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

Privacy Threshold Analysis for the
NOAA8883
National Weather Service Pacific Region (PR)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA / NWS / Pacific Region

Unique Project Identifier: NOAA8883 (PR)

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: *Provide a brief 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 Pacific Region (NOAA8883/PR) is a general support system composed of various field and headquarter office local area networks and associated networked equipment used to provide information technology support to Federal weather forecasting operations throughout the Pacific Ocean. The system is primarily administrative support in function though in limited cases provides supplemental operational data.

There have been no changes to the information collection, stored, transmitted or disseminated that create changes to the privacy posture of NOAA8883 from the previous PTA.

Address the following elements:

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 International Tsunami Information Center - Caribbean (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, used, 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. 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.*

_X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Skip 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.

_X_ 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 tothose 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		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

_X_ 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.

_X_ 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."

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

- _X_ DOC employees
- _X_ Contractors working on behalf of DOC
- _X_ Other Federal Government personnel
- _X_ 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?

_X_ 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: Title 5, U.S.C. Chapter 89 Title 5 of the Code of Federal Regulations, Part 890 Executive Order 9397 Executive Order 13478 Code of Federal Regulations, Part 178, Subpart B

____ 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?

_X_ 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.

_X_ 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 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 NOAA8883 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 NOAA8883 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Derek Ching Office: NWS Pacific Region Phone: 808-725-6030 Email: derek.ching@noaa.gov Signature: CHING.DEREK.KK.1232036318 Digitally signed by CHING.DEREK.KK.1232036318 Date: 2022.11.03 11:09:58 -10'00' Date signed: 11/3/2022	**Information Technology Security Officer** Name: Andrew Browne Office: NWS ACIO ITSSB Phone: Email:Andrew.browne@noa.gov Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2022.11.04 10:22:43 -04'00' Date signed: _____
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-270-4695 Email: Robin.Burress@noaa.gov Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2022.11.29 09:45:27 -05'00' Date signed: _____	**Authorizing Official** Name: Ray Tanabe Office: NWS Pacific Region Phone: Email: Raymond.tanabe@noaa.gov Signature: TANABE.RAYMOND.MASAHARU.1365894449 Digitally signed by TANABE.RAYMOND.MASAHARU.1365894449 Date: 2022.11.26 13:13:49 -10'00' Date signed: _____
Bureau Chief Privacy Officer Name: Mark Graff Office: NOCC OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.12.08 16:20:25 -05'00' Date signed: 14447892	