Version Number: 01-2021

U.S. Department of Commerce
National Oceanic & Atmospheric Administration

Privacy Threshold Analysis for the
NOAA8202
Office of Water Prediction (OWP)

Version Number: 01-2021

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NWS/ Office of Water Prediction (OWP)

Unique Project Identifier: NOAA8202

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: *Provide a brief description of the information system.*

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).

The Office of Water Prediction (NOAA8202), is comprised of hydrologic capabilities that include a production and operations capability, a research and development capability, and a capability that houses general administrative functions. The production and operations capability consists of products and services from modeling programs and data acquisition, processing, and dissemination programs. There is logical separation between the production and operations capability and other non-production capabilities. The research and development capability consists of applications for field offices that involve applied research and software engineering in support of applications within the NWS. The business administration capability includes office functions such as procurement, property, time and attendance, and other functions needed to carry on the daily business of an office.

Address the following elements:

a) *Whether it is a general support system, major application, or other type of system*
NOAA8202 is a general support system

b) *System location*
1) Chanhassen, MN
2) Hanover, NH (Chanhassen Web Alternate Site)
3) Tuscaloosa, AL

* Silver Springs, MD data center space for NOAA8202 was shut down, and all data was reconstituted at the Tuscaloosa, AL site. There was no PII or BII being collected or stored at the Silver Springs, MD location.

c) *Whether it is a standalone system or interconnects with other systems (identifying and*

describing any other systems to which it interconnects)

1. Cold Regions Research Engineering Laboratory (CRREL) – Army Corps of Engineers
2. Level3 - Networx
3. NOAA0550 - NOAA NWave WAN
4. NOAA8860 - Weather and Climate Computing Infrastructure Services (WCCIS)
5. NOAA8860 - NWS One NWSnet
6. *NOAA0100 - NOAA Cyber Security Center

*Note: The NOAA0100 interconnect is not a new connection and has been an interconnection since the implementation of NOAA8202. Description c) is being updated to match CSAM.

d) The purpose that the system is designed to serve

The Office of Water Prediction (NOAA8202), is comprised of hydrologic capabilities that include a production and operations capability, a research and development capability, and a capability that houses general administrative functions. The production and operations capability consists of products and services from modeling programs and data acquisition, processing, and dissemination programs. There is logical separation between the production and operations capability and other non-production capabilities. The research and development capability consists of applications for field offices that involve applied research and software engineering in support of applications within the NWS. The business administration capability includes office functions such as procurement, property, time and attendance, and other functions needed to carry on the daily business of an office.

e) The way the system operates to achieve the purpose

NOAA8202 OWP operates in the traditional client server model. Data is hosted on servers and made available via various protocols such as HTTPS, FTP, SFTP and SSH.

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

The NWS collects and maintains PII for the following administrative purposes:

- For emergency notifications: name, email, address, home telephone number, home email address, and spouse's cell phone number.
- For establishing IT system user accounts: name, office, government phone number, address and email address.
- Surveillance cameras at entry points are for additional security and images are stored on a server in our system. Such images could be used for criminal law enforcement, if applicable. Images captured could be federal employees, contractors, or the public.
- Card readers installed and maintained at the Tuscaloosa location by the University of Alabama, through a service level agreement between OWP and the university. The only information obtained by the card readers is badge number and name.

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

1. Maintainers – Information Technology Services Group (ITSG) – IT specialists (federal employees and contractors) that perform all administration on the actual hardware devices and associated software. This includes privileged access.

2. Developers – OWP scientists and developers (federal employees and contractors) who build the services. This does not include privileged access.

3. Consumers – NOAA, US Forest Service (USFS), US Army Corps of Engineers (USCOE), Academia and other federal, state and local emergency managers. This is provided by OWP.

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

An individual may access information or products from our websites; https://www.nohrsc.noaa.gov and https://hdsc.nws.noaa.gov/hdsc/pfds/. These websites contain weather-related data (rainfall/snowfall amounts, temperatures, etc.).

i) How information is transmitted to and from the system

HTTPS is used because it is a secure protocol allowing the protection of the data being transmitted.

Questionnaire:

1. Status of the Information System

1a. 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. *Continue to answer*

questions and complete certification.

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X_ No. This is not a new information system.

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.

_X_ Yes. *(Check all that apply.)*

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

____ 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
- X Contractors working on behalf of DOC
- X 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 SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

X The criteria implied by one or more of the questions above **apply** to the NOAA8202 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the NOAA8202 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Jason Letkiewicz Office: NWS/OWP Phone: 205-347-1410 Email: Jason.Letkiewicz@noaa.gov Signature: LETKIEWICZ.JASON.DANIEL.1363333377 Digitally signed by LETKIEWICZ.JASON.DANIEL.1363333377 Date: 2023.08.14 10:47:41 -05'00' Date signed: _____	**Information Technology Security Officer** Name: Andrew Browne Office: NWS OCIO Phone: 301-427-9033 Email: andrew.browne@noaa.gov Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2023.08.14 11:59:06 -04'00' Date signed: _____
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.09.13 15:01:58 -04'00' Date signed: _____	**Authorizing Official** Name: Thomas Graziano Office: NWS OWP Director Phone: 301-427-6904 Email: thomas.graziano@noaa.gov Signature: GRAZIANO.THOMAS.MARTIN.1365859252 Digitally signed by GRAZIANO.THOMAS.MARTIN.1365859252 Date: 2023.09.11 12:45:27 -04'00' Date signed: _____
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2023.10.12 09:08:27 -04'00' Date signed: _____	**Authorizing Official** Name: Beckie Koonge Office: NWS CISO Phone: 301-427-9020 Email: beckie.koonge@noaa.gov Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2023.08.14 11:59:35 -04'00' Date signed: _____