Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
Eastern Region
NOAA8882

U.S. Department of Commerce Privacy Threshold Analysis

NOAA8882 ER LAN/WAN

Unique Project Identifier: 006-000351104 00-48-02-00-02-00

Introduction: The National Weather Service (NWS) provides weather, hydrologic, and climate forecasts 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 other governmental agencies, the private sector, the public, and the global community. Issuance of warnings and forecasts is dependent on a complex interaction of many information resources. The system is designed and used to collect, process, and disseminate supplemental weather data which supports warning and forecast products. It also supports the supporting and administrative functions and supports the scientific & technical research and innovations activities of all offices within the Eastern Region including the regional headquarters.

Although there are a variety of hardware and operating systems, several of 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 Networks (LAN), host computer systems and client-server systems. The system supports a variety of users, functions, and applications. Supported applications include word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

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

General Support System.

b) System location

NOAA8882 comprised by Eastern Region HQ located in Bohemia, NY and 23 additional Weather Forecast Offices (WFO), 3 River Forecast Centers (RFC) and 4 Center Weather Service Units (CWSUs) across the region.

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

It interconnects with the following FISMA systems (ALL internal to NOAA):

NOAA8102 – Automated Surface Observation System
NOAA8104 – WSR-88D Radar Operations Center
NOAA8106 – Upper Air Observing System
NOAA8107 – Advanced Weather Interactive Processing System
NOAA8850 – Enterprise Mission Enabling System
NOAA8860 – Weather and Climate Computing Infrastructure Services

d) The purpose that the system is designed to serve

NOAA8882 data and products assist in the formation of a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community. NOAA88282 also provides administrative functions as well as scientific & technical research support for the NWS Eastern Region Headquarters (ERHQ) and all offices within the NWS Eastern Region (ER) boundary.

e) The way the system operates to achieve the purpose

NOAA8882 employs an information security architecture that promotes segmentation, redundancy, and the elimination of single points of failure to the fullest extent possible, which enables NOAA8882 to more effectively manage risk. In addition, NOAA8882 takes into consideration its mission/business programs and applications when considering new processes or services to help determine areas where shared resources can be leveraged or implemented. NOAA8882 strives to implement security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

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

NWS Eastern Region (ER) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees and volunteers who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports and performing other related administrative tasks. In addition, Weather Forecast Office (WFO)/River Forecast Centers (RFC) maintain local databases that contain information on volunteers

who provide weather reports to them.

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

Only NOAA authorized employees, contractors, associates are authorized to access the system.

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

Information is retrieved via an internal network, which requires secure authentication.

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

Information is transmitted via authorized NOAA networks, i.e. OneNWSnet.

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). *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 01-2017 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.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

_X_ 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?

____ 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.

Provide the legal authority which permits the collection of SSNs, including truncated form.

_X_ 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 NOAA8882 IT System 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 NOAA8882 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO): Nicholas Rappold

Signature of ISSO: RAPPOLD.NICHOLAS.PAUL.1459652953 Digitally signed by RAPPOLD.NICHOLAS.PAUL.1459652953 Date: 2020.09.01 15:19:55 -04'00'

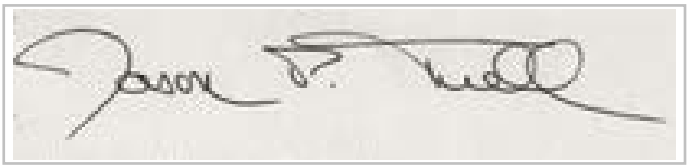
Name of Information Technology Security Officer (ITSO): Paula Reis

Signature of ITSO: REIS.PAULA.1281289523 Digitally signed by REIS.PAULA.1281289523 Date: 2020.09.08 12:56:44 -04'00'

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.09.08 13:21:44 -04'00'

Name of Authorizing Official (AO): Jason Tuell

Signature of AO: 

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: 2020.09.11 14:51:39 -04'00'