

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



**Privacy Threshold Analysis for the  
National Weather Service Pacific Region  
NOAA8883**

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

### NOAA / National Weather Service Pacific Region

**Unique Project Identifier:** 006-00035110400-48-02-00-02-00

**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:**

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

General Support System

*b) System location*

RHQ Pacific Region (Honolulu, HI), WFO Honolulu (Honolulu, HI), WFO Guam (Barrigada, GU), WSO Pago Pago (Pago Pago, AS), DCO Lihue (Lihue, HI), DCO Hilo (Hilo, HI), and the Caribbean Tsunami Warning Program (Mayaguez, PR).

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

The NWS PR interconnects with the NWS Enterprise Mission Enabling System (NOAA8850) for centralized user authentication, National Oceanic and Atmospheric Administration Corporate Services (NOAA1200) for audit collection of automated information technology records such as computer application security logs, and the NWS Weather and Climate Computing Infrastructure Services (NOAA8860) as its WAN provider

*d) The purpose that the system is designed to serve*

The system is primarily used to provide administrative support and supplemental operational services and specifically excludes from its accreditation boundary systems deemed as major applications or programs of records as well as various partner systems, though transit may be provided in some cases

*e) The way the system operates to achieve the purpose*

The NWS PR (FIMSA ID: NOAA8883) information technology general support system is composed of various field and headquarter office local area networks (LANs) and their directly connected information systems such as workstations, servers, printers, etc. which are linked together by a wide area network (WAN) used to support weather forecasting throughout the Pacific Ocean. The system is primarily used to provide administrative support and supplemental operational services and specifically excludes from its accreditation boundary systems deemed as major applications or programs of records as well as various partner systems, though transit may be provided in some cases.

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

As a course of operations contact information is collected on local Federal employees to support emergency contact rosters. In addition, various amounts of work related information as well as basic personal information is collect on employee's to support day-to-day administrative efforts such as travel documents, performance plans, in and out processing of new and current employees, system user accounts, procurement records, etc. and are stored by the employees themselves and as well as various support staff such as supervisor or administrative assistants, in addition to automatic collection by IT staff and system logs as part of day-to-day operation and maintenance such as usernames, addresses, system and network activity logging, etc.

Various amount of PII to establish identity such as passport numbers, nationality, contact information, etc. are collected from foreign national visitors and guests on a transitory basis and transmitted to the applicable security office for building and installation access as well as for the purpose of protecting deemed exports and controlled technology.

*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 Pacific Region access parts of the system in support of its mission. Select PII is shared with Department of the Defense Joint Base Pearl Harbor-Hickam Pass and ID Office, the Department of Commerce

Western Region Security Office, and various National Oceanic and Atmosphere Administration administrative offices such as Human Resources or Finance as applicable.

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

Users are identified and authenticated using DoD issued Common Access Card (CAC) and only with Government Furnished Equipment (GFE) computers. Their CACs and respective PIN are required to access the employee's Windows Domain account

*i) How information is transmitted to and from the system.*

Information transmitted to and from the system is via the NOAA 8883 N-Wave\TICAP system. If a data transmission involves a privacy consideration, a PR employee would use the DOC provided secure file transmission system. PR employee personnel recommend the DOC secure file transfer method as standard practice to receive sensitive data into the system.

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).  
*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 01-2017 or later). *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. *(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

National Institute of Standards and Technology Associates

- 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:*

New employees that are in-processing will include SSN on their SF-2809 Health Benefits Registration Form, SF-1152 Beneficiary Form, etc.

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

DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies  
OPM/GOVT-1, General Personnel Records

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 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 National Weather Service Pacific Region 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 National Weather Service Pacific Region and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Derek Ching

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

Name of Privacy Act Officer (PAO): Adrienne Thomas

Name of Authorizing Official (AO): Ray Tanabe

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