Version Number: 01-2020

U.S. Department of Commerce
National Oceanic & Atmospheric Administration

Privacy Impact Assessment
for the
NOAA1101
Information Technology Center

Reviewed by: Mark H. 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

Jennifer Goode

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

07/01/2021

Date

Version Number: 01-2020

U.S. Department of Commerce Privacy Impact Assessment
NOAA/OCIO/Information Technology Center

Unique Project Identifier: NOAA1101

Introduction: System Description

NOAA1101 is a High Value Asset (HVA) as designated by DHS, DOC and NOAA and consists 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 (OCIO).

NOAA1101 provides Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Application Support Services. These services 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 General Support System include direct, technical, and operational support of financial and administrative systems.

NOAA1101 hosts Two (2) Major Applications, Commerce Business System (CBS) and Grants Online (GOL) along with a number of minor applications and legacy databases for applications that are no longer in use. Some of these applications also consist of a number of modules and interfaces.

NOAA1101 manages a combination of Physical and Virtual servers running:
- Solaris
- Red Hat
- Windows
- ESXi VMWare
- Citrix XenApp
- Oracle and SQL Databases

NOAA1101 hosts Major and Minor Applications and stores data at the following locations:
- EDC-Ashburn Facility 21635 Red Rum Drive; Ashburn, VA 20147
- West Virginia High Tech Consortium (WVHTC) VERTEX Building 1000 Galliher Drive Fairmont, WV 26554
- Amazon Web Service (AWS)

The EDC-Ashburn Facility, under NOAA0520, acts as:
- The Primary Processing and Storage site for the NOAA1101 General Support System (GSS) and any Minor Applications that are not hosted in the cloud;
- The Primary Processing and Storage site for Grants Online (GOL); and
- The Alternate Processing and Backup Storage Site for the Commerce Business System (CBS) Application.

The WVHTC - Fairmont Facility, under NOAA0520 acts as:
- The Alternate Processing site for the NOAA1101 General Support System (GSS) and any Minor Applications that cannot be hosted in the cloud; and
- The Alternate Processing site for Grants Online (GOL); and
- The Primary Processing and Storage Site for the Commerce Business System (CBS) Application.

Amazon Web Service (AWS) S3 is the Backup Storage site for NOAA1101 General Support System (GSS), GOL and the Minor Applications.

Amazon Web Service (AWS) will be used to extend NOAA1101 Hosting Services to provide VM Hosting and Cloud Native Services.

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).

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 Facilities Operations Division (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.

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 DOC policies and 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.

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 transmits 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 Staff Directory (NSD)
The NOAA Staff Directory is a contact lookup and management system for NOAA. It allows 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.

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.

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system

NOAA1101 is a General Support System.

(b) System location

- EDC-Ashburn Facility, Ashburn, VA
- West Virginia High Tech Consortium (WVHTC), Fairmont, WV
- Amazon Web Service (AWS)

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

NOAA1101 has interconnections with the following NOAA systems:

- NOAA0201 – Web Operation Center
- NOAA4000 – Fisheries WAN Enterprise Services
- NOAA8223 – Consolidated Logistics Systems
- NOAA8884 – NWS Southern Region Fort Worth

NOAA1101 General Support System (GSS) has interconnections with Non-NOAA systems to support the missions of applications we host. The data is pushed and or pulled using an encrypted connection and is stored on a database where it is accessed by the applications using a secured connection using HTML, SFTP or SSH. All connections require the use of a VPN connection. We have interconnections with the following Non-NOAA systems:

- DOC C-Suites
- DOC CWT Sato Travel
- DOC Security Manager
- DOC SmartPay 3
- Grants.gov
- HCHB Net
- NIST
- Treasury Department
- USDA NFC

(d) The way the system operates to achieve the purpose(s) identified in Section 4

The system operates in the traditional client server model. Data is hosted on servers and made available via various protocols such as HTTPS, SFTP, and SSH. Users need to VPN into the system.

(e) How information in the system is retrieved by the user

Information hosted in NOAA1101 is retrieved by the Major and Minor applications via various protocols such as HTTPS, SFTP, and SSH. Users need to VPN into the system.

(f) How information is transmitted to and from the system

Information is transmitted to and from the NOAA1101 using an encrypted connection such as HTTPS, SFTP, and SSH. Users need to VPN into the system.

