

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



**Privacy Threshold Analysis
for
National Weather Service (NWS) Western Region General Support
System (NOAA8885)**

U.S. Department of Commerce Privacy Threshold Analysis

NOAA8885 National Weather Service (NWS) Western Region General Support System (NOAA8885)

Unique Project Identifier: 006-48-02-00-01-0511-00

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 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) provides weather, hydrologic, climate forecasts, and warnings for the United States, its territories, adjacent waters, and ocean areas. The NOAA8885 System is designed and used to collect, process, and disseminate supplemental weather data that supports warning and forecast products for the protection of life, property, and the enhancement of the national economy. NOAA8885 data and products assist in the formation of a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community. NOAA8885 also provides administrative functions as well as scientific & technical research support for the NWS Western Region Headquarters (WRHQ) and all offices within the NWS Western Region (WR) boundary.

Functional areas of NOAA8885 can be classified into six major areas.

- Observations – Meteorological/Hydrological Sensing systems.
- Operations/Production – Operations/Production of Watches, Warnings, & Forecasts.
- Dissemination – Systems used for the dissemination of NWS information.
- Administration – Office Automation, Word Processing, Email, etc.
- Security – Systems supporting the security posture of the Enterprise
- Network – Networking/Transport Infrastructure

Although there are a variety of hardware and operating systems, several of the activities are interconnected. NOAA8885 provides direct and indirect mission support for the NWS as a Government agency. The mission support infrastructure encompasses Wide Area Networks

(WAN), Local Area Networks (LAN), host computer systems; client-server and web-based server systems. The system also supports a variety of users, functions, and applications.

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	
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 (version 01-2015 or later). *Continue to answer 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.*

___√___ 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

 √ I certify the criteria implied by one or more of the questions above **apply** to the NOAA8885 system 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 NOAA8885 system and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Sean Wink

Signature of ISSO or SO: WINK.SEAN.P.1365853270  Digitally signed by WINK.SEAN.P.1365853270
Date: 2019.03.27 12:54:24 -06'00' Date: _____


Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349  Digitally signed by BROWNE.ANDREW.PATRICK.1472149349
Date: 2019.03.27 09:01:03 -04'00' Date: _____

Name of Authorizing Official (AO): Grant Cooper, Ph.D.

Signature of AO: COOPER.GRANT.ALEXANDER.IV.1047689399  Digitally signed by COOPER.GRANT.ALEXANDER.IV.1047689399
Date: 2019.03.28 08:17:22 -06'00' Date: _____

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892  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: 2019.04.01 07:17:11 -04'00' Date: _____