Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
NOAA0201
Web Operation Center (WOC)

Template Version Number: 01-2021

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/OCIO/Web Operation Center

Unique Project Identifier: NOAA0201 (006-48-02-00-01-3511-00**)**

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: *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).

As part of NOAA's Service Delivery Division (SDD), NOAA0201 WOC is a diverse information system providing a variety of cloud-based services to Line and Staff Offices within the NOAA Enterprise.

Services include Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Domain Name Service (DNS) tailored to meet customer needs. WOC hosts and supports numerous (200+) websites that disseminate a wide variety of data and information to the scientific and meteorological communities and the public at large. This data and information is used for numerous purposes, including: the study of the ocean, atmosphere, and related ecosystems; natural disaster forecasting and monitoring; climatological analysis and climate change; biodiversity; weather prediction; and the preservation of life, limb, and property.

All WOC devices are provisioned in the Federal Risk and Authorization Management Program (FedRAMP)-Certified Amazon Web Services (AWS) Cloud, including US East-West (FedRAMP moderate impact) and GovCloud (FedRAMP high impact) computing environments. For the purposes of redundancy and availability, WOC customers with high security categorization requirements have access to AWS GovCloud (based in Northern Virginia (us-gov-east-1) and Northern California (us-gov-west-2)), and WOC customers with moderate security categorization requirements have access to AWS US East-West (based in Northern Virginia (us-east-1), Ohio (us-east-2), Northern California (us-west-1), and Oregon (us-west-2)).

Address the following elements:

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

NOAA0201 WOC is a General Support System (GSS).

b) System location

AWS GovCloud: Northern Virginia (us-gov-east-1) and Northern California (us-gov-west-2).
AWS US East-West: Northern Virginia (us-east-1), Ohio (us-east-2), Northern California (us-west-1), and Oregon (us-west-2).

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

NOAA0201 is not a standalone system and interconnects with the following NOAA Information systems:
NOAA0550 – NOAA Enterprise Network
NOAA1101 – Information Technology Center
NOAA4100 – Greater Atlantic Regional Fisheries Office (GARFO)
NOAA4600 – Fishery Resource and Management (FRAM)
NOAA5006 – NESDIS Administrative Local Area Network (NESDIS Admin LAN)
NOAA5009 – National Climatic Data Center Local Area Network
NOAA5040 – Comprehensive Large Array-data Stewardship System
NOAA8860 – Weather and Climate Computing Infrastructure Services (WCCIS)
NOAA8868 – Storm Prediction Center
NOAA8873 – National Data Buoy Center

d) The purpose that the system is designed to serve

The system is used for Administrative Matters. The WOC is a diverse information technology services provider to Line and Staff Offices within NOAA. The WOC provides a wide range of information technology services and functions which include high availability, scalability, redundancy, clustering, and high-performance computing to replicate and distribute general information as well as critical time sensitive life and property information to the general public and meteorology community.

e) The way the system operates to achieve the purpose

NOAA0201 WOC provides data-dissemination business processes to distribute scientific and meteorological data, general information, and critical time sensitive life and property information to the public and meteorology community. This data is processed by other NOAA information systems and other federal agencies for use by the federal government and the public.

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

NOAA0201 WOC provides data-dissemination business processes to distribute scientific and meteorological data and information gathered from a variety of sources across the globe. This data is processed by other NOAA information systems and other federal agencies for general use by the federal government and the public.

In addition to the scientific and meteorological data, NOAA0201 contains PII in the form of contractor and federal employee contact information (name, phone number(s), email address(es), user ID) gathered from the employee(s) during the hiring process via phone, email, and in person. The information is vetted during the hiring and badging processes and used for administrative purposes only.

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

Only NOAA personnel (government employees and/or contractors) with authenticated access have access to the information and/or would be able to change or delete information.

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

Only NOAA personnel (government employees and/or contractors) with valid user accounts and authentication may access information in the system. Access requires the use of GFE. Remote access requires the use of VPN.

i) How information is transmitted to and from the system

All data is encrypted in transit.

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
- ____ 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. As documented in the NOAA4100 GARFO PIA, Tax Identification Numbers (SSNs or Employer ID Numbers) allow positive identification for cost recovery billing. A Tax Identification Number is required on all permit applications other than research or exempted fishing permits, under the authority 31 U.S.C. 7701. NOAA0201 now hosts this type of data for NOAA4100 GARFO.
Provide the legal authority which permits the collection of SSNs, including truncated form.

____ 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 NOAA0201 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 NOAA0201 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer Name: William C. Beck Office: OCIO Web Operations Center Phone: 301-628-5941 Email: william.beck@noaa.gov Signature: BECK.WILLIAM.CHRISTIAN.1406165791 Digitally signed by BECK.WILLIAM.CHRISTIAN.1406165791 Date: 2023.12.05 12:19:42 -05'00' Date signed: _____	**Information Technology Security Officer** Name: Justin May Office: OCIO Cyber Security Division Phone: 240-499-6792 Email: justin.may@noaa.gov Signature: MAY.JUSTIN.NATHANIEL.1039635980 MAY.JUSTIN.NATHANIEL.1039635980 2023.12.05 10:35:39 -07'00' 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: 2023.12.18 09:26:03 -05'00' Date signed: 12/18/2023	**Authorizing Official** Name: Douglas A. Perry Office: OCIO Deputy Chief Information Officer Phone: 301-713-9600 Email: douglas.a.perry@noaa.gov Signature: PERRY.DOUGLAS.ALLEN.1365847270 Digitally signed by PERRY.DOUGLAS.ALLEN.1365847270 Date: 2023.12.15 12:04:16 -05'00' 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: 2023.12.18 10:47:53 -05'00' Date signed: 12/18/23	