Template Version Number: 01-2021

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

Privacy Threshold Analysis for the
NOAA5011
National Geophysical Data Center Data Archive Management and User System (NGDC)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NESDIS/NGDC

Unique Project Identifier: NOAA5011

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).

NOAA's National Center for Environmental Information (NCEI) maintains the world's largest climate data archive and provides climatological services and data to every sector of the U.S. economy and to users worldwide. NCEI operates data centers in Asheville, NC, and Boulder, CO, with additional offices at Stennis Space Center, MS, and College Park, MD. NCEI located in Boulder, CO, comprises the NOAA5011 system.

The NCEI archive contains more than 37 petabytes of data, equivalent to about 400 million filing cabinets filled with documents. NCEI facilitates the acquisition of these environmental data collected by NOAA, by other agencies and departments of the U.S. government, as well as by other institutions, organizations, and governments in the U.S. and around the world.

NCEI, as part of the data stewardship mission of providing access and dissemination of the archive holdings, offers users access to tens of thousands of datasets and hundreds of products. NCEI provides search and discovery web platforms to enable the user community to efficiently find and retrieve data through a number of interfaces and services.

NCEI resources are used for scientific research and commercial applications in many fields, including agriculture, forestry, marine and coastal ecosystems, tourism, transportation, civil infrastructure, energy, transportation, water resources, energy, health, insurance, litigation, and national security. NCEI scientists work as lead contributors to the National Climate Assessment, as well publish periodic publications such as the Annual and Monthly State of the Climate Reports.

As part of the National Environmental Satellite, Data, and Information Service (NESDIS), NCEI coordinates with other data centers in related scientific and technical areas to provide standardized, robust, and efficient service.

Address the following elements:

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

NOAA's National Centers for Environmental Information (NCEI) is a General Support System (GSS).

b) System location

NOAA5011 is physically located in the David Skaggs Research Center in Boulder, CO.

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

NOAA5011 has an interconnection with NCEI-NC (NOAA5009) which was created to facilitate sharing of internal resources. The interconnection includes access to the system's intranet applications and shared code repositories. Access to resources is approved via the configuration management process. NOAA5009 and NOAA5011 are classified as moderate systems and may exchange data at that categorization level. NOAA5011 agreements are in place for services between NOAA5011 and other government agencies or universities.

The below connection agreements are in force:

Organization	Purpose	Agreement Type
NOAA0100- NOAA Cyber Security Center	SOC ISAs/SLAs	NOAA CIO Waiver
NOAA0201- Web Operation Center *	DNS Services	SLA
NOAA0550- NOAA NWAVE	NW Connectivity	ICD
NOAA5006- Headquarters Information Technology Support Local Area Network	NW/ Office Apps	ICD
NOAA5009- National Climatic Data Center Local Area Network	NCEI Interconnectivity	Organizational- Systems have the same SO and Co-AOs.
NOAA5040- Comprehensive Large Array-data Stewardship System	Internet & Office Spce	SLA
NOAA8864- Space Weather Prediction Center	Data Acquisition	ISA

*The interconnection with NOAA0201- Web Operations Center is not new. NOAA0201 provides Domain Name System (DNS) services to other NOAA information systems. NOAA5011 relies on the NOAA Web Operations Center as the registered owner and administrator of the noaa.gov domain and sub-domains to provide Domain Name System

Security Extensions (DNSSEC) services for all zones within NOAA. This has been in place for a number of years, and the interconnection was documented in our previously signed SSPs, along with the relevant controls (SC-20, SC-21 and SC-22). Element c) has simply been updated to match the information in CSAM.

d) The purpose that the system is designed to serve

NOAA5011 conducts a data and data- information service in all scientific and technical areas involving solid earth geophysics, marine geology and geophysics, glaciology, space environment, solar activity, and the other areas of solar-terrestrial physics. All data provided is publicly available and is harvested from the archive or via public web sites. None of this data is subject to interconnection agreements.

e) The way the system operates to achieve the purpose

NCEI-CO receives data from other NOAA groups, other federal government agencies such as NASA, the U.S. Air Force, the U.S. Geological Survey; federally funded research institutions such as the National Center for Atmospheric Research (NCAR), and the Woods Hole Oceanographic Institution; universities such as the University of Colorado - National Snow and Ice Data Center (NSIDC), and the Ocean Drilling Program at Texas A&M University; state agencies such as the Alaska Department of Natural Resources, California Department of Water Resources; and intergovernmental entities such as the European Space Agency, and the Australian Surveying and Land Information Group (AUSLIG).

