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

General Support System
Radar Operations Center Local Area Network
(ROC LAN)

NOAA 8877

PRIVACY IMPACT ASSESSMENT

May 15, 2012

Prepared by: William F Haden, Radar Operations Center ISSO

Reviewed by: Sarah D. Brabson, NOAA Office of the Chief Information Officer

General Support System
Radar Operations Center Local Area Network
(ROC LAN)

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

Information Technology (IT) Security System: NOAA8877

Project Description: The Radar Operations Center (ROC) is an integral part of the National Weather Service mission. The mission statement of the National Weather Service is:

> *"The National Weather Service (NWS) provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. The NWS data and products form a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community."*

The mission is accomplished by providing warnings and forecasts of hazardous weather, including thunderstorms, flooding, hurricanes, tornadoes, winter weather, tsunamis, and climate events. The WSR-88D (also known as NOAA8104 – Next Generation Weather Radar (NEXRAD)) produces details of the weather event such as the path of an event, severity, levels of precipitation, wind speed, wind direction, and other data which is recorded and may be used for analysis and research. The ROC is a key support element in ensuring the availability of the WSR-88D system used by weather forecasting organizations.

The ROC provides centralized radar operations support; 24/7 field assistance, software maintenance, and engineering support; and special depot-level support (such as bull gear replacement) of the WSR-88D units deployed by the three Tri-Agency Principal Users. The ROC performs systematic and coordinated analyses of the day-to-day operations and maintenance of WSR-88D units to determine the need for improvement, and for providing both immediate and long-term support during the WSR-88D lifecycle. The ROC analyzes, develops, tests, and evaluates proposed changes to the WSR-88D hardware/software configuration, materials, techniques, procedures, and may approve minor changes. The ROC is responsible for implementation of approved hardware, software, and documentation changes. In addition, the ROC operates and maintains a WSR-88D system to assist in the radar's lifecycle support and improvement responsibilities. The ROC Local Area Network (LAN) (NOAA8877) is designed to support the chartered functions of the Radar Operations Center (ROC). The Director of the ROC is the System Owner for both the ROC LAN and the WSR-88D information systems, and is responsible for the operation, support, and administrative IT resources that allow the ROC to support the WSR-88D radars.

1. What information is to be collected (e.g., nature and source)?

This system will collect information necessary for Department of Defense's (DOD) Air Force, military performance and promotion reports. This information includes an individual's name, rank, duty station, social security number, and performance evaluation ratings. These reports will contain information on active duty Air Force personnel working at the ROC. The ROC staff is composed of NWS employees and contractors, Air Force, DOD civilians, and Federal Aviation Administration (FAA) employees and contractors per tri-agency agreement staffing guidelines.

The system also collects information necessary to sponsor foreign visitors. The information collected includes the foreign visitor's name, date of birth, city and country of birth, and passport number. This information is maintained only by the Program Branch Chief, who is the sponsor of foreign visitors. Foreign Nationals who have "Green Cards" are not required to submit this data.

2. Why is the information being collected (e.g., to determine eligibility)?

The information collected on military employees is required to complete military performance and promotion evaluations. The information is then submitted to the Air Force Headquarters via encrypted email as per Air Force direction.

The information on foreign visitors is necessary to sponsor visitors to the ROC from foreign countries.

3. What is the intended use of the information (e.g., to verify existing data)?

The information collected 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 emailed to Offutt Air Force Base (AFB) using the Common Access Card (CAC) PKI credentials. Once processed at Offutt, the form is returned to the ROC for final signatures and then emailed to Tinker AFB who has administrative responsibility for the DOD personnel at the ROC. Tinker 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 (DOD, NWS, or FAA personnel) beyond those that are required to process it.

The information on foreign visitors is required for obtaining approval from the Western Region Security Office (WRSO) in Seattle, to ensure that the foreign visitor is authorized to enter the United States. This information is not shared with the other agencies.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

The sharing of performance and promotion reports is limited to the individual, supervisor, and authorized personnel located at the Air Force Weather Agency, Offutt AFB, Nebraska, the 72 Wing Personnel Workforce Management Flight, Tinker AFB, Oklahoma, and the Air Force Personnel Center at Randolph AFB, San Antonio, TX as part of the service member's permanent record. This information is not shared with the NWS (beyond the supervisor) or the FAA.

