

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



**National Weather Service Southern Region
Southern Region GSS (NOAA8884)
PRIVACY IMPACT ASSESSMENT**

July 2010

Prepared by: Gary Petroski, NWS Southern Region, ISSO

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

National Weather Service (NWS) Southern Region General Support System (GSS) (NOAA8884)

Unique Project Identifier: 006-48-01-12-02-3118-00 (NWS Regions and Fields)

NOAA System ID: NOAA8884

Project Description:

The NWS Southern Region General Support System (GSS) has databases which 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.

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

The NWS Southern Region GSS maintains information concerning each member of the Southern Region workforce. This information is managed by the NWS Southern Region Headquarters Administration Personnel. Only the Workforce Manager, Senior Management and the IT Database administrator have access to these workforce databases. The databases are located on SRH-S-NAS/Dirmass directory which is secured and restricted to authorized personnel only. There are miscellaneous hardcopies of files with PII information that are kept in the human resources office and secured in locked cabinets.

The information maintained includes:

- Name /Position /GS Level/Series/Service Computation Date/Date of Grade/ Date of loss
- Government e-mail addresses
- Division/Organization Name
- Regional Office Location

The NWS Southern Region GSS maintains information concerning each member of the Southern Region workforce for budgeting purposes. This information is managed by the NWS Southern Region Headquarters Administrative Management Division (AMD). Only the Administrative Management Division personnel and the IT Database administrator have access to these budget databases. This database is located on SRH-S-NAS/AMD\$ and is a secure, restricted drive.

The information maintained includes:

- Name /Position /GS Level/Series/ Service Computation Date /Date of Grade/ Date of loss

- Government e-mail addresses
- Division/Organization Name
- Regional Office Location
- Award money allocated

There are also local databases that maintain information on volunteer weather spotters who provides weather reports to the field offices. The databases hold the following personally identifiable information (PII) about each volunteer:

First and last name

Mailing address

County

Phone (home/cell)

E-mail address

Hours they can be contacted for severe weather reports

Whether they have a rain gauge, anemometer, thermometer, snow stick, or weather station

Brief description of where they live, e.g., 2 Miles West of Pleasant Hill)

Latitude / Longitude

All of this information is collected voluntarily; volunteers sign up and provide the information during spotter talks NWS provides in preparation for the severe weather season. A locally assigned person is responsible for the maintenance of each database, with occasional data entry assistance from one or two other staff members. Database information is accessible for viewing by all staff members so that they can make calls for severe weather information.

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

This information is maintained to aid in tracking job vacancies, maintaining organizational readiness, and conducting other administrative activities.

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

The information is used by Southern Region Headquarters Administration staff to aid in managing employee records, providing statistical data, tracking volunteers and students, and other administrative and program activities.

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 parties or unauthorized personnel. The information is not available to the general public, or to other NWS Regions. Official telephone and contact information is taken from the databases to populate the Southern Region employee and office locator database which is available only to members of the NWS Southern Region. Other PII about individual personnel is available only to the Workforce Manager.

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 and other information in order to be selected as a volunteer; the information is necessary for effective performance of volunteer duties. Employees and contractors are required to provide their PII as a condition of employment.

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

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 ensure the trustworthiness of the employee. Every three years, the IT system undergoes a thorough certification and accreditation (C&A) process. The C&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.

An IT Security Certification and Accreditation (C&A) in accordance with the requirements of the [Federal Information Security Act of 2002](#) (FISMA) was completed for this system and is current. 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.

Operational Controls

The information is maintained on systems located in a locked computer room located in NWS Southern Region Headquarters in Fort Worth, Texas. Access to the computer room is limited those with demonstrated need for access and support personnel. Access to the computer room is monitored and access logs are maintained. All visitors are escorted 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. Access logs are maintained and reviewed for any improprieties. Password complexity and duration of validity adhere to established Department of Commerce IT security standards.

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

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 system administrators and human resources personnel. Individuals with access are advised on the requirement to destroy all data extracts once they are no longer needed. The low risk PII in the database does not warrant investing in an electronic log data extracts system at this time.

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 (SORN) for NOAA-11, NOAA Mailing Lists applies to most of the personal information in this system. Other SORNs that may apply include:

- DEPT-5, Freedom of Information and Privacy Request Records
- DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies
- DEPT-19, Department Mailing Lists
- DEPT-20, Biographical Files

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. In accordance with GRS 20, item 3, the data is presently being retained indefinitely.

The underlying paper records relating to employees are covered by GRS 1, Civilian Personnel Records.