

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



**Privacy Impact Assessment
For the
NOAA1101 Information Technology Center
General Support System (GSS)**

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
Date: 2020.08.16 20:54:12 -04'00' 04/15/2020

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

Date

NOAA1101 General Support System (GSS) Privacy Impact Assessment

Unique Project Identifier: 006-48-01-01-01-3801-00

Introduction: System Description

NOAA1101 General Support System (GSS)

The NOAA1101 General Support System (GSS) is a High Value Asset (HVA) as designated by DHS, DOC and NOAA and is comprised of an interconnected set of information resources under the management and control of Service Delivery Division (SDD) within the NOAA Office of the Chief Information Officer (CIO).

NOAA1101 General Support System (GSS) provides Infrastructure as a Service (IaaS), Data Center Colocation, and Application Support Services that are instrumental to obtaining the objectives of the President's Management Agenda; achieving the goals of the Office of Management and Budget for effective and efficient Government; and NOAA's goal for excellence in the technical operational support of NOAA's financial, management, and administrative systems. Support activities of the GSS include direct, technical, and operational support of financial and administrative systems.

The NOAA1101 General Support System (GSS) boundary currently encompasses a primary site located at the NOAA Information Technology Center in Largo, Maryland and an alternate site in Fairmont, West Virginia. These sites house the following equipment:

- Layer 2/layer 3 Cisco Switches and fabric Extenders
- Fortinet Firewalls and IPS
- Citrix NetScalers
- F-5 Load Balancers
- Physical and virtual servers running
 - Solaris 11
 - Red Hat 7
 - Windows 2008/2012/2016
 - Oracle and SQL Databases

NOAA1101 General Support System (GSS) hosts Two (2) Major Applications, Commerce Business System (CBS) and Grants Online (GOL) along with a number of minor applications. Some of these applications are also comprised of a number of modules and interfaces.

System descriptions for these applications can be found in Appendix D System Environment Description in CSAM.

Major Applications

Commerce Business System (CBS)

CBS consists of the Core Financial System (CFS) interfaced with standard Commerce-wide administrative systems for procurement (C.Award), relocation (MLinqs - Permanent Change of Station (PCS) moves), labor cost distribution, NOAA data warehouse (NDW), and SAM /ABA (SAM /CCR).

CBS supports the NOAA integrated financial management system for NOAA and cross-serviced bureaus, EDA and Bureau of Industry and Security (BIS). No other DOC organizations obtain their Accounting Services from NOAA or have applications under this system.

CBS supports the financial functions required to track financial events, provide financial information important for the financial management of Commerce and its operating units, and required for the preparation of financial statements, and to allow Commerce to continue receiving clean financial audit opinions. NOAA CBS financial systems modules support: CFS, NOAA Permanent Change of Station (PCS – Mlinqs / Relocation Manager), and other reporting activities (NOAA Data Warehouse) that are unique to NOAA. The NOAA CBS is hosted in the NOAA Information Technology Center (ITC). The ITC is operated by the Office of the Chief Information Officer/Service Delivery Division (OCIO/SDD) Service Delivery and Hosting Services (SDHSB).

CBS enables Commerce and NOAA to meet the requirements of the Chief Financial Officers Act (CFOs Act) of 1990, P.L. 101-576; the Federal Managers' Financial Integrity Act of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.); and Office of Management and Budget (OMB) Circular A-127, Financial Management Systems. The authorities for these Systems of Records also apply:

This is a non-public system.

Access to this application is through the NOAA1101 General Support Systems (GSS) environment which is limited to authorized NOAA, BIS, and EDA staff.

Grants OnLine (GOL)

The Commerce Grants Online System provides grants management automation in support of grant application evaluation, award, and long-term management and operations processes. Specifically, Grants Online is a business workflow system that provides a standardized set of automated processes for viewing, retrieving, modifying, and deleting grants information including, applications, awards, amendments, audits, proposed scoring and commentary, progress and financial reports, as well as technical and panel peer review information. The Grants Online system electronically retrieves grant applications from Grants.gov for processing in the Grants Online system. It also interfaces with CBS, the Department's financial system of record. The system was designed to be scalable in an effort to accommodate future change and enhancements as the grants management processes and policy change. NOAA typically awards approximately \$1 billion in grants annually. In 2005, NOAA deployed Grants Online to its federal staff in an effort to streamline and automate the grants management process. In 2006 Grants Online was rolled out to NOAA's grant recipients for electronic award acceptance and post award management. Starting in FY 2008, the NOAA Grants Management Division (GMD) expanded its usage to other DOC bureaus including the Minority Business Development Agency (MBDA), the International Trade Administration (ITA), the Department of Commerce (DOC) Office of the Secretary/Office of Human Resources offices, and the National Telecommunication and Information Administration (NTIA). The Economic Development Administration (EDA) began using the system in FY 2014. The Census Bureau began using the system in FY 2016. The system has enabled rooms that were previously filled with stuffed file drawers floor to ceiling to be converted into offices and other more efficient use of space. Grants Online has also facilitated the ability for Commerce to meet its telework goals and has provided more transparency into the grants management process.

Minor Applications

Listed below are the minor applications that store PII or BII.

Archibus

Archibus is a facilities management software solution available in both Web-based and Microsoft Window-based platforms. The system, integrated with CAD design software, is currently used by FOD to manage space planning and personnel, equipment, on demand and preventive maintenance work at the National Capital Region (NCR) in Silver Spring, MD, Western Regional Center (WRC) in Seattle, WA, and Inouye Regional Center (IRC) in Honolulu, HI.

Common Access Card (CAC)

The Common Access Card web application assists CAO with processing CAC cards for NOAA's federal employees.

Damage Assessment Remediation Restoration Tracking System (DARRTS)

Damage Assessment Remediation and Restoration Tracking System is a financial tracking web application built for the NOAA National Marine Fisheries Service (NMFS), Office of Habitat Conservations (OHC), Habitat Restoration Division (HRD), Restoration Center (RC).

DARRTS helps plan estimates, and tracks actual costs for environmental restoration work required to repair coastal habitat after oil spills or hazardous waste releases.

Deep Water Horizon – LaserFiche (DWH)

The LaserFiche electronic records management system (ERMS) is the application used by the NOAA Damage Assessment Restoration and Remediation Program (DARRP) to manage federal records.

This system is not used to intentionally collect or store PII/BII. It is used by the DARRP to store and maintain substantive federal records related to natural resource damages assessment matters, as well as other (non-personnel related) program management aspects of the DARRP. There is a possibility that some records entered into the system may incidentally contain PII/BII, but this is unusual and not the purpose of the system.

Foreign National Registration System (FNRS)

FNRS was designed to provide sponsors (NOAA researchers) of Foreign National Guests (who conduct collaborative research, participate in field research activities, and perform other duties while guests of NOAA), controlled technology coordinators, and the Office of Security, a single location to enter the information required to obtain appropriate approvals for a visit. We collect FNRS information solely to meet the requirements set forth by NOAA and other Department of Commerce policies and regulations including NOAA Administrative Order (NAO) 207-12 "Technology Controls and Foreign National Access", Department Administrative Order (DAO) 207-12 Version Number: 01-2017 "Foreign National Visitor and Guest Access Program", and 15 Code of Federal Regulations (CFR) Parts 730-774, Export Administration Regulations, to sponsor a Foreign National Guest. Name, home email address, age, gender, race/ethnicity, date of birth, place of birth and passport number are collected. Sponsors do not share this information.

JustWare Case Management System

The NOAA JustWare system provides a solution for Case Tracking; Report Generation; Forms Generation; Document Storage and Management; Calendar Management; and interface with other existing NOAA databases (e.g. LEADS and, NOAA Finance). JustWare will improve NOAA's ability to gain its strategic goals and performance objectives and to achieve desired results and outcomes. JustWare also will improve NOAA's ability to comply with the Government Performance and Results Act (GPRA).

Management Analysis and Reporting System (MARS)

The Management Analysis and Reporting System (MARS) is a NOAA initiative to provide a reporting and querying facility and a commitment tracking facility that is common to all NOAA Line Offices. The Reporting and Querying Module is based on NWS' Business Objects Web Intelligence implementation and the Data Entry module is based on Oracle Application Server.

NOAA Reporting System (NRS)

The NOAA Reporting System is a windows application (web services) that transmit Common Access Card information from the Defense Enrollment Eligibility Enrollment System (DEERS) to NOAA and stores the information in an Oracle database for reporting purposes.

NOAA Rotational Assignment Program (NRAP)

NOAA Staff Directory (NSD)

The NOAA Staff Directory is a contact lookup and management system for NOAA. It allows for the public to look up basic contact information. It also allows internal users to access detailed contact information as well as add/remove relationships and users from the main NOAA directory.

OLA Members Outreach Database (MOD)

The Member Outreach Database web application bridges together and captures OLA's relationship building, service, and communication efforts with Congress. MOD provides the options for providing data in various formats to meet OLA's varying communications, planning, and reporting needs. MOD enhances OLA's, NOAA's, and the administrations service to Congress and allows us to communicate what the agency's priorities, concerns, and interests are with the varied congressional audiences. MOD also allows OLA to better communicate what Congress' priorities, concerns, and interests are back to NOAA, DOC, and the administration.

