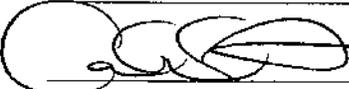


**U.S. Department of Commerce  
NOAA**



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

Reviewed by: \_\_\_\_\_, Bureau Privacy Officer or Designee

Approved by:  \_\_\_\_\_, DOC Chief Privacy Officer

Date approved: 8/25/2015

## U.S. Department of Commerce Privacy Impact Assessment NOAA8100

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

### **Introduction: System Description**

The Configuration Branch Information Technology System (CBITS) is a general support computer system that allows the Office of Operational Systems (OPS) Operations Division to collect data in order to support the management and operations of National Weather Service (NWS) equipment. CBITS is owned and operated by the NWS Configuration Branch (OPS13). 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 equipment. The applications are Accident and Illness (A&I) application records and Emergency Notification System (ENS). Data from these records are processed, and reports, such as reliability and maintainability graphs, accident/illness, and emergency notification records are created.

The authorities for the collection of this data are the Occupational Safety and Health Act (OSHA) of 1970, which requires certain employers to prepare and maintain records of work-related injuries and illnesses. Additional authorities are the Federal Continuity Directive 1, Code of Federal Regulations, Title 41, Chapter 102 Federal Management Regulation (FMR), Part 102-74 (41 CFR §102-74.230 - 102-74.260), DOC's Departmental Organizational Order (DOO) 20-6, and guidance provided by DOC's Manual of Security Policies and Procedures, Chapter 7. Also, per the System of Records Notices (SORNs) cited: 29 U.S.C. 651-78, 28 U.S.C. 2671-2680, Executive Order 12196 (DEPT-7), and 5 U.S.C. 301 (DEPT-18) (see Section 7).

**Information sharing:** Neither the A&I nor the ENS share data with other systems. Users who can use and access the Personally Identifiable Information (PII) and Business Identifiable Information (BII) are strictly limited to NOAA safety managers. The safety managers share meta data via statistical reports, graphs and illustrations pertaining to A&I information, i.e number of accidents occurred in a select period of time or injuries of a specific job title. This information, which does not include PII or BII, can be shared via emails and formal reports to senior leadership.

CBITS is categorized as a moderate impact information system.

### **Section 1: Information in the System**

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

<b>Identifying Numbers (IN)</b>			
a. Social Security	<input type="checkbox"/>	e. Alien Registration	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>
c. Employee ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>
d. File/Case ID	<input type="checkbox"/>	h. Credit Card	<input type="checkbox"/>
i. Financial Account			
j. Financial Transaction			
k. Vehicle Identifier			
l. Employer ID Number			
m. Other identifying numbers (specify):			

<b>General Personal Data (GPD)</b>			
a. Name	<input checked="" type="checkbox"/>	g. Date of Birth	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	h. Place of Birth	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	i. Home Address	<input checked="" type="checkbox"/>
d. Gender	<input type="checkbox"/>	j. Telephone Number	<input checked="" type="checkbox"/>
e. Age	<input type="checkbox"/>	k. Email Address	<input checked="" type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	l. Education	<input type="checkbox"/>
		m. Religion	<input type="checkbox"/>
		n. Financial Information	<input type="checkbox"/>
		o. Medical Information	<input checked="" type="checkbox"/>
		p. Military Service	<input type="checkbox"/>
		q. Physical Characteristics	<input type="checkbox"/>
		r. Mother's Maiden Name	<input type="checkbox"/>
s. Other general personal data (specify): Address cross street; time to contact employee			
*Medical information is related only to on-the-job injuries and illnesses.			

<b>Work-Related Data (WRD)</b>			
a. Occupation	<input checked="" type="checkbox"/>	d. Telephone Number	<input checked="" type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	e. Email Address	<input type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	f. Business Associates	<input type="checkbox"/>
g. Salary			
h. Work History			
i. Other work-related data (specify): Supervisor Name, Facility ID, Office Type (i.e. HQ, WFO, RFC, National Center, Ship), NOAA Affiliation, Line Office			

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

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

<b>Other Information (specify)</b>
Incident Information: Date, Time, Location, Type; Medical Treatment, Death or Hospitalization, Description.
Investigation: Details, Supervisory Action, Cause, Result of Violation of Safety, Confirmation of proper training, Corrective Action

1.2 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		Public Media, Internet		Private Sector	
Commercial Data Brokers					
Other (specify):					

**Section 2: Purpose of the System**

2.1 Indicate why the PII/BII in the 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	
Other (specify): For accident/illness records	X		

**Section 3: Use of the System**

3.1 Provide an explanation of how the bureau will use the PII/BII to accomplish the checked purpose(s), e.g., to verify existing data. Describe why the PII/BII that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and further the mission of the bureau and/or the Department. Indicate if the PII/BII identified in Section 1.1 of this document is in reference to a federal employee/contractor, member of public, foreign national, visitor or other (specify).

The Occupational Safety and Health Act (OSHA) of 1970 requires certain employers to prepare and maintain records of work-related injuries and illnesses. The A&I is a web-based application responsible for documenting provisions of safe and healthful workplaces and conditions of employment for all NOAA personnel. Prompt investigation and reporting of any incident involving NOAA employees, contractors, visitors or property will provide information necessary for the systematic identification and correction of safety and health hazards.

The A&I reporting system facilitates reporting of all incidents within 24 hours of the incident occurrence. If an incident is considered serious in nature, it shall be reported as soon as possible, but no later than 24 hours of occurrence.

The ENS is a web-based application. 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.

**Section 4: Information Sharing**

4.1 Indicate with whom the bureau intends to share the PII/BII in the system and how the PII/BII will be shared.

Recipient	How Information will be Shared			
	Case-by-Case	Bulk Transfer	Direct Access	Other (specify)
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.

**Section 5: Notice and Consent**

5.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or

disseminated by the system. Check all that apply.

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 6.	
x	Yes, notice is provided by other means.	Specify how: The A&I and ENS applications have links to the NOAA Privacy Policy on their respective home pages.
	No, notice is not provided.	Specify why not:

5.2 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:  Accident/Illness application: Individuals may decline to provide information, but the requested BII and information pertaining to the injury is required and will be completed by the supervisor. The Occupational Safety and Health (OSH) Act of 1970 requires certain employers to prepare and maintain records of work-related injuries and illnesses.  The ENS application provides a specific interface for the user to decline PII and BII input.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

5.3 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: NWS Privacy Policy states that provision of the information implies consent, and that consent to the particular uses of the information, is implied.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

5.4 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: Individuals may review and update their information within the system.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

## **Section 6: Administrative and Technological Controls**

6.1 Indicate the administrative and technological controls for the system. Check all that apply. Also see Appendix A, a checklist for more specific controls. This appendix will be removed after the PIA is approved.



X	All users signed a confidentiality agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff received training on privacy and confidentiality policies and practices.
X	Access to PII/BII is restricted to authorized personnel only.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization: <u>5/30/2015</u>
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST 800-122 recommended security 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.
	Other (specify):

### **Section 7: Privacy Act**

7.1 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. Provide the system name and number:  The SORNs covering Accident/Illness and Emergency Notification reporting: Systems name: Employee Accident Reports – COMMERCE/DEPT-7; and Employees Personnel Files Not Covered by Notices of Other Agencies – COMMERCE/DEPT-18.
	Yes, a system of records notice has been submitted to the Department for approval on <u>(date)</u> .
	No, a system of records is not being created.

### **Section 8: Retention of Information**

8.1 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: Weather Service Records Chapter 307-12 indicates that "Reports and logs (including Occupational Safety and Health Administration (OSHA) Forms 100, 101, 102, and 200, or equivalents) are maintained as prescribed in 29 CFR 1960 and OSHA pamphlet 2014 to document all recordable occupational injuries and illnesses for each establishment.
	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:



## Appendix A – Security Controls

In the first column, please complete as “in place,” “POAM ID # \_\_\_\_\_,” “N/A,” or “RA (Risk Accepted).”

