Version Number: 01-2017

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

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

U.S. Department of Commerce Privacy Threshold Analysis

National Oceanic and Atmospheric Administration National Weather Service Pacific Region (FISMA ID NOAA8883)

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 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.

Description of the information system and its purpose: The National Weather Service (NWS) Pacific Region (FIMSA ID: NOAA8883) information technology general support system is composed of various field and headquarter office[1] 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[2] (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.

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

[1] RHQ Pacific Region (Honolulu, HI), WFO Honolulu (Honolulu, HI), WFO Guam (Barrigada, GU), WSO Pago Pago (Pago Pago, AS), DCO Lihue (Lihue, HI), and DCO Hilo (Hilo, HI)

[2] The NWS PR interconnects with NWS Enterprise Mission Enabling System for centralized user authentication, National Oceanic and Atmospheric Administration Corporate Services for audit collection of automated information technology records such as computer application security logs, and NWS Advanced Weather Interactive Processing, and NWS Weather and Climate Computing Infrastructure Services as its WAN provider.

transmitted to the applicable security office for building and installation access as well as for the purpose of protecting deemed exports and controlled technology.

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.

This system is classified as a moderate system under the Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

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.*

_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 (version 01-2015 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. *Please describe the activities which may raise privacy concerns.*

__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 about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X_ 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..."

__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_ 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?

__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.

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.

__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, and/or 4c are "Yes," a 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 [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or Information System Owner:

CHING.DEREK.KK.1232036318

Digitally signed by CHING.DEREK.KK.1232036318
Date: 2018.03.08 08:22:32 -10'00'

Information Technology Security Officer:

BROWNE.ANDREW.PATRICK.1472149349

Digitally signed by BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.03.08 11:39:38 -05'00'

Authorizing Official:

TANABE.RAYMOND.M.1365894449

Digitally signed by TANABE.RAYMOND.M.1365894449
Date: 2018.03.08 08:56:19 -10'00'

Bureau Chief Privacy Officer:

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: 2018.03.09 17:29:51 -05'00'