

**U.S. Department of Commerce
NOAA**



**Privacy Threshold Analysis
for the
Southern Region GSS (NOAA8884)**

U.S. Department of Commerce Privacy Threshold Analysis

Southern Region GSS (NOAA8884)

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

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 and its purpose:

The National Weather Service (NWS) Southern Region 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 origination. 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.

Questionnaire:

1. 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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					
*NOAA8205 was incorporated into this collection.					

This is an existing information system in which changes do not create new privacy risks. Skip questions and complete certification.

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. Please describe the activities which may raise privacy concerns.

The Regional ISSO has been assigned the Trusted Agent (TA) duties for multiple contractors. All badging paperwork and OSY Security/Investigative coversheets for the contractors are being saved to the ISSO’s system.
 All transmission of PII data flows to other organizational entities (OSY) via secured Acellion SFTP server.
 All PII data residing on the NOAA8884 system is encrypted at rest with the use of McAfee Endpoint Security protection. This is an encrypted Directory only assessable from the user with CAC authentication.

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 about: (*Check all that apply.*)

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

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

DOC employees

Contractors working on behalf of DOC

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 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.

4c. 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, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

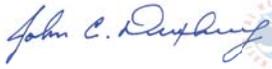
CERTIFICATION

 X I certify the criteria implied by one or more of the questions above **apply** to the Southern Region GSS (NOAA8884) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

John Duxbury (SO)

Signature of ISSO or SO:  DUXBURY.JOHN.C.1365877730
2018.01.18 07:50:53 -06'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Andrew Browne (ITSO)

Signature of ITSO: BROWNE.ANDREW.PA
TRICK.1472149349  Digitally signed by
BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.01.22 15:38:35 -05'00'

Name of Authorizing Official (AO):

Steven Cooper

Signature of AO: COOPER.STEVEN.G.136
5850930  Digitally signed by
COOPER.STEVEN.G.1365850930
Date: 2018.01.22 14:10:31 -06'00'

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1
514447892  Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.01.24 10:52:07 -05'00'