

# U.S. Department of Commerce NOAA



## Privacy Impact Assessment for the NOAA8865 – National Tsunami Warning System

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer  
 Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

**CATRINA PURVIS**

Digitally signed by CATRINA PURVIS  
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary,  
cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743  
Date: 2018.09.28 10:26:04 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

## U.S. Department of Commerce Privacy Impact Assessment 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.
- 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 has 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.
- h. Authorities from NOAA-11: [5 U.S.C. 301](#), Departmental Regulations and [15 U.S.C. 1512](#), Powers and duties of Department.  
Authorities from DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 7531–332; 15 U.S.C. 1501 et seq.; 28 U.S.C. 533–535; 44 U.S.C. 3101; Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.

Authorities from DEPT-18: Includes the following, with all revisions and amendments: 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

- i. NTWS is listed as a FIPS 199 high system.

**Section 1: Status of the Information System**

1.1 Indicate whether the information system is a new or existing system.

This is a new information system.

This is an existing information system with changes that create new privacy risks.  
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to NonAnonymous		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): Discovery of account information for tsunami information distribution					

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.

**Section 2: Information in the System**

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): Fax number					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	x	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify): All actions on NOAA8865 are subject to potential collection, analysis, and auditing.					

Other Information (specify)					

2.2 Indicate sources of the PII/BII in the system. (Check all that apply.)

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	

Telephone		Email	X		
Other (specify):					

<b>Government Sources</b>					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

<b>Non-government Sources</b>					
Public Organizations	X	Private Sector		Commercial Data Brokers	
Third Party Website or Applications					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

<p>Contact information is provided by those requesting information. Occasional test messages are issued, at which time invalid data may become known from email bounce backs to disconnected phone messages. This information is investigated to determine if incorrect data was mistakenly given, in which case correct information is requested or in the case of points of contact changing, older records are removed and replaced with new points of contacts.</p>
---

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. (Check all that apply.)

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	--

### **Section 3: System Supported Activities**

3.1 Indicate IT system supported activities which raise privacy risks/concerns. (*Check all that apply.*)

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.
---	--

### **Section 4: Purpose of the System**

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. (*Check all that apply.*)

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session )	X	For web measurement and customization technologies (multi-session )	
Other (specify):			

**Section 5: Use of the Information**

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

Contact information is stored in a contact list on the information system, printed out for hard copy look ups stored in an access controlled operations room and is stored in mailing and fax lists maintained by ISC International whose system provides confidentiality, integrity, and availability controls (members of the public).

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.

- 5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Contact information may become stale in which case phone numbers no longer working or email bounce backs are checked and records are updated as necessary. All employees complete NOAA's record retention training. If an escorted person who is in the operations room manages to take the contact list without being noticed than the names, email addresses, faxes, and/or phone numbers of our points of contacts may be exposed.

**Section 6: Information Sharing and Access**

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector		X**	
Foreign governments			
Foreign entities			
Other (specify):			

\*\*ISC International (contract notification service)

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	---

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.                  Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:                  Contact information through ISC International: Stored on a password protected account on an information system that provides confidentiality, integrity, and availability controls. More information can be found here:  <a href="http://www.iscinternational.com/security.php">http://www.iscinternational.com/security.php</a> and  <a href="http://www.iscinternational.com/technical/">http://www.iscinternational.com/technical/</a></p>
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input type="checkbox"/>	Government Employees	X
Contractors	X		
Other (specify):			



--

## **Section 7: Notice and Consent**

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: <a href="https://tsunami.gov/?page=privacy_statement">https://tsunami.gov/?page=privacy_statement</a> <i>(the link title is in process of correction)</i> . The PAS contains information on sharing the warnings with ISC International, which has the capacity needed for this size of bulk emailing.	
X	Yes, notice is provided by other means.	Specify how: Tsunami information: Individuals request to be added/modified/or removed from our list directly.  Home telephone list is posted in the operations room and employees provide contact information. Privacy Act Statement posted beneath call roster and is on phone request form provided to employee.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:  Tsunami information: Individuals may decline by not volunteering the information or requesting a removal from our system.  Employee information: Employees working on an on-call status are required to provide their home phone number on the form made available, so they may be contacted for emergencies or shift information (employee is late to start their shift so previous shift worker calls to get information).
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their	Specify how:
---	---	--------------

	PII/BII.	<p>Tsunami: Individuals specify whether or not they want to receive warning notifications, by which means. Data partners provide the method of contact they want for troubleshooting/testing/outage notifications.</p> <p>Employees: Employees may specify that they wish for their home phone number to only be used on the call roster for its intended purpose.</p>
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	<p>Specify how:</p> <p>Tsunami: NTWS can be contacted by the individual to have their data changed or removed or by an official within the individual's organization, or to have a record removed or replaced, or reviewed.</p> <p>Employee: Employees may inform managers of a change of their home telephone number and managers will produce a rectified call down list.</p>
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

**Section 8: Administrative and Technological Controls**

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access is restricted to a room with CAC badge access and a user must be on an approved list. There are cameras facing the doors of this room.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ___Feb & March 2017_____

	<input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. (Include data encryption in transit and/or at rest, if applicable).

Contact Information on the IS: Stored via access control mechanisms on the systems which are in a controlled operations room. Accessible to employees who are trained in NOAA’s record retention training.

Contact Information Hardcopy: Stored in a controlled operations room. Accessible to employees who are trained in NOAA’s record retention training

Contact Information through ISC International: Stored on a password protected account on an information system. More information can be found here:  
<http://www.iscinternational.com/security.php> and <http://www.iscinternational.com/technical/>  
 Data transferred between the IS and ISC International is via https encrypted connection.

Employee info: Protected in a secured room that is CAC controlled to enter. There are also video cameras watching the doors to this room.

**Section 9: Privacy Act**

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (A new system of records notice (SORN) is required if the system is not covered by an existing SORN).

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> <a href="#">Commerce/NOAA-11</a> , Contact Information from Members of the Public Requesting or Providing Information Related to NOAA's Mission; <a href="#">Commerce/DEPT-13</a> , Investigative and Security Records
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

## **Section 10: Retention of Information**

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Weather Forecast Office and River Forecast Centers: 1307. Chapter 300. Personnel.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

<b>Disposal</b>			
Shredding	X	Overwriting	
Degaussing		Deleting	X
Other (specify):			

## **Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level**

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels.  
(Check all that apply.)

X	Identifiability	Provide explanation: Individuals may be identified by means of PII.
X	Quantity of PII	Provide explanation: There is only contact information and employee information.
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields.
X	Context of Use	Provide explanation: The contact information is used to contact individuals with tsunami-related information. Employee information is used for managerial purposes.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Contact information is stored in the operations room behind CAC enabled doors.
	Other:	Provide explanation:

## **Section 12: Analysis**

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

If the individual in contact information no longer works in their former role, then it may be necessary for us to reach out to the organization and obtain a new point of contact, at which point the old one is removed from the system. Some organizations delegate someone on their behalf and furnish that person's point of contact information.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: Addition of a Privacy Act Statement to the Web site and to return email template.
	No, the conduct of this PIA does not result in any required technology changes.

## Points of Contact and Signatures