

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



**Privacy Impact Assessment
for the
National Water Center
NOAA8202**

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

for Dr. Katrina D. Purvis [Signature]
Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

09/26/2019
Date

U.S. Department of Commerce Privacy Impact Assessment NOAA/National Water Center

Unique Project Identifier: 006-48-01-12-02-3115-00

Introduction: System Description

The National Water Center (NWC) is a general support system consisting of a suite of hydrologic activities, including production and operations, research and development and general administrative functions. The system is physically located in the following four distinct locations: National Weather Service (NWS) Headquarters, Silver Spring, MD; National Water Center (NWC), Tuscaloosa, AL; National Operational Hydrologic Remote Sensing Center (NOHRSC), Chanhassen, MN; and the Cold Regions Research and Engineering Laboratory (CRREL), an Army Corps of Engineers facility in Hanover, NH. The facility at Hanover is a designated backup facility to Chanhassen.

Production and operations consists of products and services from modeling programs and data acquisition, processing, and dissemination programs. There is a logical separation between the production and operations capability and other non-production capabilities.

Research and development consists of applications for field offices that involve applied research and software engineering in support of applications within the NWS.

Business administration includes office functions such as procurement, property inventory, time and attendance using the DOC Web T&A, and other functions needed to carry on the daily business of an office.

The NWC collects and maintains Personally Identifiable Information (PII) for the following administrative support purposes:

- For emergency notifications: name, email address, home telephone number, home email address, and spouse's cell phone number.
- For establishing IT system user accounts: name, office, government phone number, address and email address.
- Surveillance cameras at entry points are for additional security and images are stored on a server in our system. Such images could be used for criminal law enforcement, if applicable.

Card readers installed and maintained at the Tuscaloosa location by the University of Alabama, through a service level agreement between OWP and the university. The only information obtained by the card readers is badge number and name.

An individual may access information or products from our websites; <http://www.nohrsc.noaa.gov/> and <https://hdsc.nws.noaa.gov/hdsc/pfds/>. These websites contain weather-related data (rainfall/snowfall amounts, temperature, etc.) No PII is collected.

Information sharing: The University of Alabama maintains the database of names and badge numbers. The database is located at the University of Alabama, Campus Security Office. Only Campus Security Office employees who have been given permission monitor the database. The university also distributes action cards for staff and faculty. The application requests SSNs and DOBs on the application form; once the card is complete, SSN and DOB information is shredded. This collection is by the university, not performed by NOAA, and is not stored within the boundaries of NOAA8202, and the temporary collection is only in paper form.

The card readers are for access only. Not all employees in the NWC monitor cameras and/or have access to the video surveillance recordings, and access to the stored video images is restricted to those NWS employees who require the ability to retrieve the images on a case-by-case basis for law enforcement purposes.

Contractor roles: Contractors work in IT and as researchers, such as hydrologists and climate scientists along with software developers. Those in IT have elevated privileges to the extent required to do their jobs.

The legal authority for the information collection addressed in this PIA is: 5 U.S.C. § 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records. Additional authorities: 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

This is a moderate impact 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): Emergency contact list for supervisors was created on Google Drive.					

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.

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.

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	
b. Taxpayer ID		f. Driver's License	
c. Employer ID		g. Passport	
d. Employee ID		h. Alien Registration	
		i. Credit Card	
		j. Financial Account	
		k. Financial Transaction	
		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	
b. Maiden Name		h. Place of Birth	
c. Alias		i. Home Address	X
d. Gender		j. Telephone Number	X
e. Age		k. Email Address	X
f. Race/Ethnicity		l. Education	
		m. Religion	
		n. Financial Information	
		o. Medical Information	
		p. Military Service	
		q. Physical Characteristics	
		r. Mother's Maiden Name	
s. Other general personal data (specify): Spouses' cell phone numbers			

Work-Related Data (WRD)			
a. Occupation		d. Telephone Number	X
b. Job Title	X	e. Email Address	X
c. Work Address	X	f. Business Associates	
g. Salary			
h. Work History			
i. Other work-related data (specify):			

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

*May be extracted by surveillance video

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

Other Information (specify)
The GPD information collected is on Google drive, and although not part of the NOAA8202 boundary, the information could be downloaded to individual computers with OWP.

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	<input checked="" type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input checked="" type="checkbox"/>
Other (specify):			

Government Sources			
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>
Other (specify):			

Non-government Sources			
Public Organizations	<input checked="" type="checkbox"/>	Private Sector	<input type="checkbox"/>
Third Party Website or Application	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Other (specify):			

*University of Alabama

2.3 Describe how the accuracy of the information in the system is ensured.

Users verify emergency contact information yearly or if changes should occur. Forms for cards are verified or completed by user.