Operations Planning and Control System (OPCS)

OPCS is the EDA grant information, proposal processing and project tracking system. *The grant request forms are downloaded from Grants.gov.* The grant applications are reviewed to determine eligibility. Once the grant applicant is considered eligible, some of the information from the grant applications is entered in the OPCS application. This application consists of five (5) modules which are OPCS, Security, CBS Import, Federal Funding Accountability and Transparency Act (FFATA) and Congressional District Zip Codes. The OPCS module provides the capability to track the grant project from pre-application through approval to project closeout. OPCS combines proposal tracking documentation with a variety of other information about proposals, applications and approved projects, the areas in which they are located, and the proposed and actual impacts of such projects. The following are description of the supporting modules that are associated with OPCS:

SECURITY - System Security module grants appropriate access rights to groups of users and individual users based on login and password.

CBS Import – This module imports data from the NOAA CBS system. Files are manually exported from CBS and the module imports the required data for the OPCS database. The data that are tracked in OPCS are reservation, obligation, and disbursement.

FFATA - This module provides the capability to extract certain information from the OPCS database, allows the user to review the data for quality assurance, and provides the data in the format needed to meet the guidance provided by the Office of Management and Budget (OMB) for data submission to the USA Spending web site under the Federal Financial Accountability and Transparency Act (FFATA).

Congressional District Zip Codes - This module provides the capability to upload the congressional district data.

PII and BII are mainly data at rest. The PII and BII data are accessed only by EDA authorized users and not shared outside the programs.

The collection and maintenance of the PII and BII is authorized by the Public Works and Economic Development Act of 1965, as amended by the Economic Development Administration Reauthorization Act of 2004 (Pub. L. 108-373).

Recruitments Analysis Data System (RADS)

Telecom Expense Management Solutions (TEMS)

NOAA's Enterprise TEMS facilitates the management, ordering and billing, and inventory control. The comprehensive, lifecycle telecommunication system:

- Provides management of wireline, satellite and wireless services;
- Optimizes the provision of service rate plans for voice and data that guarantees the best possible pricing;
- Consolidates the ordering of equipment and services under one order;
- Leverages existing telecommunication devices;
- Provides multiple carriers and billing formats (i.e. EDI, Electronic download, paper, etc.); and

Provides multiple tiers of wireless devices, including Section 508 compliant devices, with Assistive Technology for people with disabilities.

Web EOC

WebEOC is used to communicate with NOAA staff in the event of an emergency and to send out alerts to staff when immediate and widespread information needs to be disseminated.

Section 1: Status of the Information System

1.1. New or Existing System

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.
- This is an existing information system with no new privacy risks.

(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
<input type="checkbox"/>	a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses
<input type="checkbox"/>	b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input checked="" type="checkbox"/>	h. Internal Flow or Collection
<input type="checkbox"/>	c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data
<input type="checkbox"/>	j. Other changes that create new privacy risks (specify):				

Section 2: Information in the System

2.1. Privacy Information Collected

Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated.

Identifying Numbers (IN)					
a. Social Security*	<input checked="" type="checkbox"/>	e. File/Case ID	<input type="checkbox"/>	i. Credit Card	<input type="checkbox"/>
b. Taxpayer ID	<input checked="" type="checkbox"/>	f. Driver's License	<input checked="" type="checkbox"/>	j. Financial Account	<input checked="" type="checkbox"/>
b. Employer ID	<input checked="" type="checkbox"/>	g. Passport	<input checked="" type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employee ID	<input checked="" type="checkbox"/>	h. Alien Registration	<input checked="" type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the SSN, including truncated form:					
<p>CAC: To process/provide CAC</p> <p>CBS/GOL: Financial account information and grant/loan applications require Tax ID Numbers. These could be either SSNs or EINs. In some cases, in NOAA1101, the Tax ID is an SSN</p> <p>MARS: Uses SSN# to identify employees</p> <p>AUTHORITIES: FFATA; Federal Managers' Financial Integrity Act of 1982; Federal Financial Assistance Management Improvement Act of 1999; 16 USC 6109(a)(4), 3402; 8 USC 1324a; 41 CFR 60-4.3, E.O. 11246.</p>					

General Personal Data (GPD)					
a. Name	<input checked="" type="checkbox"/>	g. Date of Birth	<input checked="" type="checkbox"/>	m. Religion	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	h. Place of Birth	<input checked="" type="checkbox"/>	n. Financial Information	<input checked="" type="checkbox"/>

c. Alias	X	i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	X
s. Other general personal data (specify):					

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	X	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):					
FNRS: Collects photos to positively identify the foreign national.					

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):					

2.2. PII and BII Sources

Indicate sources of the PII/BII in the system.

