

**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 (NOAA8100)

Unique Project Identifier: This system is not identified with any Exhibit 300.

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 Configuration Branch Information Technology System (CBITS) is a general support computer system located in Silver Spring, MD, that 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.

NOAA8100-CBITS web-based applications are used to collect data such as equipment maintenance records, site equipment configuration records, equipment product structures, baseline documentation records, unscheduled equipment outage records, and NWS equipment site location information. Additionally, NOAA8100-CBITS host one application outside the core mission of managing and maintaining NWS' mission. This is the Station Information System (SIS) application.

SIS is an application that supports the (NWS) Cooperative Observer Program (COOP). The COOP was formally created in 1890 under the Organic Act. Its mission is two-fold: To provide observational meteorological data, usually consisting of daily maximum and minimum temperatures, snowfall, and 24-hour precipitation totals, required to define the climate of the United States and to help measure long-term climate changes; and to provide observational meteorological data in near real-time to support forecast, warning and other public service programs of the NWS. Volunteer weather observers conscientiously contribute their time so that observations can provide the vital weather data, generally temperature and precipitation information, daily.

Information sharing: 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).

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.

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.*

 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 01-2015 or later). *Continue to answer 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.*

 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 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.

___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, 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 [Configuration Branch Information Technology System] 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] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Backup Information System Security Officer (ISSO) or System Owner (SO): Brady Malone

Signature of Backup ISSO or SO: MALONE.BRADY.EDWARD.1455227050 Digitally signed by MALONE.BRADY.EDWARD.1455227050
Date: 2018.06.15 12:45:35 -04'00' Date: 06/15/2018

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

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.06.15 13:35:37 -04'00' Date:

Name of Authorizing Official (AO): Joseph Pica

Signature of AO: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961
Date: 2018.06.18 12:30:02 -04'00' Date: 06/18/2018

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 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: 2018.06.20 15:10:58 -04'00' Date: 6/20/18