

U.S. Department of Commerce NOAA



Privacy Threshold Analysis for the Emergency Notification System

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Emergency Notification System

Unique Project Identifier: [Number]

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) *Whether it is a general support system, major application, or other type of system:*
NOAA’s Emergency Notification System (ENS) is a commercial cloud-based application by which designated NOAA persons can quickly broadcast emergency alerts to NOAA staff via phone, text, and email. It provides NOAA staff with consistent event specific information and direction, and ability to account for staff in the aftermath thereof. The information in the system is obtained from the NOAA Staff Directory (NSD) and consists of: name, work phone number, work cell phone number, work email address, and work mailing address. In addition, NOAA staff may choose to enter their personal mobile phone number and personal email address into the NSD for upload to the NOAA ENS. There is no information sharing outside of NOAA other than if contact information is needed for a privacy incident response.
- b) *System location:* Silver Spring MD.
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)* This is a standalone system, to which bulk uploads are made from the NOAA Staff Directory.
- d) *The purpose that the system is designed to serve:* This is a system by which NOAA persons can quickly broadcast emergency alerts to NOAA staff via phone, text, and email. It provides NOAA staff with consistent event specific information and direction, and ability to account for staff in the aftermath thereof.
- e) *The way the system operates to achieve the purpose:* Using the staff directory information, the ENS sends out emergency broadcasts to staff work contact information.

- f) *A general description of the type of information collected, maintained, use, or disseminated by the system:* Name, work phone number, work cell phone number, work email address, and work mailing address.
- g) *Identify individuals who have access to information on the system:* Access is restricted, requiring authorized users, those with a “need to know”, to log in. These include system staff and contractors.
- h) *How information in the system is retrieved by the user:* Information from the NOAA Staff Directory is uploaded to a server and downloaded by ENS, where it is accessed by authorized personnel in order to deliver notifications.
- i) *How information is transmitted to and from the system:* Information is uploaded from the Staff Directory and alerts are sent out to NOAA staff and contractors by the system.

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.*

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). *Continue to answer 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.*

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

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...”

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

Contractors working on behalf of DOC

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?

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.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

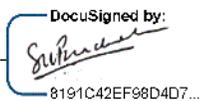
If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PIA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

 X I certify the criteria implied by one or more of the questions above **apply** to the NOAA0900 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): ISSO: SK Bhachech

Signature of ISSO or SO:  _____ Date: 2/7/2018

Name of Information Technology Security Officer (ITSO): _____

APEDO.JEAN.1 Digitally signed by APEDO.JEAN.1188076064
DN: c=US, o=U.S. Government, ou=DoD,
ou=PKI, ou=OTHER,
cn=APEDO.JEAN.1188076064
Date: 2018.02.08 08:58:22 -05'00'
Signature of ITSO: 188076064 _____ Date: _____

Name of Authorizing Official (AO): _____

PERRY.DOUGLAS.A.1365847270 Digitally signed by
PERRY.DOUGLAS.A.1365847270
Date: 2018.02.16 14:31:02
-05'00'
Signature of AO: S.A.1365847270 _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

GRAFF.MARK.HYRUM.1514 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: 2018.02.21 09:13:36 -05'00'
Signature of BCPO: 447892 _____ Date: _____