

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration
(NOAA)**



**Privacy Impact Assessment
for the
NOAA0100, NOAA Cyber Security Center**

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
 Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Catrina 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: 2016.10.07 15:47:36 -04'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA0100, NOAA Cyber Security Center

Unique Project Identifier: 006-48-02-00-01-3511-00

Introduction: System Description

NOAA0100, the NOAA Cyber Security Center (NCSC) is a functional body of technologies, processes, and practices designed to support the NCSC mission to protect NOAA networks, computers, programs, and data from cyber-attack, damage, and unauthorized access, enabled by the strategic shift of all NOAA Federal Information System Management Act (FISMA) identified systems to practicing continuous monitoring and real-time assessments. The subcomponents of NOAA0100, NCSC, are:

- 1.) NOAA Computer Incident Response Team (NCIRT)
- 2.) Security Operations Center (SOC)
- 3.) Enterprise Security Solutions (ESS)
- 4.) NOAA OCIO Compliance Review Application (NOCRA)
- 5.) Enterprise Security Administration Environment (ESAE)
- 6.) Enterprise Continuous Monitoring Operations (ECMO)
- 7.) Intrusion Detection Management (IDM)
- 8.) Enterprise Security Operations Center (ESOC)
- 9.) Trusted Internet Connection Access Points (TICAPs)

The System Administration Staff (SAS) works to ensure that the technologies supported by the NCSC are maintained. The N-CIRT, Security Operations Center (SOC), ESS, and SAS teams work together to support the NOAA mission.

Although NOAA0100 does not solicit, collect, maintain, or disseminate PII/BII, it is possible for individuals to voluntarily make such information available. Typical examples of the types of PII/BII that may become available to NOAA0100 include names of individuals and businesses, images from photos or videos, screen names, email addresses, etc. NOAA0100 does not ask individuals to post information on its SM/W2.0 websites or applications. Information that individuals voluntarily submit as part of the investigative process is entered as evidence for the NOAA Cyber Security Center [NOAA0100]. The NCSC does not solicit this information. However, although NOAA takes extensive measures to redact the sensitive PII from end user access views, un-redacted copies of NOAA Form 47-43 may include sensitive PII, and are maintained on the system for support of law enforcement activities and are accessible only to NCIRT database administrators.

As part of NOAA's Continuous Monitoring Operations, sensitive PII is subject to capture, maintenance, and dissemination as part of the NCSC functions. This collection includes Deep Packet Inspection (DPI) inspected within TICAP, and is consented to at the time of user login.

PII/BII from any government or non-government source may be in the system as evidence of a breach.

NOAA shares all breach incident information with DOC and United States Computer Emergency Readiness Team (US-CERT), as well as law enforcement if applicable.

The applicable authority is for civil employment, 5 U.S.C. 301.

The applicable authority for collection of PII as part of a breach investigation is the Privacy Act of 1974.

This is a high impact 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 collection with no changes that create new privacy risks, and is for update purposes only.

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	X	i. Credit Card	X
b. Taxpayer ID	X	f. Driver's License	X	j. Financial Account	X
c. Employer ID	X	g. Passport	X	k. Financial Transaction	X
d. Employee ID	X	h. Alien Registration	X	l. Vehicle Identifier	X
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: All information transmitted on NOAA networks is subject to network monitoring tools, inspection,					

continuous monitoring operations, and collection as part of the NCSC mission, and may involve voluminous collections of sensitive PII, including SSNs. As part of a computer incident response inquiry, the NOAA0100 system may have PII data to include Social Security Numbers included in its investigation that may have been part of the original incident. For example, if an individual transmits a list of social security numbers in violation of NOAA PII policies, this original list may be part of the investigation supporting artifacts. Additionally, if a disk image or file contains PII, the retention is pertinent to the collection of incident information from the affected system.

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

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	d. Photographs	X*	g. DNA Profiles	X
b. Palm Prints	X	e. Scars, Marks, Tattoos	X	h. Retina/Iris Scans	X
c. Voice Recording/Signatures	X	f. Vascular Scan	X	i. Dental Profile	X
j. Other distinguishing features/biometrics (specify):					
*Only if submitted as evidence; not requested or required.					

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)
Any information that is collected by any NOAA system is potentially collected during an incident investigation.

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

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

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

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): Network Monitoring Tools				

	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			To promote information sharing initiatives	
For litigation			For criminal law enforcement activities	X
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): Network Monitoring for security threats and PII	X			

policy violations		
-------------------	--	--

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).

