Version Number: 01-2017

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 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: 2018.03.07 10:57:55 -05'00'

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

(a) *Whether it is a general support system, major application, or other type of system* - 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 is the general support system for NOS and stores PII on an ad-hoc basis if and when employees receive documentation 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. Other than this information, there are no applications or databases that collect or store employee PII.

(b) *System location* - Silver Spring, MD.

(c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)* – This is a standalone system.

(d) The way the system operates to achieve the purpose(s) identified in Section 4 – The information is kept in databases within applications except for the data that is kept on the shared drives.

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 – The business owner, Policy and Constituent Affairs Division (PCAD), 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.

- GovDelivery – This is an online communications tool that delivers public information of interest by email to customers of NOS. Customers submit their email addresses to NOS, which staff enter into GovDelivery for mail-outs. This information is kept within the system. Staff use this application to generate and send out newsletters and other materials.
- FedSelect – This is a tool that stores proprietary/source selection information, used in the ProTech Oceans Domain Source Selection. This includes, but is not limited to, industry's technical proposals, management schemes, price breakdowns, etc., as well as the Government's evaluation of this data. Its purpose is to record and store data. Source selection team members use FedSelect to review and record their evaluations of the proposals. It is also used by the team as a whole to generate consensus evaluations of proposals. FedSelect derives its legal authority to collect PII and BII from the FAR Subpart 15.2 – Solicitation and Receipt of Proposals and Information. FedSelect does not share any data in this system outside of NOAA. This application is going to be in production only for FY18. The data will be retained within the NOAA6001 boundary for up to five years post-award. The expected award date is 3-4th qtr. FY18.
- 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 employee provides the information in person directly to the LRA who returns the artifacts to the user and does not store images of them in the system. The LRA has posted a privacy act statement at the LRA station. The LRA provides a hard copy of the privacy act statement to each user to whom he grants access.

NOAA6001 has four websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies 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.

(e) *How information in the system is retrieved by the user* – The information is retrieved through an application user interface, except for the data that is kept on the shared drives.

(f) *How information is transmitted to and from the system* – the information in manually inputted into the system by the administrator or through a bulk upload from a spreadsheet.

(g) *Any information sharing conducted by the system* – None of the applications share PII outside of NOAA except that NOS employee information may be shared with Commerce and other federal agencies in case of a breach.

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information* - The general legislation supporting the system is 5 U.S.C.301, one of the statutes concerning government organization and employees.

From NOAA-11: 5 U.S.C. 301, Departmental Regulations and 15 U.S.C. 1512, Powers and duties of Department.

From DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

From DEPT-18: Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

From DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

From GSA/GOVT-7: 5 U.S.C. 301; Federal Information Security Management Act of 2002 (44 U.S.C. 3554); E-Government Act of 2002 (Pub. L. 107–347, Sec. 203); Government Paperwork Elimination Act (Pub. L. 105–277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD–12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

From OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

(i) *The Federal Information Processing Standards (FIPS) 199 security impact category for the system* - **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.
__X ___ 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): The FedSelect application introduces a level of BII we have not had before. This temporary system will be disabled this fiscal year. The data will be retained within the NOAA6001 boundary for up to five years post award. The expected award date is 3-4th qtr. FY18.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

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. 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	X	l. Vehicle Identifier	
m. Other identifying numbers (specify): military identification numbers; CAC electronic data interchange personal identifier (EDIP)					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

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	X
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education	X	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	
b. IP Address		d. Queries Run		f. Contents of Files	X
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	X
Telephone		Email	X		
Other (specify):					

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

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application			X		
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 Describe how the accuracy of the information in the system is ensured.

The administrators review user data at least annually through user audits. If the data is outdated, the email audit will return an undeliverable message and the user is scrubbed from the database. User can also reply that they would like to be removed from the system or use the unsubscribe function in the email. The contracting officer review users' data prior to inputting into the system and the user reviews their data at various points in the process.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 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			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	X
For civil enforcement activities	X	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			

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. GovDelivery - holds email addresses of customers who have requested information provided by the Communications and Education Division (CED) program. This information is inputted in the system's version and is kept within the system. Only NOAA6001 staff use this application to generate and send out newsletters and other materials. The public does not have access to this system. FedSelect is a tool that stores proprietary/source selection information, used in the ProTech Oceans Domain Source Selection. This includes, but is not limited to, industry's

technical proposals, management schemes, price breakdowns, etc., as well as the Government's evaluation of this data. Its purpose is to record and store data. Federal source-selection-team members use FedSelect to review and record their evaluations of the proposals. Federal users external to this system would have to sign a non-disclosure agreement to be given access. Access to external users is discouraged. Non-Federal users are not given access to this application. It is also be used by the team as a whole to generate consensus evaluations of proposals. FedSelect derives its legal authority to collect PII and BII from the FAR Subpart 15.2 – Solicitation and Receipt of Proposals and Information. FedSelect does not share any data in this system outside of NOAA.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

If users print information from the system, there is a chance that privacy data will be viewed if the document is left in plain sight.
There is a potential for unauthorized access to the system, which would expose non-sensitive PII to an unauthorized user.
Old data is purged from the systems at least annually.
Users take privacy training at least annually in the required annual security awareness course.
Users sign rules of behavior to ensure they understand their responsibilities.

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):			

***In case of breach.**

	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 for the Constituents Database can be found at: https://webdev.nos.noaa.gov/NOSConstituentsDB/statement.html.	
X	Yes, notice is provided by other means.	Specify how: Prospective employees are given notice through the USAJobs posting site and through contractor's HR offices. Employee security data for the LRA is provided by the employee in person at the desk of the LRA. COOP information is provided in hard copy form only to the users performing roles in the COOP function (ACIO, deputy ACIO, ISSO and CTO). It is expected that the booklet will be kept in a locked cabinet. Any employee data for the COOP is gathered from the employee on a voluntary basis when they agree to take the position. GovDelivery - A warning banner referencing FedRamp appears on the page displayed following the email submission by the customer. FedSelect - Notice on the use, maintenance, and dissemination of the information collected for each company is explained, with all applicable laws and statutes (including a Privacy Policy), in the Request for Proposals (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: **Constituents Database -** 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. **Federal AAMB users** - 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). 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. **GovDelivery** provides an unsubscribe function in every email it sends to users. Users can opt out at any time and any stage in the process. **FedSelect** – All information is provided on a voluntary basis to be part of competition. To not provide BII, the offeror simply chooses not to compete.
	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: **Federal AAMB users** - 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). **Federal Users with PII** - Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Constituents Database** - 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. **GovDelivery** provides the option to opt out of email delivery with a unsubscribe function on each email received. **FedSelect** - There is only one use of the data, and the user is well aware of it. Use of BII clearly described in the RFP. The offeror must submit all information requested in the RFP to be considered for award. Individuals named in the proposal have given permission for information to be used prior to the writing of the proposal.
	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: **Federal AAMB users** - 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). **Federal Users with PII** - Applicants for positions who have used the USAJobs system are able to review/update their information in the system. Applicants for positions applying through contractor companies can review their information through their companies. For ongoing employee business, such as travel, there is only one specific use for each PII collection. **Constituents Database** – The business owner audits their user list annually. At that time the users have an opportunity to review their information (email address) and request to be removed. **GovDelivery** provides the option to opt out of email delivery with a unsubscribe function on each email received. **FedSelect** - There is only one use of the data, and the user is well aware of it. Use of BII clearly described in the RFP. The offeror must submit all information requested in the RFP to be considered for award. Individuals named in the proposal have given permission for information to be used prior to the writing of the proposal.
	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: The **Constituents Database** has audit trails enabled. **Federal AAMB users** - 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. Policy indicates 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. **GovDelivery** has audit trails enabled **FedSelect** –has audit trails enabled
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, 2017. ☐ 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 controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
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. *(Include data encryption in transit and/or at rest, if applicable).*

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. 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. **GovDelivery** – NOAA6001 encrypts the database. **FedSelect** – NOAA6001 encrypts the database. Federal source-selection-team members use FedSelect to review and record their evaluations of the proposal. Federal users external to this system would have to sign a non-disclosure agreement to be given access. Access to external users is discouraged. Non-Federal users are not given access to this application.

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, number, and link. *(list all that apply)*: 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. DEPT-13, Investigative and Security Records. OPM/GOVT-1, General Personnel Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

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. However, employee PII is generally kept on shared files of federal employees. These shares are access controlled and only available to the employee.
	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 Level

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. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	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	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: There is some sensitive data fields for employees.
X	Context of Use	Provide explanation: People or organizations provided their information voluntarily. .
X	Obligation to Protect Confidentiality	Provide explanation: FedSelect - Per the FAR, Procurement Integrity Act, and Economic Espionage Act
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 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Minimal PII is collected. NOAA6001 collects only enough information to be able to provide users with the information they need to do business with us. Users provide their information voluntarily in order to be able to receive the information they request.

12.2 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.

12.3 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.