Version Number: 01-2021

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

Privacy Impact Assessment
for the
NOAA1200
Corporate Services / CorpSrv

Reviewed by: Mark Graff Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Tahira Murphy for Charles Cutshall 5/25/2023

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

Unique Project Identifier: NOAA1200

Introduction: System Description

Provide a brief description of the information system.

NOAA1200/CorpSrv is a General Support System (GSS) supporting approximately 2,721 end users and consisting of multiple types of subsystems. NOAA1200 administers approximately 3346 workstations/servers at ten sites across the United States, and approximately 2,500 mobile devices (including smart phones, iPads, etc.). For workstations and servers, all sites are bound under an active directory domain structure (CorpSrv.NOAA.local). Windows based devices include domain controllers (DC), file and print servers, desktop / laptop workstations. NOAA1200 supports NOAA's Line offices (NWS, OAR, OMAO and NESDIS (Coop)), Executive offices and Corporate financial and administrative Program Support Units (PSU).

Address the following elements:

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

NOAA1200 / CorpSrv, is a General Support System (GSS) consisting of multiple subsystems. The NOAA1200 core system consists of user desktop and laptop workstations, Microsoft Windows' file and print servers, a limited number of network infrastructure components that support NOAA's executive offices and corporate financial and administrative services Program Support Units located at sites within the United States.

(b) System location

The eleven locations supported are: Silver Spring, MD, (SSMC1 - SSMC4); Washington, DC; Norfolk, VA (two locations); Kansas City, MO; Boulder, CO; Newport, OR; Fairmont, WV; Honolulu, HI; Seattle, WA (two locations); Norman, OK and Frederick, MD.

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

NOAA1200 is hosted in the NOAA network infrastructure and not a standalone system.

NOAA4920 - Pacific Islands Regional Office (PIRO) Network connects to NOAA1200.

NOAA0900 – leverages cloud and utilize enterprise services.

NOAA0700 – Identity, Credential, and Access Management (ICAM), Public Key Infrastructure

(PKI services), and Enhanced Security Administration Environment (ESAE).

NOAA0550- N-WAVE for datacom infrastructure between the various headquarters and regional offices.

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

NOAA 1200 supports a user base of approximately 3,000 users and provides connectivity to the NOAA network infrastructure for both local and remote access to the following basic administrative services: collaboration platforms include Google Suite for email and collaboration, network file servers, printing, file backup and restoration, and account management. Residual data from other FISMA system(s) may be stored, and/or processed on user workstations or file servers.

NOAA1200 workstations allows Application Information System (AIS) users (including Trusted Agents) to connect to other (non NOAA1200) FISMA systems of record. The process of submitting, retrieving and storing sensitive information varies with each of the various FISMA systems users connecting via CorpSrv workstations.

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

NOAA1200 users (federal employees and contractors) access data via CorpSrv workstations. Each FISMA system grants access based on individual and group authorizations and need to know. These access controls are not administered by the IT staff.

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

NOAA1200 provides connectivity to the NOAA network infrastructure for both local and remote access. VPN is required for network file servers, printing; file backup and restoration; and account management. NOAA1200 communications are encrypted in transit via HTTPS, SSH, RDP and VPN connections.

(g) Any information sharing

Information will be shared only within the bureau, with the case-by-case exception that information may be disclosed to another Federal agency in connection with the assignment, hiring, or retention of an individual, the issuance of a security clearance, or the reporting of an investigation into an individual.

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

1. 5 U.S.C 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.
2. America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science (COMPETES) Act (Public Law 110-69, Section 4002).
3. National Marine Sanctuaries Amendments Act of 2000 (Public Law 106-513 Section 318).
4. Title 31 U.S.C. 66a, 492; Title 44 U.S.C. 3101, 3309; Executive Orders 10450,

11478, 12065, and 7531-332;

5. 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; and Equal Employment Act of 1972.
6. E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.
7. 5 U.S.C. 1104, 1302, 2951, 3301, 3321, 3372, 4118, 4305, 5379, 5405, and 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.
8. 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 (HSPD–12), Federal Property and Administrative Services Act of 1949, as amended.

* Note: For details on authorities, refer to the table at the end of this PIA.

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

CorpSrv NOAA1200 is a Moderate system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_X_ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): There have been new interconnections with NOAA1200 and location changes.					

____ 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.

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

Section 2: Information in the System

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

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

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

Social Security numbers are used in the issuance of government identification cards and the hiring and retention of employees.

Credit card and financial information is in regard to government travel/purchase cards only.

*Note: Refer to section 5.1 for further explanation.

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	X
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	X
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	X		

u. Other general personal data (specify):
Education level, school transcripts, field of study, references, performance measure results while in scholarship program, and postgraduate activities, national origin, disability.

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
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	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		

l. Other work-related data (specify):
Performance information, FBI Name Checks and arrest records, foreign travel forms, accident/incident reports.

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	f. Scars, Marks, Tattoos		k. Signatures	X
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	
b. IP Address	X	f. Queries Run		f. Contents of Files	

g. Other system administration/audit data (specify):
Audit data specific to when sensitive PII/BII is processed or stored in NOAA1200 is not collected. Audit information should be collected by applicable privacy systems of records when NOAA1200 users access those systems using NOAA1200 workstations

Other Information (specify)

Religion data is collected from the Office of Civil Rights for NOAA complaints of discrimination, demographic reports, investigations, civil rights reports, etc.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone		Email	X		
Other (specify):					

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

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

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

Edit checks are in place within respective NOAA1200 supported organizations to ensure accuracy of data input. Otherwise, for applications hosted on NOAA1200, information may be verified or rejected by application users. Some applications use automated means and some human intervention.

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.* OMB Control No. 0648-0568, National Oceanic and Atmospheric Administration: (1) Office of Education, Educational Partnership Program (EPP), (2) Ernest F. Hollings Undergraduate Scholarship Program and (3) Dr. Nancy Foster Scholarship Program
	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	X
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	
For litigation	X	For criminal law enforcement activities	
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): See Section 5.1 for additional 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).

1. Names, addresses, e-mail addresses, age, race, national origin, disability, gender, maiden name,

alias, SSNs, photographs, place of birth, and date of birth are collected and maintained to enable NOAA to identify to whom we are issuing a badge (employees and contractors).
2. Names, addresses, e-mail addresses, SSNs, place of birth and date of birth, photographs, fingerprints, FBI Name Checks and arrest records, foreign travel forms and passport numbers are used to create and support records for the submission of security investigations, for potential employees or contractors (members of the public). This information is temporarily stored locally until the security checky by OSY is completed, and then it is purged from the NOAA1200 boundary.
3. Names, addresses, e-mail addresses, race, national origin, disability, gender, home phone number, education, medical information, military service, work history, email address, and SSNs are used for eligibility for hiring employees (members of the public).
4. Names, occupations, job titles, salaries and performance information are used to create and maintain federal employee performance reviews. (federal employees)
5. Names, addresses, e-mail addresses age, race, religion, national origin, disability, gender, employee ID, employee case number and SSNs are collected for labor issues, civil enforcement activities and litigations (federal employees).
6. Names, addresses, age, financial accounts, financial transactions and SSNs are collected and maintained to facilitate payroll information and records (federal employees).
7. Names, addresses, e-mail addresses, age, race/ethnicity, gender, DOB, citizenship, education level, school transcripts, field of study, references, performance measure results while in program, and postgraduate activities are used to determine awards and track students in the (1) Office of Education, Educational Partnership Program; (2) Ernest F. Hollings Undergraduate Scholarship Program; (3) Dr. Nancy Foster Scholarship Program; and (4) National Marine Fisheries Service Recruitment, Training, and Research Program (members of the public).
8. User ID, IP Address, Date/Time of Access, Queries Run, ID Files Accessed and Passcodes are collected for system administration, including system security (federal employees).
9. The Trusted Agents collect and store Form CD591 (PIV request form) for government issued IDs, LDAP and Active Directory. The Trusted Agents process security and badging forms for contractors only, not Federal employees. The processing package may include fingerprints and a photograph, both taken by the badging office (but not stored in the system), driver's license and passport number. This information is stored locally for each user on the CorpSrv NOAA1200 workstations. However, the Trusted Agents roles and responsibilities remain with the subject system. Once the Eastern Region Security Office approves a contractor for a CAC, it returns the CD-591s for the sponsored contractors and they are stored electronically. Trusted agents are instructed to complete only Section A of the CD-591. They do not include the I-9 form and have never been requested to do so by OSY.
10. OF-306 Declaration for Federal Employment is stored temporarily when the form needs to be scanned and saved to a drive prior to uploading into Accellion Secure File transfer to send to the Security Office. A paper copy of the Security Coversheet/Request for Investigation Coversheet is also stored after removing Birth Date and SSN. The only forms stored are redacted Coversheets and CD-591s which do not contain PII. (federal employees).

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.)

There is the potential for insider threat, as well as that the privacy data being processed by the NOAA1200 users could be intentionally or unintentionally disclosed or shared with other unauthorized users. However, this risk is low because of the access, physical and logical security controls that are in place to prevent this from happening.

NOAA1200 technical controls require the use of CAC/PIV cards for physical and network access, and roles and privileges for application authorization. In addition, NOAA1200 users that are involved in the handling or processing of the privacy data for the hosted applications are required to review and sign the Rules of behavior and take mandatory training in order to minimize such risks. The users are required to adhere to NOAA's policies regarding disclosure and separation of duties.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	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?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re- dissemination of PII/BII.
X	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re- dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

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 technical controls which prevent PII/BII leakage: NOAA4920 - Pacific Islands Regional Office (PIRO) Network connects to NOAA1200. NOAA0900 – leverages cloud and utilize enterprise services NOAA0700 – Identity, Credential, and Access Management (ICAM), Public Key Infrastructure (PKI services), and Enhanced Security Administration Environment (ESAE). NOAA0550 - N-WAVE for datacom infrastructure between the various headquarters and regional offices. Technical controls which prevent PII/BII leakage: AC; IA; AU & SC
	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.)*

The only collections conducted within the boundaries of NOAA1200 consists of the PII collected for the scholarship application program. All other PII collections are conducted within the respective system boundaries of the Staff and Line Offices that own the data which may then be stored and/or processed by that office using NOAA1200. As such, the respective Privacy Act Statements pertaining to those Staff and Line Office collections are maintained within their originating FISMA systems, from which the information may then be stored and/or processed within the NOAA1200 system.

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: https://www.noaa.gov/protecting-your-privacy https://sites.google.com/a/noaa.gov/noaa-ums/ https://oedwebdbapps.iso.noaa.gov/uspa/ https://oedwebdbapps.iso.noaa.gov/StudentTracker/Login.aspx https://oedwebdbapps.iso.noaa.gov/studenttracker/vaus/

	.	
X	Yes, notice is provided by other means.	Specify how: Owners of the hosted systems send notifications to individuals when information is required. Those systems which use federal-wide forms for collection have PASs. For scholarship applicants, scholarship awardees and grantees, notice is given on the Web site and on the application and tracking forms, regarding the purposes and uses of the information given, along with both security and privacy notices. (A procedure required by the system of record and is not specific for NOAA1200) For Trusted Agents Form CD591, the DOC PIV request form, provides notice in that the request for information comes from the sponsor and registrar. The information comes from the applicant, who completes the form and provides it to the sponsor. There is also a privacy act statement on this form.
	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: Members of the public may decline to provide PII/BII directly to the application owners; however, they cannot be employed by NOAA/receive applicable services. NOAA1200 implements necessary controls to protect PII/BII. Information owners are responsible for implementing necessary, operational controls regarding collection, maintenance, and dissemination. Each collection procedure under the respective and applicable SORNs will have the prescribed notification procedures regarding opportunity to decline. The following applies to collection processes supported by NOAA1200: Federal employees and contractors may decline to provide the information, but must provide the information as a condition of employment. In general, information is required for the effective administration of the center, including continuity of operations in case of an emergency. On scholarship applications, not all information is required, and optional fields are marked as such. If required information is not given, applications will be declined. Links to the NOAA privacy policy are provided to employees, contractors and members of the public. For Trusted Agents also, individuals can decline by not providing requested information to receive NOAA ID. However, without a NOAA

		ID, they cannot work at NOAA as a Federal Employee or Contractor.
	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: NOAA1200 implements necessary controls to protect PII/BII. Information owners are responsible for implementing necessary, operational controls regarding collection, maintenance, and dissemination. Each collection procedure under the respective and applicable SORNs will have the prescribed notification procedures regarding consent for use of their PII/BII. The following applies to collection processes supported by NOAA1200: Individuals are given an explanation in writing, on the applicable forms, from the application owners, as to why the required information must be provided (i.e., specific uses), as well as a link to the NOAA Privacy Policy. Per the privacy policy, completion of a form or otherwise providing the information implies consent to the particular uses of the information. For Trusted Agents, if no consent is granted, no ID will be issued as in 7.2 above. This is the only purpose for this information.
	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: For scholarship programs, students may request to review their information from their supervisors and submit updates to them at any time. On the Web sites of all other hosted applications/offices, contact information for the staff office manager is given, with the stated purpose of requesting to review and update information. Note: All collection instruments contain a PAS.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. **Explanation:** This refers only to the SAAD data collected.
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): ~~3/26/21~~ (Currently in A&A 2023) ☐ 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.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

Suitable technology has not been identified that monitor, track and/or record access across the applications in use by NOAA1200 for PII/BII and other sensitive information on the system.

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).*

1. Multifactor authentication (HSPD-12 compliant)
2. Anti-virus protection
3. Intrusion prevention and detection systems
4. Forensic analysis tools
5. Log analysis tools
6. Trusted Agents (TA) collect and maintain CD591, Declaration of Federal Employment (OF-306), OSY Cover Sheet and Fair Credit Forms. The CD-591 does not have sensitive PII only name, job title, email address and phone number. The OF-306 and OSY Cover Sheet have sensitive PII. Initially, hard copy records were collected by the TA and stored in a secure location in a locked fireproof filing cabinet. More recently, the information is being sent electronically from Project Managers and users by Accellion, a secured email transfer, to the

TA, who transfers it to the Security Office via the same method. The information is also stored locally on the TA's workstation.

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-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, **COMMERCE/DEPT-31**, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations **NOAA-14**, Dr. Nancy Foster Scholarship Program, which has been revised to include Ernest F. Hollings Undergraduate Scholarship Program and the National Marine Fisheries Service Recruitment, Training, and Research Program alumni survey. **OPM/GOVT-1**, General Personnel Records, **OPM/GOVT-2**, Employees Performance File 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:

	100-24 Information Technology Operations and Management Records and 100-27 Records of the Chief Information Officer, p.12 and the GRS 3.1, 3.2, 4.1, 4.2, 5.8, and 6.3.
	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): NOAA Staff and Line Offices: • Retain each collection of personally identifiable information (PII) for the period defined in NOAA record schedules to fulfill the purpose(s) identified in the notice or as required by law.			

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

The combination of credit card info, along with SSNs, and Financial account information, being leveraged for the GSS purposes of NOAA1200, was determined to meet the threshold--not because of the volume of PII, but rather that any breach, under the NIST 800-122 standard, would be catastrophic and lead to a complete compromise of the identity, financial, and security information of the individuals affected. In particular, the System sharing with OSY, CFO, and GC transverses virtually every Sensitive PII field captured in the PIA, and the compromise of that data meets the 800-122 standard (remember that, unlike the FIPS 199 "High" standard, the 800-122 standard is not limited by the number of individuals for whom the compromise would cause catastrophic loss).

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

(Check all that apply.)

X	Identifiability	Provide explanation: Some individuals could be identified based on the information stored.
X	Quantity of PII	Provide explanation: NOAA1200 includes the workstation disks and server file stores for the NOAA headquarters staff, who use their workstations on a daily basis to process and store PII/BII.
X	Data Field Sensitivity	Provide explanation: The confidentiality impact level is set at high because sensitive PII is present: e.g. SSN, biometrics, etc. in combination with additional non-sensitive PII.
X	Context of Use	Provide explanation: Performance plan and other work-related data could contain information regarding disciplinary actions.
X	Obligation to Protect Confidentiality	Provide explanation: Sensitive PII (e.g. SSNs).
X	Access to and Location of PII	Provide explanation: For subject systems the information collected for badging purposes contains two forms of personal identification (i.e. Passport, Driver's license, etc.) which, if exposed during the course of collection and verification, could have an adverse impact to user confidentiality.
	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.)

NOAA1200 is a FISMA system required to be compliant with all FISMA cybersecurity controls related to securing privacy systems. Annual assessments / audits by independent assessors provide what is believed to be adequate safeguards for protection of sensitive PII from unauthorized disclosure.

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.

	Programmatic Authorities (Introduction h.)	Type of Information Collected (Introduction h.)	Applicable SORNs (Section 9.2)
1.	5 U.S.C. 1302, 2951, 3301, 3372, 4118, 5379, 8347	Personnel Actions Including Training	OPM/GOVT-1
	Executive Orders 13164, 12564, 9397, as amended by 13478, 9830, and 12107		COMMERCE/DEPT-1
	31 U.S.C. 66a		COMMERCE/DEPT-18
	44 U.S.C. 3101, 3309		
	41 U.S.C. 433(d)		
	5 CFR Part 537		
	Public Law 100-71		
2.	Executive Order 12107	Employee Performance Info	OPM/GOVT-2
	5 U.S.C. Sections 1104, 3321, 4305, and 5405		
3.	Executive Orders 10450, 11478	Security Investigations	COMMERCE/DEPT-13
	5 U.S.C. 7531-332		
	28 U.S.C. 533-535		
	Equal Employment Act of 1972		
4.	Electronic Signatures in Global and National Commerce Act, Public Law 106-229	Badging & CAC Issuance	COMMERCE/DEPT-25
	5 U.S.C. 301		
	Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors		
	Federal Information Security Modernization Act of 2014 (44 U.S.C. 3554)		
	E-Government Act of 2002 (Pub. L. 107–347, Sec. 203)		
	44 U.S.C. 3101, 3309	Collection & Use of SSN	
	Executive Order 12107, 9397, as amended by 13478, 9830, and 12107		
	31 U.S.C. 66a		
5.	Executive Order 13164, 12196	Public Health Emergency Info & Reasonable Accommodation	COMMERCE/DEPT-31
	Rehabilitation Act, 29 U.S.C. 701 et. seq	(includes medical and religion accommodation requests)	OPM/GOVT-1
	Americans with Disabilities Act of 1990, as amended, 102(d), 42 U.S.C. 12112(d)	(Religion collection for Civil Rights & EEO as well)	
	29 CFR parts 1602, 1630, 1904, 1910, and 1960		
	29 U.S.C. chapter 15 (e.g., 29 U.S.C. 668)		
	5 U.S.C. 1302, 3301, 7902		

6.	31 U.S.C. 66a	Credit Card & Financial Information	COMMERCE/DEPT-1
	44 U.S.C. 3101, 3309		
7.	National Marine Sanctuaries Amendments Act of 2000 (Pub. L. 106-513 sec. 318)	Education Activities	NOAA-14
	Section 4002 of the America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science (COMPETES) Act, Public Law 110-69		
	America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science (COMPETES) Act (Public Law 110-69, Section 4002)		
8.	Executive Order 12656	Emergency Preparedness	COMMERCE/DEPT-31
	Federal Preparedness Circular (FPC) 65, July 26, 1999		COMMERCE/DEPT-18

Points of Contact and Signatures

Information System Security Officer
Name: Bamidele Arawole
Office: NOAA OCIO SDD
Phone: (202)967-8162
Email:bamidele.arawole@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Bamidele Arawole — Digitally signed by Bamidele Arawole Date: 2023.03.22 09:16:25 -04'00'

Date signed:

System Owner
Name: Jason Rickett
Office: NOAA OCIO SDD
Phone: (240) 523- 1171
Email: jason.rickett@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: RICKETT.JASON.ALLEN.1392392951 — Digitally signed by RICKETT.JASON.ALLEN.1392392951 Date: 2023.03.22 09:07:01 -04'00'

Date signed:

Information Technology Security Officer
Name: Ansaruddin Hasan
Office: NOAA OCIO CSD
Phone: 240-255-8556
Email:ansaruddin.hasan@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: HASAN.ANSARUDDIN.ISA.1376816210 — Digitally signed by HASAN.ANSARUDDIN.ISA.1376816210 Date: 2023.03.22 09:38:39 -04'00'

Date signed:

Authorizing Official
Name: Douglas Perry
Office: NOAA Deputy OCIO
Phone: (301) 713-7673
Email:Douglas.A.Perry@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: PERRY.DOUGLAS.ALLEN.1365847270 — Digitally signed by PERRY.DOUGLAS.ALLEN.1365847270 Date: 2023.03.28 16:29:34 -04'00'

Date signed:

Privacy Act Officer
Name: Robin Burress
Office: NOAA OCIO
Phone: 828-271-4695
Email: Robin.Burress@noaa.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: BURRESS.ROBIN.SURRETT.1365847696 — Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.04.10 12:52:38 -04'00'

Date signed: 04/10/23

Co-Authorizing Official
Name: Cameron Shelton
Office: NOAA OCIO
Phone: 301-628-5721
Email: cameron.shelton@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: SHELTON.CAMERON.LYLE.1365843313 — Digitally signed by SHELTON.CAMERON.LYLE.1365843313 Date: 2023.03.29 10:13:55 -04'00'

Date signed:

Bureau Chief Privacy Officer
Name: Mark Graff
Office: NOAA OCIO
Phone: 301-628-5658
Email: Mark.Graff@noaa.gov

I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy.

Signature: GRAFF.MARK.HYRUM.1514447892 — Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2023.04.13 08:57:40 -04'00'

Date signed: 4.13.23

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.