Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NWS Alaska Region NOAA8880
General Support System

U.S. Department of Commerce Privacy Threshold Analysis

National Weather Service/NOAA8880 GSS

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

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 National Weather Service (NWS) Alaska Region (NOAA8880) is a General Support System (GSS) that provides weather, hydrologic, and climate forecast and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy.

NWS data and products form a national information database and infrastructure, which can be used by our partners the public and the global community. Issuance of products, including forecasts and warning is dependent on a complex interaction of many information resources and systems.

NOAA8880 is designed and used to support the collection, processing, and dissemination of data that supports the mission of the organization. It also supports the administrative functions, scientific & technical research, and innovation activities of employees within the organization.

b) System location

The location of NOAA8880 is Anchorage, AK. 99513.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA8880 does maintain system interconnections with NOAA3090 (National Severe Storms

Laboratory Scientific Computing Facility), NOAA8106 (Upper Air Observing System), NOAA8107 (Advanced Weather Interactive Processing System), NOAA8850 (NWS Enterprise Mission Enabling System, NOAA8860 (Weather and Climate Computing Infrastructure Services) NOAA8865 (NOAA Tsunami Warning System), and other government information systems, such as the Federal Aviation Administration (FAA). No sensitive information is shared outside of NOAA8880.

d) The purpose that the system is designed to serve

The purpose of NOAA8880 is to support the NWS offices within the Alaska Region. Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct and indirect mission support for the NWS as a Government agency.

e) The way the system operates to achieve the purpose

NOAA8880 supports the NWS offices within the Alaska Region. Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct and indirect mission support for the NWS as a Government agency.

Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Network (LAN), host computer systems, client-server and web-based server systems. The system supports a variety of users, functions, and applications, including word processing, budget and requisition information, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development, and collaboration.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

The NWS Alaska Region Headquarters maintains PII concerning federal employees in the Alaska Region workforce. This information is managed by the NWS Alaska Region Headquarters Administration Personnel. The information maintained includes: Name, Age, Gender, date and place of birth, home contact information and email address, Position, GS Level/Series, Division/Organization Name, Regional Office Name/Location, work history, Financial information, medical information, military service information.

This information is maintained to aid in maintenance of organization structures, supplementing management of employee records, and providing statistical data. The information is not shared with any third parties or unauthorized personnel. There are also local databases at the local Weather Forecast Office/River Forecast Center (WFO/RFC), within the boundaries of the system, which maintain information on volunteers who provide weather reports to staff. The WFO/RFC database information is collected in order to contact volunteers when severe weather information is needed.

The database holds the following information on these volunteers: First and last name, Mailing address, Telephone number (home/cell), Email address

- Hours to be contacted for severe weather reports
- Possession of a rain gauge, anemometer, thermometer, snow stick, or weather station
- Brief description of location of spotter's personal residence
- Last time attended spotter class
- Community Weather Involvement Program Identification – (optional) not all offices use this. It's a locally assigned number from the field office.
- Latitude / Longitude

Non-sensitive PII in these databases is provided on a voluntary basis; volunteers sign up and provide the information during spotter talks* that the NWS conducts in preparation for the severe weather season. These databases are accessible to forecast staff so they can contact volunteers for severe weather information. The information is collected from members of the public.

*** On-site spotter training classes are conducted annually in various locations in the system area. The spotter training class is designed for people new to severe storm spotting, as well as those that need refresher training. The training is comprised of all of the information that spotters need to be effective and stay safe. Information on the trainings is posted on the applicable NWS Web site.**

g) Identify individuals who have access to information on the system

Only authorized employees and contractors have access to the NOAA8880 information system. Information is accessed by authorized individuals via bureau owned workstations.

h) How information in the system is retrieved by the user

Only authorized employees and contractors have access to the NOAA8880 information system. Access is based on a need-to-know and user must use CAC to log in to the Government Furnished Equipment (GFE).

i) How information is transmitted to and from the system.

NOAA8880 transmits data via LAN/WAN connectivity.

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).
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 01-2017 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. *(Check all that apply.)*

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

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.)."

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
- ____ National Institute of Standards and Technology Associates
- X Contractors working on behalf of DOC
- ____ 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?

X 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. The SSN is collected on standard federal forms, .e.g. OF-306 (Declaration of Federal Employment).

Provide the legal authority which permits the collection of SSNs, including truncated form. The statutory authority is 5 U.S.C. Sections 1302, 3301, 3304, 3328 and 8716.

____ 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 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 **NOAA8880** 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 **NOAA8880** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO): Kyle Quashnick

Signature of ISSO or SO: QUASHNICK.KYLE.OWEN.1187587413 Digitally signed by QUASHNICK.KYLE.OWEN.1187587413 Date: 2020.01.30 14:26:27 -09'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: ORTIZ.CHRISTOPHER.J.1154749175 Digitally signed by ORTIZ.CHRISTOPHER.J.1154749175 Date: 2020.02.03 09:31:38 -10'00' Date: _____

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.05.15 17:19:38 -04'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: LINDSEY.SCOTT.D.1365826109 Digitally signed by LINDSEY.SCOTT.D.1365826109 Date: 2020.05.06 07:37:26 -08'00' Date: _____

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2020.05.19 07:43:25 -04'00' Date: _____