Version Number: 01-2017

# U.S. Department of Commerce
# NOAA


## Privacy Threshold Analysis
## for the
## NOAA8865 – National Tsunami Warning System

# U.S. Department of Commerce Privacy Threshold Analysis

## NOAA/NWS/NTWS

**Unique Project Identifier: NOAA8865**

**Introduction: System Description**

a. The NOAA National 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. 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). This system is supported via the National Centers for Environmental Prediction (NCEP) for its routing/firewall/and enterprise support as well as Alaska Region Headquarters and the Inouye Regional Center for building support.
c. 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.
d. The system collects seismic data from international and domestic partners for evaluating events and warning messages are disseminated through email, phone, fax, 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.
e. Information is stored on the local Information System, in Hard Copy form in the access controlled operations rooms and email and fax lists are managed via an account with ISC International who disseminates messages to mailing lists and fax lists. Employee information is stored on the computers of the respective center's directors and encrypted.
f. Contact information is provided by the individual 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 being added to 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.
g. Notification information is shared with ISC International for storage and dissemination.

**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 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 NTWS 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.

Name of Information System Security Officer (ISSO) or System Owner (SO):
_____Anthony Vandegrift_____

X VANDEGRIFT.ANTHONY.WAYNE.1147676855 Digitally signed by VANDEGRIFT.ANTHONY.WAYNE.1147676855 Date: 2019.06.19 14:36:02 -08'00'

Anthony Vandegrift
ISSO NOAA8865

Signature of ISSO or SO:

Name of Information Technology Security Officer (ITSO): _Chris Ortiz__

X ORTIZ.CHRISTOPHER.J.1154749175 Digitally signed by ORTIZ.CHRISTOPHER.J.1154749175 Date: 2019.06.24 13:25:05 -04'00'

Chris Ortiz
NWS ITSO

Signature of ITSO:

Name of Authorizing Official (AO): _____John Murphy_____

X MURPHY.JOHN.D.1031033540 Digitally signed by MURPHY.JOHN.D.1031033540 Date: 2019.06.24 17:45:23 -04'00'

John Murphy
NOAA8865 Authorizing Official

Signature of AO:

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

X 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: 2019.07.22 07:12:30 -04'00'

Mark Graff
Bureau Chief Privacy Officer

Signature of BCPO: