U.S. Department of Commerce
National Oceanic and 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

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.03.04 18:47:53 -05'00' 03/04/2020

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NOAA1200, CorpSrv

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system.

a, b and c - NOAA1200 / CorpSrv, is a General Support System (GSS) consisting of multiple subsystems. NOAA1200 is hosted in the NOAA network infrastructure and not a standalone system.

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.

1. Boulder, CO;
2. Fairmont, WV;
3. Germantown, MD;
4. Honolulu, HI;
5. Kansas City, MO;
6. Largo, MD; and
7. Newport, OR;
8. Norfolk, VA
9. Norfolk, VA;
10. Seattle, WA;
11. Silver Spring, MD;
12. Tampa, FL;
13. Washington, DC.

NOAA1200 supports a user base of approximately 2,600 users, and provides connectivity to the NOAA network infrastructure for both local and remote access to the following basic administrative services: collaboration platforms includes Google Suite for email and collaboration, network file servers, printing; file backup and restoration; and account management.

d, e, and f - NOAA1200 workstations allows Application Information System (AIS) users (including Trusted Agents) to connect to other (non NOAA1200) privacy systems of record. The process of submitting, retrieving and storing sensitive information varies with each of the various privacy systems users connecting via CorpSrv workstations. Residual data from other privacy systems may be stored, and/or processed on user workstations or file servers.

Trusted Agents and other users access privacy systems with CorpSrv workstations. Trusted Agents and other users may store Form CD591 (PIV request form) used for government issued identification cards on corpsrv systems for archival purposes. These records which are submitted and processed in other government privacy systems of record may include fingerprints and a photograph, driver's license and passport numbers. OF-306 Declaration for Federal Employment may be archived in CorpSrv when scanned for submission to a personal

security office.

g. - NOAA1200 users share data with other DOC offices listed in the Appendix and NOAA applications, including Acquisition and Grants Office, Office of Civil Rights, Workforce Management Office, General Counsel, and the Office of the Chief Financial Officer. A case by case exception may be made 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, the reporting of an investigation of an individual.

The following cloud services are currently administered for the NOAA enterprise under NOAA1200 and will be moved to NOAA0900 FISMA compliance by the end of 3QFY2020.

Unified Messaging Service (UMS) / Google Government Suite (G-STE)

Google Services is comprised of Google's multi-tenant public and hybrid Google Apps cloud instances and multi-tenant public cloud Google App Engine. These services are built atop the Google Common Infrastructure. Google Apps is a Software-as-a-Service (SaaS) cloud deployment model that allows customers the ability to communicate, store files and collaborate with Gmail, Hangouts, Talk, Calendar, Drive, Docs, Sheets, Slides, Vault, Sites, Groups, Contacts and Classroom while managing their domain with the Admin Console.

G-STE completed an assessment and authorization (A&A) under the GSA FedRAMP program. It is authorized as a MODERATE Impact system which is adequate for the NOAA owned data processed and stored there. NOAA1200 users are not authorized to use G-STE for processing and storage of sensitive PII/BII, which is covered in the annual NOAA Information Technology Security Awareness Course (cyber security training).

ServiceNOW

ServiceNow is a suite of natively integrated applications designed to support IT service automation, resource management and shared support services. The ServiceNow platform includes customization tools to help customers create solutions for business requirements. ServiceNOW applications cover all Information Technology Infrastructure Library (ITIL) processes and are natively integrated on a single platform providing web intuitiveness and process automation. ServiceNOW is a modular solution, meaning that customers may use all, or a sub-set of the applications provided via ServiceNow. The ServiceNOW SaaS application is a group of modules, or pages, that provide related information and functionality in a ServiceNOW instance. These SaaS applications can be added or removed by enabling or disabling the application's plugin. ServiceNOW is designed to support processes, tasks, change management, and other IT processes through automation. It is a customizable environment and provides the ability for customers to design and implement applications as part of the ServiceNOW application framework.

ServiceNOW completed an assessment and authorization (A&A) under the GSA FedRAMP program.

Mobile Device Management (MDM) / IBM MaaS360

The IBM MaaS360 is a comprehensive, cloud-based security and management platform for NOAA mobile devices, applications and content. NOAA uses MaaS360 to protect data and optimize productivity, enabling employees to work anytime and anywhere through trusted mobile interactions. MaaS360 provides a cloud based, on-demand software-as-a-service (SaaS)

delivery model, built on a secure, multi-tenant architecture.

The Mobile Device Management IBM MaaS360 platform currently allows the use of facial recognition for unlocking mobile devices. This technology utilizes iris and retina scans, and other facial features including the depth, contour and shape of the face, as well as one's gaze to unlock mobile devices. However, users must also establish a passcode which can be used to bypass the facial data to unlock the devices. The biometric data collected by the device is stored, processed and encrypted locally on each device. The collection of the facial images is incidental to the device use. This data will not be collected in a system of record and will not be shared or retrieved by anyone within or outside the bureau. The only exception to this is in cases where the phone data, including the PII data collected by the phone is shared, if necessary, with law enforcement.

The IBM MaaS360 cloud service completed an assessment and authorization (A&A) under the GSA FedRAMP program.MDM Federal Information Security Management Act (FISMA)

AODocs

AODocs is a document management system that will allow NOAA to collaborate on its Google services solution to organize business critical documents, migrate files from legacy document management systems, implement business workflows, manage documents with metadata and apply document retention policies entity-wide. This solution is not yet in use at NOAA, however, in the future it will be used to distribute Standard Operating Procedures, manage quality control processes, and assist in the coordination of contract management, procurements, intranet publication and incident reporting. AODocs will not store any NOAA data on its servers, it will only leverage the Google cloud platform (Google App engine and Google Datastore). Google Drive data will remain in the G suite environment. While AODocs is not FedRAMP certified, it is hosted on the Google infrastructure to deliver its product (G Suite) and backend (Google Cloud Platform), however the operating environment is administered by AODocs.

Smartsheet

Smartsheet is a SaaS application for collaboration and work management that is developed and marketed by Smartsheet Inc. It is used to assign tasks, track project progress, manage calendars, share documents and manage other work. It has a spreadsheet-like user interface.

Smartsheet is in the process of becoming fully implemented begining 1QFY2020. It is currently undergoing a GSA FedRAMP A&A and at the time of this publication has completed its third party assessment. It is not authorized for processing or storing sensitive PII/BII.

h. Authorities

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. From NOAA-14: National Marine Sanctuaries Amendments Act of 2000 (Public Law 106-513 Section 318).
4. From DEPT-1: Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.D. 3101, 3309.
5. From DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.
6. From DEPT-18: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 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. From OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.
8. From OPM/GOVT-2: Sections 1104, 3321, 4305, and 5405 of title 5, U.S. Code, and Executive Order 12107.
9. From DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 (HSPD–12), Federal Property and Administrative Services Act of 1949, as amended.

i. This system has a FIPS 199 MODERATE impact level.

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	

_X__ This is an existing information system in which changes do not create new privacy risks, and there is not an SAOP approved Privacy Impact Assessment. (version 01-2017 or later.)

Section 2: Information in the System

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

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

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Storage is not duplicative among hosted offices: acquisition and grants, workforce management, financial, and security collect and store SSNs in their different capacities, from different populations: employees, contractors, non-NOAA customers. Authorities are those from DEPT-18 and OPM/GOVT-1, listed in the system description.

Sensitive information is stored and processed in NOAA1200 as a result of routine business processes within the NOAA organizations supported, authorized under 1. 5 U.S.C 301. There is also temporary storage of the OF-306 before transmitting to the security office.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	X*
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	X
c. Alias	X	i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. 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	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. 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	d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	X
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify): Facial features					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	

b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify): Passcodes 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.					

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

Other Information (specify)
The Mobile Device Management IBM MaaS360 platform currently allows the use of facial recognition for unlocking mobile devices. This technology utilizes iris and retina scans, and other facial features including the depth, contour and shape of the face, as well as one's gaze to unlock mobile devices. However, users must also establish a passcode which can be used to bypass the facial data to unlock the devices. The biometric data collected by the device is stored, processed and encrypted locally on each device. The collection of the facial images is incidental to the device use. This data will not be collected in a system of record and will not be shared or retrieved by anyone within or outside the bureau. The only exception to this is in cases where the phone data, including the PII data collected by the phone is shared, if necessary, with law enforcement.

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): PII received from DOC Bureaus is incidental to NOAA1200 support function for the SO/LOs.					

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 NOAA1200 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. Some of the information is covered under 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 amd (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	X
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			
There are no technologies used that contain PII/BII in ways that have not been previously deployed.			

Section 3: System Supported Activities

3.1 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	
Other (specify): Facial recognition			
There are no 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			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation	X	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	
For web measurement and customization technologies (single-session)		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).
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 Mobile Device Management IBM MaaS360 platform currently allows the use of facial recognition for unlocking mobile devices. This technology utilizes iris and retina scans, and other facial features including the depth, contour and shape of the face, as well as one's gaze to unlock mobile devices. However, users must also establish a passcode which can be used to bypass the facial data to unlock the devices. The biometric data collected by the device is stored, processed and encrypted locally on each device. The collection of the facial images is incidental to the device use. This data will not be collected in a system of record and will not be shared or retrieved by anyone within or outside the bureau. The only exception to this is in cases where the phone data, including the PII data collected by the phone is shared, if necessary, with law enforcement.
10. 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.

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.

5.2 Describe any potential threats to privacy 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 threat 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 requires the use of CAC 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 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

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

6.3 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 and the facial recognition feature of cellular phones. 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.

Privacy Act Statement - Facial Recognition Data

Authorities: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations and 44 U.S.C. 3101, Records Management by Agency Heads.

Purpose: The facial recognition feature is for accessing personal hand-held communications devices.

Routine Uses: The individual's access to the device by this means is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a**)**. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies.

Disclosure: Adding this information to the device is voluntary; however, failure to provide accurate information may prevent the individual's device access.

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: https://oedwebapps.iso.noaa.gov/uspa/Default.aspx https://oedwebapps.iso.noaa.gov/USPA https://oedwebapps.iso.noaa.gov/SSTR/ https://oedwebapps.iso.noaa.gov/studentstracker/VAUS/ https://oedwebapps.iso.noaa.gov/studentstracker/ https://sites.google.com/a/noaa.gov/noaa-ums/ _____.	
X	Yes, notice is	Specify how: Owners of the hosted systems send notifications to individuals when

	provided by other means.	information is required. Those systems which use federal-wide forms for collection have PASs. Please refer to the Appendix for these owners. 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) There is a PAS for the cellular phone facial recognition posted on the UMS Web site and posting on the phones is pending. 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 the facial recognition on cellular phones, this is entirely voluntary and not shared within the system. 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	Specify why not:

	do not have an opportunity to decline to provide PII/BII.	

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 the cellular phone facial recognition, this feature is initiated by the cell phone holder and there are no other uses. 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: 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 review and update of their PII/BII.

		The following applies to collection processes supported by NOAA1200: 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. For the cell phone facial recognition feature, any update would be performed by the cell phone holder.
	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 FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 04/01/2019 ☐ 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 and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
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 ownership rights over data including PII/BII.

	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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

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 have sensitive PII only name, job title, email address and phone number. The OF-306 and OSY Cover Sheet has 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 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 and number *(list all that apply)*: Department-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, Department-13, Investigative and Security Records, DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies, DEPT-25, Access Control and Identity Management System, GSA./GOVT-7, Personal Identity Verification Identity Management System, 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. Also, OPM/GOVT-1, General Personnel Records, OPM/GOVT-2, Employees Performance File Records would cover the personnel related records created and maintained by Supervisors, and WFMO, both those that go in the eOPF, and those held by the chain of command.
	Yes, a SORN has been submitted to the Department for approval on (date).

	No, a SORN is not being created.

Section 10: Retention of Information

10.1 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: Requirements for record retention are found in the NOAA Records Schedules: 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	
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

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.

	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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Some individuals could be identified based on the information stored.
X	Quantity of PII	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 moderate because sensitive PII is present: e.g. SSN, biometrics, etc. in combination with additional non-sensitive PII.
X	Context of Use	Provide explanation: Facial recognition is on cell phones only and is not shared.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: For subject systems The information collected for badging purposes contains two forms of personal identification (ie 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 privacy 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.