Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
National Climatic Datacenter Local Area Network (NOAA5009)

U.S. Department of Commerce Privacy Threshold Analysis
NOAA/NCDC LAN

Unique Project Identifier: [006-000321900]

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 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 (GSS)

NOAA's National Centers for Environmental Information (NCEI)-NC 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. Records in the archive range from paleoclimate data to centuries-old journals to data less than an hour old. The Center's mission is to preserve these data and make them available to the public, business, industry, government, and researchers.

NCEI-NC develops national and global datasets, which maximize the use of our climatic and natural resources while also minimizing the risks caused by climate variability and weather extremes. NCEI has a statutory mission to describe the climate of the United States and it acts as the "Nation's Scorekeeper" regarding the trends and anomalies of weather and climate. NCEI-NC's climate data have been used in a variety of applications including agriculture, air quality, construction, education, energy, engineering, forestry, health, insurance, landscape design, livestock management, manufacturing, national security, recreation and tourism, retail, transportation, and water resources management.

As part of the National Environmental Satellite, Data, and Information Service (NESDIS), NCEI-NC coordinates with other data centers in related scientific and technical areas to provide standardized, robust, and efficient service. NCEI-NC manages and contributes to a variety of climate service partnerships including the Regional Climate Services Directors, Regional Climate Centers, State Climatologists, and Cooperative Institute for Climate and Satellites– North Carolina. To facilitate a global data and information exchange, the Center also operates two World Data Centers—one for meteorology and one for paleoclimatology—and plays an active role in professional societies and user engagement activities. Data available through these partnerships does not require access accounts.

b) System location

North Carolina location:
Veach-Baley Federal Building
Asheville, NC

Mississippi location:
Mississippi State University Research and Technology Corporation (MSURTC) Building 1021 at Stennis Space Center (SSC).

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

NOAA5009 interconnects with the following general support systems to support information sharing and collaboration.

- NOAA5006, NESDIS Headquarters Information Technology Support Local Area Network
- NOAA5010, National Oceanographic Data Center Local Area Network
- NOAA5011, National Geophysical Data Center Data Archive Management and User System
- NOAA5040, Comprehensive Large Array-data Stewardship System
- NOAA5050, Geostationary Environmental Operational Satellite Series-R Ground System
- NOAA0550, NOAA Enterprise Network

d) The purpose that the system is designed to serve

NOAA's National Centers for Environmental Information (NCEI)-NC, which encompasses the NCDCLAN, 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. Records in the archive range from paleoclimate data to centuries-old journals to data less than an hour old. The Center's mission is to preserve these data and make them available to the public, business, industry, government, and researchers.

NCEI-NC develops national and global datasets, which maximize the use of our climatic and natural resources while also minimizing the risks caused by climate variability and weather extremes. NCEI has a statutory mission to describe the climate of the United States and it acts as the "Nation's Scorekeeper" regarding the trends and anomalies of weather and climate. NCEINC's climate data have been used in a variety of applications including agriculture, air quality, construction, education, energy, engineering, forestry, health, insurance, landscape design, livestock management, manufacturing, national security, recreation and tourism, retail, transportation, and water resources management.

As part of the National Environmental Satellite, Data, and Information Service (NESDIS), NCEI-NC coordinates with other data centers in related scientific and technical areas to provide standardized, robust, and efficient service. NCEI-NC manages and contributes to a variety of climate service partnerships including the Regional Climate Services Directors, Regional Climate Centers, State Climatologists, and Cooperative Institute for Climate and Satellites– North Carolina. To facilitate a global data and information exchange, the Center also operates two

World Data Centers—one for meteorology and one for paleoclimatology—and plays an active role in professional societies and user engagement activities. Data available through these partnerships does not require access accounts.

e) The way the system operates to achieve the purpose

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, use, or disseminated by the system

Environmental observations and products associated with the following type of data:

Employee Info:

- Name
- Personal email address
- Personal phone number
- Photograph for internal use (voluntary posting to intranet)
- Fingerprint template file (copied from government issued PIV card)

Climate:

- Monitoring & Extremes
- Models
- Radar
- Satellite
- Land-based stations
- Interactive maps

Ocean:

- Marine & Ocean surface
- Ocean Climatologies
- Bathymetry

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

NCEI-NC has approximately 290 users that connect within NOAA5009 security boundary. The NCEI-NC user environment consists of web developers, scientists, system administrators, administrative assistants, managers, customer service representatives, database administrators, graphic designers, order fulfillers, and computer operators.

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

Information in the system is retrieved by non-organizational users using the following protocols in a client/server model: HTTPS, SFTP, SSH, and FTP. Organizational users authenticate using GFE and their Common Access Card to access in the information system.

i) How information is transmitted to and from the system

Information is transmitted to and from the system using the following protocols using a client/server model: SFTP, FTP, SSH, and HTTPS.

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 NonAnonymous		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.)."

__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
____ 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 National Climatic Data Center Local Area Network 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 Climatic Data Center Local Area Network 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): Jason Symonds

Signature of ISSO or SO: SYMONDS.JASON.T.1366777411 Digitally signed by SYMONDS.JASON.T.1366777411 Date: 2020.04.16 15:02:05 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Frank Menzer

Signature of ITSO: MENZER.FRANK.E.1026670450 Digitally signed by MENZER.FRANK.E.1026670450 Date: 2020.04.26 12:08:45 -04'00' Date: 4/26/2020

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.04.27 22:30:11 -04'00' Date: _____

Name of Authorizing Official (AO): Mary Wohlgemuth

Signature of AO: WOHLGEMUTH.MARY.STANFORD.1228710519 Digitally signed by WOHLGEMUTH.MARY.STANFORD.1228710519 Date: 2020.04.17 08:02:41 -04'00' Date: _____

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2020.05.04 17:14:25 -04'00' Date: _____