(g) Any information sharing conducted by the system

Archibus: Information regarding both federal employees and contractors stationed at NOAA campuses in Silver Spring, MD (Silver Spring Metro Center) and Honolulu, Hawaii is collected via the NOAA Personnel Certification application where personnel access their individual record using CAC authorization or Google authentication. Information regarding both federal employees and contractors stationed at Seattle, is collected manually and manually entered in the system. Data is maintained by the ARCHIBUS Administrators.

Commerce Business Systems (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 PII identified is for federal employees and Vendors / Contractors. BII is required for companies providing services to NOAA for payment processing via the U.S. Department of Treasury.

Common Access Card (CAC/NRS): NOAA collects PII data from DEERS and it is used to process applications for CACs for federal employees. Non PII portion of CAC data is used to determine who has a CAC and expiration data and statistical reporting.

Deep Water Horizon – LaserFiche: Federal records that are placed into the system may incidentally contain PII/BII; however, 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.

Foreign Nationals Registration System (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.

Grants Online (GOL): Information is collected from applications that are downloaded from grants.gov or that have been mailed to agencies by those who are applying for Grant funds. These include individuals from academia, small business and the general public. The mailed applications are manually entered into the grants online. Look-up data feed is from SAM.gov.

Management Analysis and Reporting System (MARS): Data is extracted from the NOAA Data Warehouse (NDW), National Finance Center (NFC) files (HR), and other sources. 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 (EDA): 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. Information collected is from agencies or members of the State, Local, Tribal, and Universities.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

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.

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.

15 Code of Federal Regulations (CFR) Parts 730-774, Export Administration Regulations; NOAA Administrative Order (NAO) 207-12 "Technology Controls and Foreign National Access", and Department Administrative Order (DAO) 207-12 Version Number: 01-2017 "Foreign National Visitor and Guest Access Program"

Public Works and Economic Development Act of 1965, as amended by the Economic Development Administration Reauthorization Act of 2004 (Pub. L. 108-373).

Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C. 3101, 3309.

Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.

5 U.S.C. 5701-09; 31 U.S.C. 951-953, 4 CFR 102.4, FPMR 101-7; Treasury Fiscal Requirements Manual.

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

(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.
_____ 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):					

_____ 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.

__X__ 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 01-2017).

_____ 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 01-2019 or later).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License		j. Financial Account	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	X
c Employer ID	X	h. Alien Registration	X	l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:
Common Access Card (CAC): To process and provide the CAC.

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.

MARS: Uses SSN# to identify employees.

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	
c. Alias	X	j. Home Address	X	q. Military Service	
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	X
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color	X	l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color	X	m. DNA Sample or Profile	
d. Video Recording		i. Height	X	n. Retina/Iris Scans	
e. Photographs	X	j. Weight	X	o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	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	X	Email	X		
Other (specify): **Common Access Card (CAC):** PII is retrieved directly from the System of Record (DEERS or Security Manager).					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
Other (specify): **Common Access Card (CAC/NRS):** PII is retrieved directly from the System of Record (DEERS or Security Manager).					

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

2.3 Describe how the accuracy of the information in the system is ensured.

Archibus: Archibus information is entered by the owner of the information and verified quarterly or biannual basis.

Commerce Business Systems (CBS): CBS performs quarterly and an annual assessment of the integrity of the accounting system data. Annually, as part of its FY Close process, this financial assessment ensures that system integrity remains valid in order to support the Stage 3 close process.

Deep Water Horizon – LaserFiche: Collection of PII/BII is not an intended use of the system, so there is no mechanism to verify that information. This is an archive of documents related to Deep Water Horizon.

F**oreign Nationals Registration System (FNRS)**: Most data is captured electronically through website page visits. Processes in the System Development Lifecycle ensure there are data integrity checks to ensure valid data is entered into the system. Database constraints include Primary and Foreign Keys, Referential Integrity Constraints and Check Constraints.

Grants Online (GOL): Grants Online verifies BII against SAM.gov to ensure the accuracy.

Management Analysis and Reporting System (MARS): Before presenting data to the MARS users, the MARS Administrators first validate data loaded into the MARS data warehouse to make sure that the data will return the correct results and is free of invalid data. This data validation process is performed on a daily basis.

The MARS Data Warehouse validation procedure consists of the following checks to identify potential data problems:
Comparison of key metrics – Comparing key metrics such as Dollars and FTE between the detailed and aggregated tables in the MARS Data Warehouse and the data sources ensure that all of the data that should have been loaded into the MARS Data Warehouse actually were loaded.
Comparison of report results – Matching the results of reports run from the newly loaded data with that of a report in the source provides another useful, higher-level check of the data. It is absolutely essential to compare identical datasets when employing this test.