Directly from an 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	X	Foreign			
Other (specify)					

Non-government Sources – Loan or grant applicants					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3. Technologies that Contain PII

Indicate the technologies used that contain PII/BII in ways that have not been previously deployed.

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

There are no technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1. Activities that raise Privacy Concerns

Indicate IT system activities which raise privacy risks/concerns.

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1. Why information is Collected

Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.

Purpose			
To determine eligibility	X	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	X	For employee or customer satisfaction	X
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Details:			
<ol style="list-style-type: none"> 1. Payment processing via Treasury Financial Management System 2. Internal Revenue Service 1099 / W2 processing. 3. Loan administration. 4. Grant administration. 5. User Information 6. Employee Info, including locations, collected so that FOD can track work requests for service 			

Section 5: Use of the Information

5.1. How Information is Collected

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).

Archibus

Information regarding both federal employees and contractors stationed at NOAA campuses in Silver Spring, Seattle and Hawaii is collected in a spreadsheet and provided by each line office manager and manually entered in the system. Data is maintained by the ARCHIBUS Administrators and is used for space planning and management purposes, and to track on demand work requests. Employee location data is used to generate floor accountability rosters for emergency preparedness.

CBS

The CBS information is used to support the administrative and financial management requirements of NOAA, including, but not limited to, making payments to employees and vendors (members of the public). The information is used to ensure that financial transactions are conducted in a timely and correct manner, to protect against fraudulent transactions, and to generate and maintain financial management data adequate to meet acceptable accounting and auditing standards. Entitlement determination (in support of employee relocation / Permanent Change of Station (PCS)) and tax processing also require this information. The PII identified is for federal employees and Vendors / Contractors. BII is required for companies providing services to NOAA for payment processing via U.S. Department of Treasury.

Deep Water Horizon – LaserFiche

Federal records that are placed into the system may incidentally contain PII/BII; however, as noted above the collection and storage of PII/BII is not the purpose of the system. Records will be entered into the system by DARRP personnel when the individual custodian of the record deems that it is important enough to be retained for long term storage.

FNRS

The information collected in FNRS is used to obtain appropriate approvals for a foreign national visit. The information is collected from members of the public.

GOL

It's collected from application that are download from gratns.gov and that has been mailed to agency. The mailed applications are manually entered into the grants online.

MARS

An ETL tool, Informatica Power Center, extracts the subset of NOAA Data Warehouse (NDW) records that are pertinent to MARS. These extract jobs are currently intended to be run nightly Monday through Saturday, but are designed to be run at any time. Data extracted from the NDW is housed in a database called the Staging Area until the load is validated as complete and correct. The data validation process ensures that the extracted data matches the source data, and that the data will return correct results and is free of invalid data.

Data is extracted from the NDW, National Finance Center (NFC) files (HR), and other sources. The NDW pulls data from the production Online Transaction Processing (OLTP) systems and consolidates the data into simple transactional structures, such as AP Trans, BOP Detail, Allotment Detail, and aggregated financial balances. The NDW includes copies of the master data files, such as project, program, task, and object code information. Other data sources (Personal Property, Real Property, Acquisition Data, and Recruitment Analysis Data System) may be integrated into MARS.

MARS information is used to support the administrative and financial management requirements of NOAA. The PII identified is for federal employees. BII is required for companies providing services to NOAA.

NOAA Staff Directory (NSD)

Personal Phone Number and Email is collected for the Emergency Notification System (ENS) through the NSD web application.

OPCS

The PII and BII for OPCS is collected by the Grants.gov system. The forms are downloaded from Grants.gov. The required data are manually entered into OPCS by EDA users. Only the eligible grant applicant information is entered into OPCS. The information is collected and used to ensure that financial transactions are conducted in a timely and correct manner, to protect against fraudulent transactions. Information collected is from agencies or members of the State, Local, Tribal, and Universities.

TEMS

Information is collected directly from the individual. BII is collected related to contract and monthly invoices. Users can opt to use a database integration tool to automatically add or modify information. The system can:

- Automatically add large amounts of Bill and Circuit data
- Perform global changes to TEMS records
- Add data from legacy systems
- Import AP Data
- Update TEMS with employee termination and Line Office changes
- Automatically modify existing data
- Import Contract and Savings Discovered information
- Update database fields with new formats

Section 6: Information Sharing and Access

6.1. Sharing Information

Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the Bureau	X	X	X
DOC Bureaus	X	X	X
Federal Agencies (Treasury)		X	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. Sending and Receiving Information

Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

Yes, this system connects with or receives information from another system authorized to process PII/BII.

Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:

CBS

For purposes of payment and tax processing related to 1099s and W2 data for non-payroll related payments. NOAA CBS does not process payroll, or timecard data. WebTA is the DOC system for timecards and that system provides data to USDA /NFC. USDA/NFC process payroll and provide tax related information to Treasury; and payroll details to NOAA CBS.

CBS connects to and transfers data between the US Department of Treasury, Bureau of Fiscal Service. An encrypted VPN tunnel using AES-256 encryption is used to connect the NOAA1101 system to the Bureau of Fiscal Service and protect the PII/BII data.

GOL

Download information from Grants.gov.

Only cleared authorized users can gain access to PII/BII data; this helps to prevent leakage. This information is secured using SHA-2 Certificates and TLS v1.2.

Download information from Sam.gov.

Only cleared authorized users can gain access to PII/BII data; this helps to prevent leakage. This information is secured using SFTP.

Send information to CBS.

Only cleared authorized users can gain access to PII/BII data; this helps to prevent leakage. This information is secured using SHA-2 Certificates and TLS v1.2.

MARS

Data extracted from NDW and National Finance Center files using ETL.

NOAA Staff Directory

The NSD database schema provides access to MARS and NOAA Finance Office. MARS has Oracle account in NSD schema and accesses the data on a daily basis using ETL. NOAA Finance Office also has Oracle account in NSD schema – they have access to a view. This view contains SSNO. The Emergency Notification system gets their data through the NSD web application by logging into the system.

OPCS

Download information from Grants.gov.

Only cleared authorized users can gain access to PII/BII data; this helps to prevent leakage. This information is secured using SHA-2 Certificates and TLS v1.2.

No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

FNRS

TEMS

6.3. Access to Information

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. Notifications of Disclosure

Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system.

Yes, notice is provided pursuant to a system of records notice published in the Federal Register.

Yes, notice is provided by a Privacy Act statement and/or privacy policy.

Where is it:

GOL
The Privacy Act statement and/or privacy policy for Grants on Line can be found at: <https://grantsonline.rdc.noaa.gov>.

Yes, notice is provided by other means.

Specify how:

CBS
Information for personnel, and tax transactions and reports is provided to the employee when they are given the W-4 to complete. Also, general notice for other uses of CBS is provided in the Internal Revenue Code sections 3402(f)(2) and 6109: "Internal Revenue Code sections 3402(f)(2) and 6109 and their regulations require you to provide this information; your employer uses it to determine your federal income tax withholding." *The code references are included in the CBS training required for all users.*

GOL
Grants.gov
A specific Grants.gov notice is given in a privacy link on the initial screen of GRANTS.GOV, as part of the Grant application process. Also, on this page: <http://www.grants.gov/web/grants/applicants/organization-registration.html>, notice is given to organizations that they must provide an Employer ID Number (EIN).

SAM.GOV
<https://www.sam.gov/SAM/>
CBS
<https://cbs.rdc.noaa.gov/landing.html>

GOL

A GOL privacy act statement is also provided here:

http://www.corporateservices.noaa.gov/grantsonline/pdfs/Grants_Online_Privacy_Act_Statement.pdf

FNRS

Notice is provided on the web page through a link to the NOAA Privacy statement. Those foreign nationals using a form are provided notice on the form.

MARS

OPCS

A specific Grants. Gov. notice is given in a privacy link on the initial screen of Grants.gov, as part of the Grant application process. Also, on this page:

<http://www.grants.gov/web/grants/applicants/organization-registration.html>, notice is given to organizations that they must provide an Employer ID Number.

TEMS

Notice is provided by other means (i.e. User Account Form).

×

No, notice is not provided.

Specify why not:

Archibus

Employee data is used for space planning management, emergency preparedness purposes, and to provide service on work requests.

NOAA Staff Directory

No notice is provided.

7.2. Opportunity to Decline

Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

Yes, individuals have an opportunity to decline to provide PII/BII.

Specify how:

CBS

Employees may refuse to provide information, either verbally or in writing, to their HR contacts, but this information is required data as part of their employment, for processing payroll and tax forms.

Deep Water Horizon – LaserFiche

While the LaserFiche system is not used to collect PII/BII, the documents placed in the system that may incidentally contain PII/BII were presumably sourced from location where individuals were given the opportunity to decline.

GOL

Grantees may choose not complete required fields, but this will prevent consideration of their applications. Grantees are not required to enter taxpayer ID or DUNS numbers (the fields are not marked as required).

FNRS

Foreign National visitors/guests may decline to provide this information face to face or in writing, to the administrator, but they will not be given guest privileges.

NOAA Staff Directory

For the Emergency Notification System, the person email and phone number is optional. There are instructions on the NSD web page that informs the individual on how to opt-out.

OPCS

The individual may decline to provide the data on the Grants.gov forms, by not completing the fields. However, the individual must provide information on the form in order for the grant request to be processed.

