Version Number: 01-2015

U.S. Department of Commerce
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

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: 2017.07.31 15:02:45 -04'00'

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

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 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 designated as a 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 of office equipment, property inventory, time and attendance using the DOC Web T&A, and other functions needed to carry on the daily business of an office, none of them involving collection, storage or distribution of PII or BII.

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

1. For continuity of operations calling trees: name, job title, government phone number, address, and email address; home telephone number and home email address.
2. For establishing IT system user accounts: name, office, government phone number, address, and email address.
3. 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 are installed and maintained at the Tuscaloosa location by the University of Alabama through a service level agreement with them.
The only information that is obtained by the card readers is badge number and name.

An individual may access information or products from our website; http://www.nohrsc.noaa.gov/. This website contains weather-related data (rainfall/snowfall amounts, temperature, etc.). No information 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 can monitor the database. The

university also collects SSNs and DOBs on the badging application form, and they are then deleted once the badges are made. This collection is by the University, is not performed by NOAA, and is not stored within the boundaries of NOAA8202.

The card readers are for access only. Not all NWS 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):					

___X_ This is an existing system with no changes that create new privacy risks.

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):					

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	X*	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):					

*May be extracted from video surveillance

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

Other Information (specify)
GPD is collected for NWC personnel only for emergency purposes.

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		Online	
Telephone		Email	X		
Other (specify):					

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

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

*University of Alabama

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 (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	x
Other (specify): Card readers for CAC and University of Alabama PIV cards and video surveillance camera in 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			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X

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): Increased 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).

The NWC collects and maintains PII for the following administrative support purposes:

1. For continuity of operations calling trees: name, job title, government phone number, address, and email address; home telephone number and home email address.
2. For establishing IT system user accounts: name, office, government phone number, address, and email address (federal employees and contractors).
3. 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 are installed and maintained at the Tuscaloosa location by the University of Alabama through a service level agreement with them. The only information that is obtained by the card readers is badge number and name (federal employees and contractors). Employees also sign a consent form that they will share their names, SSNs and DOBs with the university badging office.
4. An individual may access information or products from our website; http://www.nohrsc.noaa.gov/. This website contains weather-related data (rainfall/snowfall amounts, temperature, etc.). No information is collected.

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 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.	
	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 is provided by other means.	Specify how: Through the account set-up process, employees are asked to provide info for their account set-up, or the supervisor

		provides it to the system administrator, cc'ing the employee. This is done through a Samanage ticketing application. Notice of the COOP information collection is given when the information is requested by the supervisor in writing. The supervisor will also inform the employee by email that he/she must complete a form for submission to the University of Alabama for badging, to allow them routine access to the building. The employee also signs a consent form stating that he will provide this information to the university badging office. It is explained by the supervisor the employee or contractor does not have a badge, he/she will not be able to enter the building. . There is a sign saying: "NOTICE. Monitored by video camera" for video surveillance, which employees and contractors see upon approaching any of the building entrances.
	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: Employees: Federal employees are informed in writing by their supervisors that they may decline, in writing, to provide their PII, but that the information is required for continuity of operations, account set-up, card readers and video surveillance, and thus refusal may affect their employment status. For badge set-up, there is a written consent form for new employees, also in process retroactively for current employees.
	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: Employees: Each time information is requested, an individual may consent to provide all or part of the information, in writing, as explained by the supervisor. The supervisor's explanation includes the information that all of the specific uses (COOP, user account set-up, video surveillance and badging) are required for the execution of the unit's mission, and thus, the employee's employment may be affected if the PII is not given. For badge set-up, there is a written consent form for new employees, also in process retroactively for current employees. Provided with clear notice that individuals will be monitored by camera, individuals may decline consent to video surveillance by not entering the building. However, this will affect their employment. Individuals do not have the opportunity to consent for law enforcement purposes.
	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: The supervisor sends an annual request to employees to update their PII. The updates will be used for COOP, account management, and badge management.

x	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For video surveillance, updating is not applicable.

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.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only managers have access to their employees' contact information in case of emergency. The system administrators maintain employee user accounts. 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 can monitor the database. The card readers are for access only. NWS employees, only, monitor the surveillance cameras.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): September 29, 2016. ☐ 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.
	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.

1. Only managers have access to their employees' contact information in case of emergency. The system administrators maintain employee user accounts. Password strings are encrypted and the files are readable by user root only.
2. 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 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 and number *(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, 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: 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 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.)

X	Identifiability	Provide explanation: It would not be easy to identify individuals from the PII available, unless images were deliberately 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: In order to create accounts on our system 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 who have been 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 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: A written consent form for sharing the employee's name, SSN and DOB with the University security office has been instituted.
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.