Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA4020
Science and Technology

Reviewed by: _____, 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 D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.07.25 16:13:46 -04'00'

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

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

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

Introduction: System Description

The Fisheries Finance Program (FFP) provides three types of loans: a. Direct Loans for Vessels, Shoreside Facilities, and Aquaculture; b. Mariculture Fisheries Finance and c. FFP Halibut/Sablefish and Crab Individual Fishing Quota (IFQ) loans.

The application for FFP financing (NOAA Form 88-1) provides the information needed to determine whether the applicant is a good credit risk. All applicants for FFP financing are requested to provide information such as the applicant's name and address, the amount of financing applied for, the purpose of loan, an appraisal of the vessel or facility involved, financial information including the last 3 tax returns (these are not stored electronically), a list of creditors and buyers with relevant credit terms, identification of authorized representatives (accountant, attorney, insurance agent), and legal history (status regarding bankruptcy, litigation, delinquency on and Federal debt, etc.). Annual financial statements are required of all borrowers. These statements update the financial statement information presented with the original application. The financial statements are used to monitor the borrower's financial condition and to trigger servicing actions if indicated.

Loan applications are entered into the system from paper forms completed by the public, into an online application, which is managed by NMFS NOAA4020. Regional offices access the information in order to administer loans for applicants. The loan data is stored only in NOAA4020.

The Emergency Contact List is used to track and locate staff in the office of Science and Technology. This is the only other collection of PII stored in this FISMA system.

System user ID information is collected from employees and contractors accessing the system.

Information is not shared except within the program (NMFS Headquarters, West Coast Region and Southeast Region).

Chapter 537 of the Shipping Act (formerly Title XI of the Merchant Marine Act), codified at 46 U.S.C. 53701, authorizes the Fisheries Financing Program (FFP) to assist business in financing or refinancing commercial fishing vessels, fisheries shoreside facilities, aquaculture operations, and individual fishing quotas (IFQ). All obligations involving any fishing vessel, fishery facility, aquaculture facility, or individual fishing quota issued subsequent to the Sustainable Fisheries Act are direct loan obligations. These financings contribute to the stability of the fishing industry, which continues to be viewed by the Congress as in the national interest. New regulations under the Shipping Act were enacted by Final Rule 0648-AY16, to allow crab IFQ

loans (75 FR 78619), December 16, 2010. Relevant portions of the Shipping Act are codified at 50 CFR Part 253.

The legal authority for the Emergency Contact List collection of information addressed in this PIA is:

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

This is a 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.)*
__X__ This is an existing information system with no changes that create new privacy risks.

Changes That Create New Privacy Risks (CTCNPR) - NA					
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):					

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	
b. Taxpayer ID	X*	f. Driver's License		j. Financial Account	X
c. Employer ID		g. Passport		k. Financial Transaction	X
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					

*Required for identification of the individual for payment purposes, and for verification of financial information.

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

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

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	X	Online	X*
Telephone		Email			
Other (specify):					

* For the ECL

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
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 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		For criminal law enforcement activities	
For civil enforcement activities		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): To determine loan qualifications.			

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).

Members of the public:

The Fisheries Finance Program (FFP) provides direct loans for certain fisheries costs. Vessel financing is available for the purchase of used vessels or the reconstruction of vessels (limited to reconstructions that do not add to fishing capacity). Refinancing is available for existing debt obligations. FFP loans are not issued for purposes which could contribute to over capitalization of the fishing industry. Finance or refinance fisheries shore side facilities or Aqua cultural facilities. The program provides Individual Fishing Quota (IFQ) financing (at the request of a Fishery Management Council). IFQ financing is available to first time purchasers and small vessel operators in the Halibut Sablefish fisheries. FFP also provides long term fishery buy back financing (at the request of a Fishery Management Council or Governor) to purchase and retire fishing permits and/or fishing vessels in overcapitalized fisheries.

FFP financing offers the fishing industry slightly better interest rates and longer term loans than are available elsewhere. The longer-term loans allow the industry to amortize their capital investment over the actual economic life of the fisheries asset. Lower debt service reduces economic pressure, thus allowing the borrower to more easily accommodate more restrictive fishery management initiatives. FFP regulations ensure that FFP traditional lending will not increase harvesting capacity in the fisheries but will simply permit the financing of the acquisition of existing vessels/facilities or the refinancing of existing debt for vessels/facilities already in the fishery.

Applications are required in order to determine qualification for a loan, and to provide contact information with borrowers. Annual financial statements are required of all borrowers. These statements update the financial statement information presented with the original application. The financial statements are used to monitor the borrower's financial condition and to trigger servicing actions if indicated.

This information is collected from members of the public.

The Emergency Contact List (ECL) is used to track and locate staff in the office of Science and Technology: name, occupation, work address and email. This information is collected from employees and contractors.

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

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

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		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. **Dept-18, Employees Personnel Files Not Covered by Notices of Other Agencies; NOAA-21, Fisheries Finance Division**	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The FFP Privacy Act statement and/or privacy policy can be found at: _ _ http://www.nmfs.noaa.gov/gpea_forms/mb/0012_noaaform_88_1.pdf. http://www.nmfs.noaa.gov/gpea_forms/mb/0648_0041_application_2016.pdf http://www.nmfs.noaa.gov/gpea_forms/mb/0082_cfc_application_2016.pdf	
X	Yes, notice is provided by other means.	Specify how: The FFP application specifies which information is required. The ECL now has a Privacy Act Statement: This information collection is authorized under 5 U.S.C 301, and is voluntary. The purpose is to maintain an emergency contact list. The personally identifiable information will not be shared outside the S&T. A screen shot signed by the director and operations director is included in the cover 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: For FFP, applicants may decline to provide PII/BII, but if required information is not provided, the applicant cannot receive the benefit. 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.
	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 FFP, consent for the specified use is implied by completing and signing the loan application. Notice is also provided in NOAA-21. Above the signature is this text: The Applicant certifies that: (1) it is a citizen of the United States (if a corporation, at least 75% of the stock must be held by U.S. citizens), and (2) all information in this application is true and correct to the best of the applicant's knowledge and belief and is submitted to obtain a loan from the Fisheries Finance Program. For the ECL, emergency contact is the only use for the

		information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For FFP, applicants/borrowers may provide updates at any time to the program office, by mail, fax, telephone or email, including when annual financial statements are submitted. For ECL, users may log on to the application and update the information at any time.
	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 FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ____1/4/2016 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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

The general controls used to protect the loan 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).

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies
X	Yes, a SORN has been submitted to the Department for approval.
	No, a SORN is not being created.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule: 1510-01 **Pending Application files.** Applications for loans or other forms of assistance. Subdivided by type of aid. **Disposition** 1. Approved applications: Transfer to appropriate code for case file. 2. Rejected applications: Destroy after 5 years. 1510-02 **Fishery Loan files.**

	Case files on loans made to finance or refinance costs relating to fishing vessels, including their purchase. Includes applications, case histories, insurance policies, mortgages, and related correspondence and forms. **Disposition** 1. Collateral documents: Return to borrower when loan is repaid. 2. Other documents: Cut off when loan is repaid. Destroy 3 years later. For the 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:
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 Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

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

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

X	Identifiability	Provide explanation: Loan data includes Tax ID Numbers, which. uniquely and directly identify individuals or businesses.
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: There are sensitive data fields, including

		SSN/EIN.
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 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.

12.2 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.

Points of Contact and Signatures

Information System Security System Owner Name: Frank Schwing Office: Office of Science and Technology Phone: 301-427-8220 Email: franklin.schwing@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: SCHWING.FRANKLIN.B.DR.1365840748 Digitally signed by SCHWING.FRANKLIN.B.DR.1365840748 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=SCHWING.FRANKLIN.B.DR.1365840748 Date: 2016.07.21 16:10:05 -04'00' Date signed:	**Information Technology Security Officer** Name: Bill Stearn Office: Office of the Chief Information Officer Phone: 301-427-8813 Email:bill.stearn@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Digitally signed by STEARN.WILLIAM.IVAN.1384494222 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=STEARN.WILLIAM.IVAN.1384494222 Reason: As the NMFS IT Security Program Manager, I have reviewed this document. Date: 2016.07.21 15:56:34 -04'00' Date signed:
Authorizing Official Name: Ned Cyr Office: Office of Science and Technology Phone: 301-427-8123 Email:ned.cyr@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: CYR.EDWARD.C.DR.1365869436 Digitally signed by CYR.EDWARD.C.DR.1365869436 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=CYR.EDWARD.C.DR.1365869436 Date: 2016.07.21 16:42:05 -04'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5358 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2016.07.25 09:56:04 -04'00' Date signed:

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