Version Number: 01-2021

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

Privacy Impact Assessment
for the
NOAA8877
Radar Operations Center Local Area Network (ROC LAN)

Reviewed by: Robin Burress for 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

Robin.Burress Digitally signed on 2025.12.01 15:16:00 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NWS/ROC LAN

Unique Project Identifier: NOAA8877

Introduction: System Description

Provide a brief description of the information system.

The National Weather Service (NWS) Radar Operations Center (ROC), NOAA8877, is a division of NWS Observations (OBS), and consists of a local area network (LAN) for business functions. The ROC is a tri-agency funded and staffed organization, Department of Commerce (DOC), Department of Defense (DOD), and Department of Transportation (DOT) and the ROC provides oversight to keeping operational approximately 160 weather radars in the U.S. and several overseas DOD locations. The ROC's primary mission is to keep the nation's weather radar systems operational. The ROC also performs systematic and coordinated analyses of the day-to-day operations and maintenance of radar systems to determine need for improvements, and for providing both immediate and long-term support during the life cycle.

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

NOAA8877 is a General Support System (GSS)

(b) System location

Norman, OK

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

Interconnections:

- NOAA8104 NEXRAD, a moderate impact mission system used for weather radar and with a type accreditation. The interconnection is local to a single NOAA8104 test and development system environment in Norman, OK. The NOAA8104 test environments and NOAA8877 are within the same facilities. There are no interconnections to fielded, operational systems.
- NOAA0550 N-WAVE, a high impact system that provides wide area network routing and is a NOAA Trusted Internet Connection Access Point provider.
- University of Oklahoma provides fiber plant for data transport between the main ROC buildings located at Max Westheimer Airport and a ROC branch located at the National Weather Center (NWC) facility. This one branch is located at NWC for collaboration with other NOAA weather radar federal partners. No data is shared with OU via this fiber plant, and there is no direct system or data access by OU. ROC owns and maintains the end to end fiber electronics.

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

The ROC prepares annual performance data for DOC and DOD employees in shared folders maintained on the ROC LAN by a DOC administrative person. Managers may restrict access, as they deem necessary. The ROC deals occasionally with foreign national visitors, and the POC for that duty at the ROC uses the ROC LAN to follow procedures\policies established by NOAA to support the administrative electronic paperwork for these visits.

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

Users are identified and authenticated using NOAA issued Common Access Card (CAC) and only with ROC Government Furnished Equipment (GFE) computers. Their CACs and respective Personal Identification Number (PIN) are required to access the employee's Windows Domain account.

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

Information transmitted to and from the system is via the NOAA 0550 N-Wave\TICAP system. If a data transmission involves a privacy consideration, a ROC employee would use the DOC provided secure file transmission system. ROC employee personnel recommend the DOC secure file transfer method as standard practice to receive sensitive data into the system.

(g) Any information sharing

The system only shares DOC (NOAA employees only) and DOD civilian personnel data to the extent necessary for preparation of cyclic performance, promotion, and awards for these personnel. The ROC LAN contains shared folders designated as PII secured and with restrictions per branch chief and/or team lead direction for this type of data. DOC electronic personnel related forms (NOAA employees only) may be transferred to DOC Bureau HR personnel in bulk or on a case-by-case basis via DOC's secure file transfer system (for DOC records only) or via tracked United Parcel Service (UPS) package. NOAA8877 is not a data dissemination system.

The system collects information necessary to sponsor a foreign national visitor (FNV). The NOAA Office of the Chief Administrative Officer (OCAO) coordinates or provides oversight for these visits. The information collected includes the foreign visitor's name, date of birth, city and country of birth, and passport number. This information is stored locally, only if required by the FNV program, in PII Secured folders for the local FNV program POC. FNVs who have "Green Cards" are not required to submit this data. The information on FNVs is necessary per DOC policy to sponsor visitors to the ROC from foreign countries. The information on FNVs is required for obtaining approval from the Bureau Western Region Security Office (WRSO) in Seattle, Washington to ensure that the FNV has authorization to enter the United States. FNV information is neither disseminated nor shared.

Any person that gives feedback to the ROC website and wishes a response must provide their name and email address. This is voluntary information and only required if a response to their feedback is requested.

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

	Type of Information Collected (Introduction h.)	**Applicable SORNs (Section 9.2)**	**Programmatic Authorities (Introduction h.)**
1.	**Personnel Actions Including Training**	COMMERCE/DEPT-18	44 U.S.C. 3101
			Executive Orders 12107, 13164,
			41 U.S.C. 433(d)
			5 U.S.C. 5379
			5 CFR Part 537
			Executive Order 12564
			Public Law 100-71
			Executive Order 11246
			26 U.S.C. 3402
2.	**Contact Information for the Public**	NOAA-11	5 U.S.C. 301, Departmental Regulations
			15 U.S.C. 1512, Powers and duties of Department
3.	**Foreign National Information**	COMMERCE/DEPT-27	28 U.S.C. 533-535
		COMMERCE/DEPT-9	44 U.S.C. 3101
			5 U.S.C. 301
			Executive Orders 13526, 12968, 13356, 13587
			Public Law 108-458 (Intelligence Reform and Terrorism Prevention Act of 2004)
			Intelligence Authorization Act for FY 2010, Public Law 111-259
			31 U.S.C. 951-953
			8 U.S.C. 1324a
			15 Code of Federal Regulations (CFR) Parts 730-774, Export Administration Regulations
			NOAA Administrative Order (NAO) 207-12 "Technolog Controls and Foreign National Access"
			Department Administrative Order (DAO) 207-12 Versio Number: 01-2017 "Foreign National Visitor and Guest Access Program
4.	**Managing Access Accounts and Login Names**	COMMERCE/DEPT-25	5 U.S.C. 301
			Homeland Security Presidential Directive 12, Policy for 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

NOAA8877 ROC LAN 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):					

____ 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	√	h. Date of Birth	√	o. Financial Information	
b. Maiden Name		i. Place of Birth	√	p. Medical Information	

c. Alias		j. Home Address	√	q. Military Service	
d. Gender	√	k. Telephone Number	√	r. Criminal Record	
e. Age	√	l. Email Address	√	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	√	i. Business Associates	
b. Job Title	√	f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information	√		
l. Other work-related data (specify):					

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

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

Other Information (specify)
FNV uses IN item g. and GPD items a., d., e. and h. – l. Website feedback uses GPD a. and l. Cyclic personnel data uses GPD item a. and WRD items a., b. and h.

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	√	Hard Copy: Mail/Fax		Online	√
Telephone		Email	√		
Other (specify):					

Government Sources					
Within the Bureau	√	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign*	√		

Government Sources
Other (specify): *FNVs are typically foreign government representatives.

Non-government Sources					
Public Organizations		Private Sector	* √	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): * This is not a new collection, simply overlooked in previous documents. Selecting to accurately reflect from whom information is collected.					

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

It is the responsibility of the employee to assess the data that is collected and verify the accuracy with the receiving system personnel processing the data in the case of cyclic personnel related data. NOAA8877 does not provide strict file integrity monitoring and is not a long-term repository for HR related data. FNV data is not shared and accuracy of the permanent records is the expected responsibility of the DOC FNV program. Website feedback data is voluntary and provided by the person asking the question. NOAA8877 does not provide a method to verify the accuracy of the person's name or email address. If the email address provided was invalid and the person requested email feedback, they will not receive the feedback they requested.

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.
√	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):			

√	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	

Activities
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	√	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	√
For web measurement and customization technologies (single-session)	√	For web measurement and customization technologies (multi-session)	
Other (specify): For cyclic DOC and DOC federal performance/awards, FNVs, and web feedback.			

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 DOC and DOD each have HR portals for direct input of electronic personnel data for federal employees. In some isolated situations, forms may need to be completed locally and transferred into the portal in bulk for the affected personnel. If the portals cannot be used and the data has to be sent electronically, then the DOC secure file transfer (for NOAA records only) or via tracked United Parcel Service (UPS) package. No sharing of personnel performance and award data beyond those that are required to process it within the respective HR portals.

The information on FNVs is required for obtaining approval from the Western Region Security Office (WRSO) in Seattle, Washington to ensure that the FNV has authorization to enter the United States. No further sharing of this information occurs.

Collection of a name and email is optional from anyone who makes a web query about the NEXRAD system on the ROC website feedback form. The information is necessary in instances where the person asks for a response. No further sharing of this information occurs.

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.)

DOC and NOAA provide and mandate training related to Security Awareness and Insider Threat as a common control. In addition, NOAA8877 users are required to complete annual Security Awareness Training, which includes sensitive file handling procedures pertinent to the local environment. System wipe, disk drive/media removal, and shredding are pre-cautionary steps for all NOAA8877 assets in preparation for their final disposal. This includes shared drives, backup systems, network printers, and PCs. Shredding of disks and media (including the iron keys) occurs at the end of the NOAA8877 useful life for all assets.

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	√	√	
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.

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

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

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

√	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: NOAA8877 connects with NOAA8104 (NEXRAD), NOAA0550 (NWAVE), and the University of OK. DOC Enterprise Connect web portal. NOAA8877 uploads data in specified formats to DOC Enterprise Connect. Data segregation and restricted access occurs locally on the ROC LAN in specified LAN data stores. ROC LAN shared stores have media protection controls and user procedures in place to keep the data on the ROC LAN.
	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	√
Contractors	√		
	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.)*

√	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: The ROC webpage provides the following link to the NOAA privacy policy https://www.noaa.gov/protecting-your-privacy.	
√	Yes, notice is provided by other means.	Specify how: a. Written notice is included on all personnel forms that employees complete. Notification occurs to DOC and DOD employees by their supervisors when the cyclic evaluations or awards are in process. Employees have access to view the official documents. b. A FNV receives a privacy act statement, by the U.S. sponsor or the DOC person staffing the DOC International Affairs Office, at the time of his/her appearance at the office, that completion of the information on the FNV and Guest Access request form is required for obtaining authorization for a visit. c. A link to the NOAA privacy policy is provided on the ROC webpage.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

√	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: a. Performance information is part of the official personnel record for DOD and DOC employees and contact with the employee is not required other than performance feedback. The performance record/information is required in order to conduct performance evaluations and awards. b. At the time of appearance at the DOC International Affairs Office, a FNV may verbally decline to provide the information requested of them, either to their U.S. sponsor who completes the form and provides the Privacy Act Statement, or to the DOC personnel staffing the office. However, the Department or any of its bureau can then refuse their visit. c. For web queries with expectation of a response, providing name and email is required. Anonymous feedback to the ROC Webmaster is an option on the website.
	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.

√	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: a. DOC and DOD employees do not opt not to consent to use of personnel data for awards and/or performance. This is the only purpose for this data. b. FNV may, at the time of appearance at the DOC International Affairs Office, verbally decline consent to provide the information requested of them, either to their U.S. sponsor who completes the form and the Privacy Act Statement, or to the DOC personnel staffing the office. However, the sponsoring information is required in the Department or any of its bureaus. c. ROC web queries (requests for data or for access to site-specific radar data): web site has a Privacy Policy statement, which states that provision of the information implies consent to its use.
	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.

√	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: a. DOC and DOC employees have their permanent personnel records in their respective DOD and DOC electronic official personnel folder secured repositories. They may make updates through their respective servicing HR offices. b. FNV may submit requests to review and update their forms and review the Privacy Act Statement to the DOC International

		Affairs Office. c. Web queries: An individual can review a query before sending, but cannot review or update after submitting
	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.
√	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
√	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
√	Access to the PII/BII is restricted to authorized personnel only.
√	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Windows file system auditing monitors, tracks, and records changes to the files containing PII/BII. This does not track content changes.
√	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): 5/31/2025 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
√	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
√	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).
	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
√	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): As stated in the ROC System Security Plan (SSP), all employees and contractors undergo a national agency check with inquiries (NACI) security check as a condition of employment. This involves a check of Federal and local law enforcement records to help ensure the trustworthiness of the employee. The user (internal or external) signs the NOAA8877 Rules of Behavior (ROB) indicating that they have read and understand the ROB. In addition, ROC LAN users review and acknowledge the current NOAA8877 ROB annually and the complete updated NOAA Security Awareness Training (SAT) on the anniversary of their training date. A section of the ROB provides PII\BII definitions; how to store in restricted folders; how to share using DOC secure file transfer; and how to report PII\BII incidents. To protect mobile information, all ROC laptops are fully encrypted using the NOAA enterprise supplied encryption software. NOAA8877 encrypts sensitive data at rest using AES 256 encryption on the volume containing PII and data backups, in compliance with NIST 800-53 Rev 5 SC-28(1) and OMB M-22-09.

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).*

Segregation of data with granularity of control on data shares to the user or group level, as appropriate. Controlled access for servers and data storage areas limited to only ROC LAN system administrators. FIPS encryption for all mobile laptop devices. Rules of Behavior annual supplemental training on where to store PII and how to handle transfers locally and via DOC secure file transfer. Two specific scanner locations for PII that are not network connected and to ensure PII data is not emailed via multi-function scanner/copier. SMB encryption is enabled to protect data in transit from tampering and eavesdropping. NOAA8877 encrypts sensitive data at rest using AES 256 encryption on the volume containing PII and data backups, in compliance with NIST 800-53 Rev 5 SC-28(1) and OMB M-22-09.

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."

√	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: Personnel Actions: COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies. This covers all ROC employees. Contact Information for the Public: NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission. Foreign National Information: COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons COMMERCE/DEPT-27, Investigation and Threat Management Records Managing Access Accounts and Login Names: COMMERCE/DEPT-25, Access Control & 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.)*

√	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Specific Records Schedule: NOAA 203-03 Personnel Records: Supervisor's and Duplicate Documentation NOAA 600-07 Foreign Visitors NOAA 1301-05 Sensors and Equipment Project Case Files NOAA 1301-07 Radar Project Case Files NOAA2300 General Technology Management Records. General Record Schedule GRS-3.2 for information systems related data
	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:
√	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	√	Overwriting	
Degaussing		Deleting	
Other (specify): Asset wipe or set to default.			

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.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

√	Identifiability	Provide explanation: NOAA8877 ROC LAN does not have an aggregation of individual PII data, as would NOAA or DoD personnel systems and DOC financial and travel systems. There are no ROC personnel specific datasets on the ROC LAN that would expose all employees or make all employees easily identifiable. NOAA8877 does not have aggregations of PII on members of the public to support identifiability.
√	Quantity of PII	Provide explanation: NOAA8877 ROC LAN has fewer than 150 users total. Breakdown of ROC personnel is < 42% DOC and < 10% DoD. The impact as a result of loss of employee PII at the ROC is estimated to be minor and is anticipated to have limited adverse effect on continued performance of primary mission function.
√	Data Field Sensitivity	Provide explanation: Examples of the most sensitive situation examples would be foreign government visitor information that is required to be kept by the ROC employee host. Release of employee or foreign visitors names and contact information would not likely cause harm to the individuals.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
√	Access to and Location of PII	Provide explanation: End users do not access data (PII or otherwise) on NOAA8877, except with NOAA secured and encrypted assets approved for the specific purpose. Per rules of behavior, PII is accessed or used for its intended purpose on the system via directly connected nodes, and is not transferred to or transported on NOAA mobile devices. PII is established in designated/protected shared access folders and is made accessible only to those with a need to know.
√	Other:	Provide explanation: All end of life cycle NOAA8877 disks servers, multi-function copier/printers/faxes, and end user desktop/laptop components are wiped (e.g. set to default) and media is shredded per policy and not reused in any manner.

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.)

Threats to privacy would primarily be insider threat, whether malicious or unintended. There have been instances where individuals have sent their own or another person's privacy data via Bureau email instead of secure file transfer. The individuals are counseled and re-trained when this occurs and is reported or was detected.

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:
√	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:
√	No, the conduct of this PIA does not result in any required technology changes.