Version Number: 01-2015

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: Mark Graff _____, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2017.08.31 16:54:24 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/FCDAS Admin LAN

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) is the 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 2008/2012 Server and Windows 7 Pro operating systems. The services include links into internal and external host computers, interactive and batch processing, disk storage and retrieval, printing, file backup and restoration; the host computers do not process or provide access to PII or BII.

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

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. Personnel records include SF-52s, performance plans, award documents, position descriptions and recruitment-related documents that are sent to Workforce Management (WFM). Copies of the WFM certifications are retained for 90 days and then destroyed.

The PII/BII information collected is shared with other agencies or parties on a case-by-case basis, as described below. If any of the data is sensitive or For Official Use Only (FOUO), then the data is restricted by drives and folders to only FCDAS Admin LAN personnel authorized to access the information.

Transfers - The system collects PII of DOC (NOAA employees only) personnel to the extent necessary for preparation of performance, promotion, and awards for these personnel. The FCDAS Admin LAN contains personally assigned network shares which are accessible only by the person assigned the shared drive.

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 DOC Accellion (for DOC records only) or via FedEx package.

Information obtained for CAC background investigations and issuance is transmitted to DOD via the DOD CVS system and is not collected or retained on the local network. Background check information is inputted directly, by the applicant, to OPM and OSY. The CAC application hard copy is transcribed into the Trusted Agent, outside of this system.

Foreign national visitors are required to provide personal information as specified in DOC Directive DAO 207-12. This information is shared with the DOC Office of Security (OSY).

Authorities: For needs associated with employment, the FCDAS LAN statutory authorities for collecting (PII) for civil service employment are: 5 U.S.C. 1302, 2951, 3301 and 4118, 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".

From the DEPT-6 System of Records Notice: 5 U.S.C. 301; 44 U.S.C. 3101

From the OPM Govt-1 System of Records Notice; 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

This is a FIPS 199 moderate level system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-		e. New Public Access		h. Internal Flow or	

Anonymous				Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_X____ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 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*	X	e. File/Case ID	X	i. Credit Card	
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: In accordance with 10 U.S.C. 133 and E.O. 9397, DoD requires SSNs for security clearance/background checks, classified material courier designation, and access to certain information systems such as Trusted Agent. *Information is in the system only until entered into the DoD system.*					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	X*
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	X	r. Mother's Maiden Name	
s. Other general personal data (specify): citizenship (for foreign nationals)					

* The OGE Form 450 is required annually for purchase agent and COR, for conflict of interest information only. See 11.2

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
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		f. Vascular Scan		i. Dental Profile	

Recording/Signatures					
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	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 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		Email	X		
Other (specify):					

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

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		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	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Foreign National visitors in accordance with DAO-207-12.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the 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
- Maintain a current emergency contact listing
- Maintain a current phone listing with room number assignment
- Track security and facilities related matters (keys, badges, magnetic key cards, room numbers, etc.)
- Financial reporting for COR (OGE form 450) and qualifications for federal purchase card/travel card/warrants.
- Track Foreign National visitors (contact information, date and place of birth, citizenship, passport number, job description)
- 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 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
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.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: (on the photograph consent form sent with this PIA). _____.	
X	Yes, notice is provided by other means.	Specify how: • For use of photographs, there is a written consent form with a privacy act statement. • Notice is provided on the CAC card application. • Written notice is included on all personnel forms that employees complete. • For DOC performance/award documents, employees are informed by their supervisors that the evaluations are in process. Employees have access to view the official documents. • For COOP or emergency recall in the NOAA directory, employees are notified in writing by their supervisors when collecting the applicable information. • For responses to solicitations, notice is given on the request for information (RFI) or request for proposal (RFP).
	No, notice is not provided.	Specify why not:

