Version Number: 01-2021

U.S. Department of Commerce
National Oceanic & Atmospheric Administration

Privacy Impact Assessment
for the
NOAA8202
Office of Water Prediction (OWP)

Reviewed by: Mark H. 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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2024.10.15 17:58:17 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment

NOAA/NWS/OWP

Unique Project Identifier: NOAA8202

<u>Introduction</u>: System Description

The Office of Water Prediction (OWP) (NOAA8202), is comprised of hydrologic capabilities that include a production and operations capability, a research and development capability, and a capability that houses general administrative functions. The production and operations capability consist of products and services from modeling programs and data acquisition, processing, and dissemination programs. There is logical separation between the production and operations capability and other non-production capabilities. The research and development capability consist of applications for field offices that involve applied research and software engineering in support of applications within the National Weather Service (NWS).

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

NOAA8202 is a general support system.

(b) System location

1) Chanhassen, MN
2) Tuscaloosa, AL

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

1. Level3 Networx for WIFI Guest Network
   a. Guest Network which is an air gapped network from internal data.
2. NOAA0550 - NOAA NWave Wide Area Network (WAN)
   a. Transport only
3. NOAA0100 – NOAA Cyber Security Center
   a. Security stack tool and corresponding data from Trellix HX, Tenable and NBFS (HCL BigFix) is being stored in each platform.

* Interconnections Cold Regions Research Engineering Laboratory (CRREL), NOAA8860, NOAA8501 were removed from the FY’23 PIA as these are no longer required for the business needs of NOAA8202. There will be no systems added to replace these removed interconnections and no additional privacy risks will be introduced.

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

NOAA8202 OWP operates in the traditional client server model. Data is hosted on servers and made available via various protocols such as Hypertext Transfer Protocol Secure (HTTPS), File Transfer Protocol (FTP), Network File System (NFS), Secure File Transfer Protocol (SFTP) and Secure Shell (SSH).

(e) How information in the system is retrieved by the user

An individual may access information or products from our websites; https://www.nohrsc.noaa.gov and https://hdsc.nws.noaa.gov/hdsc/pfds/. These websites contain public weather-related data (rainfall/snowfall amounts, temperatures, etc.). NOAA8202 employees and contractors have direct internal access from government furnished and operated device via NOAA virtual private network or NOAA8202 site(s) networking connections to the information systems assets and applications.

(f) How information is transmitted to and from the system

HTTPS is the only protocol used. Because it is a secure protocol allowing the protection of the data being transmitted.

(g) Any information sharing

The NWS collects and maintains personally identifiable information (PII) for the following administrative purposes:

- Emergency notifications: Name, email, address, home telephone number, home email address. This data is only for NOAA employee's only.
- NOAA employee and contractor IT system user account set up: 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. This data could be of federal employees, contractors, or the public.
- Facility access: Card readers are 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.

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

Type of Information Collected	Applicable SORNS	Programmatic Authorities
Building Entry/Access & Surveillance Log Data	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
System Administration/Audit Data (SAAD)	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
		Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		28 U.S.C. 533-535
Emergency Preparedness/COOP	COMMERCE/DEPT-18	Executive Order 12656
		Federal Preparedness Circular (FPC) 65, July 26, 1999
Managing Access Accounts and Login Names	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
		Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		28 U.S.C. 533-535

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

NOAA8202 is a Moderate FIPS-199 security impact.

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.

_X__ 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) Two interconnections were removed (Cold Regions Research Engineering Laboratory (CRREL) which was decommissioned and NOAA8860, Weather & Climate Computing Infrastructure Services (WCCIS)). The references to business administration capabilities was removed as that is no longer performed within this system. The reference to emergency contact information for spouses was removed as that is not collected. Only emergency contact information of federal staff and contractors is collected.					

____ 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.

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. Marital Status	
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	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify): Employee badge information (at card reader)					

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	X	i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): Photographs may be extracted by surveillance video if requested by law enforcement.					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	f. 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		Online	X
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	X	Commercial Data Brokers	
Third Party Website or Application					
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. NOAA8202 visually verifies two forms of identification from the account requestor, but this information is not replicated or stored within the NOAA8202 system, just verified before any account creation.

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.

<u>Section 3</u>: 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	
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): To 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).

Emergency notifications: Name, email, address, home telephone number, home email address. This data is only for NOAA employee's only.

IT system user account set up: Name, office, government phone number, address and email address. (federal employees and contractors).

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. Images could be of federal employees, contractors, or the public.

Facility access: 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: https://www.nohrsc.noaa.gov/ and https://hdsc.nws.noaa.gov/hdsc/pfds/. These websites contain weather-related data (rainfall/snowfall amounts, temperature, etc.).

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.)

Any potential threats to privacy lie within the organization. Mandatory NOAA cyber training is provided to all end users of NOAA8202's systems regarding the proper handling of sensitive information. This information is retained in accordance with the retention schedule. There is also the possibility of insider threat. However, users are required to take IT security & privacy training annually in order to minimize such risks.

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

* NOAA8202 uses NOAA mandated security agents and devices to transfer data (logs and events) to NOAA0100 (Security Operations Center). See 6.3 for further explanation.

** University of Alabama

*** Only Emergency contact information of the NOAA employed contractor or federal personnel.

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

*surveillance images may be shared with the University of Alabama and external law enforcement agencies for security purposes.

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: NOAA0100: NOAA8202 deploys mandated agents and systems within its information system (IS) boundary from NOAA0100. These systems and agents help protect the IS from cyber threats. Any PII that would by sent from NOAA8202 to NOAA0100 is protected by encrypted channels, communication protections. Any PII residing within the NOAA0100 system or agent is Systems protected by configuration management (DISA STIGs), access controls (least privilege, Role Based Access), system protections (Firewall, Multi Factor Authentication) and System and information Integrity controls (Malicious Code Protection, Monitoring, Flaw Remediation and Software, Firmware Integrity).
	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): Academia and other federal, state, and local emergency managers. This class of users do not have access to PII/BII on the system.			

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: Policy: https://www.weather.gov/privacy .

X	Yes, notice is provided by other means.	Specify how: When emergency contact information is created or updated by the employee on google drive and any changes are notified to the document group that the documented has been updated. For emergency contact information NOAA employees provide an alternate non-government number for recall and emergency situations. This contact is for the NOAA employee only. Screenshot of the privacy act statement is attached below. 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 are informed in writing by their supervisor or contract lead that they may decline, in writing, to provide the PII, but in doing so may affect their employment status.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: NOAA8202 employees may not decline to have their video graphic image captured by deciding not to enter the surveillance area as this a requirement for employment.

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 have the opportunity to consent to particular uses of this PII/BII. Supervisors explain the information is only used for the account setup in order to accomplish unit mission. Employees have the opportunity to consent to particular uses of their emergency contact information. Employees consent to the use of their PII for a Personal Identity Verification (PIV) card by signing a written consent form and receiving a PIV card. Individuals consent to their PII being captured on video surveillance by continuing to access the surveillance area.
	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 each individual's contact information sent out to all employees.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Video surveillance cannot be altered.

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:** NOAA8202 system administrators maintain employee user accounts. Only authorized University of Alabama Security Office employees maintain the database of PIV cardholders for access to University controlled areas. NOAA8202 surveillance monitoring, tracking and recording are done by NOAA8202 assigned users and assets within a controlled area.
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): 5/03/2024 ☐ 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.
	Contracts with customers establish DOC 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 are encrypted and the files readable by system and administrative accounts only. The University of Alabama maintains the database of names and badge numbers. Only Campus Security Office employees with permissions 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. Any emergency contacts information is protected within Google Drive via Access Control Lists.

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)*: 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	X
Degaussing		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.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	**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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: It would not be easy to identify individuals from the PII available, unless images are 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 with permissions can monitor the database. The card readers are for facility access only. NWS employees at the National Water Center, Tuscaloosa, AL, only monitor the surveillance cameras.
X	Obligation to Protect Confidentiality	Provide explanation: Using ACLs within Google Drive to protect emergency contact list.
X	Access to and Location of PII	Provide explanation: Only system administrators have access to system information.
	Other:	Provide explanation:

<u>Section 12</u>: 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 divisional spreadsheet on Google Drive is more advantageous since each user can update as needed. Now, all staff within a OWP Division has the rights to see everyone's personal information within that division only. 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. But, NOAA8202 does internally use access control lists (ACLs) to limit access within OWP at a minimum at the divisional level, but can be restricted even further to a team or individual level if required.

