

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



**Privacy Impact Assessment
for the
Configuration Branch Information
Technology System (CBITS)
NOAA8100**

Reviewed by: _____Mark Graff_____, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
 Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open
Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.10.07 15:23:37 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

**U.S. Department of Commerce Privacy Impact Assessment
NOAA National Weather Service Configuration Branch Information
Technology System (NOAA8100)**

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

System Description

The Configuration Branch Information Technology System (CBITS) is a general support computer system that allows the Office of Observations (OBS) to collect data in order to support the management and operations of National Weather Service (NWS) equipment. CBITS is owned and operated by the OBS Surface and Upper Air Division. CBITS hosts Oracle based applications used to collect data via web-based data entry forms.

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, CBITS host two applications outside the core mission of managing and maintaining NWS mission. The applications are National Oceanic and Atmospheric Service (NOAA) Emergency Notification System (ENS) and Cooperative Station Services Accountability (CSSA). CSSA was formerly in NOAA8900.

The National Oceanic and Atmospheric Service (NOAA) Emergency Notification System (ENS) is a tool/application hosted by CBITS supporting NOAA Homeland Security Program Office. This application allows NOAA, in the field and at headquarters, to quickly broadcast consistent emergency information to affected employees via cell phone, email, text, and office phone. Information is collected via the NOAA Staffing Directory (NSD) web site [https://nsd\[dot\]rdc\[dot\]noaa.gov/nsd/](https://nsd[dot]rdc[dot]noaa.gov/nsd/).

Cooperative Station Services Accountability (CSSA), 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 daily.

Information sharing: Neither the CSSA, nor the ENS share privacy data with other systems. Authorized users who can use and access the Personally Identifiable Information (PII) and Business Identifiable Information (BII) are strictly limited to NOAA Homeland Security manager, for ENS; for CSSA, the program administrators and managers (NOAA employees and contractors).

CBITS is categorized as a moderate impact information system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

This is a new information system.

This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging	X	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): CBITS expanded the authorization boundary to include the Cooperative Station Services Accountability (CSSA) application.					

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)

a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address		h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Supervisor Name, Facility ID, Office Type (i.e. HQ, WFO, RFC, National Center, Ship), NOAA Affiliation, Line Office					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)					

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify)					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCBPNPD)					
--	--	--	--	--	--

Smart Cards	X	Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify): CBITS utilizes the NOAA infrastructure Common Access Cards (CAC) for privilege users administrating the system.			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
--	--

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.
---	--

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The ENS is an internal oracle application; without a web interface. It is a notification system that provides tools for reaching contacts during an emergency situation. The purpose of the ENS is to simplify the management of emergency communication processes and procedures in order to communicate quickly and easily with all employees, contractors and associates. The communications system allows NOAA to reach staff rapidly and efficiently wherever they are located. This ensures the life, safety and security of all staff (including contractors) during emergencies.

The Cooperative Station Service Accountability (CSSA) is a computerized national data base containing descriptions of the Cooperative stations' information for 11,000+ Cooperative Observer Program (COOP) sites/members including the location, observer's name, equipment in use, where and how data are submitted, and driving directions to the site. PII is collected from members of the public.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			X
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.
--	---

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.noaa.gov/protecting-your-privacy .	
X	Yes, notice is provided by other means.	Specify how: ENS: The staff directory has a link to the NOAA Privacy Policy. The COOP Observer program web pages have links to the NOAA Privacy Policy.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: ENS: Individuals may decline, to their supervisors in writing, to provide PII/BII. Provision of the information is voluntary. CSSA application: Volunteers do not provide information unless they want to participate in the COOP program. During COOP station inspection, the COOP representative manually collects the station observer's name and station location and then NWS personnel manually enter information into the CSSA application.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: ENS: Since there is only one use for the ENS, unless the individual declines in writing, per 7.2, consent is implied.
---	--	---

		CSSA: Volunteers receive the explanation of the purposes of the information collection in writing, from the COOP representative, and if they consent to those uses, they provide the information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: ENS: Individuals may review and update their information within the system upon accessing the NOAA Staff Directory web page. There are specific instructions on the Staff Directory site. CSSA: Although volunteers do not have access to the CSSA or data, individuals are advised, during the annual station inspection, that they may provide updated information during the inspection, to the COOP representative, in writing.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: According to Department of Commerce Information Technology Security Program Policy DOC ITSPP for auditing and accountability, CBITS ensured specific table entries are included in the auditable events; logs are reviewed manually weekly and in real time via NOAA Security Operations Center (SOC). Moreover, CBITS tracks all computer-readable data extracts from databases holding sensitive information.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 9/5/2015___ <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts

	required by DOC policy.
X	Contracts with customers establish ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

CBITS utilizes enterprise wide services to aid in security monitoring, vulnerability scanning and secure baseline management. CBITS deployed the enterprise cybersecurity monitoring operations (ECMO) i.e. IBM Big Fix agents to 100% of the inventory. The product ensures the CCB approved baseline is maintained and anomalies are tracked in real time. CBITS administrators conduct authenticated internal and external vulnerability scanning against the inventory and apply remediation accordingly. CBITS adhere to a two factor authentication for user requiring privilege access i.e. system and database administration. CBITS web applications use NOAA email account and password. CBITS has a connection to the NOAA LDAP directory that provides synchronized changes to Oracle Single Sign On, as email accounts are added, changed or deleted from the NOAA LDAP directory. Oracle Databases applies two levels of encryption schemes.

For all data, CBITS uses two levels of encryption to protect PII in the data base. The first is Tablespace Level Encryption at the data file level. This method encrypts using an external wallet which holds the master encryption key. In order to access the encrypted tablespaces, the wallet must be “open,” which requires a password. The second encryption method is column level encryption. Columns which contain privacy data are encrypted using the DBMS_ENCRYPT built in package. This encrypts the data within the column. The encryption method utilizes a key value which must be used at the time the data is retrieved. Both encryption methods, data files at the bit level and within the column ensure in the event of unauthorized data extraction, data will be unreadable.

CBITS is using ArcSight for audit management.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.

§ 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : The SORN covering employee information: Employees Personnel Files Not Covered by Notices of Other Agencies – COMMERCE/DEPT-18. For volunteer information, NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA’s Mission, covers volunteer
---	--

	information.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NWR follows NOAA Records Schedule Chapter 2300-04, Information Technology Operations and Management Records National Archives General Records Schedule GRS 3.1 General Technology Management 3.1 020 Retention: DAA-GRS-2013-0005-0004 (GRS 3.1, item 020)
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing	X	Deleting	
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

Identifiability	Provide explanation:
-----------------	----------------------

	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: There is no sensitive information in this system.
X	Context of Use	Provide explanation: Due to the nature of the collecting data to support statistical data analysis and reporting, notification to individuals in the event of an emergency and ensure accuracy of reports, with respect to weather metadata, reliability and maintainability graphs submission, the release of phone book information (name, address and phone number) would not likely cause harm to the individual.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Privacy data is strictly limited to program managers and administrators. All access to the database occurs from within the organization and not shared with other information system.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.