

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



**Privacy Impact Assessment
for the
NOAA5044
NOAA Satellite Operations Facility (NSOF) Administrative LAN**

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 D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open
Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.10.20 10:52:02 -04'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment [NESDIS/NOAA5044]

Unique Project Identifier: 006-000351101 00-00-02-00-02-00

Introduction: System Description

System Description:

(a) General Description – NSOF Admin LAN (NOAA5044) is physically located in the NOAA building at 4231 Suitland Road, Suitland, Maryland, a suburb of Washington, D.C. The building is owned by NOAA and managed and secured by the General Services Administration. The NSOF Admin LAN provides standard office automation for all NESDIS employees located within the NSOF. It also provides access to the Internet. The LAN provides end-to-end connectivity and network access to all LAN Federal employee and contract users, to increase productivity through the use of applications, data resources, or other electronic office automation tools.

The two types of applications supported by the NSOF Admin LAN—server applications and client applications—are considered minor applications in that they are accredited as a GSS rather than separately. There are no major applications (as defined by OMB A-130) in the NSOF Admin LAN environment.

There are five user communities located in the NSOF: the Office of Satellite Ground Systems (OSGS), the Office of Satellite and Product Operations (OSPO), the General Services Administration (GSA), the National Ice Center (NIC) and the Defense Meteorological Satellite Program (DMSP). These user communities have dedicated workstations connected to the NSOF Admin LAN.

NOAA5044 provides access to automated programs and systems supporting administrative programs such as budget and financial management, personnel management, procurement, building operation and management, interagency programs, IT planning, and IT security. The system also supports access to the Internet.

There is electronic personnel related information about NOAA employees and prospective employees maintained on the NSOF Admin LAN, containing information such as SSN, Passport, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone Number, Email Address, Financial Information, Military Service, Occupation, Job Title, Work Address, Telephone Number, Work History. In addition, the system maintains onboarding forms, training forms (SF-182), resumes, and vehicle information for parking.

DOC and DOD performance evaluation are also compiled and maintained in the system. The appropriate forms are completed on the NOAA5044 Manager's secure home directory. They are then printed, hand-carried for signature, and then transferred via the agency-specific secure electronic transfer procedure.

There is also ESPC account management, collecting contact information from individuals or organizations wishing to access ESPC data via its distribution mechanisms, or to supply data as may be appropriate. This information is voluntarily submitted through the use of forms or email and is stored in restricted areas of the shared drive only accessible by authorized personnel. The information is collected to ensure the user receives the correct products in line with their request, or to allow an ESPC program manager to validate that a proposed supplier is a legitimate organization able to supply the information being proposed. The information may also be used to notify users and suppliers in the event of an outage or other type of service disruption. In addition, the NOAA5044 collects PII of NSOF LAN personnel on a voluntary basis for purposes of Continuity of Operations Planning (COOP). This data is stored on a LAN shared drive only accessible by authorized personnel.

(c) The PII/BII information collected by NOAA5044 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 NSOF Admin LAN personnel authorized to access the information.

Transfers - The system collects PII of DOC (NOAA employees only) and DOD civilian and military personnel to the extent necessary for preparation of performance, promotion, and awards for these personnel. The NSOF Admin LAN contains personally assigned network shares (H:\), 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 tracked United Parcel Service (UPS) package.

(d) Authority - Statutory or regulatory authorities for collection and maintenance of the information include:

- 15 USC 1512 (Powers and Duties of the Department of Commerce)
- 5 USC 2101 to 10210 (Government Organizations and Employees, Part III, Employees)
- 5 USC 301 (Departmental Regulations)
- 10 USC 8010 to 9448 (Armed Forces - Air Force - Organization, Personnel, and Training)

(e) Categorization – NOAA5044 NSOF Admin LAN is a moderate impact 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-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.

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		i. Credit Card	X
b. Taxpayer ID		f. Driver's License	X**	j. Financial Account	X
c. Employer ID		g. Passport	X**	k. Financial Transaction	X***
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	X
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Performance and award forms require the individual's SSN. <i>The ISSO will bring up the possibility of not including the SSN on these documents.</i>					
**For CAC					
***Contract information					

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		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	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		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)					
Offeror responses to RFIs and RFPs, predecisional					

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	X	Email	X		
Other (specify):					

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

Non-government Sources					
Public Organizations		Private Sector	X	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 (TUCBPNPD)					
Smart Cards		X	Biometrics		

Caller-ID		Personal Identity Verification (PIV) Cards	X
Other (specify):			

	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	X
Video surveillance		Electronic purchase transactions	X
Other (specify):			

	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	X
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):			

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).

