Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
NOAA4020
Science and Technology

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

for Dr. Catrina D. Purvis LISA MARTIN Digitally signed by LISA MARTIN Date: 2020.04.14 14:02:43 -04'00' 03/05/2020

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA4020 Science and Technology

Unique Project Identifier: 006-03-02-00-01-0511-00

Introduction: System Description

The NOAA4020 Science and Technology (S&T) system functions as a general data processing system for NOAA and NMFS headquarters located in Silver Spring, MD. It provides resources to support scientific operations and research, data and information management, fisheries surveys, statistical analysis, stock assessments, socio-economic analysis, ecosystem management, other national program database and applications development, and management decisions needs. The user base of this system reaches across different headquarter offices and across regions and science centers within NMFS. Many of these automated systems are built in support of the NOAA Fisheries mission.

1) International Trade Data System (ITDS)
ST6 International Trade Data System (ITDS) is used to support a number of NMFS offices/programs to monitor imports of fisheries products. Types of BII data collected are name of business, address, contact information, and product information. The data is collected by U.S. Customs and Border Protection (CBP) provided to NMFS via SFTP for inclusion in the ITDS database. Reasons for the NMFS database:

(1) The ITDS is an inter-agency, distributed system that allows businesses to submit trade data to a single agency (CBP). CBP then makes these data available to participating ITDS agencies via secure, system integration.

(2) The NMFS component of the ITDS is an import monitoring system designed to improve the efficiency and accuracy of NMFS trade monitoring programs by utilizing the data and services provided by CBP via the national ITDS architecture. NMFS trade monitoring programs supported by the NMFS ITDS include the Antarctic Marine Living Resources (AMLR) program, the Highly Migratory Species (HMS) program, the Seafood Import Monitoring Program (SIMP), and the Tuna Tracking Verification Program (TTVP). The NMFS ITDS is also integrated with the NMFS National Permit System (NPS) to provide international trade permit data to NMFS trade monitoring programs and to CBP.

2) Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL)
The Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL) system is a tool to collect and process recreational saltwater fishing license and registration data from the Atlantic and Gulf of Mexico coastal states for inclusion in the National Saltwater Angler Registry (NSAR).Types of PII collected include fishing license information, name, address, driver's license number, phone, email, and date of birth.

This section was changed to improve the clarity and accuracy of the text. Nothing significant changed on any of these applications. This does not impact our overall privacy risk as far as being a moderate FISMA system.

3) National Saltwater Angler Registry - NSAR
The National Saltwater Angler Registry (NSAR) system serves as a consolidated phone book of the nation's recreational saltwater anglers. NSAR data is used to furnish frames for the MRIP surveys. Types of PII collected include fishing license information, name, address, driver's license number, phone, email, and date of birth.

4) NOAA Fisheries Committee on Scientific Stature. This is not an outside advisory committee.
The NOAA Fisheries Committee on Scientific Stature (NFCSS) is a national-level Performance Management Advisory Committee (PMAC) established to review the contributions, impact and stature of NOAA Fisheries Band IV and V non-supervisory research scientists. The NFCSS evaluates scientists whose primary responsibility is to conduct research and develop scientific products for resource management advice, other scientific advice, publications, and reports that represent new or more comprehensive understanding of a subject. The NFCSS members are Band V scientists, who are subject matter experts, from the regional science centers appointed to three-year terms by the respective regional Science Director. There is a website and database to manage and record the results of NFCSS member reviews conducted for the purpose of evaluating a scientist's credentials and contributions to allow them to be assigned to a higher pay Band without being a supervisor and to produce a standard report for the committee chair (OSTScience Director). In 2014, OST upgraded the NFCSS website and database to enable password protected, role-based secure storage and retrieval of review package documents. Access to the database is restricted to the OST Science Director, the six regional Deputy Science Directors, one Band V research scientist from each regional science center, the NOAA Fisheries HR Business Partner, and the NFCSS database administrator and is provided by the NFCSS database administrator only at the request of the NFCSS Chair. Information collected: name, work contact information, letters of reference and curricula vitae, performance plan, science director memoranda and name of immediate supervisor. The administrator uploads copies of a memorandum from the NFCSS

Chair to the Science Center director of staff being reviewed. The data (name, email, documents) for staff being reviewed are entered by their Deputy Science Director. The review comments are entered by the NFCSS members.

5) Protected Resources National Inventory of Marine Mammals (NIMM) System.

The National Inventory of Marine Mammals (NIMM) system maintains current and past data (it replaces previous inventory databases maintained by NMFS since the 1970s) on marine mammals under NMFS' jurisdiction (dolphins, porpoises, whales, seals, and sea lions) held in permanent captivity for public display. In addition, NIMM includes information on marine mammals held in permanent captivity for scientific research, enhancement, and national defense purposes. NIMM includes beached/stranded marine mammals only if they have been deemed non-releasable and cannot be returned to the wild. NIMM allows marine mammal Owners and Facilities to enter inventory data directly into the online system. NIMM will eventually provide the public with real-time access to the national inventory. Types of BII collected include institution name, address, email, phone, and fax.

6) NOAA Emergency Contact List

The Emergency Contact List stores store contact information for ST staff and staff emergency contacts to be used in case of emergency. This is PII data.

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

The NOAA4020 Science and Technology (S&T) system is a general support system for NMFS headquarters.

(b) System location

NOAA4020 NMFS headquarters located in SSMC3 Room 12244 in Silver Spring, MD.

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

NOAA4020 is a subsystem of NOAA4000.

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

NOAA4020 provides application servers, database servers, proxy servers, file servers, sftp servers to achieve its purpose.

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

NOAA users login to the web based application within NOAA. External users access the information via public-facing, web-accessible applications and web sites.

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

The information is transmitted within NMFS via Local and Wide area Networks using secure connections. Information is transmitted to external users through secure internet connections.

(g) Any information sharing conducted by the system

The NOAA4020 system shares data with various NOAA internal and external systems. These relationships are documented in Interconnect Security Agreements (ISAs). We also share data with NOAA internal and external individuals and organizations on a per request basis subject to data request procedures specific to each data set.

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

From NOAA-19: Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 et seq. (Magnuson-Stevens Act); 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; the American Fisheries Act, Title II, Public Law 105-277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101-5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951-961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C., Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 et seq. (Halibut Act); the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431-2444; the Western and Central Pacific Fisheries Convention Implementation Act, 16 U.S.C. 6901 et seq. (WCPFCIA); the Marine Mammal Protection Act, 16 U.S.C. 1361; and Taxpayer Identifying Number, 31 U.S.C. 7701.

From NOAA-21: Title XI of the Merchant Marine Act of 1936 as amended and codified, 46 U.S.C. 1177 and 46 U.S.C. 53701 et seq., the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 et seq., and provisions of the Debt Collection Improvement Act as codified at 31 U.S.C. 7701.

From DEPT-18: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

From DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972. Types of PII data collected is Contact Name, Phone Number and Address.

The legal authority for the Emergency Contact List 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.

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

This is a FIPS 199 moderate level 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 (version 01-2015).

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License	X	j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	X
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

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

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X		
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
k. Other work-related data (specify): For NOAA **Fisheries Committee on Scientific Stature** l. Performance Plan m. Supervisor Justification n. Science Director Memoranda o. Letters of Reference p. Curriculum Vitae					

q. Position Description

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

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

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

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

* For the ECL

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

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

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

The web applications used to collect information contain various front-end and back-end validations to check for accuracy. Data that are not collected directly from the subject of the information are run through various quality control procedures, including format and content validation and standardization. In some cases data are reconciled against other data sets to check for data errors or updates.

In addition, various controls are in place to ensure that only those who are authorized and have a need to modify the data are able to so.

The general controls used to protect the PII involve controlled physical and logical access, role based access control, proper data segmentation and protection via encryption at rest and proper audit logging of events. Adequate media marking, transport and storage and incident monitoring and response are also used.

The levels of implementation for these technologies meet the criteria required by NIST 800-53, Rev 4 under the following controls: Access Enforcement (AC-3), Separation of Duties (AC-5), Least Privilege (AC-6), Remote Access (AC-17), User-Based Collaboration and Information Sharing (AC-21). , Auditable Events (AU-2), Audit Review, Analysis, and Reporting (AU-6), Identification and Authentication (Organizational Users) (IA-2), Media Access (MP-2) , Media Marking (MP-3), Media Storage (MP-4), Media Transport (MP-5), Media Sanitization (MP-6), Transmission Confidentiality (SC-9), Protection of Information at Rest (SC-28), Information System Monitoring (SI-4).

In addition to following database CIS benchmarks and best practices, all Oracle tables that contain PII/BII data are stored in an encrypted tablespace.

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 Number: 0648-0578
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

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

Section 3: System Supported Activities

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

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

X	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			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation	X	For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify): To maintain databases for tracking international seafood trading tracking, angler registration, for use in reviewing scientists' research products, and a Protected Resources marine mammal inventory.			

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).

Emergency Contact List (ECL)
The Emergency Contact List stores store contact information for ST staff and staff emergency contacts to be used in case of emergency. PII collected includes name, relationship, address, and phone. This information is collected from employees and contractors.

International Trade Data System (ITDS)
ST6 International Trade Data System (ITDS) is used to support a number of NMFS offices/programs to monitor imports of fisheries products. Types of BII data collected include

name of business, address, contact information, and product information. The data is collected from U.S. Customs and Border Protection.

MRIP ETL
The Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL) system is a tool to collect and process recreational saltwater fishing license and registration data from Atlantic and Gulf of Mexico coastal states for inclusion in the National Saltwater Angler Registry (NSAR). Types of PII collected include fishing license information, name, address, driver's license number, phone, email, and date of birth of the angler. The MRIP ETL collects data from the NSAR, below.

National Saltwater Angler Registry - NSAR
The National Saltwater Angler Registry (NSAR) system serves as a consolidated phone book of the nation's recreational saltwater anglers. NSAR data is used to furnish frames for the MRIP surveys. Types of PII collected include fishing license information, name, address, driver's license number, phone, email, and date of birth. The NSAR is only applicable to anglers ages 16 and older. The date of birth is used for validation of this requirement.

NOAA Fisheries Committee on Scientific Stature. This is not an outside advisory committee.
The NOAA Fisheries Committee on Scientific Stature (NFCSS) is a national-level Performance Management Advisory Committee (PMAC) established to review the contributions, impact and stature of NOAA Fisheries Band IV and V non-supervisory research scientists. The NFCSS evaluates scientists whose primary responsibility is to conduct research and develop scientific products for resource management advice, other scientific advice, publications, and reports that represent new or more comprehensive understanding of a subject. The NFCSS members are Band V scientists, who are subject matter experts, from the regional science centers appointed to three-year terms by the respective regional Science Director. There is a website and database to manage and record the results of NFCSS member reviews conducted for the purpose of evaluating a scientist's credentials and contributions to allow them to be assigned to a higher pay Band without being a supervisor and to produce a standard report for the committee chair (OST Science Director). In 2014, OST upgraded the NFCSS website and database to enable password protected, role based secure storage and retrieval of review package documents. Access to the database is restricted to the OST Science Director, the six regional Deputy Science Directors, one Band V research scientist from each regional science center, the NOAA Fisheries HR Business Partner, and the NFCSS database administrator and is provided by the NFCSS database administrator only at the request of the NFCSS Chair. Information collected: name, work contact information, letters of reference and curricula vitae, performance plan, science director memoranda and name of immediate supervisor. The administrator uploads copies of a memorandum from the NFCSS Chair to the Science Center director of staff being reviewed. The data (name, email, documents) for staff being reviewed are entered by their Deputy Science Director. The review comments are entered by the NFCSS members.

Protected Resources National Inventory of Marine Mammals (NIMM) System.
The National Inventory of Marine Mammals (NIMM) system maintains current and past data (it replaces previous inventory databases maintained by NMFS since the 1970s) on marine mammals under NMFS' jurisdiction (dolphins, porpoises, whales, seals, and sea lions) held in permanent captivity for public display. In addition, NIMM includes information on marine

mammals held in permanent captivity for scientific research, enhancement, and national defense purposes. NIMM includes beached/stranded marine mammals only if they have been deemed non-releasable and cannot be returned to the wild. NIMM allows marine mammal Owners and Facilities to enter inventory data directly into the online system. NIMM will eventually provide the public with real-time access to the national inventory. Types of BII collected include institution name, address, email, phone, and fax.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There is always the potential threat to privacy due to insider threat, but this threat is greatly mitigated by the controls we have in place.

All staff, federal employees and contractors, are required to take annual IT Security Awareness and Privacy Training.

Dissemination of PII/BII is subject to controls in place to restrict access to only those who need access to the data. Everyone who does have access to the data must provide signed copies of the NOAA Administrative Order 216-100 Data Confidentiality form, including the Statement of Nondisclosure.

If the data is to be shared with an external organization (e.g. contracting company or university) then a representative of the external organization must complete the Agreement of Access form and each representative of the external organization who will be accessing the data will have to provide a signed Certificate.

There are also various controls in place to ensure that only those who are authorized and have a need to modify the data are able to so.

The general controls used to protect the PII involve controlled physical and logical access, role based access control, proper data segmentation and protection via encryption at rest and proper audit logging of events. Adequate media marking, transport and storage and incident monitoring and response are also used.

The levels of implementation for these technologies meet the criteria required by NIST 800-53, Rev 4 under the following controls: Access Enforcement (AC-3), Separation of Duties (AC-5), Least Privilege (AC-6), Remote Access (AC-17), User-Based Collaboration and Information Sharing (AC-21). , Auditable Events (AU-2), Audit Review, Analysis, and Reporting (AU-6), Identification and Authentication (Organizational Users) (IA-2), Media Access (MP-2) , Media Marking (MP-3), Media Storage (MP-4), Media Transport (MP-5), Media Sanitization (MP-6), Transmission Confidentiality (SC-9), Protection of Information at Rest (SC-28), Information

System Monitoring (SI-4).

In addition to following database CIS benchmarks and best practices, all Oracle tables that contain PII/BII data are stored in an encrypted tablespace.

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

*In case of breach

** NIMM

	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: NOAA4020 connects with NOAA4000. Technical boundary controls are in place to prevent BII leakage. NOAA4020 consists of servers that support the development and deployment of application offerings that facilitate the provision of mission related services to the general public, authorized organizational and non-organizational users. NOAA4000 provides general support system (GSS, i.e. LAN/WAN network connectivity) services to NOAA4020.
	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	X*	Government Employees	X
Contractors	X		
Other (specify):			

*NIMM

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: NSAR Site and PAS: https://www.countmyfish.noaa.gov/register/ The ECL PAS: *Site not available to non-NOAA staff. A screen shot with the PAS is included in the cover email for this PIA.* .	
X	Yes, notice is provided by other means.	Specify how: The ECL has a Privacy Act Statement: This information collection is voluntary. The purpose is to maintain an emergency contact list. The personally identifiable information will not be shared outside the S&T. ITDS: The data is collected from the U.S. Customs and Border Protection's ITDS database, who provides notice at the time of collection.
	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: For the ECL application, employees and contractors may decline to their supervisors in writing, but they may then not be notified in case of emergencies. ITDS: the NMFS ITDS is not the original point of collection. NIMM: An individual can choose not to be the responsible official or the primary contact. NSAR: The individual will not register if he wishes to decline. MRIP ETL: No data collected directly by 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: For the ECL, emergency contact is the only use for the information. ITDS: the NMFS ITDS is not the original point of collection. NIMM: Reporting is required. NSAR: Anglers may choose not to register. There is no option to register and opt out of the survey. An angler may decline to

		respond to the survey if contacted. MRIP ETL: No data collected directly by 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: For ECL, users may log on to the application and update the information at any time. ITDS: the NMFS ITDS is not the original point of collection. NIMM: Those with NIMM user accounts have access rights to review and update their data. NSAR: Information may be updated at the time of registration renewal. MRIP ETL: No data collected directly by the system.
	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.)*

X	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: Audit log
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): 06/06/2019 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. MODERATE
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.

	Other (specify):

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).*

The general controls used to protect the PII in these applications, involve controlled physical and logical access: role based access control, proper data segmentation and protection via encryption at rest and proper audit logging of events. Adequate media marking, transport and storage and incident monitoring and response are also used.

The levels of implementation for these technologies meet the criteria required by NIST 800-53, Rev 4 under the following controls: Access Enforcement (AC-3), Separation of Duties (AC-5), Least Privilege (AC-6), Remote Access (AC-17), User-Based Collaboration and Information Sharing (AC-21). , Auditable Events (AU-2), Audit Review, Analysis, and Reporting (AU-6), Identification and Authentication (Organizational Users) (IA-2), Media Access (MP-2), Media Marking (MP-3), Media Storage (MP-4), Media Transport (MP-5), Media Sanitization (MP-6), Transmission Confidentiality (SC-9), Protection of Information at Rest (SC-28), Information System Monitoring (SI-4).

In addition to following database CIS benchmarks and best practices, all Oracle tables that contain PII/BII data are stored in an encrypted tablespace.

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/NOAA-19**, Permits and Registrations for United States Federally Regulated Fisheries **COMMERCE/NOAA-21**, Financial Services Division **COMMERCE/DEPT-18**, Employees Personnel Files Not Covered By Notices of Other Agencies **COMMERCE/DEPT-13**, Investigative and Security Records.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule: NFCSS: Chapter 300 Personnel Management Files 301-09 Supervisors' Personnel Files. Records on positions, authorizations, pending actions, position descriptions, training records, individual development plans, telework agreements, award recommendations, and records on individual employees not duplicated in or not appropriate for the OPF. These records are sometimes called supervisors' working files, unofficial personnel files (UPFs), and employee work folders or "drop" files. DAA-GRS-2017-0007-0012 (GRS 2.2, item 080) Supersedes NOAA Schedule Items: 303-22a (GRS 1, item 18a) 303-22b (GRS 1, item 18b) **TEMPORARY**. Review annually and destroy superseded documents. Destroy remaining documents 1 year after employee separation or transfer. Chapter 1500 – Fishery and Living Marine Resource Functional Files ECL: DAA-GRS- 2013-0006-003. Disposition instruction: Temporary. Destroy when business need ceases.
	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:
	Yes, retention is monitored for compliance to the schedule.
X	No, retention is not monitored for compliance to the schedule. Provide explanation: We are not currently monitoring compliance as we are in the process of reconciling our records management policy with our data management policies to ensure that the records management policy is comprehensive and accurate.

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

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

X	Identifiability	Provide explanation: The PII/BII currently collected and stored presents a moderate impact of identifiability.
X	Quantity of PII	Provide explanation: Collective harm to individuals, but also harm to the organization's reputation and the cost to the organization in addressing a possible breach was considered.
X	Data Field Sensitivity	Provide explanation: Multiple applications contain contact information that are not considered sensitive PII/BII.
X	Context of Use	Provide explanation: The purpose for which PII is collected, stored, used, processed, disclosed, or disseminated was considered. Whether disclosure of the mere fact that PII is being collected or used could cause harm to the organization or individual was considered.
X	Obligation to Protect Confidentiality	Provide explanation: Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801, Section 402b.
X	Access to and Location of PII	Provide explanation: The nature of authorized access to PII - The number and frequency of access was also considered. The degree to which PII is being stored on or accessed from teleworkers' devices or other systems, such as web applications, outside the direct control of the organization and whether PII is stored or regularly transported off-site by employees was considered.
	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.)

We collect PII from states for including in the National Saltwater Angler Registry (NSAR). We collect the information from the states because it is more efficient, cost-effective, and less burdensome to the public than collecting the information from the individuals. There is some potential risk in collecting the data from the states, but this risk is greatly mitigated by the controls

we have in place.

Submission is controlled via authenticated, role-based, access to a web application using secure socket layer (SSL) certificates or via secure file transfer protocol (SFTP) using private/public key pairs.

PII is encrypted at all time during transmission and while at rest.

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

	Yes, the conduct of this PIA results in required business process changes.

	Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.