The foreign visitor information is shared with DOC Security only for the purposes described above. The information is not shared with the DOD or the FAA.

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how may individuals grant consent?

Performance information is part of all service members' official personnel record. The performance record/information is not granted by voluntary consent, it is mandatory, as per AFI 36-2406.

Foreign Nationals must supply the information requested of them, in order to be granted access to NOAA facilities. Refusal to supply the information will result in being denied access.

6. How will the information be secured (e.g., administrative and technological controls)?

-

The military evaluation forms are stored on the supervisor's personal network drive.

The information for the foreign visitors is maintained only by the Program Branch Chief on his personal network drive.

There are three general classes of security controls described in the National Institute of Standards and Technology (NIST) Special Publication NIST 800-SP-53 rev 3: management, operational, and technical. These security controls are organized into eighteen families within these three classes. Each security control family contains security controls related to the security functionality of the family. The classes and families in the security control catalog and the associated security control family identifiers are as follows:

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational

MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

NIST-800-SP 53, Recommended Security Controls for Federal Information Systems and Organizations, rev. 3, August 2009, identifies security controls for high, low, and moderate impact systems. The ROC LAN is categorized as moderate impact. The current Authorization to Operate (ATO) under the Federal Information Security Management Act of 2002 (FISMA) was issued on May 15, 2010 and is affirmed each year thereafter. Under the ROC LAN Continuous Monitoring plan, one third of the ROC LAN security controls are evaluated every year to ensure compliance with operational, management, and technical controls established by the Department of Commerce.

Management Controls

The *Management Controls* address security topics that can be characterized as managerial. They are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization.

Specific Controls:

-PL-4, Rules of Behavior – Every individual must take the annual NOAA Security Awareness Training and acknowledge the NOAA Rules of Behavior. Everyone with access to the ROC LAN must also undergo security training from Information Technology and Services (IT&S) as part of their orientation and sign the ROC Rules of Behavior.

-PL-5, Privacy Impact Assessment – A Privacy Threshold Analysis and Privacy Impact Analysis are conducted annually in accordance with the Office of Management and Budget (OMB) policy.

By ROC policy, any PII must be stored on P: (personal) network drive of the employee who is responsible for the information.

Operational Controls

The *Operational Controls* focus on controls that are, broadly speaking, implemented and executed by people, as opposed to systems. These controls are put in place to improve the security of a particular system or group of systems. They often require technical or

specialized expertise, and often rely upon management activities as well as technical controls.

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. Initial and annual security awareness training with a section on data privacy is mandatory for all new and existing ROC staff, as well as anyone who is authorized access to the information system. This training includes a section on Privacy Act information. As part of the initial training conducted by the ROC, the user (internal or external) signs the ROC Rules of Behavior (ROB) indicating that they have read and understand the ROB.

Access rights to all information on the ROC LAN is controlled by group administration, which is defined by organizational components and then by roles. Although the system secures information through assigning a user a unique identifier, and assigning that user to a group with restricted access, the user could still cut and paste information or copy information to a non-secure source. This type of activity is mitigated by the annual security training and, to protect mobile information, all ROC laptops are fully encrypted using the NOAA supplied SafeBoot software.

Specific Controls:
-SI-3, Malicious Code Protection – The ROC IT&S uses patch management software (VMware vCenter Protect Essentials Plus) to scan all Windows computers, including servers, and apply the latest Microsoft patches.

The McAfee ePolicy Orchestrator (ePO) server updates and distributes the latest virus signature files. Software patches, service packs, and hot fixes are tested for effectiveness on information systems prior to being fully installed.

Virus protection capabilities are centrally managed through the ePO agent. This system automatically updates virus protection capabilities. System managers and administrators ensure all systems have:

- Anti-virus software installed
- Automatic update capabilities included in malicious code protection capabilities
- Centrally managed virus protection capabilities

ROC LAN users are prevented, via group policy and the practice of “least privilege”, from disabling or otherwise re-configuring the Anti-Virus, local firewall, and patching mechanisms in place.