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

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: • A background 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. • For DOC personnel data, employees may opt not to provide PII/BII – at the time of the request, and in

		writing 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 DOC employees and information is added to the eOPF in conjunction with the employee mid-year and annual reviews. The performance record/information is required in order to conduct performance evaluations. • For use of an employee photograph for in house purposes, the employee's supervisor provides a consent form with a privacy act statement. The employee may choose to decline, by not signing, or by writing "declined" over the signature. • For COOP or emergency recall in the NOAA directory, employees are asked permission in writing by their supervisors when collecting the applicable information, and may decline at that time. This information is not required. • For solicitations or RFIs, individuals may decline to provide the information, but this will affect their eligibility for consideration.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: • The background investigation is a job requirement and there is only one specified use, for acquiring a CAC card. • Consent is included on all personnel forms that employees complete, and consent to the uses explained on the forms is implied by completion of the forms. • There is a consent form for use of photographs, for in-house use or publication. If the employee does not wish to have his/her photograph used, he/she will not sign the form, or write "declined" and sign. • For DOC personnel data, employees may opt not to provide PII/BII – at the time of the request, and in writing 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 DOC employees and information is added to the eOPF in conjunction with the employee mid-year and annual reviews. The performance record/information is required in order to conduct performance evaluations. This is the only use. • For FCDAS LAN COOP or emergency recall, there is only one use, and consent to that use is implied by the voluntary provision of the information for that intended use. • For solicitations and RFIs, an individual may opt not to

		consent to the one use – review and consideration for award – but this will affect their eligibility for consideration.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 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** • An employee may update information on personnel forms at any time by contacting their HR representative – as explained during orientation. • For Emergency and COOP information, the employee may not review the information, because it contains other staff's PII unless there is need-to-know, but may request updates from the assigned administrative staff, as explained by that staff when requesting the information. • An employee may update information used for their DOD-issued CAC by contacting the NOAA Trusted Agent and DOD DEERS Office. • Offerors will contact the office to which the proposal was submitted, with updated information.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit logs from each computer system are recorded and monitored with various tools including Tripwire, Solarwinds Kiwi, Veeam, and ArcSight.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ___9/29/2016_____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts

	required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

PII is protected through a combination of measures, including operational safeguards, privacy specific safeguards, and security controls. Policies and awareness training are provided annually. The minimum amount of PII necessary to meet the mission is collected. Once the PII is no longer relevant or necessary it is properly destroyed. Security controls are in place, such as data at rest encryption and access controls limiting access to PII/BII. This information is consolidated into one folder that is encrypted and has restricted access limited to authorized NOAA staff. Further, if someone that doesn't have access attempts to access to a folder containing PII/BII, then a failed access log is created. We also employ security monitoring tools that can detect PII in unauthorized locations. The FCDAS Admin LAN provides dedicated drives with user access restrictions for those that store PII/BII. Windows Encrypted File System (EFS) is used for encrypting PII/BII data at rest.

The FCDAS Admin LAN has NIST 800-53 Rev 4 security controls in place, including, but not limited to: the Access Control family, limiting access to allow only the necessary functions for users to operate within the FCDAS LAN. Account privileges are tied directly to job function and designed to enable the user to accomplish only what the job requires and no more. The Audit and Accountability family utilizes tools such as Tripwire to record, store and manage logs for auditable events. The Identification and Authentication family to identify users and require two factor authentication. The Media Protection family to monitor access to stored data and the approved sanitation methods for all media. This IT system uses approved DoD software run seven times to ensure no data remains on IT system media. The System and Information Integrity family is minimized exposures to exploits that could compromise the system. This IT system is monitored using various tools Nessus, McAfee, and Cisco.

Section 9: Privacy Act

9.1 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 an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: 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; COMMERCE/DEPT-6, Visitor Logs and Permits for Facilities Under Department Control OPM GOVT-1, General Personnel Records.

	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 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:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Personnel records, COOP contract information for employees, foreign national visitor information.

X	Quantity of PII	Provide explanation: PII limited – Records for 5 NOAA staff and home contact info for 42 contractors, plus foreign national visitors.
X	Data Field Sensitivity	Provide explanation: Limited financial information for gov't staff (OGE Form 450 and travel card applications)., foreign national passport number, employee SSNs
X	Context of Use	Provide explanation: Personnel (NOAA) performance evaluations, personnel actions.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Performance plans/evaluations/records for NOAA staff limited to supervisor and admin. Foreign national information is restricted to NOAA staff only.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: Implementation of a photograph permission form with PAS.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.