- 1) There is electronic personnel related information about NOAA employees and prospective employees maintained on the NSOF Admin LAN, containing information such as SSN, Passport, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone Number, Email Address, Financial Information, Military Service, Occupation, Job Title, Work Address, Telephone Number, Work History. In addition, the system maintains onboarding forms, training forms (SF-182), resumes, and vehicle information for parking. The documents are usually completed by the individual or preparer (administrative person that prepares the document for an individual employee). The files are entered into HR databases that are outside of the NSOF admin LAN or stored locally and transferred by the individual or preparer via DOC Accellion or via tracked United Parcel Service (UPS) package. This information is not shared with anyone beyond those that are required to process it within the respective bureau.
- 2) For contractual and budgetary purposes, the NSOF admin LAN stores procurement and contract information, purchase requests, and accounting information which is stored locally or in restricted areas of the shared drive accessible only by authorized personnel.
- 3) The system's audit logs collect User ID, IP Address, Date/Time of Access, Queries Run, ID Files Accessed, and Contents of Files for hosts connected to the network and stored locally or into restricted areas of the server which only accessible by authorized personnel. The NOAA Directory collects PII in the form of name, email and contact number for COOP. This information is stored on the NSOF Admin LAN and accessible by authorized personnel.
- 4) ESPC account management processes typically collect name, address, phone number, and email address from individuals or organizations wishing to access ESPC data via its distribution mechanisms, or to supply data as may be appropriate. This information is voluntarily submitted through the use of forms, or email and is stored locally or into restricted areas of the shared drive only accessible by authorized personnel. The information is collected to ensure the user receives the correct products in line with their request, or to allow an ESPC program manager to validate that a proposed supplier is a legitimate organization able to supply the information being proposed. The information may also be used to notify users and suppliers in the event of an outage or other type of service disruption.
- 5) Performance awards that contain full Social Security Numbers for military and civilians assigned to the Naval Ice Center are stored on the NSOF Admin LAN. Access to the folder is restricted to those that have a need to know.

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	X	

DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*With OPM if an employee hired by another agency; with State if foreign travel (Federal employees)

<input type="checkbox"/>	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.

X	<p>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:</p> <p>NOAA WFMO Recruitment Analysis Data System (RADS). NOAA5044 uploads data in specified formats to RADS. NSOF LAN has media protection controls in place as well as user procedures on how to protect this information.</p>
<input type="checkbox"/>	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	<input type="checkbox"/>	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.
<input type="checkbox"/>	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:

X	Yes, notice is provided by other means.	Specify how: <ul style="list-style-type: none"> a. Written notice is included on all personnel forms that employees complete. b. For DOC and DOD performance/award documents, employees are informed by their supervisors that the evaluations are in process. Employees have access to view the official documents. c. For NSOF LAN COOP or emergency recall in the NOAA directory, employees are notified in writing when collecting the applicable information. d. For ESPC, information is voluntarily submitted when a user completes the account request form. e. 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: <ul style="list-style-type: none"> a. An individual may decline to provide PII when applying for a position, by not completing all required forms, but his employment status may be affected. b. For DOD and 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 DOD and 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. c. For NSOF LAN 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. d. For ESPC, information is voluntarily submitted through email and is stored locally. An individual may choose not to provide the information, by not answering the questions, but then will not have access to requested information. e. Responses to RFPs/RFIs are voluntary, based on the offeror’s decision to respond.
	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.	<p>Specify how:</p> <ul style="list-style-type: none"> a. There is only one use for information provided during employee onboarding. b. 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. c. For DOD and 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 DOD and 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. d. For NSOF 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. e. For ESPC, the only use is to provide information as requested. f. For contract offerers, there is only one use of the information provided, acceptance of that use is implied by proposal submission.
	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.	<p>Specify how:</p> <ul style="list-style-type: none"> a. An employee may update information on personnel forms at any time by contacting their HR representative – as explained during orientation. b. For DOD personnel data, employees may update their PII/BII – by contacting their HR representative, as explained during orientation. c. b. 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. d. For ESPC, information can be updated by contacting the ESPC help desk. – as stated on the Web page. e. Offerors will contact the office 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: If someone that doesn't have access and 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.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>12/15/2015</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
	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 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.
X	Other (specify): As stated in the NSOF Admin LAN 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. The user (internal or external) signs the NSOF LAN Rules of Behavior (ROB) indicating that they have read and understand the ROB. To protect mobile information, all NSOF Admin LAN laptops are fully encrypted using the NOAA enterprise supplied encryption software.

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

The NSOF Admin LAN has NIST 800-53 Rev 4 security controls in place, including, but not limited to: Separation of duties, access controls, encryption in transit, role-based privacy training, and auditing.

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 NSOF Admin LAN provides dedicated drives with user access restrictions for those that store PII/BII. Windows allows the user the option of encrypting PII/BII data at rest.

We are currently not contemplating overall encryption of data at rest. It would definitely be costly for a system that is slated to be consolidated with NESDIS HQ LAN (NOAA5006) by the end of FY17. Once we consolidate into NOAA5006, we will take on their baseline.

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 <i>(list all that apply)</i> : DEPT-18, Employees Information Not Covered by Records of Other Agencies. NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission; OPM/GOVT-1, General Personnel Records, OPM-2, Employees Performance File Records, OPM-GOVT-9, System for Award Management.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	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: NOAA Chapter 100 – General, Chapter 200 – Administrative and Housekeeping Records, and Chapter 300 – Personnel.
	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: Individuals may be identified based on the PII stored.
X	Quantity of PII	Provide explanation: There is a large amount of PII in the system.
X	Data Field Sensitivity	Provide explanation: There are several types of sensitive PII/BII collected.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Access to PII is restricted to need to know. If someone that doesn't have access and 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. We also employ security monitoring tools that can detect PII in unauthorized locations.
	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: We have recommended to the business process owner responsible for processing DoD awards and performance evaluations that the collection of SSN is not necessary for this activity.
	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.