U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOS Enterprise Information System
NOAA6001

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: 2017.03.23 12:51:31 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOS Enterprise Information System
NOAA6001

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

The National Ocean Service (NOS) Enterprise Information System (EIS) is an integrated collection of components designed to provide general office automation, infrastructure and connectivity services to NOS Headquarters and component program and staff offices either resident in Silver Spring, MD, or logically connected to the system through WAN links.

NOAA6001 groups elements of the system into three areas, each of which serves a distinct and specific function:

- **Network Devices** -- NOS SSMC (Silver Spring Metro Center) campus backbone and NOS Wide Area Network (WAN)
- **NOS Domain Servers** -- The NOS domain infrastructure components and Headquarters Local Area Network (File, Print, Application) services
- **Web Application Servers** -- NOS application and database hosting services

In addition to the general purpose office automation support (file/printer sharing, application hosting, collaboration, etc.) provided by NOAA6001, the system provides help desk services and supports a number of internal web sites and a minor application which collects, stores and/or disseminates PII. NOAA6001 also stores BII information on file shares.

- Constituents Database – PII, no BII – Office of the Assistant Administrator, Management and Budget (AAMB). upgraded the Constituents Database to a newer version of .NET and encrypted the fields that house privacy data. This version addresses issues identified in the 2014 SCA assessment. This upgrade reduces the risk over the former version of the application

Information Sharing

NOAA6001 collects and stores information related to the AAMB.

NOAA6001 collects and stores limited PII, specifically, names, telephone numbers and email addresses (voluntarily submitted by data providers and customers) to facilitate external coordination with data providers.

NOAA6001 is the general support system for NOS and stores PII on an ad-hoc basis as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

AAMB collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally financial information included with the acquisition package.

Other than the system noted above, there are no applications or databases that collect or employee PII. AAMB does not have a separate HR division, but utilizes the NOAA Workforce Management Office.

In NOS, the Local Registration Authority (LRA) is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card, for example Driver License card. The form also contains common access card (CAC) card electronic data interchange personal identifier (EDIP), full name, work email, work phone number. Only the numbers are collected from the artifacts and stored in the system. The LRA returns the artifacts to the user and does not store images of them on NOAA6001 systems.

NOAA6001 has four websites using Tier 2 multi-session cookies that are not collecting PII. They are used for analytics and for improving the customer experience. The four sites are: http:// oceanservice.noaa.gov, http:// oceantoday.noaa.gov, http://celebrating200years.noaa.gov and http://estuarinebathymetry.noaa.gov.

> The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:
>
> "A. All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." and
>
> "C. Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".
>
> The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

A citation of the legal authority to collect PII and/or BII

> The general legislation supporting the system is 5 U.S.C.301, one of the statutes concerning government organization and employees. In addition, the Uniform Trade Secrets Act, 18 U.S.C 1905 and 44 U.S.C.3101, Records Management by Agency Heads apply.

The Federal Information Processing Standard (FIPS) 199 security impact category for NOAA6001 is moderate.

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 with no changes that 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		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: military identification numbers; CAC electronic data interchange personal identifier (EDIP)					

General Personal Data (GPD)					
a. Name	**X**	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	**X**	p. Military Service	

e. Age		k. Email Address	**X**	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	c. Telephone Number	**X**	f. Salary	
b. Job Title	**X**	d. Email Address	**X**	g. Work History	X
c. Work Address	**X**	e. Business Associates			
h. Other work-related data (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		a. Queries Run		f. Contents of Files	
d. 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): Procurement data is provided in proposals and other procurement documents					

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

Non-government Sources					
Public Organizations		Public Media, Internet	X*	Private Sector	**X**
Commercial Data Brokers					
Other (specify): Procurement data is provided in proposals and other procurement documents.					

* The Constituents Database is compiled from public media providing names and business addresses of people with whom NOS routinely engages who have a known interest in the NOS mission and program, from public-facing websites.

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 no 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 no 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)	X	For web measurement and customization technologies (multi-session)	X
Other (specify): For procurement and grant award activities	X		

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).

Constituents Database information is used to create mailing lists of NOS stakeholders and constituents. In general, the laws that created the various NOS programs include provisions for the program to accomplish a mission. The mission may involve partnerships and educating the public. The collection and storage of information is part of accomplishing the legislated mission of those programs, the NOS, and NOAA (members of the public and federal employees).

NOAA6001 stores PII on an ad-hoc basis as part of the application and hiring of employees, including electronic copies of resumes and the processing of HR data about employees including hiring ranking are stored temporarily during the hiring phase, including, standard HR information such as travel authorization and vouchers, passports and international travel forms, information for transmitting the security badge request email which includes only an email address and possibly a phone number, and performance appraisal ranking. The travel information collected is kept in both hard and soft forms. The hard copies are kept in a locked file cabinet and the soft copies are kept on the shared drive in a folder accessible only to travel admins. The travel documents contain only the traveler's name, home address, and a truncated vendor number associated to the traveler's name. There are no social security numbers or dates of birth.

