Version Number: 01-2015

U.S. Department of Commerce
NOAA

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

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 PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.01.24 14:39:58 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA8877 ROC LAN

Unique Project Identifier: 006-48-01-12-3103-00

Introduction: System Description

(a) General Description - NOAA8877 is a moderate impact General Support System (GSS), which provides a small to medium enterprise LAN for the National Oceanic and Atmospheric Administration (NOAA)/National Weather Service (NWS) Radar Operations Center (ROC) and its tri-agency personnel. The ROC's primary mission is to support operations, maintenance, and sustainment of the tri-federal agency (Department of Commerce (DOC), Department of Defense (DOD), and Department of Transportation (DOT)) Next Generation Weather Radar (NEXRAD) weather radar fleet. NOAA8877 provides general office collaboration software and tools together with highly specialized software and hardware systems, which enable ROC's personnel in four branches (Operations, Engineering, Program Support, and Applications) to perform their respective System Development Life Cycle (SDLC) functional roles. Operations Branch runs a 24x7 radar hotline, performs independent testing of modifications and software, and provides on-site technical field support for specialized and particularly difficult radar modifications. Engineering Branch does multi-year planning, project management, development, unit and integration testing, security design, and implementation for all the hardware and software modifications to the radar systems. Program Support Branch provides logistics support, contract maintenance, configuration management, and documentation. Applications Branch leads data quality analysis and improvement initiatives. In addition, this branch leads the scientific groups that make determination on readiness of new science for integration into the radar.

Information in the NOAA8877 ROC LAN general support system primarily consists of programmatic and technical documentation for the NOAA8104 NEXRAD, NOAA8212 Terminal Doppler Weather Radar Supplemental Product Generator (TDWR SPG), and NOAA3065 weather radar data major application programs. If any of the data is sensitive or For Official Use Only (FOUO) programmatic or technical data, then the data is restricted by drives and folders to only ROC personnel authorized to access the information.

(b) Typical Transaction - A typical transaction might be the initiation of a DOC or DOD performance evaluation. The appropriate forms are completed on the ROC team leader's P: drive. It will then be printed, hand-carried for signature, and then transferred as described via UPS. Alternately, the agency-specific secure electronic transfer procedure is followed.

Another transaction example might be the collection of an individual's or other entity's (member of the public, public organization, or private sector) name and email address (work or home, whichever is applicable), who visits the ROC website and voluntarily wishes to have a question answered. In addition, there are work-related secure ROC website databases that store radar system specific data, which may be accessed by tri-agency civilian and military personnel about the radar they are responsible to maintain and/or operate. Further, the field radar maintenance and/or operations personnel may voluntarily provide comments or corrections on technical

documentation. The information is collected only to the extent needed to answer the question(s) posed or to request clarifications, if necessary.

(c) Information Sharing\Transfers - The system collects PII of DOC (NOAA employees only) and DOD civilian and military personnel to the extent necessary for preparation of performance, promotion, and awards for these personnel. The ROC LAN contains personally assigned network shares (P:\), which are accessible only by the person assigned the shared drive. Per ROC directives, DOC and DOD team leaders are required to use only their P: drive to initiate and prepare forms data necessary for awards and performance.

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 Accellion (for DOC records only) or via tracked United Parcel Service (UPS) package.

DOD civilian and military performance and awards data initiated at the ROC is required per Air Force Directive-Instructions (AFIs) 36-2406, 36-2502, and 36-2606 to document the individual job performance. The transfer of the information is then submitted to the appropriate Air Force HR personnel via encrypted email or via UPS tracked package as per the applicable AFI.

In addition, the system collects PII of ROC personnel for purposes of emergency recall and ROC Continuity of Operations Planning (COOP). The emergency recall and COOP data is stored on a LAN shared drive only accessible by authorized personnel and on Federal Information Processing Standards (FIPS) 140-2 encrypted iron keys provided by the ROC LAN Information System Security Officer (ISSO) to the ROC director and branch chiefs for emergency recall.

The system collects information necessary to sponsor foreign visitors. The DOC International Affairs Office 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, if required, on the P: drive only of the Program Branch Chief, who is the sponsor of foreign visitors. Foreign National visitors who have "Green Cards" are not required to submit this data. The information on foreign visitors is necessary to sponsor visitors to the ROC from foreign countries. The information on foreign visitors is required for obtaining approval from the Bureau Western Region Security Office (WRSO) in Seattle, Washington to ensure that the foreign visitor is authorized to enter the United States. This foreign visitor information is not disseminated or shared external to ROC.

(d) Authority - Statutory or regulatory authorities for collection and maintenance of the information include:

- 15 USC 1151(Dissemination of Technological, Scientific, and Engineering Information)
- 15 USC 1512 (Powers and Duties of the Department of Commerce)
- 5 USC 2101 to 10210 (Government Organizations and Employees, Part III, Employees)
- 5 USC 301 (Departmental Regulations)
- 10 USC 8010 to 9448 (Armed Forces - Air Force - Organization, Personnel, and Training)
- DAO 207-12 Foreign Visitor and Guest Access Program

(e) Categorization - 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.

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**	X	e. File/Case ID		i. Credit Card**	x
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
Explanation for the need to collect, maintain, or disseminate the Social Security number and credit card information, including truncated form: * Government only issued travel and purchase cards. ** DOD performance and award forms require the individual's SSN; DOC does not require it.					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	
b. Maiden Name		h. Place of Birth	x	n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender	x	j. Telephone Number	x	p. Military Service	x
e. Age	x	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	x	d. Telephone Number	x	g. Salary	
b. Job Title	x	e. Email Address	x	h. Work History	x
c. Work Address		f. Business Associates	x		
i. Other work-related data (specify):					

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

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. 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		Hard Copy: Mail/Fax	x	Online	
Telephone		Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus	x	Other Federal Agencies	x
State, Local, Tribal		Foreign (visitors)*	x		
Other (specify): * Foreign Visitors are foreign government representatives.					

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

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	
Other (specify):			

x	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	
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	x
For administrative matters	x	To promote information sharing initiatives	x
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 emergency recall and COOP			

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 information collected on DOD military and civilian personnel is used to complete military performance and promotion evaluation forms for Air Force personnel. The performance evaluations are required by Air Force Directive-Instruction (AFI) 36-2406 to document the individual's job performance. The performance or promotion evaluation is completed by the NWS or DOD supervisor, discussed with the military member, and securely emailed to Offutt Air Force Base (AFB) using the Common Access Card (CAC) Public Key Infrastructure (PKI) credentials or alternately via tracked UPS package. Once processed at Offutt, the form is returned to the ROC for final signatures and then emailed securely or hand-carried to Tinker Air Force Base (AFB), which has administrative responsibility for the DOD personnel at the ROC (*outside the ROC LAN boundary*). Tinker AFB electronically files a copy in the individual's personnel file and then sends the form to Randolph AFB for final disposition. Per Air Force direction, all forms are transmitted and signed electronically. This information is not shared with anyone beyond those that are required to process it within the respective agency.

Electronic personnel related forms of NOAA employees only are transferred to NOAA HR in bulk or on a case-by-case basis via DOC Accellion (for NOAA records only) or via tracked United Parcel Service (UPS) package. This information is not shared with anyone beyond those that are required to process it within the respective bureau.

The information on foreign visitors is required for obtaining approval from the Western Region Security Office (WRSO) in Seattle, Washington to ensure that the foreign visitor is authorized to enter the United States. This information is not shared outside of the system, by ROC.

NEXRAD technical documentation and telecommunications information is FOUO. The tri-agency (DoD, FAA, and DOC) maintenance or operations field personnel must request access and be authorized to access site specific data, which is maintained at the ROC. Their identifying information (name, work email, and work telephone number) are used to create an account.

Name and email (work or home, whichever is applicable) contact information is collected on a voluntary basis from anyone who makes a web query about the NEXRAD system on the ROC website feedback form. The information is requested in order to provide a response directly to the requestor or make clarifications, when necessary (members of the public, public organizations, private sector).

ROC collects PII of ROC personnel on a voluntary basis for purposes of emergency recall. Employees may decline. ROC collects PII of ROC personnel assigned by the director to the ROC COOP team for COOP recall purposes. COOP employees must provide their PII recall information to be assigned a COOP team role. The employee recall and employee COOP data is stored on a LAN shared drive only accessible by authorized personnel and on FIPS 140-2 encrypted iron keys provided by the ROC LAN ISSO to the ROC director and branch chiefs for emergency recall.

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	X	X	
Federal agencies	X	X	
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 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: NOAA WMFO Recruitment Analysis Data System (RADS). NOAA8877 uploads data in specified formats to RADS. Locally, data is segregated 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.

6.3 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): DoD Military personnel for DoD Personnel Data.			

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: https://www.roc.noaa.gov/WSR88D/PAStatement_NOAA8877.aspx .	
x	Yes, notice is provided by other means.	Specify how: a. Web Inquiries –Notice is provided by a privacy statement on the Web site. b. Written notice is included on all personnel forms that employees complete. For DOC and DOD performance/award documents, employees are informed by their supervisors that the evaluations are in process. Employees have access to view the official documents. c. For ROC emergency recall and COOP, employees are asked permission in person when collecting the applicable information. All ROC personnel are informed of the intended purpose. d. Notice is provided verbally to a foreign visitor, 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 Foreign National Visitor and Guest Access request form is required for obtaining authorization for a visit.
	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: a. For web queries, providing PII/BII is voluntary to those wishing to receive a response. Feedback only to the ROC Webmaster may be provided anonymously. c. For the emergency recall roster, ROC personnel can inform their supervisor or administrative officer in person or in writing that they decline to provide PII/BII. COOP team employees must provide their recall information. If a COOP team member declines, they would not be able to perform the duties of this function for the ROC, and they would be removed from this

		role. b. For DOD personnel data, employees may opt not to provide PII/BII – at the time of the request, and to the personnel administration representative who is assisting them - but this information is needed for processing awards. Performance information is part of the official personnel record for DOD and DOC employees and can be added without contacting employees. The performance record/information is required in order to conduct performance evaluations. d. Foreign visitors may, at the time of appearance at the DOC International Affairs Office, verbally decline to provide the information requested of them, either to their U.S. sponsor who completes the form, or to the DOC personnel staffing the office. However, refusal to supply the required data will result in being denied access to the Department or any of its bureaus.
	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: a. ROC web queries (requests for data or for access to site specific radar data): a Privacy Policy statement, stating that provision of the information implies consent to its use, is provided on the Web site. b. Employees may opt not to consent to use of PII/BII – at the time of the request to the personnel administration representative who is assisting them - but this information is needed for processing awards. c. For ROC employees' emergency recall and COOP, the information is used for only one the stated emergency recall purpose. d. Foreign visitors 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, or to the DOC personnel staffing the office, but this information is needed for sponsoring them in the Department or any of its bureaus.
	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: a. Web queries: An individual can review a query before sending, but cannot review or update after submitting. b. Personnel records are obtained/reviewed through the respective DOD and DOC electronic official personnel folder secured repositories but updates must be provided to the servicing HR office.

		c. For Emergency and COOP information, the employee may not review the information, because it contains other staff's PII, but may provide updates to the assigned administrative staff. d. Foreign visitors may submit requests to review and update to the DOC International Affairs Office.
	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.
x	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.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): **5/26/2017 with DOC PO approved PIA 5/12/2017.** ☐ 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.
	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.
x	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 when employed or contracted. 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 ROC Rules of Behavior (ROB) indicating that they have read and understand the ROB. In addition, as of September 2015, ROC LAN users review and acknowledge the current ROC ROB annually in concurrence with the release of the NOAA annual IT security awareness training. The Feb 2016 ROB update includes a section for PII definition, storage, sharing, and how to report PII incidents. To protect mobile information, all ROC laptops are fully encrypted using the NOAA enterprise supplied encryption software.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

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 140-2 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 Accellion. Two specific scanner locations for PII that are not network connected and to ensure PII data is not emailed with multi-function scanner/copier.

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)*: For employee information, the applicable SORN is COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies. This covers all ROC employees. NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission. Specifically, the SORN covering the Foreign Visitor/Guest Information: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons--COMMERCE/DEPT-9.
	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 Specific Records Schedule 100-24 IT Operations and Management Records, General Record Schedule GRS-20 for general IT related data, NOAA 302-03 Personnel Actions, NOAA 600-07 Foreign Visitors, NOAA 1301-05 Sensors and Equipment Project Case Files, NOAA 1301-07 Radar Project Case Files
	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		Deleting	
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.

	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 levels. *(Check all that apply.)*

x	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.
x	Quantity of PII	Provide explanation: NOAA8877 ROC LAN has fewer than 160 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.

x	Data Field Sensitivity	Provide explanation: Examples of the most sensitive situation examples would be ROC employee names and phone numbers on an emergency call roster, a list of the few ROC employee names and government purchase card numbers, or 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:
x	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.
x	Other:	Provide explanation: All end of life cycle NOAA8877 disks servers, multi-function copier/printers/faxes, and end user desktop/laptop components are wiped and shredded per policy and not reused in any manner.

Section 12: Analysis

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

x	Yes, the conduct of this PIA results in required business process changes. Explanation: More stringent privacy data related procedures were put in place to address gaps identified in NOAA8877 processes and technologies. Summary of adjustments is given below: • Administrative personnel were trained on use of two local PC/non-networked scanners to control transfer of personnel related PII into ROC LAN for eventual upload to NOAA WMFO or other appropriate HR systems. This avoids problems with PII on paper copies being scanned via multi-function copier, which can only send as email attachments to recipient. • Primary users of PII are administrative personnel, branch chiefs, and team leaders. They occasionally have need to share data in folders with others to continue processing of the paperwork, for submission, and/or for peer review purposes. These folders are designated on the ROC LAN as PII-Secured and locked down to specific users.
	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.

x	Yes, the conduct of this PIA results in required technology changes. Explanation: USB connected scanners were added in two specific building locations to facilitate the transfer of potentially sensitive personnel data (awards, ratings, hiring, etc.) from paper copies to the system for processing in NOAA WMFO systems.
	No, the conduct of this PIA does not result in any required technology changes.