Version Number: 01-2017

# U.S. Department of Commerce
# NOAA


## Privacy Threshold Analysis
## for the
## NOS Enterprise Information System
## (NOAA6001)

# U.S. Department of Commerce Privacy Threshold Analysis

# NOS Enterprise Information System

# (NOAA6001)

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

**Introduction:**

(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 purpose that the system is designed to serve* – In addition to 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.
- 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 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. 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. The fields that include PII are encrypted at rest.

- 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 on the system.

(e) *The way the system operates to achieve the purpose* - 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

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.

*(f) A general description of the type of information collected, maintained, use, or disseminated by the system* - NOAA6001 systems collect non-sensitive PII and BII such as names, email addresses of individuals and businesses, financial information, and information related to hiring.

*(g) Identify individuals who have access to information on the system* – The users of the NOAA6001 systems that collect non-sensitive PII and BII are authorized government and contractor workers within the program office. These systems are not accessible to the general public

*(h) 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.

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

**Questionnaire:**

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

_X___ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

| **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. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

_X___ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

_X___ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

_X___ Companies
_X__ Other business entities - 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 this is financial information included with the acquisition package.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

***If the answer is "yes" to question 4a, please respond to the following questions.***

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X___ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

FedSelect – Is an application that enables contracting evaluators to document their strength, weakness, and deficiency comments and their ratings and rationale electronically in one data file. Allows contracting officers and specialists to monitor the progress of an evaluation and move directly from individual evaluations to consensus. This system may contain

GovDelivery is used to send newsletters and information about NOS to stakeholders. The system collects email addresses of recipients, but not names or addresses.

The Constituents' database collects limited PII from stakeholders involved with or interested in information provided by the National Ocean Service.

NOAA6001 collects and stores information related to the Office of the Assistant Administrator, Management and Budget (AAMB), which includes limited PII, specifically, names, telephone numbers and email addresses (voluntarily submitted by data providers and customers) to facilitate external coordination with data providers.

NOAA6001 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.

NOS has a Local Registration Authority (LRA) who 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.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

***If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.***

# CERTIFICATION

__X___ I certify the criteria implied by one or more of the questions above **apply** to the NOS Enterprise Information System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of Information System Security Officer (ISSO): Jason MacMaster

Signature of ISSO: MACMASTER.JASON.RICHARD.1096271197 Digitally signed by MACMASTER.JASON.RICHARD.1096271197 Date: 2018.01.30 12:01:33 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO): John D. Parker

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.01.30 07:43:35 -05'00' Date: _____

Name of Authorizing Official (AO): Paul Scholz

Signature of AO: SCHOLZ.PAUL.M.1365867239 Digitally signed by SCHOLZ.PAUL.M.1365867239 Date: 2018.01.30 08:22:55 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.30 12:36:23 -05'00' Date: _____