Version Number: 01-2015

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

Privacy Impact Assessment
for the
NESDIS Headquarters Information System NOAA5006

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: 2017.05.16 16:44:56 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
[NESDIS/NOAA5006]

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

(a) a general description of the information in the system

NOAA5006 is a General Services System which operates under the authority of the NESDIS Office of Chief Information Officer –
Satellites (OACIO-S), located in NOAA, NESDIS Headquarters facility in the Silver Spring Metro Center (SSMC) Building 1 and Building 3. NOAA5006 provides the Local Area Network (LAN) for NESDIS Headquarters, the NOAA Joint-Polar Satellite System (JPSS) Office (NJO) located in the Aerospace building and GreenTec4 [GT4] building of the NASA Goddard Space Flight Center (GSFC) as well as the National Centers for Environmental Information (NCEI) offices located in Maryland, Mississippi, Colorado and North Carolina. NOAA5006 Also supports the Office of Space and Commercialization (OSC) located in the Herbert C. Hoover Building located at 1401 Constitution Avenue Washington, DC. NOAA5006 does not provide LAN or VoIP services to OSC. The purpose of NOAA5006 is to provide mission support and resources for IT management functions and overall office automation support for the programs, offices, and staff of:

- Office Assistant of Chief Information Officer –Satellites (OACIO-S)
- International and Interagency Affairs Division (IIA)
- Branches of Office of System Development (OSD)
- NESDIS Assistant Administrator (AA)
- Chief Financial Officer / Chief Administrative Officer (CFO/CAO)
- NOAA Joint Polar Satellite System (JPSS) Office (NJO)
- Commercial Remote Sensing Regulatory Affairs (CRSRA)
- Office of Satellite Ground System (OSGS)
- Office of Satellite Architecture and Advance Planning (OSAAP)
- Office of Space Commercialization (OSC)
- National Centers for Environmental Information – Maryland (NCEI-MD)
- National Centers for Environmental Information – Mississippi (NCEI-MS)
- National Centers for Environmental Information – Colorado (NCEI-CO)
- National Centers for Environmental Information- North Carolina (NCEI-NC)

The NESDIS HQ ITS LAN provides mission support and resources for IT management functions and overall office automation support for the programs, offices, and staff of the NESDIS HQ. NESDIS HQ ITS LAN provides access to automated programs and systems in support of administrative programs such as budget and financial management, personnel management, procurement, building operation and management, programs within the system, IT planning, and IT security. The system also supports access to the Internet and supports

webpages providing NOAA information and data to the public (available by browsing, no account required).

Information Sharing

The PII/BII information collected by NOAA5006 may be shared with other systems on a case-by-case basis. The type of information that may be shared includes but is not limited to passport data (shared with the State Department for issuance and renewal purposes), employment history and verification (shared with other agencies should an employee transfer to another line office with in NOAA or another DOC bureau or another agency) as well as information related to background checks of existing and new employees (shared with OPM to initiate the investigation process).

Legal Authorities to collect PII and BII

This information is collected under the authority of 5 U.SC., including Section 301. In addition, Title 31 U.S.C. 66a, 492, Title 44 U.S.D. 3101, 3309 and the Federal Collection Claim Act of 1966 apply. Additional authorities include E-Government Act of 2002 (Pub. L. 107–347) Section 204 and Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25.

NOAA5006 is a Federal Information Processing Standard (FIPS) 199 moderate security impact category 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):					

__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		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		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: The Social Security Numbers are collected on NESDIS HQ LAN contractors and government employees for the purposes of conducting background investigations, and for processing of Human resources data such as benefits and payroll for government employees. *The SSN and background investigation information are not stored electronically in the system.*

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		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	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates	X		
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	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

Contract support Information
Foreign Lenders and amounts of debt

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	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	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 (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):			

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).

NJO collects and stores Employment Eligibility Verification Form I-9, government issued ID and has requestors sign a non-disclosure agreement to be granted access to International Traffic in Arms Regulations (ITAR) data, which may contain BII. This information is stored on paper only.

Social Security Numbers are collected on NESDIS HQ LAN contractors and government employees for the purposes of conducting background investigations, and for processing of Human resources data such as benefits and payroll for government employees. *The SSN and background investigation information are stored on paper only and stored in locked cabinets.*

The above information PII/BII is collected on Federal employees, and contractors.

