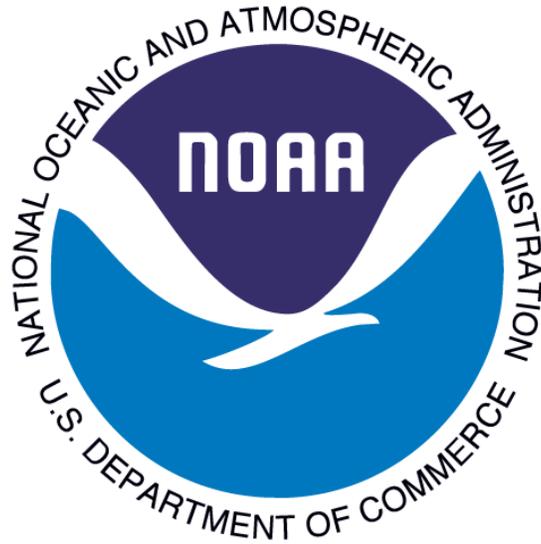


**U. S. Department of Commerce
National Oceanic and Atmospheric Administration**



**Fairbanks Command and Data Acquisition Station
(FCDAS)
Administrative Local Area Network (LAN)
[NOAA5008]**

PRIVACY IMPACT ASSESSMENT

February 24, 2011

Prepared by: Russell Worman, FCDAS Administrative LAN ISSO

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

Fairbanks Command and Data Acquisition Station (FCDAS) Administrative Local Area Network (LAN)

Unique Project Identifier: NOAA5008

Project Description: The Fairbanks Command and Data Acquisition Station (FCDAS) Local Area Network (LAN) functions as the overall general support system for the NOAA-NESDIS Command and Data Acquisition Station (CDAS) offices located in Fairbanks, Alaska. It provides access to automated systems typically found in NESDIS CDAS within the federal government. It supports Fairbanks CDA station and remote antenna facility in Barrow AK.

There are a variety of hardware platforms and operating systems interconnected on this network system. The system supports a variety of users, functions, and applications with varying security requirements. Computer services are provided via Windows 2003/2008 Server, Windows 7/XP Pro, and LINUX operating systems. The services include links into host computers, interactive and batch processing, disk storage and retrieval, printing, file backup and restoration.

The primary functions that the LAN provides are:

- File and database sharing
- E-mail and file transfer capabilities
- Network application sharing
- Internet access via wide area network connections
- Access to shared printers
- Resource scheduling

The categories of data inputted, stored and processed include administrative, satellite operations, statistical, and technical.

The FCDAS LAN is located in five buildings on the station. The address for the station is:

Fairbanks Command and Data Acquisition Station
1300 Eisele Rd
Fairbanks, AK. 99712

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

Both Privacy Act/personally identifiable information (PII) and business identifiable information (BII) for the federal (5) and contractor (40) employees) are collected on the FCDAS LAN. The primary purpose of this system is to support the Satellite Operations done by the engineers and staff at the Fairbanks Command and Data Acquisition Station. The following table lists the general categories of data collected. This represents the primary data collections maintained at FCDAS.

| | |
|---|----------------|
| Satellite Operations Procedures and maintenance | Administrative |
| Property Tracking | Administrative |
| Purchasing Tracking | Administrative |
| Personnel Data System | Administrative |

PII in the LAN consists of:

Name
Position Information
Hire Date
FT/PT
Employment Status
Position Title
Pay Band
Managerial Position
Location
Office
Phone
Cell Phone
Email Address
Home Phone
Cell/Alt Number
Home Address
Emergency Contact Name
Emergency Contact Phone No.
Training Class Attendance
Date of Birth
Denied Entities List
Controlled Equipment/Technology

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

All information collected is extracted from paper records supplied by the individual or derived from other sources. Information stored is not used for decision-making. Source documents are pulled for final reference when needed. Most of the personnel data collected is used to satisfy management and operational needs associated with employment and Foreign National visitors to the FCDAS.

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

Information in the system is used in various tracking, compliance, and reporting uses.

