NOAA Privacy Impact Assessment Guidance

Title:	NOAA PRIVACY IMPACT ASSESSMENT GUIDANCE		
Current Version Date:	August 14, 2017		
Effective Date:	02-11-2008	Expiration Date:	
Originator:	Sarah Brabson	Current Editor:	Sarah Brabson

KEYWORDS

Personally identifiable information (PII), Privacy Impact Assessment (PIA), IT system, records

PURPOSE AND SCOPE

A PIA is a process for determining the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting information in identifiable form.

A Privacy Impact Assessment must be completed for any IT system containing personally identifiable information (e.g. name and/or contact information, financial information, date of birth and/or SSN) for any individuals *including* federal employees and contractors.

For systems under DOC, a second trigger for a PIA is business identifiable information: "trade secrets and commercial or financial information obtained from a person that is privileged or confidential" (Privacy Act of 1974, 5 U.S.C 552(b)(4)). *See more detailed definition below.*

A PIA should be submitted as soon as possible when it is determined that one is required (e.g. through a Privacy Threshold Analysis). PIA submissions are coordinated by the Privacy Specialist, Sarah Brabson (Sarah.Brabson@noaa.gov or 301-628-5751).

Scope of this Standard: **Guidance**

Intended Use of this Standard: **Procedure and template**

AUTHORITIES: Please go to http://www.cio.noaa.gov/services_programs/privacy-related_statutes_and_memoranda.html

INTENDED AUDIENCE

- Assistant/Chief Information Officers
- IT Security Officers, Information System Security Officers, System Owners
- Project Managers
- Exhibit 300 Managers

DESCRIPTION

Supporting documents:

- PIA Template
- Example
- Documents listed under "Authority", accessible through links (above).

This subject of policy or guidance falls into the category: **Privacy**.

DEFINITIONS

Personally identifiable information (PII)

Personally identifiable information (PII) is information that identifies individuals directly or by reference. Examples include direct references such as name, address, social security number, and e-mail address. It also includes any information that could be used to reference other data elements that are used for identification, such as gender, race, and date of birth.

Business identifiable information (BII)
For the purpose of this guidance, business identifiable information (BII) consists of:

(a) Information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity.

Or

(b) Commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)

Privacy Act System of records/SORN:
Any system of records as defined in section (a)(5) of the Privacy Act (" . . .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") and noted in a System of Records Notice (SORN) in the FEDERAL REGISTER either by the Department of Commerce or by another Federal agency.

GUIDANCE - *Detailed guidance, following current template, begins with 3, below*

1. It is determined by the administrator of an IT system – either through consultation with line office and/or OCIO administrators or as part of an Assessment and Authorization (A&A) process (Privacy Threshold Assessment determines that the system contains PII) – that a PIA is required.
2. NOAA will provide the administrator with the DOC template/example and work with him/her to develop a draft PIA for submission to DOC. *See review process at the end of this guidance.*
3. **The PIA has the following sections:**

Introduction:

a. Identifying information, including the OMB Exhibit 300 identification number; name of system or OMB information collection control number;

b. Brief description of the system, its purpose, and the nature of the data that are to be protected (not all data elements need to be listed, just types of data), *with a paragraph for each item (e.g. administration, data subscribers, volunteers). Recent DOC guidance: this includes all types of information, PII/BII or otherwise (e.g. data).*

c. The law or regulation that authorizes the collection and maintenance of the information: For much of NOAA PII, there are one or more statutes that authorize collection of information from the general public – e.g. the Magnuson-Stevens Fishery Conservation and Management Act, or the Marine Mammal Protection Act. Information on permit applications for programs associated with these statutes inevitably includes PII. Collection of the Tax Identification Number is authorized by 31 U.S.C. 7701. Information collections under the Paperwork Reduction Act (PRA) include language about how the information is protected, and any statutes authorizing confidentiality.

For PIAs regarding information collected from employees, and thus covered by the SORN COMMERCE/DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies, you should state:

"The legal authority for 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.

For PIAs covered, or also covered, by the SORN COMMERCE/NOAA-11, NOAA Mailing Lists (collecting information from the public for the purpose of sharing data or information with them, or for volunteer activities such as weather spotting), you should use or add this statue and associated language:

"15 U.S.C. § 1512 is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.
See also U.S. Department of Commerce and NOAA official Privacy Act system of records

These examples were provided by Glenn Tallia, NOAA GC.

Starting March 2017, the DOC Privacy Act Officer has begun requiring more than one authority. If you have only 5 U.S.C.301, please choose one or more authorities from one or more of the SORNs that you state in Section 9.1 provide coverage for this system. The link to government-wide, DOC and NOAA SORNs is available in Section 9.1.

d. Any information sharing conducted by the system, whether or not PII or BII. Recent guidance from DOC: *must be consistent with 6.1. If sharing with an outside agency, please include an information sharing agreement/MOU/MOA.*

e. The impact level of the system (low, moderate or high).

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) See explanatory PIA handout					
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. What information is being collected, maintained, or disseminated (add checks by applicable information and add items not included in the template). *In the first list, Identifying Numbers, **if you check SSN**, please put an asterisk and explain below the list, why you collect and if you store, why and how (e.g. only on director's drive). Include reason(s), even though you will explain also in **Section 5, Use of the System**. DOC needs to see if there is a good reason why you cannot simply access SSNs from OSY or WFM.*

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

General Personal Data (GPD)					
a. Name		g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		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		**d. Telephone Number**		**g. Salary**	
b. Job Title		h. Email Address		h. Work History	
c. Work Address		i. Business Associates			
i. Other work-related data (specify):					

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

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):					

2.2. Sources of the PII/BII in the system (add checks) – This must be in agreement with information in the Introduction.

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

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

Non-government Sources					
Public Organizations		Public Media, Internet		Private Sector	
Commercial Data Brokers					
Other (specify):					

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

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		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 – NEW QUESTION – see PTA and explanatory PIA handout

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):			

	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 - check this only if you are using computer matching. Otherwise, "for administrative matters" applies.		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities – if you check this, also check criminal law enforcement		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 System - organize by purposes checked in 4.1

5.1 Provide an explanation of how the bureau will use the PII/BII to accomplish the checked purpose(s), e.g., to verify existing data. Describe why the PII/BII that is collected, maintained, or disseminated is necessary **to accomplish the checked purpose(s) above** and further the mission of the bureau and/or the Department.

Indicate if the PII/BII identified in **Section 2.1** of this document is in reference to a federal employee/contractor, member of public, foreign national, visitor or other (specify). *If you have several paragraphs, include this information at the end of each one.*
Any categories of PII/BII or data elements referred to here must appear also in the Intro. If listed in the Intro, can be summarized here, or vice versa. But do not add a data element here that was not either listed or referred to in the Intro, ie. if you list work telephone number here, be sure that it's either listed or summarized under work contact info in the Intro, or vice versa.

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.) If you need to explain or add information for any of the checkmarks, please use an asterisk. This information should be consistent with the introduction.*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
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 – **NEW Question**

	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: encryption, for example.
	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.)* – **NEW QUESTION**

Class of Users			
General Public		Government Employees	
Contractors			
Other (specify):			

Section 7: Notice and Consent

See suggestions in boxes below for Sections 5.1-5.4. Note also that if an answer can be a Yes, even if the result means not receiving the benefit, or not keeping one's job, then it should be written as a Yes; e.g. An individual may decline to provide the information, but he will not be able to receive data/will not be hired/retained as an employee.

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

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 6. *Please check this one unless there is NO SORN covering this system, but you must still check at least one more of the options below.*	
	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: _____ _____.	Please provide the forms, or links to the forms, that are used to collect information from the public, or in the case of employees, an example of a federal employment form. The form should have a link to a Privacy Act Statement (PAS) which applies specifically to the information collected on the form, and its purpose. The link

		here is to a sample PAS, approved by the DOC Privacy Act Officer.
	Yes, notice is provided by other means.	Specify how: *For those groups of individuals/businesses to whom notice is given, specify at what point in the information collection process it is given, and if in person (face to face, phone, email)and by whom (role, position), or on a form to be completed. In this and rest of Section 5, put a separate paragraph for each set of individuals/businesses if the answer is different. If notice is given on a form, please provide a link to the form, or include a copy in your transmittal email.*
	No, notice is not provided.	Specify why not: *For those groups of individuals/businesses to whom notice is not provided, explain why – generally including that the information is automatically collected for the functioning of the office/program.*

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: *Explain how this option is conveyed and by whom. This may be by the original collector of the data, eg. OPM.*
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: *For those who may not decline, explain – generally similar answer to the "no" question in 5.1.*

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: *For those who have this opportunity, please explain what the uses and related options are -or if there is only one use - and how they are made aware of use(s) and options. If people are completing a form, you can put a link to the NOAA Privacy Policy, which states that "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose." The opportunity may be given by the original collector of the data, e.g. OPM.*
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: *If there is only one stated use for the information, then say that, and include how the intended use is explained.*

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

	Yes, individuals have an opportunity to review/update	Specify how: *Include how they KNOW they can review/update, and to whom they give the information (role, position of person) and who makes the updates. In*

	PII/BII pertaining to them.	*some cases, with a web-based system, the person can do his own review and update, but otherwise, if the person cannot directly review the info, can the person to whom they give the updates read or send the info to them for review?*
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: *If not, does another person, e.g. a supervisor, make the updates? What other reason(s) would there be for no such opportunity?*

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.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
	Access to the PII/BII is restricted to authorized personnel only.
(NEW)	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
(NEW)	NIST Special Publication (SP) 800-122 **and NIST SP 800-53 Revision 4 Appendix J recommended privacy controls** for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM). Links to Appendix J and DOC/NOAA Controls Allocation . Also see the NOAA Privacy Page (http://www.cio.noaa.gov/services_programs/privacy.html) for Privacy Control Implementation Statements and the PIA template with the sections mapped to the controls. With each PIA, a security and privacy controls assessment must now be submitted.
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
(NEW)	Contracts with customers establish ownership rights over data including PII/BII.
(NEW)	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 **– NEW QUESTION**

This would include access protection, audit logs, encryption of data, and any applicable technological controls listed in 8.1. Do not include information at a level which would be helpful to hackers.

Note: since the OPM breaches, DOC had begun asking that sensitive PII/BII is encrypted at rest, or that there is a POA&M.

The encryption requirement is now in OMB A-130, Appendix 1(4)i(14): Encrypt all FIPS 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information is technically infeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations; and the risk of not encrypting is accepted by the authorizing official and approved by the agency CIO, in consultation with the SAOP (as appropriate).

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). This is the only part of Section 9.*

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."

	Yes, this system is covered by an existing system of records notice. Provide the system name and number: *If more than one SORN, please list. There may be one or more already existing and one or more that have been submitted to the Department. Here is the link to Government-Wide, DOC and NOAA SORNs .* *March 2017: DOC now requires that each listed SORN have the hyperlink included.*
	Yes, a system of records notice has been submitted to the Department for approval on (date). *If not yet at the dept. level, give the status.*
	No, a system of records is not being created. *Although DOC's current position is that ALL systems collecting PII/BII should be covered by a SORN, there are a few instances, such as databases, e.g. for Grants Online, where, because data is NOT retrieved by means of PII, this answer may be accepted.*

If it is determined by NOAA that a system of records notice (SORN) must be written, i.e. if files in the system are retrievable by any of the PII or BII elements, and there is/are NOT a SORN(s) covering the information, and the exception in the third box above does not apply - then Sarah Brabson provides the IT administrator with the template, reviews, and submits to DOC.

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.

	There is an approved record control schedule. Provide the name of the record control schedule: *For instances in which retention is not monitored, as in below, the following may be the response: 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.*
	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. *Please be sure to check this or the box below, these questions are often missed.*
	No, retention is not monitored for compliance to the schedule. Provide explanation: *This box may be checked in a situation like this one, where only employee contact information is collected: We keep only the most recent information provided voluntarily by the employee. Individual information is updated manually as we receive information; or else at least annually as documents are reviewed and updated as part of regular document maintenance.*

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

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	
Other (specify): (another option is storage)			

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

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. See **explanatory PIA handout**

	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.
	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.)* – **NEW Question.** *See* **explanatory PIA handout. Select all items that you have considered. Please consider all, whether the explanation explains that there is a risk, or that there is little risk. For systems that we have been checking 'moderate', DOC has started asking us to check 'high'. This designation will not require the addition of any controls. The high rating is based on sensitive PII, including sensitive identifying numbers, financial data and date of birth. Medical and military records may also contain sensitive information. As required by NIST SP 800-122, the risk of harm is not mitigated by a lower number of individuals affected by a potential incident. As such, if the risk of harm posed to one individual about whom the PII pertains would be catastrophic--such as a comprehensive loss of SSN, Financial Data, and medical information--then the High Confidentiality Impact Level is appropriate, even if the FIPS 199 system categorization remains 'Moderate.'"**

	Identifiability	Provide explanation:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation: Check this only if there is a specific statute or other authority for this information.
	Access to and Location of PII	Provide explanation:
	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 (example, you realized you no longer needed to maintain SSNs electronically). Explanation:
	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. example: We added (a) security/privacy control(s). Explanation:

	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures – Sample only, to show AO added

Information System Security Officer or System Owner	**Information Technology Security Officer**
Name: Office: Phone: Email: 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: _____ Date signed: _____	Name: Office: Phone: Email: 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: _____ Date signed: _____

Authorizing Official – note this change. This means the LO or SO AO, no co-AO needed unless this is a high impact system.	**Bureau Chief Privacy Officer**
Name: Office: Phone: Email: 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: _____ Date signed: _____	Name: Office: Phone: Email: 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: _____ Date signed: _____

Review process:

1. The completed draft PIA is sent to the Bureau Privacy Officer's (BPO's) assistant.
2. Once comments are addressed, the PIA is forwarded to the BPO for review.
3. After PO review and any further edits, the PIA is pdf'd and signed by the Program ISSO or SO, ITSO and AO, then sent to the BPO for signature.
4. The draft PIA and the signed pdf are forwarded by NOAA to the DOC Office of the CIO, who distributes it for review to security (brief check of Section 6), the CPO's assistant, and the CPO.
5. At each stage where comments are received, NOAA consults with the program and sends a revised draft to the reviewer. If no further changes are requested by DOC, DOC approves the PIA and the DOC CPO signs.
6. NOAA posts the approved PIA on the PIA page on the NOAA OCIO website: http://www.cio.noaa.gov/services_programs/pia.html.

7. DOC maintains a link to this page on its IT Privacy page: http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/dev01_003746.