The system 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

NOAA5011 data and data-information services encompass all scientific and technical areas involving solid earth geophysics, marine geology and geophysics, glaciology, space environment, solar activity, and the other areas of solar- terrestrial physics. The Center prepares systematic and special data products and performs data-related research studies to enhance the utility of the service to the users. It performs all functions related to data acquisition, archiving, retrieval, indexing, quality assessments, evaluation, synthesis, dissemination, and publication.

No sensitive PII/BII is collected, and only minimal general personal data (GPD) and work-related data (WRD) is collected.

System Administration/Audit Data (SAAD):
As part of meeting audit and monitoring requirements, connection and transaction related information is logged, for example, User IDs, IP Address, etc.

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

NOAA5011 has approximately 300 organizational users, Government, contractor and cooperative institute employees, that connect within NOAA5011's security boundary (internal users). The NOAA5011 user environment consists mainly of web developers, scientists, system administrators, administrative assistants, managers, customer service representatives, database administrators, and graphic designers.

External users include, but are not limited to, the general public, other federal government agencies such as NASA, the U.S. Air Force, the U.S. Geological Survey; federally funded research institutions such as the National Center for Atmospheric Research (NCAR), and the Woods Hole Oceanographic Institution; universities such as the University of Colorado - National Snow and Ice Data Center (NSIDC), and the Ocean Drilling Program at Texas A&M University; state agencies such as the Alaska Department of Natural Resources, California Department of Water Resources; and intergovernmental entities such as the European Space Agency, and the Australian Surveying and Land Information Group (AUSLIG). External users have access to publicly available scientific data and information, but, do not have access to PII, other than Data Provider's PII, including name, email and physical address that may be included with publicly available metadata for contributed data.

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

Internal NOAA5011 users retrieve data via internal file servers, the public web presence, and via anonymous FTP. External users retrieve data via the NOAA5011 public web presence and via anonymous FTP downloads of public data.

Organizational users authenticate using GFE (Government Furnished Equipment) and their Common Access Card to access in the information system. This provides users secure access that is managed by the program and supported by NOAA 5011.

i) How information is transmitted to and from the system

NOAA5011 (NCEI-CO) has a dedicated 10 gigabits per second (Gbps) link providing Wide Area Network (WAN) access from NCEI-CO to the Internet through the NOAA NWAVE (NOAA0550). Physical connectivity is provided via standard Ethernet configured at 10 Gbps. Endpoint access to the Internet is configured at 30 Gbps and provided via the NWAVE TICAP Service in Boulder, CO. In addition, NCEI-CO receives data from NOAA ships via external disk drives for data processing. The data from these disks are loaded onto local file servers on NOAA5011.
Information is transmitted to and from the system using the following protocols using a client/server model: SFTP, FTP, SSH, and HTTPS.

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. *Skip 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.

____ 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
__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 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 NOAA5011 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 NOAA5011 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 Symonds Office: NOAA/NESDIS/NCEI Phone: (828) 271-4733 Email: Jason.symonds@noaa.gov Signature: SYMONDS.JASON.THOMAS.1366777411 Digitally signed by SYMONDS.JASON.THOMAS.1366777411 Date: 2023.05.01 12:20:44 -04'00' Date signed:	**Information Technology Security Officer** Name: Rick Miner Office: NOAA/NESDIS Phone: (240) 628-4945 Email: rick.miner@noaa.gov Signature: Digitally signed by MINER.RICHARD.SCOTT.1398604519 Date: 2023.05.16 11:09:24 -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: 2023.05.22 10:01:55 -04'00' Date signed: 05/22/2023	**Authorizing Official** Name: Derek Arndt Office: NOAA/NESDIS/NCEI Phone: (828) 271-4476 Email: derek.arndt@noaa.gov Signature: ARNDT.DEREK.SHANE.1384496519 Digitally signed by ARNDT.DEREK.SHANE.1384496519 Date: 2023.05.15 16:20:24 -04'00' Date signed: 6519
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: 2023.05.22 13:04:07 -04'00' Date signed: 5/22/23	