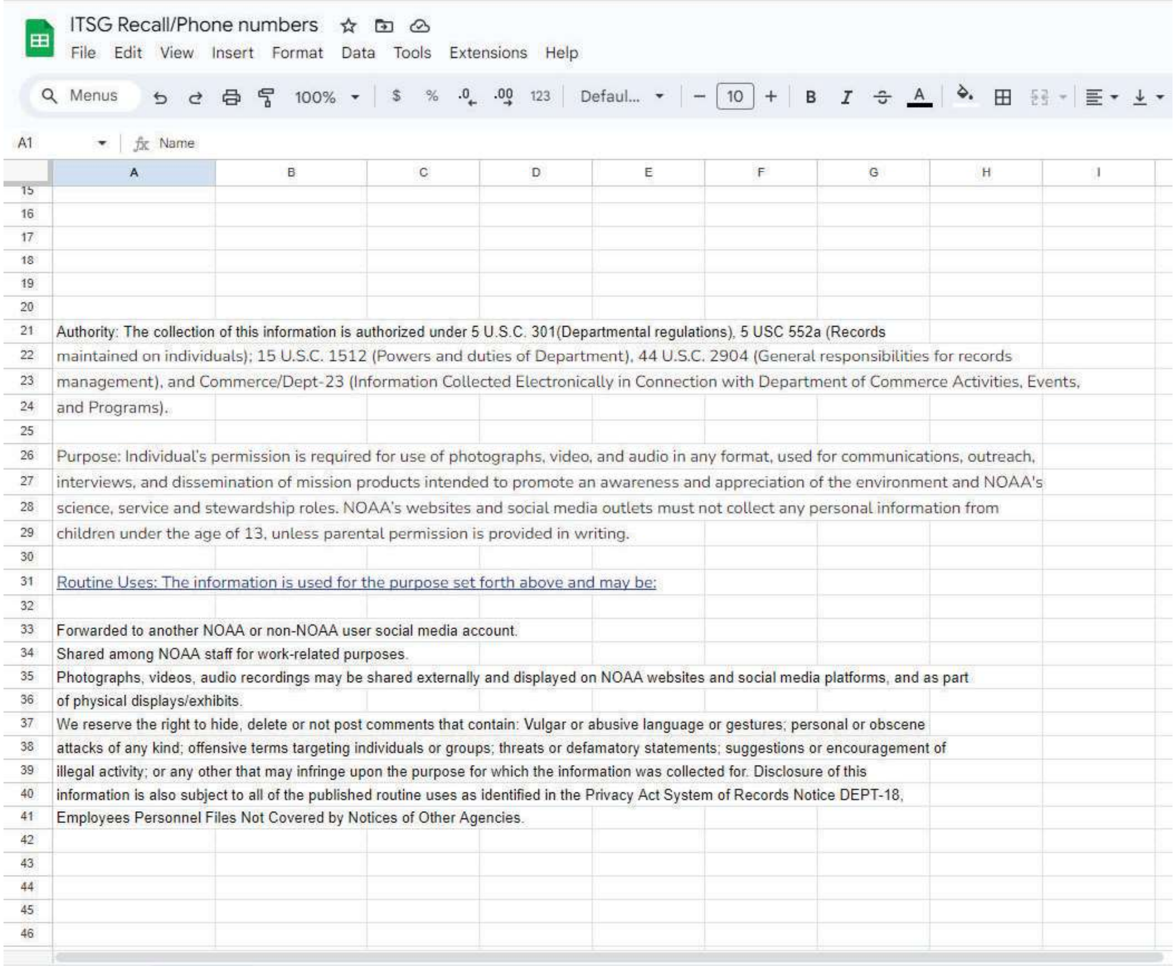
12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	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.

Privacy Act Statement for Emergency Contact List.



Authority: The collection of this information is authorized under 5 U.S.C. 301(Departmental regulations), 5 USC 552a (Records maintained on individuals); 15 U.S.C. 1512 (Powers and duties of Department), 44 U.S.C. 2904 (General responsibilities for records management), and Commerce/Dept-23 (Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs).

Purpose: Individual's permission is required for use of photographs, video, and audio in any format, used for communications, outreach, interviews, and dissemination of mission products intended to promote an awareness and appreciation of the environment and NOAA's science, service and stewardship roles. NOAA's websites and social media outlets must not collect any personal information from children under the age of 13, unless parental permission is provided in writing.

Routine Uses: The information is used for the purpose set forth above and may be:

Forwarded to another NOAA or non-NOAA user social media account.
Shared among NOAA staff for work-related purposes.
Photographs, videos, audio recordings may be shared externally and displayed on NOAA websites and social media platforms, and as part of physical displays/exhibits.
We reserve the right to hide, delete or not post comments that contain: Vulgar or abusive language or gestures; personal or obscene attacks of any kind; offensive terms targeting individuals or groups; threats or defamatory statements; suggestions or encouragement of illegal activity; or any other that may infringe upon the purpose for which the information was collected for. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies.