Version Number: 01-2021

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

Privacy Impact Assessment
for the
NOAA4300
NMFS Southeast Region Office Local Network

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

GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2023.08.08 05:59:14 -06'00'

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

Version Number: 01-2021

U.S. Department of Commerce Privacy Impact Assessment
NOAA/ NMFS/Southeast Region Office Local Network

Unique Project Identifier: NOAA4300

Introduction: System Description

Provide a brief description of the information system.

NOAA4300 is a general Support System. It supports all offices within the Southeast Region (SER) which includes the Regional Administrator's Office; Operations, Management & Information Services Office; State/Federal Liaison Office; Sustainable Fisheries Division; Protected Resources Division; and, Habitat Conservation Division.

The system also supports non-SERO offices located in St. Petersburg including NOAA SE Office of General Counsel (GCSE), Damage Assessment Center (DAC), and NMFS SE Financial Services. The information for these Non-SERO offices is covered by the NOAA4020 Privacy Impact Assessment.

Address the following elements:

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

NOAA4300 is a general Support System.

(b) System location

NOAA4300 is physically housed in a leased portion of a three-story building located within the city limits of Saint Petersburg, Florida. The building is 85% occupied by NOAA and NMFS offices. The network servers, web servers, and network management workstations are located in a secure room on the second floor.

While there are field offices for NOAA4300 located in Charleston, SC, Beaufort, SC, Galveston, TX, Baton Rouge, LA, Miami, FL, and Fernandina Beach, FL, these users and endpoints are located outside the system boundary of NOAA4300 and connect to the system using VPN. These offices are either hosted within other system boundaries, or on an independent ISP and completely remote.

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

NOAA4300 has an interconnection with NOAA4000 (NMFS WAN) for the following purposes:

- NMFS to NMFS network access
- Core backbone network services with Internet connectivity (TICAP)

- Enterprise Active Directory
- Coordination of IP address (DNS)
- Real-time network monitoring
- VMS and PIMS Data for purposes of Catch Shares (IFQ) program and Permits Management System (PIMS)*

*Data exchange over the existing interconnection due to the PIMS application being migrated to the cloud instance hosted by NOAA4000. PIMS data is now exchanged over the existing secure interconnection shared with NOAA4000. Even though it is hosted by NOAA4000, the application is considered to be within NOAA4300's system boundary due to the supposed architecture of the instance.

NOAA4300 uses the interconnection with NOAA4000 to share permit related data with NOAA4400 (SEFSC) in Miami.

NOAA4300 also has an interconnection with NOAA4011 for purposes of fishery management in conjunction with NFPLRS, and the hosting of the Catch Shares Online System.

NOAA4300 is currently preparing to migrate the Catch Shares Online System from NOAA4011 to a cloud instance hosted by the NOAA WOC as part of the Amazon Government Web Services Cloud (a FedRAMP certified cloud vendor). The instance containing the migrated Catch Shares Online System is managed by NOAA4300, and the instance and application will fall within the NOAA4300 System Boundary. The contractor currently managing the application (Tesa) within NOAA4011 will be performing the migration to the new instance, and ensuring all functionality and data remain intact.

The function of the application and data it contains will be unchanged. There is no change to the type of data stored or processed by NOAA4300.

Upon completion of the migration to the new instance, both NOAA4011 and NOAA4300 staff will verify functionality and data integrity/minimization prior to the migrated application going into production.

NOAA4300 has been provided the estimated completion dates for the following critical milestones from Tesa for the CSOS migration:

- Application migration – August 4th, 2023
- Functionality and data reviews - August 15th, 2023
- Production cutover – August 25th, 2023

In order to comply with modifications to both the Gulf of Mexico Charter Vessel and Headboat Reporting Requirement Rule (https://www.fisheries.noaa.gov/action/gulf-mexico-modifications-charter-vessel-and-headboat-reporting-requirements) and the South Atlantic Charter Vessel and Headboat Reporting Requirement Rule (https://www.fisheries.noaa.gov/action/south-atlantic-modifications-charter-vessel-and-headboat-reporting-requirements), NOAA4300 is required to share permit holders' date of birth (DOB) and email addresses with ACCSP.

This interconnection agreement with ACCSP was established in November, 2020, and will continue to be renewed annually, contingent upon ACCSP providing documentation to NMFS OCIO (NOAA4000) verifying a successful Assessment and Independent Validation and Verification of compliance with all applicable security policies, controls, and requirements of a FIPS199 Moderate (or equivalent) system on an annual basis. In 2021, a centralized Interconnection Agreement with ACCSP was created by NOAA4000 in order to prevent duplication of effort in terms of system interconnection agreements between ACCSP and multiple regional offices. NOAA4000 is responsible for ensuring ACCSP remains certified as a FIPS 199 Moderate (equivalent) system and that it complies with all applicable security policies, rules, and

requirements. Regional offices send in their updates annually or as needed so that the central document is kept up to date.

In order to maintain this system interconnection, ACCSP will be required to provide annual verification of Continuous Monitoring methodology practices and current FIPS199/NIST SP800-171 compliance through third party audit results prior to the renewal of any system interconnect or data sharing agreements. NMFS OCIO will also be required to provide annual documentation indicating their approval of ACCSP's Authority to Connect to NMFS systems.

A replacement for the NOAA4300 Permits Information Management System (PIMS) went into production in September 2021. This upgrade is a complete rewrite of the old application, whose programming code had reached End of Life. The upgraded version of PIMS is now hosted in an AWS instance held under contract with NOAA4000, where NOAA4300 occupies an instance within that environment for the PIMS application. The application is hosted by Appian, a FEDRAMP approved vendor, and managed by Nuvitek. Connectivity to NOAA4300 is secured through VPN. The Appian instance hosting PIMS is within the NOAA4300 system boundary.

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

NOAA4300 collects and stores information that consists of basic identifying information about employees, contractors, volunteers, and partner agency staff who are facility occupants or system users. The information is maintained as a supplement to other records for purposes of human resource activities (including managing security clearances), Continuity of Operations (COOP) execution, and performing other related administrative tasks, e.g., travel, awards, facility management, and staff training requirements in support of individual job duties and requirements. Information collected to manage security clearances may include: full name, home address, home phone number, e-mail address, educational background, Social Security Number (SSN), and employment history.

Information maintained for COOP and other administrative processes includes: full name, grade level and/or position within the organization, role/responsibility, home address, home phone number, and mobile phone number.

NOAA4300 also collects and stores permit-related data. In order to manage U.S. fisheries, the NMFS requires the use of permits or registrations by participants in the United States. The information collected by NMFS SERO includes the contents of permit applications and supporting artifacts. Typical transactions include initial or renewal permit applications. The permit holder or applicant completes a blank application downloaded from the applicable NMFS Web site, received in the mail, or obtained through visiting the Permits office, and submits it to the applicable office via online, or in person, including any required supporting documentation and proof of payment through pay.gov. Approved permits are mailed to applicants. For permit transfers within a family, marriage certificates, divorce decrees, and/or death certificates may be required. Tax Identification Numbers (TINs) allow positive identification and cost recovery billing of Individual Fishing Quota (IFQ) holders.

In addition, information is collected to facilitate public education, outreach, or collaboration with partners on research/conservation projects. For these activities, the name, address, e-mail address, telephone number, and other non-sensitive organizational information may be temporarily stored. These individuals, businesses or organizations may be workshop participants, business contacts, members of mailing lists, etc. In all cases the information is voluntarily submitted.

NOAA4300 employs contractors in a variety of roles in order to support its mission, primarily in the Habitat/Sustainable Fisheries/Protected Resources branches. All contractors undergo the same security clearance process as Federal Government employees. Access to information collected and maintained within the system boundary of NOAA4300 is determined by the individual's job duties and role within the

organization. Any request involving the sharing of sensitive data, whether internal or external, must be documented in a Memorandum of Understanding (MoU) or Interconnection Security Agreement (ISA), and approved by each system's Authorizing Official. Information is shared within the Southeast Region in order to coordinate monitoring and management of sustainability of fisheries and protected resources. Sources of information include the permit applicant/holder, other NMFS offices (Such as the Office of General Counsel and the Southeast Division of the NMFS Office of Law Enforcement), the U.S. Coast Guard and the Department of Justice. Information will also be shared at the state or interstate level for the purpose of determining an applicant's eligibility when data collected by the state affects permit eligibility.

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

Employees can contact the HR representative for NOAA4300 and review their information, or a personal contact information form can be completed and given to HR, who will then update the information accordingly.

Permits: Information may be reviewed/updated when completing or renewing a permit application or supporting document, or by calling or emailing the applicable NMFS office at any time.

Partners for public outreach and education may update their information at any time by contacting the appropriate staff member assigned as their coordinator.

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

Information is manually collected through mail, over the telephone, in person, email, fax, and online.

Information is currently transmitted to and from the system through a network connection internal to the NMFS WAN employing Virtual Private Network encryption (TCP/IP using TLS) to secure the data.

Data is sent to ACCSP via encrypted connection to ACCSP (using AES-256 Encryption over a dedicated connection). Once transferred, authorized SER staff can access the data through the SAFIS web interface, which uses HTTPS to secure the connection.

(g) Any information sharing

NOAA4300 uses the interconnection with NOAA4000 to share permit related data with NOAA4400 (SEFSC) in Miami, and NOAA4011 (NFPLRS). PIMS uses this interconnection as well, even though the instance hosting PIMS is within the NOAA4300 system boundary.

OLE (NOAA4000) accesses the Permits Information Management System (PIMS) for Fishery Management/Law Enforcement purposes.

In order to comply with modifications to both the Gulf of Mexico Charter Vessel and Headboat Reporting Requirement Rule (https://www.fisheries.noaa.gov/action/gulf-mexico-modifications-charter-vessel-and-headboat-reporting-requirements) and the South Atlantic Charter Vessel and Headboat Reporting Requirement Rule (https://www.fisheries.noaa.gov/action/south-atlantic-modifications-charter-vessel-and-headboat-reporting-requirements), NOAA4300 is required to share permit holders' date of birth (DOB) and email addresses with ACCSP.

This interconnection agreement with ACCSP was established in November, 2020, and was made part of a central ISA through NOAA4000 in 2021. The centralized ISA was created to prevent duplication of effort from multiple regions that have an active data sharing agreement with ACCSP. The main document of the NOAA400/ACCSP ISA outlines overall security requirements and verification that these requirements are met, and each region has its own appendix describing specific details of their connection. The agreement will continue to be renewed annually, contingent on ACCSP providing documentation to NOAA4000 verifying a successful Assessment and Independent Validation and Verification of compliance with all applicable security policies, controls, and requirements of a FIPS199 Moderate (or equivalent) system on an annual basis.

In order to maintain this system interconnection, ACCSP will be required to provide annual verification of Continuous Monitoring methodology practices and current FIPS199/NIST SP800-171 compliance through third party audit results to NOAA4000 prior to the renewal of any system interconnect or data sharing agreements. NMFS OCIO will be required to provide annual documentation indicating their approval of ACCSP's Authority to Connect to NMFS systems, and maintain the central ISA documentation.

Although the PIMS system (referenced in Section C) now resides in a cloud instance, there has been no change to the sharing of data or function of the system itself.

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

Reference the table at the end of this document for the authorities.

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

NOAA4300 is a FIPS199 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.

_____ 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.

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	X	h. Alien Registration	X	l. Vehicle Identifier	X
d. Employee ID	X	i. Credit Card	X	m. Medical Record	X
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:
Tax Identification Numbers/Social Security Numbers are collected to allow positive identification for cost recovery billing of Individual Fishing Quota holders. SSNs are also collected from federal employees and contractors for security clearance purposes.

Medical Record information refers to employee Reasonable Accommodation information and documentation.

For Permits: Captain's license, State and Federal Dealer Numbers (if applicable), permit or license numbers for Federal or state permit/licenses issued and start and end dates and other permit status codes, vessel registration number.

The credit card and financial account data contained in the system is for Federal purchase and travel cards, and

travel accounts. No personal financial data or credit card information is collected, maintained, or disseminated.

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

u. Other general personal data (specify): Permit applicant, permit holder, permit transferor/transferee, vessel owner, vessel operator, dealer applicant, dealer permit holder, marriage certificates, divorce decrees, or death certificates.

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	X		

l. Other work-related data (specify):
Grade level and/or position within the organization and role/responsibility

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

p. Other distinguishing features/biometrics (specify):
* For background check

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	

g. Other system administration/audit data (specify):

Other Information (specify)

Species, aggregate catch data and statistics, quota share balance, quota pound balance, quota pound limits, listings of endorsements and designations (i.e., gear endorsement, size endorsement, sector endorsement, permit tier) associated with the permit, name of physical IFQ landing site, Exemptions (i.e., Owner on Board - Grandfathered

Exemption, Owner on Board, as stated in code of federal regulations) and exemption status, contact persons, Catch/Observer Discard Data, Quota Share/Quota Pound Transfer Data, Business Operation Information (Business Processes, Procedures, Physical Maps).

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): * For clarification of previously submitted information only.					

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

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

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

Employees can contact the HR representative for NOAA4300 and review their information, or a personal contact information form can be completed and given to HR, who will then update the information accordingly.

Permits: Information may be reviewed/updated when completing or renewing a permit application or supporting document, or by calling or emailing the applicable NMFS office at any time.

Partners for public outreach and education may update their information at any time by contacting the appropriate staff member assigned as their coordinator.

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 Nos: 0648- 0013, 0648-0016, 0648-0205, 0648-0358. 0648-0543, 0648-0551, 0648-0703.

	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	X	Electronic purchase transactions	
Other (specify): The facility housing NOAA4300 maintains a video surveillance and access control system, which is used only for the purposes outlined in DEPT-13 Routine Uses (security-related and law enforcement records access requirements).			

	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	X	For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	

For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

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).

For PII/BII in reference to federal employees, contractors, foreign national guest/visitors, student interns, and volunteers:

The information required for determining Security Clearance by DOC Security for federal employees, contractors, interns, and volunteers may include full name, home address, home phone number, e-mail address, educational background, SSN, and employment history. The SERO Security Officer collects information in-person, via telephone (for clarifications/corrections on completed forms), via email/fax and submits forms for clearance process. A security clearance is required to gain access to the SERO facility. This information is collected from the individual requesting the clearance (employee, contractor, foreign national guest/visitor, student intern, or volunteer).

The information is maintained as a supplement to other records for purposes of human resource activities, Continuity of Operations (COOP) execution, and performing other related administrative tasks includes full name, grade level and/or position within the organization, role/responsibility, home address, home phone number, and mobile phone number. This information is collected from the individual employee, contractor, student intern, or volunteer. Information is also used by Human Resources regarding current employees and job applicants for administrative purposes. This information is collected from the individual employee or applicant.

For Permit-related PII/BII: This information will allow NMFS to identify owners and holders of permits and non-permit registrations and vessel owners and operators for both civil and criminal enforcement activities, evaluate permit applications, and document agency actions relating to the issuance, renewal, transfer, revocation, suspension or modification of a permit or registration. NMFS may use lists of permit holders or registrants as sample frames for the conduct of surveys to collect information necessary to the administration of the applicable statutes. NMFS posts non-sensitive permit holder, vessel-related, and/or IFQ information for the public, via Web sites and Web Services, per notice given on permit applications. This information is considered to be part of the public domain.

Tax Identification Numbers allow positive identification for cost recovery billing of IFQ holders. Also, as stated in the routine uses of COMMERCE/NOAA-12 and COMMERCE/NOAA-19, a Tax Identification Number is required on all permit applications other than research or exempted fishing permits, under the authority 31 U.S.C. 7701. For purposes of administering the various NMFS fisheries permit and registration programs, a person shall be considered to be doing business with a Federal agency including, but not limited to, if the person is an applicant for, or recipient of, a Federal license,

permit, right-of- way, grant, or benefit payment administered by the agency or insurance administered by the agency pursuant to subsection (c) (2) (B) of this statute.

Information will also be collected to facilitate public education, outreach, or collaboration with partners on research/conservation projects. For these activities, the name, address, e- mail address, telephone number, and other non-sensitive organizational information may be temporarily stored. These individuals, businesses or organizations may be workshop participants, business contacts, members of mailing lists, etc. In all cases, the information is voluntarily submitted by the individuals or representative of the business or organization.