-CP-9, Information System Backup – All data files (including the personal drives) are backed up nightly in accordance with the ROC Backup Plan.

Technical Controls

The *Technical Controls* focus on security controls the computer system executes. These controls are dependent upon the proper functioning of the system for their effectiveness.

Least privilege is the concept applied when storing information and providing access to information. Least privilege is the practice of granting the least amount of access possible to a user while still allowing fulfillment of job responsibilities. Groups are created to control the management of information access. Groups are determined by organizational components, e.g., Engineering Branch, Program Branch, Admin, IT&S, etc., and then further defined by function and/or role, e.g., administrators, budget, etc. Authorized membership to groups is determined by the data owner, but managed by system administrators, who have annual security role training requirements.

Specific Controls:

-AC-3, Access Enforcement – The ROC LAN controls access to data by the use of share/file level security settings.

-AC-11, Session Lock – The ROC LAN prevents access to the system by initiating a session lock after 15 minutes of inactivity or when initiated by the user. The session lock remains in effect until the user reestablishes access using established identification and authentication procedures.

Data Extract Log and Verify – Currently, the process for logging and monitoring data extracts is manual. Access to pertinent files or information is limited to system administrators and the individual creating the records. Individuals with access are advised on the requirement to destroy all data extracts once they are no longer needed. The PII handled by this system is considered low risk and electronic logging has not been implemented.

-AU-2, Auditable Events – All network devices, security devices, operating systems, server applications, and services that manage identification and authentication log the minimum audit events; specifically, logon success and failure.

-AU-3, Content of Audit Records – All network devices, security devices, operating systems, server applications and services produce (generate) audit records that contain sufficient information to a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

-AU-6, Audit Review, Analysis, and Reporting – All critical network devices, security devices, operating systems, server applications and services that collect audit records are manually reviewed weekly for inappropriate or unusual activity.

-AU-11, Audit Record Retention – All network devices, security devices, operating systems, server applications and services retain logs for 120 days.

-The personal drive (P: drive) is only accessible by the individual and the system administrators.

The ROC LAN undergoes an annual Security Assessment and Authorization (A&A) in accordance with the Risk Management Framework (RMF) process as described in NIST SP 800-37 rev 1.

7. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

The System of Records Notices (SORNs) for the Air Force can be found at:
http://dpclo.defense.gov/privacy/SORNS/component/airforce/

Specifically, the following SORNs apply:
F036 AF PC A – Office and Enlisted performance reporting records
F036 AF PC M – Officer Promotion
F036 AFPC K – Enlisted Promotion

The SORNs for the DOC and NOAA can be found at:
http://www.rdc.noaa.gov/foia/sorns/

Specifically, the SORN covering the Foreign Visitor/Guest Information is:
System name: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons--COMMERCE/DEPT-9

8. Are these records covered by an approved records control schedule?

The Air Force is responsible for the permanent retention of the military performance reports. These reports are kept locally by the service member's supervisor for two years after they leave the ROC, the records are then deleted. Air Force Instruction 33-322, Records Management Program, establishes policy and assigns responsibilities for lifecycle management (i.e., creation, maintenance and use, and disposition) of information. This instruction is attached.

The information on the foreign visitors is covered by the NOAA Records Disposition Handbook, Chapter 600: International Activities Records, Rev. 5/95, Chapter 600-07. The appropriate chapter states:

600-07 Foreign Visitor, Training or Assistance Files
(Supersedes NC1-370-75-1, Item IA3)
Case files containing correspondence, memorandums, reports, background, technical, or biographical information, and other records relating to protocol matters and assistance in arranging travel plans and visits for foreign officials and other visitors. The files may also contain travel, sponsorship, training, and course records related to NOAA-sponsored international training programs conducted for visitors, foreign scientists, or foreign officials.

AUTHORIZED DISPOSITION: Destroy when 3 years old.

The DOC Security Office is responsible for the permanent retention of the foreign guest information. Locally, the Foreign National Visitor/Guest Information Report Form is maintained at the ROC by the Program Branch Chief and deleted when no longer required or three years maximum.