Validation of the MARS Data Warehouse is divided into two types, referred to as the type 1 and type 2 validation procedures:

Type 1 validation consists of comparing dollars and FTE totals in the MARS Data Warehouse detailed and aggregated tables against the dollars and FTE totals in the data sources.

Type 2 validation consists of comparing reports from the MARS Data Warehouse to similar reports in the main data source the NOAA Data Warehouse.

NOAA Staff Directory (NSD): Currently new records and separations are added or removed respectively to the NOAA Staff Directory (NSD) through our hourly sync with ICAM. All updates comes directly from the NOAA community or by the individual themselves. Any changes made to the individual's entry will receive an email notification of the changes and who made the change.

OPCS (EDA): The application has two signature review processes for confirming data accuracy and approval of the grant. In addition, EDA headquarters have staff members that review the data for accuracy before the reports are provided to EDA upper management and constituents.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0648-0538
	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 not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

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

Section 4: Purpose of the System

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

(Check all that apply.)

Purpose			
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	
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)	

Other (specify):

Archibus
1. User info collected for access
2. Employee info, including locations, collected so that FOD can track work requests for service.

Common Access Card (CAC/NRS)
1. Payment processing via Treasury Financial Management System
2. Internal Revenue Service 1099 / W2 processing.
3. Loan administration.
4. Grant administration.

Commerce Business Systems (CBS)
1. Payment processing via Treasury Financial Management System
2. Internal Revenue Service 1099 / W2 processing.
3. Loan administration.
4. User Information

Grants Online (GOL)
1. Grant administration.
2. To determine eligibility

OPCS (EDA)
1. Payment processing via Treasury Financial Management System
2. Internal Revenue Service 1099 / W2 processing.
3. Grant administration.

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).

Archibus: Information regarding both federal employees and contractors stationed at NOAA campuses in Silver Spring, MD (Silver Spring Metro Center) and Honolulu, Hawaii is collected via the NOAA Personnel Certification application where personnel access their individual record using CAC authorization or Google authentication.

Information regarding both federal employees and contractors stationed at Seattle, is collected manually 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.

Commerce Business Systems (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 the U.S. Department of Treasury.

Common Access Card (CAC/NRS): NOAA collects PII data from DEERS and it is used to process applications for CACs for federal employees. Non PII portion of CAC data is used to determine who has a CAC and expiration data and statistical reporting.

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.

Foreign Nationals Registration System (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.

Grants Online (GOL): Information is collected from applications that are downloaded from grants.gov and that have been mailed to agencies. The mailed applications are manually entered into the grants online. Look-up data feed is from SAM.gov.

Management Analysis and Reporting System (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 (EDA): 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.

5.2 Describe any potential threats to privacy, such as insider threat, 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.)

While there is a possibility of Insider Threat, All NOAA users receive annual Security Awareness Training that includes Insider Threat Training.

Archibus: There are no foreseeable risks to privacy. At the application level, ARCHIBUS leverages role-based access controls, as well as strong user account IA controls. The ARCHIBUS application comes with built in role-based access controls as a COTS product which are applied to meet NOAA business needs. Accounts of departed users are promptly deactivated by ARCHIBUS Administrators. Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.

Common Access Card (CAC/NRS): Encrypting data at rest and in transit. Annual IT Security Training. Annual Records Management Training.

Commerce Business Systems (CBS): There are no foreseeable risks to privacy. At the application level, CBS leverages role-based access controls, as well as strong user account IA controls.

Deep Water Horizon – LaserFiche: Any PII/BII stored in the system will be minimal and inadvertently collected. Other identifiable information will generally be work-related contact information, e.g., as listed in a signature block on a document/email or an email address. Accordingly, any privacy threat is minimal. The system has an automated process for purging information pursuant to federal records schedules.

Foreign Nationals Registration System (FNRS): There is mandatory security awareness training for all system users. All data is encrypted and role-based, access control to data is restricted to authorized, authenticated, users.

Grants Online (GOL): IT Security Awareness and Privacy Training; Quarterly Grants Online system training as per user role; and Training Webinars.

Management Analysis and Reporting System (MARS): No user will be granted access to MARS until the User Access Request form, MARS Non-Disclosure form and Rules of Behavior have been signed and completed.

Users are also required to complete the annual IT Security Awareness Training Course in order to continue to use NOAA computing resources.

MARS Administrators will report all IT security related incidents to the NOAA CIRT (N-CIRT).

NOAA Staff Directory (NSD): Annual IT Security Training

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	X	X
DOC bureaus	X	X	X
Federal agencies	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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII. CAC/NRS Commerce Business Systems (CBS) Grants Online (GOL) NSD
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities. Archibus Deep Water Horizon – LaserFiche Foreign Nationals Registration System (FNRS) Management Analysis and Reporting System (MARS) OPCS (EDA)

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

X	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: NOAA1101 have the following NOAA-to-NOAA connections that are used to support the applications listed below. NOAA0201 – Web Operation Center NOAA4000 – Fisheries WAN Enterprise Services NOAA8223 – Consolidated Logistics Systems NOAA8884 – NWS Southern Region Fort Worth External connections include: DOC C-Suite, DOC CWT Sato Travel, DOC Security Manager, DOC SmartPay 3, Grants.gov, HCHB Net, NIST, U.S. Treasury Dept, and USDA NFC **Common Access Card (CAC):** Security Manager (DOC) and DMDC's DEERS. At NOAA, data is encrypted at rest and when transmitted.

	Commerce Business Systems (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. **Grants Online (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. **Management Analysis and Reporting System (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 an Oracle account in NSD schema and accesses the data on a daily basis using ETL. NOAA Finance Office also has an 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 (EDA):** OPCS connects with NOAA CBS instance. Manually 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.
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. Archibus Deep Water Horizon – LaserFiche Foreign Nationals Registration System (FNRS)

6.4 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 and/or privacy policy can be found at: **GOL** The Privacy Act statement and/or privacy policy for Grants on Line can be found at: https://grantsonline.rdc.noaa.gov.	
X	Yes, notice is provided by other means.	Specify how: **Commerce Business Systems (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.* **Foreign Nationals Registration System (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. Users are notified that photographs may be taken at organizational events. Notice is either provided by posting notice in the area where photographs will be taken or verbally/in writing of occasions where photos may be taken. **Grants Online (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** www.sam.gov **GOL** A GOL privacy act statement is also provided here:

		http://www.corporateservices.noaa.gov/grantsonline/pdfs/Grants_Online_Privacy_Act_Statement.pdf **Management Analysis and Reporting System (MARS):** Notice is provided on the applicable personnel forms. **NOAA Staff Directory (NSD):** On the NSD ENS page, there is written information displayed that the data will be shared to ENS. **OPCS (EDA):** 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: Organization Registration | GRANTS.GOV, notice is given to organizations that they must provide an Employer ID Number.
	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: **CAC/NRS:** Data is collected when the individual applies for and accepts employment at NOAA. The individual can decline to provide their PII in which case this information will not be entered in the Security Manager system nor will it be transmitted to DEERS. However, this may affect their employment. **Commerce Business Systems (CBS):** Employees may refuse to provide PII, 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 and could affect their employment. **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. **Foreign Nationals Registration System (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. **Grants Online (GOL):** Grantees may chooses not to submit the application if they intend not to provide PII/BII information. **Management Analysis and Reporting System (MARS):** 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. **NOAA Staff Directory (NSD):** 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 (EDA):** 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.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not **Archibus:** Employees do not have the opportunity to decline to provide PII. Employee data is used for space planning management, emergency preparedness purposes, and to provide service on work requests.

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: **CAC/NRS:** Data is collected when the individual applies for and accepts employment at NOAA. There is only one use for the PII and while the individual can decline consent to use their PII, this information would not get entered in the Security Manager system nor will it be transmitted to DEERS and they would not be issued a CAC. **Commerce Business Systems (CBS):** Employees have the opportunity to consent in writing to particular uses of their PII. However, the CBS – Treasury Fiscal Requirements Manual states that applicable information is required for processing payroll and tax information. **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 consent to particular uses of their PII. **Foreign Nationals Registration System (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.

		Grants Online (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. **Management Analysis and Reporting System (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. **NOAA Staff Directory (NSD):** 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 (EDA):** 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.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: **Archibus**: Employees do not have the opportunity to consent to particular uses of their PII as there is only one use for this information. Employee data is used for space planning management, emergency preparedness purposes, and to provide service on work requests.