An interconnection agreement with ACCSP was established in November, 2020, and was made part of a central ISA through NOAA4000 in 2021. The centralized ISA was created to prevent duplication of effort from multiple regions that have an active data sharing agreement with ACCSP. The main document of the NOAA400/ACCSP ISA outlines overall security requirements and verification that these requirements are met, and each region has its own appendix describing specific details of their connection. The agreement will continue to be renewed annually, contingent on ACCSP providing documentation to NOAA4000 verifying a successful Assessment and Independent Validation and Verification of compliance with all applicable security policies, controls, and requirements of a FIPS199 Moderate (or equivalent) system on an annual basis.

In order to maintain this system interconnection, ACCSP will be required to provide annual verification of Continuous Monitoring methodology practices and current FIPS199/NIST SP800-171 compliance through third party audit results to NOAA4000 prior to the renewal of any system interconnect or data sharing agreements. NMFS OCIO will be required to provide annual documentation indicating their approval of ACCSP's Authority to Connect to NMFS systems, and maintain the central ISA documentation.

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.)

Disclosure of data from an internal source is considered the biggest potential threat to the PII/BII contained within NOAA4300. To mitigate this threat, the following measures are in place:

- All users are subject to a Code of Conduct that includes the requirement for confidentiality.
- All staff (employees and contractors) receive training on privacy and confidentiality policies and practices.
- Access to the PII/BII is restricted to authorized personnel only.
- The information is secured in accordance with FISMA requirements for a Moderate System.
- 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).

- A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
- Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.

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	X		
Public			X
Private sector	X**		
Foreign governments			
Foreign entities			
Other (specify):			

*Case by case with DOJ and U.S. Coast Guard if applicable (criminal enforcement leading to litigation).
**The PII/BII in the system will not be shared unless required and authorized to do so on a case-by-case basis, such as with ACCSP, after successfully achieving FIPS199/equivalent requirements for a Moderate system.

	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.
	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 and describe the technical controls which prevent PII/BII leakage: **NOAA4000, NOAA4011, and NOAA4400** All applicable controls are in place, including encryption of data at rest and during transfer. **Atlantic Coastal Cooperative Statistics Program (ACCSP)| Atlantic Coastal Fisheries Information Network (ACFIN)** All applicable controls reported as in place for ACCSP by NOAA4000, who manages the centralized ISA for NMFS/ACCSP data sharing.
	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	X*	Government Employees	X
Contractors	X		
Other (specify): * The public only has access to non-sensitive PII/BII that is already part of the public domain. This consists of publicly available information that is not considered sensitive (hull number, permit type, etc.)			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.fisheries.noaa.gov/national/fisheries-observers/privacy-act-statement .	
X	Yes, notice is provided by other means.	Specify how: Notice is provided on the applicable employee forms. Permits: Notice is provided on the permit or related application. Outreach: Notice is given in the email response to the individual's email. Video Surveillance: Signs are posted at all points of entry to the facility and at vehicle entrances.
	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: Information submitted for security clearances for access to federal networks/facility access is voluntary (may be declined, in writing, to the supervisor) but is required by federal regulations. Therefore, if the information is not provided, no access will be granted. Information submitted for Human Resource activities such as hiring is voluntary (may be declined, in writing, to the supervisor), but if the required information is not provided, employment cannot be granted. Once employed, information is kept on file with Human Resources for COOP and other administrative purposes. Permits: The personal information is collected when the individual completes the appropriate application. On the application, the individual is advised that NMFS will not be able to issue a permit if the individual does not provide each item of information requested. The individual may choose to decline to provide the required personal information at that time, but will not be able to receive a permit. Information for public outreach and education is strictly voluntary, by an email request. If information is not provided, it may affect the level or amount of services requested.
	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: Security Clearance: Information is used solely for security clearance, and is only accessible to those employees whose job duties require access to this information. This information is usually submitted by completion of a form. The form outlines the NOAA Privacy Policy, linked to NOAA web pages, which states that "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose." Information submitted for Human Resource activities such as hiring by completing a form. The form outlines the NOAA Privacy Policy, which states that "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose." Employee information is kept on file with Human Resources for COOP and other administrative purposes.

	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: Employees can contact the HR representative for NOAA4300 and review their information, or a personal contact information form can be completed and given to HR, who will then update the information accordingly. Permits: Information may be reviewed/updated when completing or renewing a permit application or supporting document, or by calling or emailing the applicable NMFS office at any time. Partners for public outreach and education may update their information at any time by contacting the Southeast Regional Office.
	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:** Access to PII is tracked through database/application logging. Network administrators can track user access through these logs.
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): 1/23/2023 ☐ 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.
X	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).*

There is no public access to NOAA4300. Users are only allowed access to information that is required for them to fulfill their job duties. All portable computers are encrypted with McAfee Disk Encryption.

Access to PII is controlled through access control policies and access enforcement mechanisms. Separation of duties is strictly enforced for duties involving access to PII.

Least privilege is enforced for all NOAA4300 users, enforcing the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Access to information system media containing PII, including digital media, is restricted to authorized personnel. Users are uniquely identified and authenticated through either 2-factor authentication or USGCB compliant passwords before accessing PII.

PII, both in paper and digital forms, is securely stored until destroyed or sanitized using approved equipment, techniques, and procedures.

Removable media and mobile devices containing PII that are transported outside the organization-controlled space are protected using both physical methods and data encryption.

The confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape, is protected through full disk/tape encryption. Any printed output containing PII/BII is secured in a locked file cabinet or drawer.

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-5, Freedom of Information and Privacy Request Records COMMERCE/DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies COMMERCE/DEPT-20, Biographical Files NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. COMMERCE/DEPT-25, Access Control and Identity Management System GSA/GOVT-7, Federal Personal Identity Verification Identity Management System (PIV IDMS) Permits: COMMERCE/DEPT-13, Investigative and Security Records. NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Exempted Applicants COMMERCE/DEPT-14, Litigation, Claims, and Administrative Proceeding Records. COMMERCE/DEPT-31, Reasonable Accommodation (RA) records related to COVID-19 or other public health emergencies
	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: NOAA Chapter 100: Enterprise-Wide Functions Electronic Records schedule: NARA General Records Schedule: 3.1 General Technology Management Records 3.2 Information Systems Security Records 4.1 Records Management Records Individual records are removed manually from the system at personnel separation Permits: There are approved record control schedules for both Sustainable Fisheries and Marine Mammal Protection permits. NOAA 1504-11 NOAA 1514-01
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.

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

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

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

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: The information contained within the system could be used to identify individuals, and potentially verify their identity to third parties. Compromise of PII could result in adverse effects on individuals (Identity Theft), as well as a loss of public trust in the organization, which would hinder the agency's overall mission.
X	Quantity of PII	Provide explanation: Full name, home address, home phone number, e-mail address, educational background, SSN, and employment history. Any or all of these could be used to the detriment of the individual to whom they belong.
X	Data Field Sensitivity	Provide explanation: Data field sensitivity ranges from moderate to high value PII/BII.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: Magnuson-Stevens Fishery Conservation and Management Act
	Access to and Location of PII	Provide explanation:

	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.)

As information is collected from the individual, little to no threat to privacy exists at point of collection. All information collected is the minimum required by policy or statute to accomplish the agency's mission and/or fulfill the purpose the information is being collected for.

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

X	Yes, the conduct of this PIA results in required business process changes. Explanation: NOAA4300 is currently preparing to migrate the Catch Shares Online System from NOAA4011 to a cloud instance hosted by the NOAA WOC as part of the Amazon Government Web Services Cloud (a FedRAMP certified cloud vendor). The instance containing the migrated Catch Shares Online System is managed by NOAA4300, and the instance and application will fall within the NOAA4300 System Boundary. The contractor currently managing the application (Tesa) within NOAA4011 will be performing the migration to the new instance, and ensuring all functionality and data remain intact. The function of the application and data it contains will be unchanged. There is no change to the type of data stored or processed by NOAA4300. Upon completion of the migration to the new instance, both NOAA4011 and NOAA4300 staff will verify functionality and data integrity/minimization prior to the migrated application going into production. NOAA4300 has been provided the estimated completion dates for the following critical milestones from Tesa for the CSOS migration: • Application migration – August 4th, 2023 • Functionality and data reviews - August 15th, 2023 • Production cutover – August 25th, 2023 .
	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.	Executive Orders 10450, 11478	Security Investigations (Security Clearance actions)	COMMERCE/DEPT-13
	5 U.S.C. 7531-332		
	28 U.S.C. 533-535		
	Equal Employment Act of 1972		
2.	Executive Order 12656	Emergency Preparedness/COOP	COMMERCE/DEPT-18
	Federal Preparedness Circular (FPC) 65, July 26, 1999		
3.	Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 et seq.	Fisheries Permits & Registrations	NOAA-19
	High Seas Fishing Compliance Act of 1995, 16 U.S.C 5501 et seq.		
	International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters, 50 CFR 300.120		
	American Fisheries Act, Title II, Public Law No. 105–277		
	Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101-5108, as amended 1996		
	Tuna Conventions Act of 1950, 16 U.S.C. 951-961		
	Atlantic Tunas Convention Authorization Act, 16 U.S.C., Chapter 16A		
	Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 et seq.		
	Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431-2444		
	Western and Central Pacific Fisheries Convention Implementation Act, 16 U.S.C. 6901 et seq.		
	Dolphin Protection Consumer Information Act, 16 U.S.C. 1385		
	Marine Mammal Protection Act, 16 U.S.C. 1361 et seq		
	Commerce, Justice, Science and Related Agencies Act, 2018, Division B, Section 539 (Pub. L. 115-141)		
	Taxpayer Identifying Number, 31 U.S.C. 7701		

4.	The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq	Marine Mammal / Endangered Species Permits	NOAA-12
	Fur Seal Act, 16 U.S.C. 1151 et seq		
	Endangered Species Act, 16 U.S.C. 1531 et seq.		
	31 U.S.C. 7701.		
5.	31 U.S.C. 66a	Personnel Actions Including Training	COMMERCE/DEPT-1
	44 U.S.C. 3101, 3309		
	Title 5 U.S.C.		
6.	5 U.S.C. 552, Freedom of Information Act	FOIA & Privacy Act Requests	COMMERCE/DEPT-5
	5 U.S.C. 552a, Privacy Act of 1974 as amended		
	5 U.S.C. 301		
	44 U.S.C. 3101		
7.	5 U.S.C. 301	Biographical Info / Social Networks	COMMERCE/DEPT-20
	15 U.S.C. § 1516		
	E.O. 11625		
	Presidential Memorandum to the Heads of Executive Departments and Agencies on Transparency and Open Government, January 21, 2009		
	OMB Open Government Directive, M-10-06, December 8, 2009		
	OMB Guidance for Online Use of Web Measurement and Customization Technologies, M-10-22, June 25, 2010		
8.	5 U.S.C. 301, Departmental Regulations	Contact Information for the Public	NOAA-11
	15 U.S.C. 1512, Powers and duties of Department		
9.	5 USC 301	System Administration/Audit Data (SAAD)	COMMERCE/DEPT-25
	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		

10.	5 U.S.C. 301	Badging & CAC Issuance	GSA/GOVT-7
	Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors		
	Federal Information Security Management Act of 2002 (44 U.S.C. 3554)		
	E-Government Act of 2002 (Pub. L. 107–347, Sec. 203)		
11.	5 U.S.C. 301	Litigation	COMMERCE/DEPT-14
	28 U.S.C. 533-535 and 1346(b)		
	44 U.S.C. 3101		
12.	Rehabilitation Act, 29 U.S.C. 701 et. seq	Public Health Emergency Info & Reasonable Accommodation	COMMERCE/DEPT-31
	Americans with Disabilities Act of 1990, as amended, 102(d), 42 U.S.C. 12112(d)		
	29 CFR parts 1602, 1630, 1904, 1910, and 1960		
	29 USC chapter 15 (e.g., 29 U.S.C. 668)		
	Executive Order 12196		
	5 U.S.C. 7902		