TEMS

They agree to the terms by signing the User Account form.

No, individuals do not have an opportunity to decline to provide PII/BII.

Specify why not:

Archibus

Employee data is used for space planning management, emergency preparedness purposes, and to provide service on work requests.

MARS

Federal workers sign a privacy release pursuant to the Privacy Act of 1974 during on-boarding with NOAA and the Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

7.3. Consent to Use

Indicate whether and how individuals have an opportunity to consent to uses of their PII/BII.

Yes, individuals have an opportunity to consent to particular uses of their PII/BII.

Specify how:

CBS
Employees may decline, in writing to their supervisors, the use of their PII for payroll and taxes but the CBS – Treasury Fiscal Requirements Manual states that applicable information is required for processing payments.

Deep Water Horizon – LaserFiche
While the LaserFiche system is not used to collect PII/BII, the documents placed in the system that may incidentally contain PII/BII were presumably sourced from location where individuals were given the opportunity to decline.

GOL
When an individual or entity completes an application, he/she effectively gives consent for it to be used to determine whether he/she qualifies for a grant. There are no other uses for this information than the application itself.

FNRS
There is only one purpose for each information collection. Those who provide information via Web pages have a link to the NOAA Privacy Policy, which states that provision of the information implies consent to the stated use(s). For provision of information in person, the purpose of the information is stated by the NOAA staff person

NOAA Staff Directory
In the Emergency Notification System page on NSD, there are instructions for the individual to consent if they want their personal phone number displayed in our system. If so, ONLY logged in users to NSD will have access to this information.

OPCS
When an individual or entity completes an application, he/she effectively gives consent for it to be used to determine whether he/she qualifies for a grant. There are no other uses for this information than the application itself.

TEMS
Consent via the User Account Form and signature.

No, individuals do not have an opportunity to consent to particular uses of their PII/BII.

Specify why not:

Archibus
Employee data is used for space planning management, emergency preparedness purposes, and to provide service on work requests.

MARS
Federal workers sign a privacy release pursuant to the Privacy Act of 1974 during on-boarding with NOAA and the Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

7.4. Opportunity to Review/Update

Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

Yes, individuals have an opportunity to review/update PII/BII pertaining to them.

Specify how:

CBS

Employees may review/update information on their Employee Personal Page via the National Finance Center, while vendors can access the CCR to update their data, which then flows into CBS.

Deep Water Horizon – LaserFiche

While the LaserFiche system is not used to collect PII/BII, the documents placed in the system that may incidentally contain PII/BII were presumably sourced from location where individuals were given the opportunity to decline. NOAA does not have the ability to identify those individuals whose PII may be incidentally been collected, so there is no opportunity to update.

GOL

Applicants enter all PII at the time of completing the Grant application and it can be modified by contacting the GOL Help Desk which verifies updates against the SAM.gov before making the update in GOL.

FNRS

Users have limited access. Only users with a need to access the system as part of their duties and as approved by the appropriate authorizing official may directly access their data. Individuals with no access to the applicable database may request to review information and submit updates through secure means, with the person and office who collected their information originally.

NOAA Staff Directory

Individuals can log into NSD and view their Emergency Notification System info and make changes if necessary. We also have a 6-month validation that will navigate to the Emergency Notification System page upon logging into the NSD to allow the individual to repopulate the information.

OPCS

The grantee must contact the EDA point of contact to update the information.

TEMS

This can be achieved manually via a request from the user to review/update information.

No, individuals do not have an opportunity to review/update PII/BII pertaining to them.

Specify why not:

Archibus

Employee data is used for space planning management, emergency preparedness purposes, and to provide service on work requests.

MARS

Any updates of information must be made in the official systems such as OPM or NFC. MARS does not update official records.

Section 8: Administrative and Technological Controls

8.1. Controls

Indicate the administrative and technological controls for the system. *(Check all that apply.)*

All users signed a confidentiality agreement or non-disclosure agreement. (EDA systems, contractors only)

All users are subject to a Code of Conduct that includes the requirement for confidentiality.

Staff (employees and contractors) received training on privacy and confidentiality policies and practices.

Access to the PII/BII is restricted to authorized personnel only.

Access to the PII/BII is being monitored, tracked, or recorded.

Explanation:

NOAA ITC System Administrators identify the various logs on each supported system or devices that require monitoring to identify any security incidents as identified in ITC-IR-01 NOAA ITC Incident Response Policy, and ITC-AU-01 NOAA ITC Auditing Policy. The administrator implements automated alert monitoring tools that are set to send email alerts so the responsible administrator is notified of the problem immediately. Auditable events include logon (successful and failed), remote connections, audit log failures, and access violations at a minimum.

