

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



**Privacy Threshold Analysis  
for the  
NOAA8880 General Support System**

## U.S. Department of Commerce Privacy Threshold Analysis

### National Weather Service/NOAA8880 General Support System

**Unique Project Identifier:** [Number]

**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:** *Provide a general description of the information system and its purpose in a way that a non-technical person can understand.*

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).

NOAA8880 is a General Support Services system that supports NWS offices within the Alaska Region. 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 users, functions, and applications. Supported applications include weather forecaster supporting web applications, word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

The NWS Alaska Region (AR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees. 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. The system also collects and maintains information on volunteers who provide weather reports to system personnel.

The PII/BII in this system is not shared. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is available only to employees of the NWS Alaska Region. Specific information about individual personnel is available only to authorized NWS Alaska Region Headquarters Administration Staff. The volunteer databases are accessible to forecast staff so they can contact volunteers for severe weather information.

#### 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.*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
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. *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. There are building entry card readers and electronic purchase transactions.

\_\_\_\_\_ 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:

☒ 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 **NWS Alaska Region General Support System (GSS) (NOAA8880)** 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): \_\_\_\_\_

Signature of ISSO or SO: Angel Corona  Digitally signed by CORONA.ANGEL.M.1187109503  
Date: 2017.11.15 12:57:02 -09'00' Date: \_\_\_\_\_


Name of Information Technology Security Officer (ITSO): \_\_\_\_\_

Signature of ITSO: BROWNE.ANDREW.PA TRICK.1472149349  Digitally signed by BROWNE.ANDREW.PATRICK.1472149349  
Date: 2017.11.15 11:28:40 -05'00' Date: \_\_\_\_\_

Name of Authorizing Official (AO): \_\_\_\_\_

Signature of AO: VARN.RICHARD.ALAN.II. 1073462041  Digitally signed by VARN.RICHARD.ALAN.II.1073462041  
Date: 2017.11.16 08:39:46 -05'00' Date: \_\_\_\_\_

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: 2017.11.16 08:48:05 -05'00' Date: \_\_\_\_\_