Version Number: 01-2020

U.S. Department of Commerce

National Oceanic and Atmospheric 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

GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2021.05.27 11:29:40 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NWS/Configuration Branch Information Technology System (CBITS)

Unique Project Identifier: NOAA8100

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(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 and NOAA0550 for a Common Control provider.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

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 CO-OP Station metadata management where the authenticated and authorized weather forecasting officers and meteorologists will enter and manage the metadata via secure portal.

(e) 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 their roles, users will have access to canned reports and capabilities ranging from editing and submitting the data to approving and rejecting the updates.

(f) 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.

(g) Any information sharing conducted by the system

SIS does not share privacy data with other systems, except in case 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). In case of security or privacy breaches, 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.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

- 5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.
- 15 U.S.C. § 1512 is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531- 332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.
- 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

NOAA8100-CBITS is categorized as a FIPS-199 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		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.

____ 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 01-2017).

_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 01-2019 or later).

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*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
k. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	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		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 Describe how the accuracy of the information in the system is ensured.

Volunteers, federal employees, and contractors provide their own information directly. NOAA8100- CBITS utilizes enterprise-wide services to aid in security monitoring, vulnerability scanning, and secure baseline management. The system also uses a NOAA enterprise service application for audit log management.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 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 (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	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			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
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)	X	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 Station Information System (SIS) enclave of NOAA8100-CBITS is a computerized national database 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, all information provided by the observers are voluntary. PII is collected from members of the public.

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.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Privacy data is subject to the same level of information security as system specific, in this case weather, data. Therefore, all applicable controls such as Access Control, Audit and Accountability, Media Protection, and Physical and Environmental Protection families are in force for the system components and software that store, process, and transmit PII.

NOAA's use of the information would still be subject to any potential insider threats, as individuals with authorization and need-to-know will have access to the PII within the system. Additionally, as a separate standalone system, damage or corruption of the system or its data could result in a loss of the PII or NOAA's ability to use the system. NOAA's privacy controls, including the controls referenced above and in particular the access controls, significantly mitigate the risk of either of these threats.

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		X**
DOC bureaus	X		
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

** Web application into which staff put volunteer information.

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

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

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

X	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: NOAA8100 connects with, NOAA8850 and NOAA0550 to supply networking, malicious software mitigation, and common controls respectively. No PII and/or BII data is stored or processed outside the system boundary.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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: https://sis.nws.noaa.gov/pages/privacyActStatement.jsp	
X	Yes, notice is provided by other means.	Specify how: The COOP Observer program web pages have links to the PAS and 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: SIS 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 SIS application. Employees and contractors are able to decline to sign the Rules of Behavior but this may affect their employment,
	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: SIS: All-users 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. Users who decline to provide information cannot access the system.
	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: End-users do not have access to SIS or data inside. Individuals are advised during annual station inspection, that they may provide updated information during inspections in writing. Government employees and contractors then have the ability to update associated information.
	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, NOAA8100-CBITS ensures that 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, NOAA8100-CBITS tracks all computer-readable data extracts from databases holding sensitive information.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 09/30/2020 ☐ 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 controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).

X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
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 DOC 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. *(Include data encryption in transit and/or at rest, if applicable).*

NOAA8100-CBITS utilizes enterprise-wide services to aid in security monitoring, vulnerability scanning, and secure baseline management. NOAA8100-CBITS uses two levels of encryption to protect PII in the database. All data is encrypted at rest in addition to field level encryption of sensitive data in the database. All security settings and configuration are subject to FISMA compliance and audits.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(list all that apply)*: The SORN covering employee information: Employees Personnel Files Not Covered by Notices of Other Agencies – COMMERCE/DEPT-18. https://osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html For volunteer information, NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. COMMERCE/DEPT-13, Investigative and Security Records, covers breach information. https://osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-13.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

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	X	Overwriting	
Degaussing	X	Deleting	X
Other (specify):			

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

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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:

		Only non-sensitive PII is contained in the system. There is no sensitive information or sensitive PII in this system
X	Context of Use	Provide explanation: Due to the nature of the data collection, the release of phone book information would not likely cause harm to any individual who uses the system.
	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 systems.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

For NOAA8100-CBITS, the threat to privacy is limited to the release of federal and contractor business contact information. For the SIS application, the threat to privacy is limited to the release of geographical location for COOP equipment hosted by members of the general public. This information is provided directly by members of the public.

The privacy information collected regarding federal and contractor employees for NOAA8100-CBITS, and the general public for the SIS application is strictly limited to necessary data. Gathering less data would negatively impact the system's mission.

12.2 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.

12.3 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.