The information is secured in accordance with FISMA requirements.

Provide date of most recent Assessment and Authorization (A&A):

-OR-

This is a new system. The A&A date will be provided when the A&A package is approved.

The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.

NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).

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. Protection of Privacy Data

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

Access controls for authorized users are implemented on production systems through the use of the Common Access card, unique system usernames and passwords as well as database (application) usernames and passwords to authenticate each user. NOAA 800-53 rev 4 access controls are enforced for access to all applications. User accounts are obtained through the application account managers. Upon log-in the user is prompted to change his/her initially assigned password. For system accounts, the user is required to contact the NOAA1101 General Support System (GSS) account managers to receive his or her initial password.

Currently, all individuals at NOAA and the various NOAA centers utilizing NOAA subsystems are in possession of a Homeland Security Presidential Directive 12 (HSPD-12) compliant NOAA Identification Card. This verification of personal information is utilized to generate and validate via the HSPD-12 chip used in each card. HSPD-12 cards/Common Access Cards (CACs) are manufactured for individuals whose personal information has been validated by a background investigation conducted by the NOAA Office of Security Division. CAC readers are installed on all Corporate Services Local Area Network (CORPSRV) domain member workstations and servers. All ITC support personnel have valid CACs and are required to utilize the CACs as part of the two-factor authentication to access CORPSRV domain workstations and servers.

This process is also additionally supplemented by two factor authentications utilizing the Virtual Private Network (VPN) Server, RSA* tokens and other factors for remote administration and log on. At this point in time, all NOAA systems utilized are in process of being provided card readers for the HSPD-12 compliant ID Cards.

Users or processes acting on behalf of users are uniquely identified through user accounts. Password authentication is in place and required for all user accounts, applications, and system access. This level of authentication meets NIST Special Publication 800-63 guidance. Passwords must adhere to current NOAA guidelines (minimum length, aging, history, combination of character types, etc.) before access is granted.

Access logs are kept and reviewed for any anomalies.

CBS data is encrypted at rest, in an Oracle Table Space.

*This is a brand, not an acronym.

FNRS

Encryption at rest - Data is encrypted (storage, laptops and backup media).

Access management control - Only users with authorization may access the data.

The activities of users are tracked through audit logs and monitoring.

Transmission - certificate used to access the web interface.

UMS files are shared via Google Drive (https:)

Any files shared with non NOAA federal recipients are shared via Accellion.

The levels of implementation for these technologies meet the criteria required by NIST 800-53, Rev 4 under the following controls: Access Enforcement (AC-3), Separation of Duties (AC-5), Least Privilege (AC-6), Remote Access (AC-17), User-Based Collaboration and Information Sharing (AC-21), Auditable Events (AU-2), Audit Review, Analysis, and Reporting (AU-6), Identification and Authentication (Organizational Users) (IA-2), Media Access (MP-2), Media Marking (MP-3), Media Storage (MP-4), Media Transport (MP-5), Media Sanitization (MP-6), Transmission Confidentiality (SC-9), Protection of Information at Rest (SC-28), Information System Monitoring (SI-4).

Section 9: Privacy Act

9.1. System of Record Notice (SORN)

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.”

Yes, this system is covered by an existing system of records notice (SORN).

Provide the SORN name and number (*list all that apply*):

<u>COMMERCE/DEPT-1:</u>	Attendance, Leave, and Payroll Records of Employees and Certain Other Persons is an applicable SORN. Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C. 3101, 3309.
<u>COMMERCE/DEPT-9:</u>	Travel Records (Domestic and Foreign) of Employees and Certain Other Persons. Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.
<u>COMMERCE/DEPT-2:</u>	Accounts Receivable. 5 U.S.C. 5701-09; 31 U.S.C. 951-953, 4 CFR 102.4, FPMR 101-7; Treasury Fiscal Requirements Manual.
<u>OPM GOVT-1:</u>	General Personal Records. 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Order 9397 as amended by E.O.13478, E.O 9830, and E.O. 12107,
<u>COMMERCE/DEPT-13:</u>	Investigative and Security Records.
<u>COMMERCE/DEPT-18:</u>	Employees Personnel Files Not Covered by Notices of Other Agencies

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. Records Control Schedule

Indicate whether these records are covered by an approved records control schedule and monitored for compliance.

(Check all that apply.)

There is an approved record control schedule.

Provide the name of the record control schedule:

CBS

NOAA Records Management Handbook Chapter 400, specifically Section 404-11 Accounting Files.

FNRS

Chapter 100 – General
Chapter 200 - Administrative and Housekeeping Records
Chapter 1500 - Marine Fisheries
NOAA 1504-11
NOAA 1513-01
NOAA 1514-01
NOAA 1516-01
NOAA 1517-01

Deep Water Horizon – LaserFiche

NOAA Record schedules, Chapters 100, 1500 and 1600.

OPCS

The General Record Retention schedule is used. For BII and PII, the record control schedule is EDA DAA-0378-2014-0413.

TEMS

The General Record Retention schedule is used.

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:

Archibus

Held preliminary discussions with NOAA Records Manager (Andre Sivels). In the process of additional conversations to establish this process.

GOL

A records control schedule will be developed and submitted to NARA for approval. Pending the development and approval of a schedule by NARA, the electronic grants records must continue to be retained.

Yes, retention is monitored for compliance to the schedule.

No, retention is not monitored for compliance to the schedule.

Provide explanation:

GOL does not yet have a records schedule.

10.2. Disposal

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 SP 800-122 PII Confidentiality Impact Levels [NEW]

11.1. Impact of Disclosure

Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

LOW

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

MODERATE

The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

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. Determination Factors

Indicate which factors were used to determine the above PII confidentiality impact levels.

(Check all that apply.)

Identifiability

Provide explanation:

CBS

Collects personal information for employees, vendors, and customers.

GOL

Collects personal information from customers.

FNRS

The data collected is enough to identify an individual.

MARS

Collects and stores the following groups of PII information: Identifying Numbers (Social Security, Employee ID...), General Personal Data (Name, Gender, Age, Race/Ethnicity...), Work-Related Data (Job Title, Grade, Email, work related travel...), System Administration/Audit Data (User ID, Date/Time of Access, Queries Run...).

PII information for employees, vendors, and customers is collected.

NOAA Staff Directory

PII information is for employees to be used for emergency notifications.

Quantity of PII

Provide explanation:

CBS

Collects a moderate amount of PII.

Deep Water Horizon – LaserFiche

Occurrences of PII in the ERMS are rare/accidental and incidental to the system’s mission.

GOL

Grants Online collects a minimal amount of PII/BII.

MARS

MARS collects a moderate amount of PII

OPCS

Include a few PII data fields.

Data Field Sensitivity

Provide explanation:

Archibus

None of the data stored is Sensitive PII/BII.

CBS

Contains sensitive PII and BII.

Deep Water Horizon – LaserFiche

The only PII that may predictably be in the ERMS are the occasional inadvertent inclusion of an individual’s personal phone number or email address, and these occurrences are extremely rare.

FNRS

Some of the data requested contains information such as SSN that could be exploited for financial gain (this includes permit and loan applications).

Grants Online

Contain sensitive BII.

MARS

MARS contains sensitive PII and BII

OPCS

Contain sensitive BII.

Context of Use

Provide explanation:

CBS

Uses PII to support payment processing and tax reporting.

Deep Water Horizon – LaserFiche

These records are not regularly “used” in daily operations. Rather, the ERMS is generally used for long term storage of federal records.

	<p>MARS MARS PII information is used to support payroll, personnel forecasting, travel analysis, payment processing, and financial reporting.</p> <p>GOL Uses PII to assist with determining an applicant's financial integrity.</p>
<p><input checked="" type="checkbox"/> Obligation to Protect Confidentiality</p>	<p>Provide explanation:</p> <p>FNRS The Privacy Act of 1974 requires us to safeguard the collection, access, use, dissemination and storage of BII and PII.</p> <p>Grants Online The Privacy Act of 1974 requires us to safeguard the collection, access, use, dissemination and storage of BII and PII.</p>
<p><input checked="" type="checkbox"/> Access to and Location of PII</p>	<p>Provide explanation:</p> <p>Archibus Application is located in NOAA server, and access is restricted to approved users.</p> <p>Deep Water Horizon – LaserFiche A very small group of individuals would have access to most records, and those individuals will almost always be the ones who put the information into the ERMS in the first place.</p> <p>FNRS Data is encrypted at rest and access is restricted.</p> <p>Grants Online Data is encrypted at rest and access is restricted.</p>
<p><input checked="" type="checkbox"/> Other:</p>	<p>Provide explanation:</p> <p>TEMS Data stored regarding an individual is public information.</p> <p>The confidentiality rating is based on the type of information collected and the risk levels associated as outlined in FIPS-199. The information for each application is stored separately, encrypted at rest, and access control for authorized users strictly enforced. Based on the segregability of the data, the risk of disclosure is mitigated, thus allowing a confidentiality impact assessment of Moderate.</p>

Section 12: Analysis

12.1 Business Process Changes

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.

No, the conduct of this PIA does not result in any required business process changes.

12.2 Technology Changes

Indicate whether the conduct of this PIA results in any required technology changes.

Yes, the conduct of this PIA results in required technology changes.

No, the conduct of this PIA does not result in any required technology changes.