In Place	<b>Access Enforcement (AC-3).</b> Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).
In Place	<b>Separation of Duties (AC-5).</b> Organizations can enforce separation of duties for duties involving access to PII.
In Place	<b>Least Privilege (AC-6).</b> Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
In place	<b>Remote Access (AC-17).</b> Organizations can choose to prohibit or strictly limit remote access to PII.
In Place	<b>User-Based Collaboration and Information Sharing (AC-21).</b> Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.
N/A, There is no mobile device access within the system boundary	<b>Access Control for Mobile Devices (AC-19).</b> Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization’s facilities).
In Place	<b>Auditable Events (AU-2).</b> Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
In Place	<b>Audit Review, Analysis, and Reporting (AU-6).</b> Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
In Place	<b>Identification and Authentication (Organizational Users) (IA-2).</b> Users can be uniquely identified and authenticated before accessing PII.
In Place	<b>Media Access (MP-2).</b> Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm).
In Place	<b>Media Marking (MP-3).</b> Organizations can label information system media and output containing PII to indicate how it should be distributed and handled.
In Place	<b>Media Storage (MP-4).</b> Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
In Place	<b>Media Transport (MP-5).</b> Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization’s controlled areas.
In Place	<b>Media Sanitization (MP-6).</b> Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.
In Place	<b>Transmission Confidentiality (SC-9).</b> Organizations can protect the confidentiality of transmitted PII.
In Place	<b>Protection of Information at Rest (SC-28).</b> Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.
In Place	<b>Information System Monitoring (SI-4).</b> Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events.

This page is a supplement for item 6.1. Upon final approval, this page must be removed prior to publication of the PIA.

### Points of Contact and Signatures

<p><b>Information Technology Security Officer</b>  Name: Sherry Richardson  Office: Office of the Chief Information Officer  Phone: 301-427-9034  Email: sherry.richardson@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BI processed on this system.</p> <p>Signature: <u>RICHARDSON.S HERRY.ANN.10</u>  <small>Digitally signed by RICHARDSON.S HERRY.ANN.108717191 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=RICHARDSON.S HERRY.ANN.108717191 Date: 2015.08.24 08:52:46 -0400</small></p> <p>Date signed: <u>18717391</u></p>	<p><b>System Owner</b>  Name: Kelvin Taylor  Office: NWS/OOS/OPS1/OPS13 Configuration Branch  Phone: 301- 427- 9205  Email: kelvin.taylor@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BI processed on this system.</p> <p>Signature: <u>TAYLOR.KELVIN.LAMARK.10</u>  <small>Digitally signed by TAYLOR.KELVIN.LAMARK.1062624120 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=TAYLOR.KELVIN.LAMARK.1062624120 Date: 2015.08.21 12:45:46 -0400</small></p> <p>Date signed: <u>62624120</u></p>
<p><b>NOAA Privacy Officer or Designee</b>  Name: Robert Swisher  Office: NOAA Office of the Chief Information Officer  Phone: 301-628-57551  Email: Robert.swisher@noaa.gov</p> <p>I certify that the PII/BI processed in this system is necessary and this PIA ensures compliance with DOC policy to protect privacy.</p> <p>Signature: <u>SWISHER.DONALD.ROBERT.1</u>  <small>Digitally signed by SWISHER.DONALD.ROBERT.1376511460 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=SWISHER.DONALD.ROBERT.1376511460 Date: 2015.08.24 13:49:28 -0400</small></p> <p>Date signed: <u>376511460</u></p>	<p><b>DOC Chief Privacy Officer</b>  Name: Catrina Purvis  Office: Office of Privacy and Open Government  Phone: 202-482-1190  Email: CPurvis@doc.gov</p> <p>I certify that I have reviewed this PIA for compliance with DOC policy to protect privacy and authorize for this PIA to be published on DOC websites.</p> <p>Signature:   Date signed: <u>8/25/2015</u></p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.