Version Number: 01-2019

U.S. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA)

Privacy Threshold Analysis
for the
Configuration Branch Information Technology System (CBITS)
NOAA8100

U.S. Department of Commerce Privacy Threshold Analysis

NOAA National Weather Service Configuration

Branch Information Technology System

(CBITS) NOAA8100

Unique Project Identifier: NA

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: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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

The Configuration Branch Information Technology System (CBITS) is a general support computer system.

b) System location

The Configuration Branch Information Technology System (CBITS) is located in Silver Spring, MD.

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

The Configuration Branch Information Technology System (CBITS) allows the Office of Observations (OBS) to collect data in order to support the management and operations of National Weather Service (NWS) equipment. NOAA8100-CBITS is owned and operated by the OBS Surface and Upper Air Division. NOAA8100-CBITS hosts Oracle based applications used to collect data via web-based data entry forms. Additionally, NOAA8100-CBITS host one application outside the core mission of managing and maintaining NWS mission. This is the Station Information System (SIS) application. NOAA8100-CBITS uses NOAA8850 as a network service provider.

d) The purpose that the system is designed to serve

The CBITS is an administrative system. The main purpose of the system is to collect data used to support management, the regions, and the field sites within the NWS. The types of data collected include equipment maintenance information, station metadata, and configuration information about NWS systems. In addition the CBITS hosts a requirements building application.

e) The way the system operates to achieve the purpose

The user community accesses the CBITS applications via web portals designed to allow entry of data collected by the users and to generate reports used by NWS management. The data is collected and stored in multiple Oracle databases.

Additionally, SIS is a web based COOP Station metadata management where the authenticated and authorized weather forecasting officers and meteorologists will enter and manage the metadata via secure portal.

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

NOAA8100-CBITS stores federal and contractor user names, work emails, work phone numbers and the IP addresses from which those users are accessing the NOAA8100-CBITS.

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

NOAA8100 does not share privacy data with other systems, except in cases of security or privacy breaches, when information is shared within the bureau, with the Department, and with other Federal agencies, most probably the Department of Justice. Authorized users who can use and access the Personally Identifiable Information (PII) and Business Identifiable Information (BII) are strictly limited to the program administrators and managers (NOAA employees and contractors).

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

Information in the CBITS is served to the users via daily reports and is also accessed via web pages that provide the ability for users to query the system.

For SIS: The users login to the application using their credentials and based on the roles the users have users will have access to canned reports and capabilities ranging from editing and submitting the data to approving and rejecting the updates.

i) How information is transmitted to and from the system.

Information is transmitted to and from the system via web forms and reports, via ingestible data files, and through secure FTP. For SIS: The data is transmitted to and from the systems via SSL encrypted HTTPS layer to the backend database.

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):					

____ 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 01-2018 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.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

X 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 Configuration Branch Information Technology System (CBITS) NOAA8100 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 Configuration Branch Information Technology System (CBITS) NOAA8100 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): Dr. Thomas Day

Signature of ISSO or SO: DAY.THOMAS.J.1395205826 Digitally signed by DAY.THOMAS.J.1395205826 Date: 2020.07.20 08:38:43 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Paula Reis

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2020.07.23 14:00:40 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.07.29 09:16:39 -04'00' Date: _____

Name of Authorizing Official (AO): Thomas Cuff

Signature of AO: CUFF.THOMAS.JAMES.1071092450 Digitally signed by CUFF.THOMAS.JAMES.1071092450 Date: 2020.07.28 15:34:34 -04'00' Date: _____

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2020.08.03 16:24:55 -04'00' Date: _____