NJO asset tracking system information collected by Management Operation Division contains such information as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people as well as work telephone numbers and work mobile number. The above information PII/BII is collected on Federal employees, and contractors

JPSS stores BII contract support information about its contractors on its share drives for contract related deliverables.

The above information BII is collected on contractors.

CRSRA collects and maintains license application data about businesses that apply for and operate private earth remote sensing space systems. This information collected includes but is not limited to the name, street address and mailing address, telephone number of the applicant as well as any affiliates or subsidiaries, each foreign lender and amount of debt, as well as a copy of the charter or other authorizing instrument certified by the jurisdiction in which the applicant is incorporated or organized and authorized to do business.
The above BII information is collected on businesses.

The OCIO-S system stores NOAA employee passport information for tracking and records purposes regarding international travel. The NESDIS intranet site contains Travel Order Registry database for traveler names and passport information, for tracking and records purposes.
The above PII is collected on Federal employees.

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.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement for CRSRA and/or privacy policy can be found at: https://docs.google.com/a/noaa.gov/forms/d/1STEt0B6EUweGMmk1QyXAoo1KZAnQ1G8JJcnsuifO1SA/viewform?edit_requested=true]_____.	
X	Yes, notice is provided by other means.	Specify how: Individuals are notified of the uses of BII/PII in their employment terms and agreements as well as the contract/license terms and agreements.
	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: Individuals have an opportunity to decline during on-boarding, processes and forms in-place. If individuals decline they're not granted access. Businesses providing information for licensing may decline to provide BII but will not then receive a license.
	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	Specify how:

	consent to particular uses of their PII/BII.	Individuals have an opportunity to consent to particular uses of BII/PII in their employment terms and agreements as well as the contract/license terms and agreements.
	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: Information is reviewed and updates can be made by updating their individual licensing information or contact information where applicable. Updates to licensing information must be submitted in writing to the NOAA NESDIS HQ office. Also, personnel can contact the HR department manager and provide any updates or changes to their 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: We do not have any databases stored on our network that house PII/BII information. We monitor or network devices using Solar Winds and our User accounts are monitored using Active Administrator.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): __06/22/2016_____ ☐ 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.

All PII/BII data stored in our system is located on our internal network. NOAA5006 has boundary protection devices such as firewalls and Intrusion detection/prevention systems in place to protect this data. Also all users who access PII data in our system are required to use CAC authentication which uniquely identifies and authenticates them before they access any PII data.

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)*: NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission, DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons and DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons. Also, DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; GSA/GOVT-9, System for Award Management and GSA/GOVT-10, Federal Acquisition Regulation (FAR) Data Collection System.
	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: **NOAA5006 approved Record Control Schedules under NOAA Chapter 100, 200 and 1400. In addition the information system follows NARA's General Records Schedule where applicable.** **Chapter 100-General** **100-11 Program Correspondence Subject Files** **100-12 Program and Correspondence Subject Files** **100-19 Interagency Cooperative Documents/ Agreements** **100-22 Electronic Records** **100-24 Information Technology Operations & Management** **100-27 Records of the Chief Information Officer** **Chapter 200-Administrative** **200-03- Budget Background Records** **200-04 Budget Estimate and Narrative Statement Records** **200-06 Agency-wide Budget Projection Records** **200-30 Technical Reference Materials** **Chapter 1400 – Satellites and Data Centers** **1401Original Non-disclosure Agreement (NDA) (DAA-370-2012-0001)** **1402 International and Interagency Affairs Office**
	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		Overwriting	X
Degaussing		Deleting	X
Other (specify): If hardware that contains BII/PII cannot be wiped using our DoD approved tools the hardware will be destroyed.			

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.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	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: The information contained can directly identify government and contractor employees. Only authorized personnel have access to this information and must access PII data in our system using their CAC authentication which uniquely identifies and authenticates them before they access any PII data.
X	Quantity of PII	Provide explanation: There is a significant quantity of PII.
X	Data Field Sensitivity	Provide explanation: In some cases the information contained in the data field may be the government or contractors' SSNs. Such data is not publically available and is located on our internal network. NOAA5006 has boundary protection devices such as firewalls and Intrusion detection/prevention systems in place to protect this data. Also all users who access PII data in our system are required to use CAC authentication which uniquely identifies and authenticates them before they access any PII data.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

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

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	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.