- Maintain a current employee listing and organizational chart
- Track security and facilities related matters (keys, badges, magnetic key cards, room numbers, etc)
- Track Foreign National visitors
- Maintain a current emergency contact listing

- Maintain a current phone listing with room number assignment
- Track training completion
- Track authorized drivers of government vehicles
- Track Credit Cards/Travel Cards
- Respond to facilities and other HQ data calls
- Track and maintain Employee vacation and work schedules
- Comply with Department Administrative Order (DAO 207-12) and NOAA Administrative Order (NAO-207-12)
- Comply with Executive Order (EO) 10450.

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

Foreign National and deemed exports information is shared with NESDIS HQ, NOAA CAO, and NOAA Security Office (Western Region). Foreign National and Deemed exports information is shared in order to comply with DAO-207-12, NAO-207-12, and EO 10450.

Personnel and human resources data is shared with the NESDIS HQ HR office and NOAA finance office to support employee pay, benefits, and appraisals.

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?

All employees are apprised of the use of this information, and that it is used solely for management and operational purposes. At the point of collection of the data, individuals are advised of the right to refuse to provide the information requested and how this will affect them.

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

Management Controls:

The Information Systems Security Officer of the FCDAS identifies the need for application updates, system updates, and security updates and notifies the Information and Technology Systems (ITS) staff who will then update and test the system as required. Upon completion of successful testing, ITS will request that an Administrative Support Specialist conduct final testing. The ITS uses configuration change management processes to assure management and technical oversight and review. Hard copy reports that contain PII data are maintained in locked cabinets. Any proposed use of the data collected must be approved by the Station Director.

Operational Controls:

The NOAA 5008 central computer room is located at 1300 Eisele Rd, Fairbanks, AK. 99712. The facility has a uniformed guard service, video cameras covering entrances, and is staffed around the clock seven days a week, and has key card controls limiting access to all

production servers. Nightly backups are performed with backup media being stored remotely in a four meter antenna shelter on the station campus. Integrity checks of the backups are performed monthly. Data is restricted to the least number of users that requires access to the information. The data is not accessible to the public, and any user must be authorized to have access to the data.

Technical Controls:

Please describe your process for logging/monitoring data extracts, including the process for reviewing the logged information to determine: 1) how it is used, and 2) if there is still a need for it after 90 days (such extracts must be destroyed after 90 days if no longer needed). If the logging/monitoring process is automated, please describe the process used for implementing [NIST-800-53 Rev 1](#), Security Controls for Auditable Events (AU-2, "Auditable Events", AU-3, "Content of Audit Record", AU-6, "Audit Monitoring, Analysis and Reporting" and AU-11, "Audit Record Retention"). Please include the requirement to verify that PII extracts are logged, verified and erased within 90 days in the auditable events criteria in AU-2 and AU-11.)

The PII data is stored on a network share which employs Windows Active Directory for data access rights, permissions, and audit logging. The data is stored in Word documents, Adobe PDFs, and Excel spreadsheets. Data access is monitored and audited via audit logging which is set to record object access, privileged use, and logon events, both success and failure. System audit logs are collected and stored on a centralized logging system (Trip Wire Log Center) where audit logs are reviewed on a weekly basis. Data is manually destroyed (deleted) when no longer needed, i.e. when one of the five staff (the only staff on whom information is collected and stored) leaves. There is no need for actual extraction, as opposed to reading, of data.

A Security Certification and Accreditation (C&A) in accordance with the requirements of the [Federal Information Security Act of 2002](#) (FISMA) was completed for FCDAS Administrative LAN (NOAA5008) on September 29, 2008; a new C&A is in process. The C&A process is an audit of policies, procedures, controls, and contingency planning, required to be completed for all federal government IT systems every three years.

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

No. The existing Privacy Act system of records notice for DEPT-2, Accounts Receivable, applies to the personal information in this system.

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

The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the Federal Government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. GRS 6, item 1 authorizes the disposal of the equivalent paper copies six years and three months after the period covered by the account, **EXCEPT:** Accounts and supporting documents pertaining to American Indians are not authorized for disposal. Such records must be retained indefinitely

since they may be needed in litigation involving the Government's role as trustee of property held by the Government and managed for the benefit of Indians.