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: **CAC/NRS:** Employees and contractors submit updated information to the Security Manager servicing their account at the time their CAC is being renewed. **Commerce Business Systems (CBS):** Employees may review/update information on their Employee Personal Page via the National Finance Center, while vendors can access the SAM/CCR to update their data, which then flows into CBS. **Foreign Nationals Registration System (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. **Grants Online (GOL):** Grantees can update the BII at SAM.gov and review it at grants online. **NOAA Staff Directory (NSD):** Individuals can log into the NSD and view their Emergency Notification System (ENS) info and make changes if necessary. We also have a 6-month validation that will navigate to the ENS page upon logging into the NSD to allow the individual to repopulate the information.

		OPCS (EDA): The grantee must contact the EDA point of contact to update the information.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: **Archibus:** Employees do not have the opportunity to review or update their PII for logistical purposes. Employee data is used for space planning management, emergency preparedness purposes, and to provide service on work requests. **Management Analysis and Reporting System (MARS):** Any updates of information must be made in the official systems such as OPM or NFC. MARS does not update official records **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 have been incidentally collected, so there is no opportunity to update.

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. Commerce Business Systems (CBS) Foreign Nationals Registration System (FNRS) Management Analysis and Reporting System (MARS) EDA is not part of NOAA1101 but the contractors do sign an NDA to access CBS applications
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: DOC identifies the types of logs each system or devices is required to monitor in their Information Technology Security Baseline Policy. NOAA1101 sends all audit logs to ArcSight. ArcSight has filters configured to monitor various parameters to identify any security incidents or potential security incidents in accordance with NCSC Auditing and Incident Response Policies and Procedures.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 7/6/2020 ☐ 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 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 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 DOC ownership rights over data including PII/BII.

X	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).*

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 login 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 and GOL PII/Privacy Act data is encrypted at rest, in an Oracle Encrypted Tablespace.

*This is a brand, not an acronym.

Archibus
At the application level, ARCHIBUS leverages role based access controls, as well as strong user account IA controls. The ARCHIBUS application comes with built in role based access controls as a COTS product which are applied to meet NOAA business needs. User accounts are managed and secured through Keycloak, another COTS product provided by Red Hat.

Management Analysis and Reporting System (MARS): PII is encrypted by the ITC during data dissemination, data extraction, and transmission.

Other protocols and techniques used to hide privacy data within MARS:

Users who don't have access to privacy data: the Business Objects security model allows us to hide reports with privacy for users who don't have access to privacy data. Moreover, in the Business Objects universes, folders with privacy data are hidden to those users.

We have implemented a combination of row level restriction (restriction based on the user's Org Code) and

column level restriction (to restrict database columns containing PII/BII information), using a security database table and the row level security feature in the Business Objects Universe Designer tool, to address the following scenarios:
Users are allowed to see privacy data only for a list of LOs/FMCs/Org Codes: privacy data for organizations other than the list of allowed LOs/FMCs/Org Codes will be displayed as "RESTRICTED" on the MARS reports.
Users allowed to see privacy data only for their home FMCs (FMCs they belong to), and at the same time they can access non-privacy data only for a specific list of LOs/FMCs: privacy data for organizations outside of their home FMCs will be displayed as "RESTRICTED" on the MARS reports.

Within the Data Entry Module for DB Storage, we use encryption for SSN.
There are also Oracle DB roles to access restricted information.
On the Data Entry site, Java Spring Framework security is used and we have implemented Java HTML5.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

__X___ Yes, the PII/BII is searchable by a personal identifier.

_____ No, the PII/BII is not searchable by a personal identifier.

9.2 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)*: COMMERCE/DEPT-1: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons. COMMERCE/DEPT-9: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons. COMMERCE/DEPT-2: Accounts Receivable. OPM GOVT-1: General Personal Records. COMMERCE/DEPT-13: Investigative and Security Records. COMMERCE/DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-25, Access Control and Identity Management System
	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: Chapter 100 – General Chapter 200 - Administrative and Housekeeping Records Chapter 300 - Personnel Chapter 400 - Finance, specifically Section 404-11, Accounting Files Chapter 700 - Procurement Supply and Equipment Maintenance Chapter 900 - Facilities Security & Safety Chapter 1500 - Marine Fisheries NOAA 1504-11 NOAA 1510-01 NOAA 1510-02 NOAA 1513-01 NOAA 1514-01 NOAA 1516-01 NOAA 1517-01 NOAA 1600 - Ocean Programs GRS 3.2 - Information Systems Security Records **OPCS (EDA) :** The General Record Retention schedule is used. For BII and PII, the record control schedule is EDA DAA-0378-2014-0413.
	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, and does not have to be 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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: **Commerce Business Systems (CBS**): Collects PII/BII on employees, vendors, and customers. **Foreign Nationals Registration System (FNRS):** The data collected is enough to identify an individual. **Grants Online:** Collects business/ personal information from customers. **Management Analysis and Reporting System (MARS):** 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). **NOAA Staff Directory (NSD):** PII information is for employees to be used for emergency notifications.
X	Quantity of PII	Provide explanation: **Commerce Business Systems (CBS):** Collects personal information for employees, vendors, and customers. **Deep Water Horizon – LaserFiche**: Occurrences of PII in the ERMS are rare/accidental and incidental to the system's mission. **Grants Online (GOL)**: Grants Online collects a minimal amount of PII/BII. **Management Analysis and Reporting System (MARS):** MARS collects a moderate amount of PII **OPCS (EDA):** Include a few PII data fields.
X	Data Field Sensitivity	Provide explanation: **Archibus:** None of the data stored is Sensitive PII/BII. **Commerce Business Systems (CBS):** Collects a moderate amount of PII **Deep Water Horizon – LaserFiche:** The only PII that may

		predictably be in the ERMS are the occasional inadvertent inclusion of and individual's personal phone number or email address, and these occurrences are extremely rare. **Foreign Nationals Registration System (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 (GOL):** Contain sensitive BII. **OPCS (EDA):** Contain sensitive BII.
X	Context of Use	Provide explanation: **Commerce Business Systems (CBS):** Contains sensitive PII and BII use 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. **Grants Online (GOL):** Uses BII to support payment processing and determine an applicant's financial integrity. **Management Analysis and Reporting System (MARS):** MARS PII information is used to support payroll, personnel forecasting, travel analysis, payment processing, and financial reporting.
X	Obligation to Protect Confidentiality	Provide explanation: **Commerce Business Systems (CBS):** The Privacy Act of 1974 requires us to safeguard the collection, access, use, dissemination and storage of BII and PII. **Grants Online (GOL):** The Privacy Act of 1974 requires us to safeguard the collection, access, use, dissemination and storage of BII and PII.
X	Access to and Location of PII	Provide explanation: **Archibus:** Application is located in NOAA server and access is restricted to approved users. **Common Access Card (CAC):** There is a secure connection to bring over PII from Security Mgr and DEERS and data is stored in database under NOAA 1101. **Commerce Business Systems (CBS):** Data is encrypted at rest and in motion and access is restricted. **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. **Foreign Nationals Registration System (FNRS):** Data is encrypted at rest and access is restricted. **Grants Online (GOL):** Data is encrypted at rest / in motion and access is restricted.

	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.)

Archibus: There are no foreseeable threats to privacy as information collected is not sensitive in nature. Loss of confidentiality, integrity, or availability could be expected to have an extremely limited adverse effect on organizational operations, organizational assets, or individuals. Information is collected directly from Line Offices designated managers. Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.

CAC/NRS: PII is collected from the individual and stored in the Security Manager and DEERS and retrieved by the CAC & NRS systems. The CAC system also pushes data collected from Security Manager to DEERS.

Commerce Business Systems (CBS): CBS collects SSN / TIN for employees / vendors to process payments and W2 / 1099 tax information. Identify of the employee / vendor could be compromised, but this is a low risk due to encryption of data at rest, in motion, and for backup purposes

Deep Water Horizon – LaserFiche: Risk of privacy threat is extremely low, as collection of PII/BII is not an intended use of this system, and collection of this information is rare and inadvertent.

Grants Online (GOL): Identity of the company for tax purposes could be compromised.

SAM.gov is the official site to register for any external organization to conduct the business with government. Organizations register with EIN number in order to apply for federal Grants.

External organizations apply for Grants through Grants.gov and grants online application pull the grants application from it. Data is needed for federal employee to performance due diligence in determining recipient eligibility to receive federal funds.

Management Analysis and Reporting System (MARS): No exfiltration risks exist with minimal infiltration threats. Protocols are in place for users being granted access to MARS with quantity and type of information given to only users on must know basis. The MARS Non-Disclosure form and Rules of Behavior have been signed and completed and approved.

Users are also required to complete the annual IT Security Awareness Training Course in order to continue to use NOAA computing resources.

MARS Administrators will report all IT security related incidents to the NOAA CIRT (N-CIRT).

NOAA Staff Directory (NSD): Yes, PII is collected from the individual but it's voluntary. PII data are individual's personal cell number and their personal email address.

OPCS(EDA): There are no known potential threats to privacy that exists. The PII and BII data are collected to process grants and to determine the eligibility of the grant.

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.