Template Version Number: 01-2021

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

Privacy Impact Assessment for the
NOAA1101
Information Technology Center (ITC)

Reviewed by: Robin Burress for 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

Robin.Burress Digitally signed on 2025.12.11 14:32:01 -05'00'

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

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

Unique Project Identifier: NOAA1101

Introduction: System Description

Description of the General Support System (ITC):

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

NOAA1101 is General Support System (GSS) 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.

NOAA1101 hosts one (1) Major Applications, Commerce Business System (CBS), along with a number of minor applications and legacy databases for applications. 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
- Elastic Sky X (ESXi) VMWare
- Citrix XenApp
- Oracle and Simple Query Language (SQL) Databases

NOAA1101 hosts Major and Minor Applications and stores data at the following locations:

- Enterprise Datacenter (EDC) - Ashburn Facility, Virginia
- West Virginia High Tech Consortium (WVHTC)
- Amazon Web Service (AWS) - United States (US) East/West

Major Applications containing Personally Identifiable Information (PII) or Business Identifiable Information (BII)

CBS

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. NOAA1101 hosts the NOAA Data Warehouse (NDW),

Core Financial System (CFS) and Online Transaction Processing (OLTP). All previous financial services have since migrated to the Department of Commerce (DOC) Business Application Solutions (BAS). Access to this application is through the NOAA1101 GSS environment, which is limited to authorized NOAA and Bureau of Industry and Security (BIS). The application will be partially decommissioned in Fiscal Year (FY) 2025. There will be no connections to the remaining portions of CBS and NDW, only CBS administrators will have access. The PII identified is for federal employees and vendors/contractors. BII is required for companies providing services to NOAA for payment processing via the US Department of Treasury.

Minor Applications containing PII/BII

Archibus
Archibus is a facilities management tool which tracks service requests for facility maintenance. The application is available in both Web-based and Microsoft Window-based platforms. The system, integrated with Computer Aided Design (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. Vendor BII is collected when they are on-site. There is no PII within this application.

Common Access Card (CAC)
The Common Access Card web application assists the Chief Administrative Officer (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, sex, race/ethnicity, date of birth, place of birth, citizenship, and passport number are collected. Sponsors do not share this information.

NOAA Reporting System (NRS)
The NOAA Reporting System is a windows application (web services) that transmits CAC

information from the Defense Enrollment Eligibility 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.

Address the following elements:

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

NOAA1101 is a GSS.

(b) System location

- EDC - Ashburn Facility, Ashburn, VA
- West Virginia High Tech Consortium (WVHTC), Fairmont, WV
- AWS - US East/West

(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 (WOC)
• NOAA0550 – NOAA Enterprise Network (N-Wave)
• NOAA4000 – Wide Area Network (WAN)
• NOAA4000 – Trident

NOAA1101 has interconnections with the following non-NOAA systems:
• DOC Security Manager - is used to process CAC information.
• DOC SmartPay 3 - is used to process data for NIST and Census (e.g., accounting codes, invoices, etc.).

These do not interconnect with DOC BAS; although an Information Exchange Agreement exists which transfers NOAA Core files to BAS via SFTP each month.

NOAA1101 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 Hypertext Transfer Protocol Secure (HTTPS), Hypertext Markup Language (HTML), Secure File Transfer Protocol (SFTP). All connections require the use of a Virtual Private Network (VPN) connection.

(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 and SFTP. 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 and SFTP. 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 and SFTP. Users need to VPN into the system.

(g) Any information sharing

Archibus: Information is collected for all employees and contractors working in NOAA facilities under NOAA management/oversight. This is requested from the employee/contract Manager/Federal Lead. When requested to provide this information, users are sent an email with a login request to Archibus where they are required to login and provide the requested information.

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.

CAC/NRS: NOAA collects PII data from DEERS and it is used to process applications for CACs for federal employees. The non-PII portion of CAC data is used to determine who has a CAC and expiration data and statistical reporting (e.g., age of CAC cards, last used, etc. No PII statistical information is included in this reporting). This information is not purged.

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.

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

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

Personnel Actions Including Training – (COMMERCE/DEPT-18):

5 U.S.C. 1302, 2951, 3301,
3372, 4118, 5379, 8347
Executive Orders 9397, as amended by 13478, 9830, and 12107; 13164, 12564, 11246
31 U.S.C. 66a
44 U.S.C. 3101, 3309
41 U.S.C. 433(d)
5 CFR Part 537
Public Law 100-71
26 U.S.C. 3402

Security Investigations – (COMMERCE/DEPT-13):
Executive Orders 10450, 11478
5 U.S.C. 7531-332
28 U.S.C. 533-535
Equal Employment Act of 1972

Badging & CAC Issuance – (COMMERCE/DEPT-18):
Electronic Signatures in Global and National Commerce Act, Public Law 106-229
5 USC 301
Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors

Collection & Use of SSN – (COMMERCE/DEPT-1, DEPT-2, DEPT-18 & OPM/GOVT-1):
44 U.S.C. 3101, 3309
Executive Orders 9397, as amended by 13478, 9830, and 12107
31 U.S.C. 66a
28 U.S.C. 3101-3105
Debt Collection Act of 1982 (PL 97-365)

Credit Card & Financial Information – (COMMERCE/DEPT-1, DEPT-2):
31 U.S.C. 66a, 3711
44 U.S.C. 3101, 3309
28 U.S.C. 3101-3105
Debt Collection Act of 1982 (PL 97-365) 26 U.S.C. 6402(d)
Federal Financial Assistance Management Improvement Act of 1999
Public Works and Economic Development Act of 1965, as amended by the Economic Development Administration Reauthorization Act of 2004 (Pub. L. 108-373)
4 CFR 102.4
Chief Financial Officers Act (CFOs Act) of 1990, P.L. 101-576
Federal Managers' Financial Integrity Act of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.);
Office of Management and Budget (OMB) Circular A-127, Financial Management Systems

Travel Records – (COMMERCE/DEPT-9):

Budget and Accounting Act of 1921 Accounting and Auditing Act of 1950 Federal Claim Collection Act of 1966 FPMR 101-7
5 U.S.C. 5701-09

Education Activities – (NOAA-14):
National Marine Sanctuaries Amendments Act of 2000 (Pub. L. 106-513 sec. 318)
Section 4002 of the America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science (COMPETES) Act, Public Law 110-69

Emergency Preparedness – (COMMERCE/DEPT-18):
Executive Order 12656
Federal Preparedness Circular (FPC) 65, July 26, 1999

Foreign National Information – (COMMERCE/DEPT-27):
31 U.S.C. 951-953
8 USC 1324a
15 Code of Federal Regulations (CFR) Parts 730-774, Export Administration Regulations
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

Property Accountability Files – (COMMERCE/DEPT-16):
5 U.S.C. 301; 44 U.S.C. 3101; 40 U.S.C. 481-92; 15 U.S.C. 1518
41 CFR Chapter 102
Federal Managers' Financial Integrity Act of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.);
Office of Management and Budget (OMB) Circular A-127, Financial Management Systems

System Administration/Audit Data (SAAD) - (COMMERCE/DEPT-25)
5 USC 301
Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
Electronic Signatures in Global and National Commerce Act, Public Law 106-229
28 U.S.C. 533-535

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system.

As a designated enterprise platform as a service (ePaaS) provider for NOAA, the confidentiality, integrity and availability system categorization is a High Impact level. As a High system categorization, ITC supports the criticality of customer data and applications to be hosted within the system boundary. In addition, ITC as the GSS does not collect, process, store or transmit BII/PII information. Each major/minor application is responsible for the ensuring the protection of all BII/PII within their applications.

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.

NOAA1101 previously had two applications that no longer reside within the ITC boundary: 1) Management Analysis and Reporting System (MARS) has been decommissioned; and Grants Online (GOL), which no longer resides within the NOAA1101 information system.

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	X	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:

CAC: PII/BII information is collected from NOAA personnel to process and provide the CAC via the DEERS system.

CBS: Financial account information and grant/loan applications require Tax ID Numbers. These could be either SSNs or EINs which the grant applicants provide when they submit their applications. Once received via mail

the information is manually entered.

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	X
d. Sex	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship	*X	n. Religion			
u. Other general personal data (specify): * During the CAC process, information is retrieved from Security Manager and then indicates which citizenship a person holds.					

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	X	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	X	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	d. 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): **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): **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 biannually.

CBS: CBS performs quarterly and annual assessments of the integrity of the accounting system data. Annually, as part of its Fiscal Year 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 the information. This is an archive of documents related to Deep Water Horizon.

FNRS: Most data are 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.

NSD: Currently new records and separations are added or removed respectively to the NSD through our hourly sync with identify credential access management (ICAM). All updates come 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 change(s) and show who made the change(s).

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, 4040-0010, 4040-0020, 1545-0008, 0690-0030, 0690-0033.
	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	X
Other (specify):			

	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	X
For civil enforcement activities	X	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
User info collected for access
Employee info, including locations, collected so that FOD can track work requests for service.

CAC/NRS
Payment processing via Treasury Financial Management System
Internal Revenue Service 1099 / W2 processing.
Loan administration.
Grant administration.

CBS
Payment processing via Treasury Financial Management System
Internal Revenue Service 1099 / W2 processing.
Loan administration.
User Information

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, HI, 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.

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 (i.e., System for Award Management (SAM) /Central Contractor Registration CCR) is required for companies providing services to NOAA for payment

processing via the U.S. Department of Treasury.

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.

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.

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: Risks to privacy have been mitigated. At the application level, Archibus leverages role-based access controls, as well as strong user account identity and authentication (IA) controls. The Archibus application comes with built in role-based access controls as a Commercial off-the-shelf software (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.

CAC/NRS: Encrypting data at rest and in transit. Annual IT Security Training. Annual Records Management Training.

CBS: Risks to privacy have been mitigated. 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.

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.

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	X
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments	X*		
Foreign entities			
Other (specify):			

* Foreign national guest/visitor work authorization.

	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 CBS 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 FNRS

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 has interconnections with the following NOAA systems: • NOAA0201 – Web Operation Center (WOC) • NOAA0550 – NOAA Enterprise Network (N-Wave) • NOAA4000 – Wide Area Network (WAN) • NOAA4000 – Trident NOAA1101 has interconnections with the following non-NOAA systems: • DOC Security Manager - is used to process CAC information. • DOC SmartPay 3 - is used to process data for NIST and Census (e.g., accounting codes, invoices, etc.). These do not interconnect with DOC BAS; although an Information Exchange Agreement exists which transfers NOAA Core files to BAS via SFTP each month. NOAA1101 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 Hypertext Transfer Protocol Secure (HTTPS), Hypertext Markup Language (HTML), Secure File Transfer Protocol (SFTP). All connections require the use of a Virtual Private Network (VPN) connection.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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.
	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:

	.	
X	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 to determine federal income tax withholding. *The code references are included in the CBS training required for all users.* **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. *https://www.noaa.gov/protecting-your-privacy* 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. **NSD:** On the NSD ENS page, there is written information displayed that the data will be shared to ENS. See snapshot in Appendix A. **Archibus**: Employee receives an (e)(3) statement at the time of providing data.
X	No, notice is not provided.	Specify why not: **CAC/NRS:** Data is collected when the individual applies for and accepts employment at NOAA. CAC & NRS do not have direct communication with the individual. **Deep Water Horizon – LaserFiche:** The system is not used to collect PII/BII. This is an archive of documents.

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: **Archibus:** Employee receives an (e)(3) statement at the time of providing data. **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. **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 the location where individuals were given the opportunity to decline. **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. **NSD:** For the NSD, the person's email and phone number are optional. There are instructions on the NSD web page that informs the individual on how to opt-out.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **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 get entered in the Security Manager system nor will it be transmitted to DEERS. **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 the location where individuals were given the opportunity to decline. **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. **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. **Archibus**: Employee receives an (e)(3) statement at the time of providing data.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **CAC/NRS:** Employees and contractors submit updated information to the Security Manager servicing their account at the time their CAC is being renewed. **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. **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. **NSD:** Individuals can log into the NSD and view ENS info and make changes if necessary. There is also a 6-month validation that will navigate to the ENS page upon logging into the NSD to allow the individual to repopulate the information.
X	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. **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 the 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. CBS, FNRS
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 which is a Security Information and Event Management tool provided by NOAA Cybersecurity Center. 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): April 9, 2025 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the 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 CAC, 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 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/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 VPN Server, Rivest-Shamir-Adleman (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 PII/Privacy Act data is encrypted at rest, in an Oracle Encrypted tablespace.

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. Access to the application's contents (data) requires an active personnel certification event and/or the user is assigned as a Personal Computer (PC) manager.

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 2: Accounts Receivable. Credit Card & Financial Information COMMERCE/DEPT-9: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons COMMERCE/DEPT-13: Investigative and Security Records. COMMERCE/DEPT-16: Property Accountability Files COMMERCE/DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-25: Access Control and Identity Management System COMMERCE/DEPT-27: Investigation and Threat Management Records NOAA-14: Dr. Nancy Foster Scholarship Program; Office of Education, Educational Partnership Program (EPP); Ernest F. Hollings Undergraduate Scholarship Program and National Marine Fisheries Service Recruitment, Training, and Research Program OPM GOVT-1: General Personnel Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: 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
	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		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: **CBS**: Collects PII/BII on employees, vendors, and customers. **FNRS:** The data collected is enough to identify an individual. **NSD:** PII information is for employees to be used for emergency notifications.
X	Quantity of PII	Provide explanation: **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.
X	Data Field Sensitivity	Provide explanation: **Archibus:** None of the data stored is Sensitive PII/BII. **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. **FNRS:** Some of the data requested contains information such as SSN that could be exploited for financial gain (this includes permit and loan applications).
X	Context of Use	Provide explanation: **CBS:** Contains sensitive PII and BII that is used 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.
X	Obligation to Protect Confidentiality	Provide explanation: **CBS:** 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. **CAC:** There is a secure connection to bring over PII from Security Manager and DEERS and data is stored in a database under NOAA1101. **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. **FNRS:** Data is encrypted at rest 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 Office 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 Managers to DEERS.

CBS: CBS collects SSN/TIN for employees/vendors to process payments and W2/1099 tax information. Identification 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.

NSD: Employee/Contractor contact information such as Phone Number and Email is collected for the ENS through the NSD web application. The information displayed to the public does not specify if the contact information provided is personal or business.

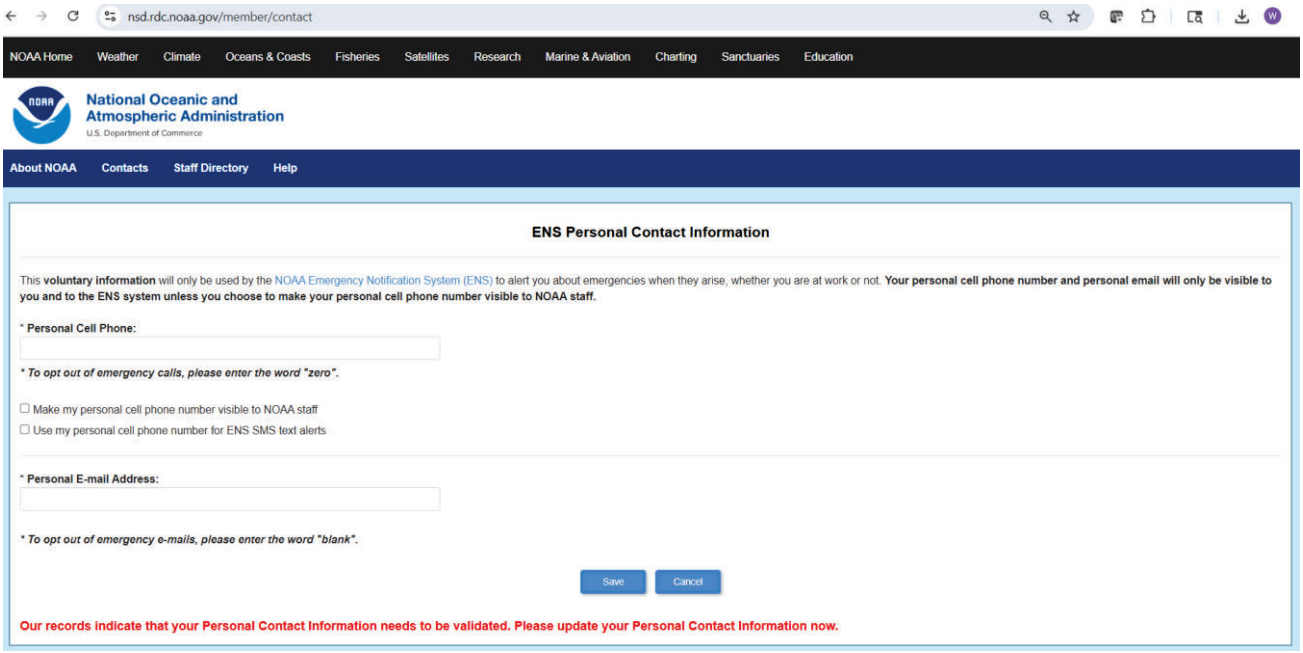
12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	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.

Appendix A


nsd.rdc.noaa.gov/member/contact
NOAA Home
Weather
Climate
Oceans & Coasts
Fisheries
Satellites
Research
Marine & Aviation
Charting
Sanctuaries
Education
National Oceanic and Atmospheric Administration
U.S. Department of Commerce
About NOAA
Contacts
Staff Directory
Help
ENS Personal Contact Information
This voluntary information will only be used by the NOAA Emergency Notification System (ENS) to alert you about emergencies when they arise, whether you are at work or not. Your personal cell phone number and personal email will only be visible to you and to the ENS system unless you choose to make your personal cell phone number visible to NOAA staff.
* Personal Cell Phone:
* To opt out of emergency calls, please enter the word "zero".
Make my personal cell phone number visible to NOAA staff
Use my personal cell phone number for ENS SMS text alerts
* Personal E-mail Address:
* To opt out of emergency e-mails, please enter the word "blank".
Save
Cancel
Our records indicate that your Personal Contact Information needs to be validated. Please update your Personal Contact Information now.