Template Version Number: 01-2020

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


## Privacy Threshold Analysis
## for the
## NOAA8865
## NOAA Tsunami Warning System (NTWS)

# 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 and its purpose:** *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

*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 Honolulu, 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 Dart Buoy Center (NOAA8873 – NDBC) as well as Alaska Region Headquarters and the Inouye Regional Center for building support. 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).

*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. BII is collected to include name, email address, and telephone numbers to ensure we can contact partners and providers for trouble shooting 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*

Dissemination lists are maintained on the ISC International servers and protected via username and password by the centers. Local copies are also retained. The employee call down list is provided in the 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.*

____ 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 01-2017). *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 01-2019 or later). *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 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.

_X_ Yes. *(Check all that apply.)*

| **Activities** | | | |
|---|---|---|---|
| Audio recordings | | Building entry readers | X** |
| Video surveillance | X* | Electronic purchase transactions | |
| Other (specify): *At PTWC in Hawaii, video surveillance is operated and maintained by NOAA1200; at NTWC in Palmer, AK, video surveillance is maintained by NOAA8865. **At PTWC in Hawaii, CAC readers are operated and maintained by NOAA1200. | | | |

____ 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.)."

_X_ 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."

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?

____ 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 I certify the criteria implied by one or more of the questions above **apply** to the NOAA Tsunami Warning System 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 NOAA Tsunami Warning System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

| | |
|---|---|
| **Information System Security Officer or System Owner**<br>Name: Anthony Vandegrift<br>Office: NOAA/NWS/NTWS<br>Phone: 1 907 861 4225<br>Email: Anthony.vandegrift@noaa.gov<br><br>Signature: VANDEGRIFT.ANTHONY.WAYNE.1147676855 Digitally signed by VANDEGRIFT.ANTHONY.WAYNE.1147676855 Date: 2021.06.28 15:13:35 -08'00'<br><br>Date signed: 6/28/21 | **Information Technology Security Officer**<br>Name: Chris Ortiz<br>Office: NOAA/NWS/ACIO<br>Phone: 1 (303) 709-4070<br>Email:<br><br>Signature: ORTIZ.CHRISTOPHER.J.1154749175 Digitally signed by ORTIZ.CHRISTOPHER.J.1154749175 Date: 2021.06.29 09:09:33 -04'00'<br><br>Date signed: 6/29/21 |
| **Privacy Act Officer**<br>Name: Adrienne Thomas<br>Office: NOAA OCIO<br>Phone: 828-257-3148<br>Email: Adrienne.Thomas@noaa.gov<br><br>Signature: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2021.06.30 10:56:45 -05'00'<br><br>Date signed: 6/30/21 | **Authorizing Official**<br>Name: John Murphy<br>Office: NOAA/NWS COO<br>Phone: 1 (301) 427-9119<br>Email: john.d.murphy@noaa.gov<br><br>Signature: MURPHY.JOHN.DANIEL.1031033540 Digitally signed by MURPHY.JOHN.DANIEL.1031033540 Date: 2021.06.29 12:25:32 -04'00'<br><br>Date signed: 6/29/21 |
| **Bureau Chief Privacy Officer**<br>Name: Mark Graff<br>Office: NOAA OCIO<br>Phone: 301-628-5658<br>Email: Mark.Graff@noaa.gov<br><br>Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2021.07.13 07:22:10 -04'00'<br><br>Date signed: 7/13/21 | |