

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



Privacy Threshold Analysis for the
NOAA8884
Southern Region (SR) General Support System (GSS)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/ Southern Region (SR) General Support System (GSS) Unique

Unique Project Identifier: NOAA8884

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system:

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The National Weather Service (NWS) Southern Region (SR) General Support System (GSS) provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including forecasts and warning is dependent on a complex interaction of many information resources and systems. This system is designed and used to support the collection, processing, and dissemination of data that supports the mission of the organization. It also supports the administrative functions and the scientific & technical research and innovations activities of employees within the organization.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems; client-server and web- based server systems. The system supports a variety of users, functions, and applications; including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development and collaboration.

Address the following elements:

a) Whether it is a general support system, major application, or other type of system

This is a General Support System (GSS).

b) System location

System headquarters is located in Fort Worth TX, but the WAN extends across 11 southern and southeastern states which support 32 Weather Forecast Offices (WFO), 4 River Forecast Centers (RFC), and 7 Center Weather Service Units (CWSU).

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The SR GSS is a system with interconnections only to trusted NWS-NOAA internal systems with no direct interconnections to the outside. Although there are a variety of hardware and operating systems, all the operational activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems, and client-server systems. The system supports a variety of users, functions, and applications, including word processing, employee data, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development, and collaboration.

The following systems are NOAA-internal interconnections with NOAA8884:

NOAA0201 - Web Operation Center (H)

NOAA1101 - Information Technology Center (M)

NOAA8106 - Upper Air Observing System (UAOS)

NOAA8107 - Advanced Weather Interactive Processing System (AWIPS)

NOAA8850 - NWS Enterprise Mission Enabling System (MES)

NOAA8860 - Weather and Climate Computing Infrastructure Services (WCCIS)

NOAA8860 – OneNWSNet is an existing connection as well, but is not documented in CSAM as it is not currently available as a selection for an internal connection in the CSAM Interconnections module.

d) The purpose that the system is designed to serve

The system is designed to serve weather forecasts, products and raw data to the public and other agencies of the National Oceanic and Atmospheric Administration. It also serves to accommodate the work of the Administration staff to support the financial and logistical functions of the Southern Region facilities and personnel.

e) The way the system operates to achieve the purpose

The NWS SR GSS provides weather, hydrologic, and climate forecasts and warnings for the NWS defined Southern Region of the United States, its territories, adjacent waters and ocean areas, for the

protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

During the course of operations, contact information is collected on local Federal employees to support emergency contact rosters. Various amounts of work-related information, as well as basic personal information, is collected on employees to support day-to-day administrative efforts. These include, but are not limited to, payroll processing, travel documents, performance plans, in- and out-processing of new and current employees, system user accounts, procurement records. This data may be stored by the employees themselves and as well as various support staff (supervisors and administrative assistants), in addition to automatic collection by IT staff and system logs as part of day-to-day operation and maintenance to include, but not limited to, as usernames, addresses, system and network activity logging.

- A. Volunteer Weather Observers:** who provide daily weather observations. Observer information is stored on electronic media located within each of the 32 Weather Forecast Office data centers within the NOAA8884 accreditation boundary.
- B. MARS Employee Information:** includes, but not limited to: name of the employee, the email address of the employee, CBS employee number, job title, employee grade, step, series, org code, project-task, employee salary, employee benefits, FLSA code, and BUS code. This information is accessed via NOAA1101 but does not reside on NOAA8884.

g) Identify individuals who have access to information on the system

Federal civil servants and private contractors under contract with the NWS working on behalf of the Southern Region access parts of the system in support of its mission have access to the system. Select PII is shared with the Department of Commerce Security Office and various National Oceanic and Atmospheric Administration administrative offices such as Human Resources or Finance as applicable.

h) How information in the system is retrieved by the user

MARS Data:

Authorized users log into MARS via interconnection with NOAA1101. This data does not reside within 8884.

Volunteer Observer Data:

Access to the data is done manually and resides within each of the 32 Weather Forecast Offices on workstation hard drives or centralized network attached storage devices.

i) How information is transmitted to and from the system

All data is transmitted and received via OneNWSNet cloud. All internal NWS data is on the Internal cloud network and all Internet connectivity is supplied through the NOAA TIC sites.

MARS Data:

All access to the MARS reports is done via web browser, all data transmission is one way, from MARS to the SR Portal and then the users pull their set of data for restricted internal use.

Volunteer Observer Data:

There is no PII information transmitted to and from the system.

Questionnaire:**1. Status of the Information System****1a. What is the status of this information system?**

- ☐ This is a new information system. *Continue to answer questions and complete certification.*
- ☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

- ☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*
- ☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

- ☐ Yes. This is a new information system.
- ☐ Yes. This is an existing information system for which an amended contract is needed.
- ☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.
- ☒ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. (Check all that apply.)

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

☒ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: (Check all that apply.)

- ☒ DOC employees
- ☒ Contractors working on behalf of DOC
- ☐ Other Federal Government personnel
- ☒ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.

Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PIA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

 X The criteria implied by one or more of the questions above **apply** to the NOAA8884 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

 The criteria implied by the questions above **do not apply** to the NOAA8884 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<p>Information System Security Officer or System Owner Name: John Duxbury Office: SRH Phone: 682-703-3703 Email: John.Duxbury@noaa.gov : Signature: _____ Date signed: _____</p>	<p>Information Technology Security Officer Name: Paula Reis-Cypress Office: NWSHQ Phone: 202-816-2992 Email: paula.reis-cypress@noaa.gov Signature: _____ Date signed: _____</p>
<p>Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov Signature: _____ Date signed: _____</p>	<p>Authorizing Official Name: Mike Coyne Office: SRH Phone: 682-703-3700 Email: mike.coyne@noaa.gov Signature: _____ Date signed: _____</p>
<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: _____ Date signed: _____</p>	