Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
Southeast Regional Office Local Area Network
(NOAA4300)

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
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.11.09 13:51:12 -05'00' October 16, 2018

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

U.S. Department of Commerce Privacy Impact Assessment
NMFS Southeast Regional Office Local Area Network

Unique Project Identifier: 006-48-01-14-02-3305-00

Introduction: System Description

The Southeast Regional Office NOAA4300 system functions as the overall office automation support system for the NOAA/NMFS offices in St. Petersburg, Florida. It provides access to automated systems typically found in administrative offices within the federal government. It supports all offices within the Southeast Region (SER) which include 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.

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, 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. To manage U.S. fisheries, the NOAA National Marine Fisheries Service (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 allow positive identification and cost recovery billing of 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.

eDiscovery Application: The eDiscovery Platform system is a web-based application used to simplify agency response to Freedom of Information Act (FOIA) requests, aid in the processing Administrative Records (AR), and to a lesser extent, Congressional Inquiries and Legal Holds. The system serves as a single point for the collection, review, tagging, redaction and export of responsive records.

NOAA4300 will have a data sharing agreement with the Atlantic Coastal Cooperative Statistics Program (ACCSP). The ACCSP requires a unique identifier for each for-hire SER Permit holder in order to validate landing reports. ACCSP will provide an algorithm to NMFS, who will run the algorithm for each applicable permit holder in order to generate the identifier, and then share the encrypted identifier with ACCSP. Although the identifier will be comprised of fragmentary PII (birthdate, email address, and phone number), there will be no exploitable data contained in the generated identifier.

ACCSP was established through NOAA's provision for Fishery Information Networks (FIN) to address data deficiencies that constrained the management of fisheries along the Atlantic coast. With the proposed implementation of the South Atlantic Fishery Management Council's electronic logbook reporting for the for-hire sector by the National Marine Fisheries Service (NMFS), there is a need for efficient and cost-saving data collection. The implementation team for the for-hire reporting investigated numerous options for data housing, with the decisive elements including 1) accessibility to NMFS staff and program patterns, 2) flexibility in database design, 3) integration with other agency programs (e.g., state programs, NMFS Mid-Atlantic,

VMS), 4) staffing needs to develop and maintain the system, and 5) estimated initial and annual costs.

Data housing solutions were limited to those either run by the government or funded through the government, such as FIN, as these groups would be most experienced with confidential data requirements. The Implementation team reviewed the various options and settled on using ACCSP as the first line choice for a variety of factors, with top factors including costs, flexibility, and integration. ACCSP has an existing data warehouse structure and data collection system that will meet the needs of for-hire electronic logbook reporting, saving NMFS significant initial costs ($500 K to $1.5 M) and annual costs ($120K to $240K for software renewals and staffing). The ACCSP system is a flexible system that has the ability to integrate with various other NMFS and state agencies. Furthermore, ACCSP has a long-standing working relationship with NMFS and already is the first receiver of federal dealer data supplied by the Gulf and South Atlantic states. ACCSP has also been developing front-end user tools and interfaces that allow for a free mobile app to be available for any participant to use to enter the required data elements.

For this system to work effectively, ACCSP will need to link the data collected from electronic reports with data contained within NMFS permit system. In addition, the ACCSP would need to establish the linkage at the time of the creation of user accounts in ACCSP. The information needed to successfully link the two, in the absence of using a Tax ID Number (SSN or FEIN), would be a unique identifier generated from fragments of each permit holder's name, email address, birth date, and phone number. This unique identifier would be generated using an algorithm supplied by ACCSP. Without providing ACCSP access to this information, there is a high likelihood that NMFS will not be able to move forward with using the ACCSP as the data warehouse, which would significantly delay implementation of the reporting program as well as cost NMFS significant money.

The overall legal authority for collection of information addressed in this PIA is:

5 U.S.C. § 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

FOIA-related authorities: 5 U.S.C. 552 and 552a, 15 CFR Part 4.

Permit and registration data are collected from individuals under the authority of the Magnuson-Stevens Fishery Conservation and Management Act, the High Seas Fishing Compliance Act, the American Fisheries Act, the Tuna Conventions Act of 1950, the Atlantic Coastal Fisheries Cooperative Management Act, the Atlantic Tunas Convention Authorization Act, the Northern Pacific Halibut Act, international fisheries regulations regarding U.S. Vessels Fishing in Colombian Treaty Waters, the Marine Mammal Protection Act, the Endangered Species Act and the Fur Seal Act. The authority for the mandatory collection of the Tax Identification Number is 31 U.S.C. 7701.

From: COMMERCE/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; Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.

From: COMMERCE/DEPT-14: 5 U.S.C. 301; 44 U.S.C. 31101; 42 U.S.C. 3211; 31 U.S.C. 240; 28 U.S.C. 533-535 and 1346(b); 15 U.S.C. 277 and 278e(b); E.O. 10450; E.O. 11478, as amended and all other authorities of the Department.

From COMMERCE/DEPT-18: 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.

From: COMMERCE/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 and IRS Publication-1075.

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

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

____ 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.

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		i. Credit Card	X
b. Taxpayer ID	X	f. Driver's License	X	j. Financial Account	X
c. Employer ID	X	g. Passport	X	k. Financial Transaction	X
d. Employee ID	X	h. Alien Registration	X	l. Vehicle Identifier	

m. Other identifying numbers (specify):
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.

Tax Identification Numbers allow positive identification for cost recovery billing of Individual Fishing Quota holders.

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.

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:
*Information required for Security Clearance by DOC Security. Security Officer collects information and submits forms for clearance process. Human Resources staff use truncated SSNs to verify employee identification. This information is stored on an encrypted hard drive, accessible only to authorized NOAA4300 personnel.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	
c. Alias	X	i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	X
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	

s. Other general personal data (specify): Permit applicant, permit holder, permit transferor/transferee, vessel owner, vessel operator, dealer applicant, dealer permit holder, spouse, former spouse, decedent.

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):

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X*	d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos	X*	h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	

j. 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	X	Personal Identity Verification (PIV) Cards	
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

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

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

*For entrance to secure areas only, not for building entrance.

	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.

eDiscovery Application: Any PII/BII contained in the data flagged as relevant by the application based upon the search criteria applied is used in the review process and is redacted before it is released to the requestor. The application does not actually save the data; it only saves the metadata or pointers to the scanned document.

NOAA4300 will have a data sharing agreement with ACCSP. The ACCSP requires the generation of a unique identifier made up of fragmentary data drawn from the name, email address, telephone number, and birthdate of all for-hire SER Permit holders in order to validate landing reports. ACCSP will collect the unique identifier of SERO permit holders through an interconnection agreement with NOAA4400, Southeast Fisheries Science Center.

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.)

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			
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.

6.2 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: NMFS Office of Law Enforcement (OLE) Access Enforcement (AC-3). Access to PII is controlled through access control policies and access enforcement mechanisms (e.g., access control lists). Separation of Duties (AC-5). Separation of duties for duties involving access to PII is enforced. Least Privilege (AC-6). Organizations can enforce 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. Remote Access (AC-17). Organizations can choose to prohibit or strictly limit remote access to PII. Access Control for Mobile Devices (AC-19). Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization‘s facilities). Auditable Events (AU-2). Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII. Audit Review, Analysis, and Reporting (AU-6). Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions. Identification and Authentication (Organizational Users) (IA-2). Users can be uniquely identified and authenticated before accessing PII. Media Access (MP-2). Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm). Media Marking (MP-3). Organizations can label information system media and output containing PII to indicate how it should be distributed and handled. Media Storage (MP-4). Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures. Media Transport (MP-5). Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization‘s controlled areas. Media Sanitization (MP-6). Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse. Transmission Confidentiality (SC-9). Organizations can protect the confidentiality of transmitted PII. Protection of Information at Rest (SC-28). Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.

	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.)*

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. A link to the Privacy Act statement and/or privacy policy can be found on the bottom of page 6 at: https://www.google.com/url?q=http://sero.nmfs.noaa.gov/operations_management_information_services/constituency_services_branch/permits/permit_apps/documents/vessel/vesseleezapplication.pdf&sa=D&source=hangouts&ust=1528309033039000&usg=AFQjCNECgLXvGJhQqDT17X5QAhmLixX1iw (Go to Page 6 of the Instructions for vessels fishing in the Exclusive Economic Zone. Follow instruction on the last line on that page. "For Privacy Act information related to SERO Permits and Permit Applications go to …") . eDiscovery Application: The information is redacted as part of the FOIA review process. The user voluntarily submits the information; if not, the business cannot be conducted. The Privacy Act Statement can be found at the e Discovery login screen: https://155.206.130.32/esa/public/login.jsp	
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.
	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. eDiscovery Application: The BII/PII is collected via email as part of conducting business. Not providing the information affects the ability to access the system.
	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.

		Permits: The individual consents to the intended uses by completion of the application. Information for public outreach and education is strictly voluntary. The email response to the individual outlines the NOAA Privacy Policy, which states that "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose." Individuals are directed to the Web pages or other resources. eDiscovery Application: The BII/PII is collected via email as part of conducting business. Not providing the information affects the ability to access the system.
	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. eDiscovery Application: The BII/PII is collected via email as part of conducting business.
	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:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/8/2017 ☐ 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 supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish 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 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's 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 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)*: DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons DEPT-5, Freedom of Information and Privacy Request Records DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies DEPT-19, Department Mailing Lists DEPT-20, Biographical Files NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. eDiscovery Application: Commerce/DEPT-5, Freedom of Information Act and Privacy Act Request Records also applies to this application. Permits: COMMERCE/DEPT-13, Investigative and Security Records. COMMERCE/NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Exempted Applicants COMMERCE/DEPT-14, Litigation, Claims, and Administrative Proceeding Records. COMMERCE/DEPT-25, Access Control and Identity Management System GSA/GOVT-7, Federal Personal Identity Verification Identity Management System (PIV IDMS)
	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 20, Electronic 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 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 levels. *(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: There will be no more mailing of completed permit applications from applicants to NOAA.
	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.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: ACCSP will provide an algorithm to NOAA4300, who will run the algorithm for each applicable permit holder to generate a unique identifier. NOAA4300 will add a table to the PIMS database to store the identifier.
	No, the conduct of this PIA does not result in any required technology changes.