AAMB collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

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

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.)*

Information Kept on the System

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:	There are warnings/messages on the front page of the Constituents' Database (**www9.nos.noaa.gov/NOSConstituentsDB)** with reference to the Privacy Act of 1974. There is an electronic privacy policy that describes the collection and use of the privacy information. A Privacy Statement has now been added to this page. Note that this notice is only for the employees who enter PII into the database.
X	Yes, notice is provided by other means.	Specify how: Prospective employees are given notice in writing. Notice is provided to businesses who are providing proprietary information in support of federal acquisition actions as part of the acquisition process and is not handled by NOAA6001.
	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: Information is provided on a voluntary basis through individuals who provide their business cards. If they do not want to be placed in the database, they do not provide their business cards. Federal employees may decline in writing to provide PII to their supervisors, but this may affect their employment. Private businesses may decline to provide PII/BII by not including it in their proposals to the federal government, but this may affect their ability to obtain contracts. NOS gathers names and business addresses of people with whom NOS routinely engages who have a known interest in the NOS mission and program from public-facing websites **where there is an expectation of being contacted** with information related to the ocean field, or from emails users send to NOS. They do not have an opportunity to decline to provide PII/BII, but those users who no longer want to receive information from NOS can send an email requesting that they be removed from the database.
	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: Businesses provide information related to procurement activities on a voluntary basis through proposals. All information

		received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR). Applicants for positions are providing their personal information on a voluntary basis through their resumes. There is only one use for this information. For ongoing employee business, such as travel, there is only one specific use for each PII collection. Those individuals who are placed in the Constituents Database without preliminary consent may request to be removed from this database, for which there is only one use.
	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 annual process requires stakeholders to send an email to all individuals in the Constituents database, providing them an opportunity to opt out or update their contact information. Constituents Database: Users may submit updates to the Web site administrator based on information obtained from a mass mailing. Federal employees, and businesses review the information prior to providing it. Any updates required for the information provided can be made by resubmitting the documents previously submitted through the channel previously used to submit.
	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.)*

	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 monitored, tracked, or recorded.

	Explanation: The Constituents Database has audit trails enabled. Procurement information within NOAA6001 is not monitored or tracked. It is kept on shared drives, access to which is restricted by access control lists (ACLs). Laptop tops are configured with full disk encryption. If PII is kept on a laptop, the data is encrypted. NOAA6001 restricts access to shared folders by ACL. PII is not centralized in a database, and it cannot be easily monitored for access. However, as stated above, the access to the shared folders is restricted by ACL. Employee evaluations and potential employee resumes are not monitored, tracked, or recorded within NOAA6001. They are kept on shared drives, access to which is restricted by ACL. NOAA policy requires users not to keep data on their local drives, that they should save it on their own ACL-restricted folders on the shared drive. Policy also requires users to remove all PII from their file share when no longer needed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): Current ATO was issued on March 31, 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 information is stored within the accredited boundaries of NOAA6001is in network data shares controlled by established permission based on the organizational, project, or employee access rights. Any access to specific restricted files or folders is requested through an access change request, which is reviewed and documented by the NOAA6001 Information System Security Officer for authorization and mission 'need-to-know' requirement prior to implementation. NOAA6001 implements least privilege through file share permissions to ensure privacy and open only to those demonstrating a "need to know."

Any PII information, which is transmitted electronically, must follow the federal government and NOAA standard procedure of secure packaging such as utilization of Department of Commerce (DOC) Accellion for encryption in transit.

NOAA6001 IT staff implements the security controls listed in NIST Special Publication 800-

53 R4 required for a moderate system. NOAA6001 is under a current Authorization to Operate (ATO) was issued on December 1, 2016. In compliance with NIST Special Publication 800-53 rev 4, AAMB has a full security program, with performance measures and goals, in order to complete continuous monitoring activities, which include annual security control reviews, quarterly vulnerability scanning, monthly review of security access control list, weekly review of audit logs, handling of access change requests and change control board activities. The risk assessment includes the possible threats and vulnerability to the confidentiality, integrity, and availability of mission and sensitive PII data along with the countermeasures.

Every year the IT system uses and independent contractor that performs a thorough continuous monitoring for the assessment and authorization (A&A) process. The A&A process ensures that the security plan and operational, management, and technical controls meet Department of Commerce (DOC) and NOAA guidelines for continued operation.

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. Provide the system name and number: NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission; DEPT-18, Employees Information not covered by other Notices. DEPT-25, Access Control and Identity Management System and GSA/GOVT-7, Personal Identity Verification Identity Management System.
	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 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: 1609-06 in the NOAA Disposition Handbook
	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.
X	No, retention is not monitored for compliance to the schedule. Provide explanation: Employee PII is generally kept on shared files of federal employees. These shares are access controlled and only

	available to the employee.

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

	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: Individuals (federal employees) may be identified.
X	Quantity of PII/BII	Provide explanation: There is the potential of PII collected and stored on 133 employees as well as contact information for constituents. NOAA6001 Users may be keeping on shared drives and computers an unknown amount of BII on companies who provided information as part of the acquisition process.
X	Data Field Sensitivity	Provide explanation: Data is sensitive but unclassified
X	Context of Use	Provide explanation: People or organizations provided their information voluntarily. .
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: NOAA6001 users keep information on access-restricted shared drives and/or encrypted laptops.
	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: Constituents database owners documented their business process related to the handling of PII as a result of the assessment. Also a Privacy Statement was added to the main page.
	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.

Information Kept in the System

	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.