2.4 Is the information covered by the Paperwork Reduction Act?

<input type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
<input checked="" type="checkbox"/>	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): Card readers for CAC and University of Alabama PIV cards and video surveillance camera both externally and internally throughout the National Water Center building.			

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	X
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

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	
For litigation		For criminal law enforcement activities	X
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Increase security at the National Water Center building in Tuscaloosa, AL.			

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).

*For emergency notifications: name, email address, home telephone number, home email address, and spouse's cell phone number.

*For establishing IT system user accounts name, office, government phone number, address and email address.

*Surveillance cameras at entry points are for additional security and images are stored on a server in our system. Images may be used for criminal law enforcement, if warranted.

*Card readers are installed and maintained at the Tuscaloosa location by the University of Alabama. The information obtained by the card readers is badge number and name (federal employees and contractors).

* An individual may access information or products from our websites:

<http://www.nohrsc.noaa.gov/> and <https://hdsc.nws.noaa.gov/hdsc/pfds/>. These websites contain weather-related data (rainfall/snowfall amounts, temperature, etc.) No information is collected.

- 5.2 Describe any potential threats to privacy 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.)

Any potential threats to privacy lie within the organization. Originally, each manager maintained the emergency list for his or her staff. Now, senior management has decided a spreadsheet on Google Drive would be more advantageous since each user can update as needed. Now, all staff have rights to see everyone's personal information. This includes all staff, federal and contractor.

Emergency contact data (1) will not include sensitive PII, and (2) is outside of the accreditation boundaries of NOAA8202, but rather would fall within NOAA1200.

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

* Law enforcement if applicable, from surveillance camera images (DOJ) (administrative support)

**University of Alabama

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 are notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

X	Yes, notice provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	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:	
X	Yes, notice provided by other means.	Specify how: Employees provide information through their supervisor for account setup. Emergency contact information provided by the employee. Employees provide info on application for University of Alabama PIV card. Employees instructed access to Tuscaloosa location by PIV or CAC only. Multiple signs around the Tuscaloosa building state, "NOTICE. Monitored by video camera".
	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: New employees informed in writing by their supervisor or contract lead that they may decline, in writing, to provide their PII, but in doing so may affect their employment status. For emergency contact information, that is strictly voluntary, but you need to be able to provide some kind of contact information.
---	---	--

	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: Supervisors explain the information for the account setup is necessary to accomplish unit mission. Supervisors explain the information for the emergency contact is strictly voluntary. Employees sign a written consent form for the PIV card.
	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: Annual request to update your contact information sent out to all employees. Video surveillance cannot be altered and is N/A.
	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.)*

	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. (With the exception of emergency contact information).
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only system administrators maintain employee user accounts. Only certain University of Alabama Security Office employees maintain the database of PIV cardholders for access only, and only for surveillance monitoring.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>8/30/2018</u> <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 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 supporting 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.
	Contracts with customers establish ownership rights over data including PII/BII.
	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).

The system administrators maintain employee user accounts. Password strings encrypted and the files readable by user root only.

The University of Alabama maintains the database of names and badge numbers. The database is located at the University of Alabama, Campus Security Office. Only Campus Security Office employees given permission can monitor the database. The University also collects and temporarily stores SSNs and DOBs from the employees.

The card readers are for access only. NWS employees at the National Water Center, Tuscaloosa, AL, only, monitor the surveillance cameras.

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, number, and link. (list all that apply): COMMERCE/DEPARTMENT-18, Employees Information not covered by notices of other agencies; COMMERCE/DEPARTMENT-25, Access Control and Identity Management System;
	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: NOAA Records Schedule Chapter 100-24, Information Technology Operations and Management Records Chapter 1301-20, Customer Inquiries
	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 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.)*

X	Identifiability	Provide explanation: It would not be easy to identify individuals from the PII available, unless images extracted from the surveillance cameras.
X	Quantity of PII	Provide explanation: There is little PII other than images that could be extracted from the

		surveillance cameras.
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields.
X	Context of Use	Provide explanation: To create accounts for employees, we need their name, office phone and location in the building. The University of Alabama maintains the database of employee and contractor names and badge numbers. The database is located at the University of Alabama, Campus Security Office. Only Campus Security Office employees given permission can monitor the database. The card readers are for access only. NWS employees at the National Water Center, Tuscaloosa, AL, only, monitor the surveillance cameras.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Only system administrators have access to system information.
	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.)

Any potential threats to privacy lie within the organization. Originally, each manager maintained the emergency list for his or her staff. Now, senior management has decided a spreadsheet on Google Drive would be more advantageous since each user can update as needed. Now, all staff have rights to see everyone's personal information. This includes all staff, federal and contractor.
Emergency contact data (1) will not include sensitive PII, and (2) is outside of the accreditation boundaries of NOAA8202, but rather would fall within NOAA1200.

- 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.