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

Privacy Threshold Analysis
for the
NOAA8877
Radar Operations Center Local Area Network (ROC LAN)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NWS/ROC LAN

Unique Project Identifier: NOAA8877 (system ID)

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The National Weather Service (NWS) Radar Operations Center (ROC), NOAA8877 is a division of NWS Observations (OBS), and consist of local area network (LAN) for business functions. The ROC is a tri-agency funded and staffed organization (DOC DOD & DOT) and the ROC provides oversight to keeping operational the 160 weather radars in the U.S. and several overseas DOD locations. ROC's primary mission is to keep the nation's weather radar systems operational. 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 provide 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. ROC owns and maintains the end to end fiber electronics.

d) The purpose that the system is designed to serve

Purpose of NOAA8877 is to serve as small to medium enterprise LAN for the NOAA\NWS ROC and its tri-agency personnel. The ROC's primary mission is to support operations, maintenance, and sustainment of the tri-federal agency (DOC, DOD, and DOT) NEXRAD weather radar fleet.

e) The way the system operates to achieve the purpose

ROC has an emergency recall roster maintained on the LAN shares by a DOC administrative person. This excel spreadsheet has all ROC DOC federal, DOD federal, and DOC contract team members home and/or personal mobile numbers for COOP purposes. ROC prepares annual performance data for DOC and/or DOD employees in the shared folders and managers may restrict access, as they deem necessary. 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.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

NOAA8877 maintains general business information for ROC's mission, which is supporting weather radars. The business data resides on NOAA8877 in common, branch, and personal Windows shares. NOAA8877 is not a data dissemination system. NOAA8877 relies on NOAA0201 for NOAA enterprise email services. Although not interconnected to NOAA0201, information to/from NOAA8877 relies on NOAA0201 for dissemination. Types of information related to privacy would be recall roster, federal personnel performance draft input data, and NOAA's foreign visitor related forms.

g) Identify individuals who have access to information on the system

Common shares are generally accessible by all ROC employees (both federal and contractor). Branch shares are accessible by the employees of the respective branch. Personal shares are accessible by the individual employee. As required, a federal branch chief or team lead can establish and restrict a shared folder to a particular group of employees. An example would be the federal director might establish a folder restricted only to federal branch chiefs and team leads for a performance or award cycle. No one would have access to this folder, unless they were given permissions by the director.

h) 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 PIN are required to access the employee's Windows Domain account.

i) 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and complete certification.*

__√__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

√ No. This is not a new information system.

2. Is the IT system or its information used to support any activity, which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

√ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

√ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

√ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

√ DOC employees
____ National Institute of Standards and Technology Associates
√ Contractors working on behalf of DOC

√ Other Federal Government personnel
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide and explanation for the business need requiring the collection of SSNs, including truncated form.

Provide the legal authority, which permits the collection of SSNs, including truncated form.

√ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

√ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

√ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

√ I certify the criteria implied by one or more of the questions above **apply** to the NOAA8877 ROC LAN and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA8877 ROC LAN and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Sallie Ahlert Office: DOC\NOAA\NWS\OBS1 (ROC) Phone: 405-573-8870 Email: Sallie.M.Ahlert@noaa.gov  Digitally signed by AHLERT.SALLIE.M.1365877706 Date: 2021.02.19 20:21:31 -06'00'	**Information Technology Security Officer** Name: Andrew Browne Office: DOC\NOAA\NWS\ACIO Phone: 301- 427-9033 Email: Andrew.Browne@noaa.gov BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2021.02.22 10:17:27 -05'00'
Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 828-257-3148 Email: Adrienne.Thomas@noaa.gov THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2021.02.24 17:44:09 -06'00'	**Authorizing Official** Name: Thomas Cuff Office: DOC\NOAA\NWS\OBS Phone: 301- 427-9778 Email: Thomas.Cuff@noaa.gov CUFF.THOMAS.JAMES.1071092450 Digitally signed by CUFF.THOMAS.JAMES.1071092450 Date: 2021.02.24 08:08:02 -05'00'
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2021.02.27 08:33:32 -05'00'	