details regarding the site are also included. The record keeping copy is kept at each WFO; reference copies are also kept at Regional Headquarters and the RFCs.

AUTHORIZED DISPOSITION:

- A. Record keeping copy: Destroy or delete when WFO is closed, or when networks are replaced by newer equipment or facilities.
Transfer to new facility that assumes responsibility.
- B. Reference copies: Destroy when no longer needed for reference.
- C. Electronic copies created on word processing and electronic mail

FOR OFFICIAL USE ONLY

NWS ER LAN/WAN

systems: Delete after record keeping copy is produced.

Workforce database records are retained until the data is determined to be incorrect or no longer current. The data is then updated to reflect current information. When a record is corrected, the corrected information overwrites the incorrect information, which is not retained.