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 8865 –NTWS

Unique Project Identifier: NOAA 8865

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 of the information system in a way that a non-technical person can understand.*

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) The NOAA National Tsunami Warning System 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 on at the Inouye Regional Center in Honolulu, Hawaii (Pacific Tsunami Warning Center) and one in Palmer, Alaska (National Tsunami Warning Center).
c) This system is supported via the National Centers for Environmental Prediction (NCEP) for it's routing/firewall/and enterprise support as well as Alaska Region Headquarters and the Inouye Regional Center for building support. Outside of NOAA 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.
d) The system serves to issue tsunami warnings to emergency managers, media, and the public via evaluating information received from seismic partners and ran through models.
e) The system receives seismic data from partners around the world. After detecting an earth quake its properties are evaluated to determine if there is a tsunami risk. It is ran through a model to determine possible impact. Emergency managers that supply their contact info are notified, messages are also sent via numerous NOAA emergency notification systems, social media, and our web site.
f) Seismic data is collected by the system, evaluated and appropriate warning/watch/statement is issued/modified/retracted. Titles, names, phone numbers, emails, and fax numbers are collected for seismic data points of contacts and necessary parties that need to be notified in the event of a tsunami related message. Personnel information is acquired for supervisory tasks related to employment at NOAA.

g) Only NTWS employees have access to the information system and hard copies of the points of contacts for warnings and seismic entities. Only managers and the employee for which the information is about has any kind of access to personnel information.
h) Point of contact information is kept in a database that can be looked up on the information system. Emails and faxes are sent to email lists maintained with ISC International that we create, manage, and remove entries for. Personnel information can be requested for the person the documents are about.
i) Emails and faxes are sent to points of contacts from ISC International once it receives an email from us. For certain locations phone calls may be necessary to ensure proper parties have been notified. For personnel files the information follows the policies set forth by NOAA personnel management.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__ X__ 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	X
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 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_____

3/20/2018

X VANDEGRIFT.ANTHONY.WAYNE.1147676855
Digitally signed by VANDEGRIFT.ANTHONY.WAYNE.1147676855
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=VANDEGRIFT.ANTHONY.WAYNE.1147676855
Date: 2018.04.03 11:20:35 -04'00'

Signature of ISSO or SO:

Name of Information Technology Security Officer (ITSO): _Beckie Koonge__

X BROWNE.ANDREW.PATRICK.1472149349
Digitally signed by BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.09.28 09:13:25 -04'00'

NWS ITSO

Signature of ITSO:

Name of Authorizing Official (AO): _____Zachery Goldstein_____

X GOLDSTEIN.ZACHARY.G.1228698985 Digitally signed by GOLDSTEIN.ZACHARY.G.1228698985 Date: 2018.04.03 13:11:08 -04'00'

Zachary Goldstein
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: 2018.04.03 13:22:55 -04'00'

Mark Graff
Bureau Chief Privacy Officer

Signature of BCPO: