U.S. Department of Commerce
NOAA

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

Reviewed by: ________________________________, Bureau Privacy Officer or Designee

Approved by: ________________________________, DOC Chief Privacy Officer

U.S. Department of Commerce Privacy Impact Assessment

Radar Operations Center (ROC) Local Area Network (LAN) (NOAA8877)

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

Introduction: System 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.

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 Accellion Secure File Transfer (for DOC records only) or tracked by 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 UPS tracked package as per the applicable AFI.

In addition, the system collects PII of ROC personnel on a voluntary basis for purposes of emergency recall and ROC Continuity of Operations Planning (COOP). This 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.

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.

Statutory or regulatory authorities for collection and maintenance of the information are 15 USC 1151, 5 USC 1302, 5 USC 2951, 5 USC 3301, 5 USC 4118, 5 USC 301, and 10 USC 8013.

Section 1: Information in the System

1.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. Check all that apply.

Identifying Numbers (IN)					
a. Social Security*	☒	e. Alien Registration	□	i. Financial Account	□
b. Taxpayer ID	□	f. Driver's License	□	j. Financial Transaction	□
c. Employee ID	□	g. Passport	☒	k. Vehicle Identifier	□
d. File/Case ID	□	h. Credit Card	□	l. Employer ID Number	□
m. Other identifying numbers (specify): *DOD performance and award forms require the individual's SSN; DOC does not require it.					

General Personal Data (GPD)					
a. Name	☒	g. Date of Birth	☒	m. Religion	□
b. Maiden Name	□	h. Place of Birth	☒	n. Financial Information	□
c. Alias	□	i. Home Address	☒	o. Medical Information	□
d. Gender	☒	j. Telephone Number	☒	p. Military Service	☒
e. Age	☒	k. Email Address	☒	q. Physical Characteristics	□
f. Race/Ethnicity	□	l. Education	□	r. Mother's Maiden Name	□
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	d. Telephone Number	☒	g. Salary	□
b. Job Title	☒	e. Email Address	☒	h. Work History	☒
c. Work Address	□	f. Business Associates	☒		
i. Other work-related data (specify): Performance evaluation ratings, rank or grade, duty station					

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)

1.2 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*	☒		
Other (specify): *Foreign visitors are government representative.					

Non-government Sources					
Public Organizations	☒	Public Media, Internet	□	Private Sector	☒
Commercial Data Brokers	□				
Other (specify):					

Section 2: Purpose of the System

2.1 Indicate why the PII/BII in the system is being collected, maintained, or disseminated. Check all that apply.

Purpose			
To determine eligibility	☒	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	□
Other (specify): For emergency recall and COOP	☒		

Section 3: Use of the System

3.1 Provide an explanation of how the bureau will use the PII/BII to accomplish the checked purpose(s), e.g., to verify existing data. Describe why the PII/BII that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and further the mission of the bureau and/or the Department. Indicate if the PII/BII identified in

Section 1.1 of this document is in reference to a federal employee/contractor, member of 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 tracked by 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 Human Resources (HR) in bulk or on a case-by-case basis via Accellion Secure File Transfer (for NOAA records only) or tracked by 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 (members of the public, public organizations, private sector). The information is requested in order to provide a response directly to the requestor or make clarifications, when necessary.

In addition, ROC collects PII of ROC personnel on a voluntary basis for purposes of emergency recall and ROC COOP. This 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 4: Information Sharing

4.1 Indicate with whom the bureau intends to share the PII/BII in the system and how the PII/BII will be shared.

Recipient	How Information will be Shared			
	Case-by-Case	Bulk Transfer	Direct Access	Other (specify)
Within the bureau	☒	☒	□	
DOC bureaus	□	□	□	
Federal agencies	☒	☒	□	
State, local, tribal gov't agencies	□	□	□	
Public	□	□	□	
Private sector	□	□	□	
Foreign governments	□	□	□	
Foreign entities	□	□	□	
Other (specify):	□	□	□	

□	This information will not be shared.

Section 5: Notice and Consent

5.1 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 6.	
☒	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. 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:

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

☒	Yes, individuals have an opportunity to	Specify how:

	decline to provide PII/BII.	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. 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. c. For the emergency recall roster/COOP, ROC personnel can inform their supervisor or administrative officer in person or in writing that they decline to provide PII/BII. 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

5.3 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. 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, employees are asked permission in person before collection to use their home phone number, mobile phone number, and personal email. 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 into 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:

5.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☒	Yes, individuals have an opportunity to	Specify how:

	review/update PII/BII pertaining to them.	a. Web queries: An individual can review a query before sending, but cannot review or update after submitting. b. Personnel records are obtained and reviewed through the respective DOD and DOC electronic Official Personnel Folder secured repositories and updates must be requested from the servicing HR office. c. For Emergency and COOP information, employees may not review the information because it contains other staff member's PII, but they may request for updates to be made to their PII from the assigned administrative staff. d. Foreign visitors may submit requests to review and update their PII through the DOC International Affairs Office.
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 6: Administrative and Technological Controls

6.1 Indicate the administrative and technological controls for the system. Check all that apply.

□	All users signed a confidentiality agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff received training on privacy and confidentiality policies and practices.
☒	Access to PII/BII is restricted to authorized personnel only.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization: 6/5/2014
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST 800-122 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM). See Appendix A.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	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 2014, ROC LAN users review and acknowledge the current ROC ROB annually in concurrence with the release of the NOAA annual IT security awareness training. To protect mobile information, all ROC laptops are fully encrypted using the NOAA enterprise supplied encryption software.

Section 7: Privacy Act

7.1 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."

☒	Yes, this system is covered by an existing system of records notice. Provide the system name and number: 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. For foreign visitor information, the applicable SORNs are: COMMERCE/DEPT-6, Visitor Logs and Permits for Facilities Under Department Control, and COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
□	Yes, a system of records notice has been submitted to the Department for approval on (date).
□	No, a system of records is not being created.

Section 8: Retention of Information

8.1 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 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:
☒	Yes, retention is monitored for compliance to the schedule.
□	No, retention is not monitored for compliance to the schedule. Provide explanation: