U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
Fairbanks Command and Data Acquisition Station (FCDAS)
Administrative Local Area Network (LAN)
NOAA5008

Reviewed by: _____, Bureau Privacy Officer or Designee

Approved by: _____, DOC Chief Privacy Officer

Date approved: 6/19/2014

U.S. Department of Commerce Privacy Impact Assessment for NOAA/NESDIS/OSPO/FCDAS (NOAA5008)

Unique Project Identifier: NOAA5008 is not associated with an Exhibit 300

Introduction: System 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 2008 Server and Windows 7 Pro 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

Privacy Act/personally identifiable information (PII) collected on the FCDAS LAN is primarily used for management and operational needs associated with employment and Foreign National visitors to the FCDAS. For needs associated with employment the FCDAS LAN statutory authority for collecting (PII) for civil service employment is; 5 U.S.C. 301, and Executive Order 10450. For Foreign National visitors, FCDAS complies with Department Administrative Order (DAO) 207-12 and Technology Controls and Foreign National Access (NAO) 207-12 of the "Foreign National Visitor and Guest Access Program."

This is a moderate level system.

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	x	i. Financial Account	
b. Taxpayer ID		f. Driver's License	x	j. Financial Transaction	
c. Employee ID		g. Passport	x	k. Vehicle Identifier	
d. File/Case ID		h. Credit Card		l. Employer ID Number	
m. Other identifying numbers (specify):					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth		m. Religion	
b. Maiden Name	x	h. Place of Birth		n. Financial Information	
c. Alias	x	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	
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	x	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures	x	f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

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

Government Sources					
Within the Bureau	x	Other DOC Bureaus	x	Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

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	x	For administering human resources programs	x
For administrative matters	x	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
Other (specify):Foreign National visitors	x		

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).

Information in the system is used in various tracking, compliance, and reporting uses. FCDAS PII/BII data is collected only for federal employees and contractors working on behalf of NOAA, and tracking Foreign National visitors to the facility to meet the following requirements:

- 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
- 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 Technology Controls and Foreign National Access (NAO) 207-12 of the "Foreign National Visitor and Guest Access Program"
- Comply with Executive Order 10450—Security Requirements for Government employment

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	x			
DOC bureaus	x			
Federal agencies	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.

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.	
x	Yes, notice is provided by other means.	Specify how: Notice is provided on the CAC card application.
	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 decline to provide PII/BII.	Specify how:
x	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: The investigation is a job requirement. Providing the information is voluntary, but choosing not to provide the required information will result in not meeting the requirements of the job and therefore not being considered further.

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.
x	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The investigation is a job requirement and there is only one specified use, for acquiring a CAC card.

5.4 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: The Western Region Security Office provides information for individuals to contact OPM regarding their investigation file on the investigation Web site: Background Investigation Requests: *You may request a copy of your investigation file under the provisions of the Privacy Act. For an Office of Personnel Management (OPM) investigation request, write to OPM-CIS, FOIP, Post Office Box 618, Boyers, PA 16018-0618. You must include your full name, Social Security Number, date and place of birth, and you must sign your request. Visit the OPM website for additional information.*
	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. *Also see Appendix A, a checklist for more specific controls. This appendix will be removed after the PIA is approved.*

x	All users signed a confidentiality agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff received training on privacy and confidentiality policies and practices.
x	Access to PII/BII is restricted to authorized personnel only.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization: 9/29/2013
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	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.
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Other (specify):

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."

x	Yes, this system is covered by existing system of records notices. Provide the system name and number. COMMERCE/DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies; 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.

x	There is an approved record control schedule. Provide the name of the record control schedule: FCDAS file maintenance and disposal plan: NOAA Records Schedules: General: 100-2, 100-5, Administrative: 200-1, 200-6, 200-9, 200-12, 200-23, 200-26, 200-27, 200-30, 200-34

	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: