

**U.S. Department of Commerce
NOAA**



**Privacy Threshold Analysis
for the
National Water Center
NOAA8202**

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Water Center

Unique Project Identifier: 006-48-01-12-02-3115-00

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: The *National Water Center*, NOAA8202, is a system of hydrologic capabilities that include a production and operations capability, a research and development capability, and a capability that houses general administrative functions. The system is physically located in four distinct locations; National Weather Service (NWS) Headquarters, Silver Spring, MD; NWS National Water Center, Tuscaloosa, AL; National Operational Hydrologic Remote Sensing Center (NOHRSC), Chanhassen, MN and Cold Regions Research and Engineering Laboratory (CRREL), an Army Corps of Engineers facility in Hanover, NH. The facility at Hanover is designated as the backup facility to Chanhassen.

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.

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): Emergency contact list for supervisors was created on Google Drive.			

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). *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. *Please describe the activities which may raise privacy concerns.*

NOAA collects security surveillance camera footage for the building, as well as entry card readers.

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 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 National Water Center, NOAA8202, 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 National Water Center, NOAA8202, 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): James V. Rawls

Signature of ISSO or SO: RAWLS.JAMES.VIRGIL.111268 0779 Digitally signed by RAWLS.JAMES.VIRGIL.1112680779 Date: 2019.03.27 12:41:33 -05'00' Date:

Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 CK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2019.04.01 15:06:27 -05'00' Date:

Name of Authorizing Official (AO): Thomas Graziano

Signature of AO: GRAZIANO.THOMAS.M.DR.1365859252 .M.DR.1365859252 Digitally signed by GRAZIANO.THOMAS.M.DR.1365859252 Date: 2019.04.01 11:40:51 -04'00' Date:

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 892 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: 2019.04.01 17:17:45 -04'00' Date: