Template Version Number: 01-2021

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

Privacy Threshold Analysis for the
NOAA8865

NOAA Tsunami Warning System; NTWS

Template Version Number: 01-2021

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NWS/NTWS

Unique Project Identifier: NOAA8865

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 NOAA Tsunami Warning System (NTWS) provides tsunami alert information to the US and other countries in the Pacific Ocean, Atlantic Ocean and Caribbean Sea. The NTWS is composed of two Tsunami Warning Centers: the National Tsunami Warning Center (NTWC) in Palmer, Alaska and the Pacific Tsunami Warning Center (PTWC) in Pearl Harbor, Hawaii.

These Centers have a widespread client base: emergency managers, the scientific community, and the public. They are responsible for gathering information from observational systems; detecting potential tsunami-generating events; processing and analyzing the events to determine tsunami danger; developing decision support information for operational and scientific decision makers; and disseminating warning and notification products to the public and other entities.

Address the following elements:

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

The NOAA Tsunami Warning System (NTWS) is a general support system that acts to evaluate seismic data and determine possible tsunami hazards. The system then notifies parties responsible for emergency management.

b) *System location*

The system is split between two centers: one at the Inouye Regional Center in Pearl Harbor, Hawaii (Pacific Tsunami Warning Center) and one in Palmer, Alaska (National Tsunami Warning Center).

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

This is not a standalone system. There is a connection with ISC International, which stores information on a password protected account. ISC International is based in Milwaukee WI. ISC also stores information for the Pacific Tsunami Warning Center (PTWC), based on a list from the Intergovernmental Oceanographic Commission. Both centers contract with ISC for dissemination of warnings and outages. This system is supported via the National Centers for Environmental Prediction (NCEP) for its routing/firewall which is part of the Weather and Climate Computing Infrastructure Services (NOAA8860 – WCCIS), The National Data Buoy Center (NOAA8873 – NDBC) as well as Alaska Region Headquarters (NOAA8880). The system also interconnects with the Advanced Weather Interactive Processing System (NOAA8107 – AWIPS) for development on a potential system replacement.

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

The NOAA Tsunami Warning System monitors global seismic activity, sea level, and Deep-ocean Assessment and Reporting of Tsunamis (DART) buoy data to determine earthquake characteristics to feed Tsunami models to alert emergency managers and the public, both in the United States and countries with agreements with the United States Government or the United Nations Education, Science, and Cultural Organization (UNESCO).
PII/BII within the system is collected for administrative matters, to promote information sharing initiatives, to improve Federal services online, and for web measurement and customization technologies.

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

The system collects seismic data from international and domestic partners for evaluating events and warning messages are disseminated through email, phone, fax, Emergency Managers Weather Information Network (EMWIN), social media, and the web. Data collected helps improve the Federal Service by notifying emergency managers about tsunami threats or troubleshooting data outages with seismic data providers. In the case of any legal action, this information may be subpoenaed and made available if legally required to do so. Employee information is stored by the respective center's directors.

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

Seismic, water level, and DART buoy data are interpreted and text products are made available as well as graphical information for emergency managers. PII is collected to include name, email address, and telephone numbers to ensure we can contact partners and providers for troubleshooting and partners and customers with products. Contact information is provided by the provider or partner directly to the center. Customers who receive email/fax products usually enroll through UNESCO and that information is furnished to us to build our dissemination lists. Internal employee PII including address and phone number are collected for emergency

notification usage (such as an all hands event or in case a watch stander does not show up for their shift or support staff is needed) and is provided by the employee.

g) Identify individuals who have access to information on the system

Information received from UNESCO is organized and put into a contact list that Federal employees maintain on the ISC International system. This list is then used by the centers to issue email and fax alerts to those recipients. Federal and Contract employees have access to help maintain dissemination lists as well as access to internal employee phone numbers for call ups for events or issues.

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

Contact information lists used for tsunami warnings and alerts are maintained on the ISC International servers and protected via username and password accessible via the Internet by both of the tsunami centers. These lists are also accessible over the Internet accessible by Application Programming Interface (API). API access requires authentication and is configured such that automated tsunami alerts can be sent to emergency managers and other personnel on the ISC International lists. Local copies are also retained.
An employee call-down list is provided on paper in the access-controlled operations room under a privacy sheet telling employees their privacy rights.

i) How information is transmitted to and from the system

Contact information is provided by the individual in a voluntary manner via the United Nations Education, Science, and Cultural Organization (UNESCO) via an encrypted HTTPS session and is added via an HTTPS web interface to ISC International. This information is used in order to facilitate communication in either the event of a warning, communication about data changes or outages, and/or tests. A Privacy Act Statement is available on the Web site and to the reply email. A list of employee home phone numbers is also contained in the access-controlled room as a 'phone down' list in case they need to be called in for work or an emergency.

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
- ____ 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?

____ 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.

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

_X_ 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 NOAA8865 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 NOAA8865 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Joshua Reaves Office: NOAA/NWS/NTWS Phone: (907) 271-5109 Email: joshua.reaves@noaa.gov Signature: REAVES.JOSHUA.MICHAEL.1256395696 Digitally signed by REAVES.JOSHUA.MICHAEL.1256395696 Date: 2023.06.01 09:35:20 -08'00' Date signed:	**Information Technology Security Officer** Name: Andrew Browne Office: NOAA/NWS/ACIO Phone: (301) 427-9033 Email: andrew.browne@noaa.gov Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2023.06.01 13:38:50 -04'00' Date signed:
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.06.07 10:06:39 -04'00' Date signed:	**Authorizing Official** Name: Mike Coyne Office: NOAA/NWS COO (acting) Phone: (817) 978-1000 Email: mike.coyne@noaa.gov Signature: COYNE.JOHN.MICHAEL.1365870485 Digitally signed by COYNE.JOHN.MICHAEL.1365870485 Date: 2023.06.01 13:10:09 -05'00' Date signed:
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2023.06.20 17:39:22 -04'00' Date signed:	