Although NOAA0100 does not solicit, collect, maintain, or disseminate PII/BII, it is possible for individuals (federal employees or contractors) to voluntarily make such information available. PII/BII may become available to NOAA0100 as part of investigation of PII policy violations and criminal law enforcement. These may include names of individuals and businesses, images from photos or videos, screen names, email addresses, etc. Information that individuals voluntarily submit as part of the investigative process is entered as evidence for the NOAA Cyber Security Center [NOAA0100] (NCSC). The NCSC does not solicit this information. There is no purpose for this information, unless it is retained as part of a breach investigation.

PII/BII is collected and monitored via network monitoring tools for security threats, incident response, law enforcement activities, and network protection. This information may be in the system as evidence of a breach and retained as part of a breach investigation. The only purpose for this information is if it is retained as part of a breach investigation.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. (Check all that apply.)

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify): Law enforcement	X		

	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: NOAA's Enterprise Messaging System (NEMS). The connection to the NEMS system NOAA0300 is via Transport Layer Security and LDAP Secure to prevent leakage of data in transit between the systems. Controls at NOAA0300 to prevent leakage are through the requirement of authenticated logon to retrieve certain entry attributes used in NOAA0100 NOAA Form 47-43 authorization.
	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.
	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: _____.
X	Yes, notice is provided by other means. Specify how: For those reporting a breach, NOAA Form 47-43 states: "This is a United States Federal Government computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied or disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person, whether authorized or unauthorized, CONSTITUTES CONSENT to these terms."
	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: An employee/contractor enters his/her credentials through Form 47-43 and NEMs authenticates the user to allow access to the reporting system. An employee/contractor can decline to provide PII by not logging into the Form 47-43.
---	--

	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: Consent is granted prior to log-in. A warning notice includes “Access or use of this computer system by any person, authorized or unauthorized, constitutes consent to these terms. If you do not agree, click on cancel to avoid continuing to the site.”
	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: The reporter’s contact information is imported from the staff directory. Updates to the staff directory transfer to the 47-43 database. Employees are informed verbally and in writing as part of their employee orientation that they may update contact information by logging into the staff directory.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

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.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	Any PII/BII collected through the NOAA0100 system for computer security incident investigations is restricted to access by NOAA Computer Incident Response Team (NCIRT) personnel. Access to records are monitored and recorded within system event logs.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>12/9/2015</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
N/A	Contracts with customers establish ownership rights over data including PII/BII.
N/A	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.

Discretionary access controls are implemented throughout NOAA0100 for access to forensic data. In the NOAA Form 47-43 this is also augmented with a pro forma implementation of mandatory access controls to restrict access to specific reports. However, any sensitive PII on NOAA Form 47-43 is redacted from end user views, and copies maintained on the database are only shared for law enforcement activities. The NSCS Network Monitoring is only conducted by privileged users who sign a confidentiality or non-disclosure agreement. Access to physical enclaves is implemented as a physical security control to NOAA0100 resources; this would include access to physical articles in evidence that may include PII/BII.

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 (<i>list all that apply</i>): COMMERCE/DEPT-13, Investigative and Security Records; COMMERCE/DEPT-18, Employees Information Not Covered by Notices of Other Agencies; COMMERCE/DEPT-25, Access Control and Identity Management System.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	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: NARA General Records Schedule 24, Item 7: Computer security incident handling: Destroy/delete 3 years after all necessary follow-up actions have been completed. (N1-GRS-03-1 item 7)
	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: With the information available, large volumes of individuals may be identified.
x	Quantity of PII	Provide explanation: The quantity of PII will vary, but depending on the number and size of breaches, disclosure could have a catastrophic adverse effect on the organization or on individuals.
x	Data Field Sensitivity	Provide explanation: There may be large volumes of sensitive PII in the system, as a result of both continuous monitoring, and voluntary sensitive PII submissions retained for law enforcement purposes.
x	Context of Use	Provide explanation: Voluminous Sensitive PII, including SSNs may be retained for law enforcement purposes, collected through Network Monitoring Tools as well as voluntary submissions of Sensitive PII incident to the submission of a Form 47-43.
x	Obligation to Protect Confidentiality	Provide explanation: The Privacy Act of 1974.
x	Access to and Location of PII	Provide explanation: Access to the Sensitive PII through NSCS Network Monitoring is restricted to privileged users who have signed a non-disclosure agreement.
	Other:	Provide explanation:

Section 12: Analysis

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

X	Yes, the conduct of this PIA results in required business process changes. Explanation: The conduct of the PIA has resulted in the business process change of the upcoming implementation of encryption of data at rest within NSCS. This change is also considered a technology change below.
	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.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: The conduct of the PIA has resulted in the technology change of the upcoming implementation of encryption of data at rest within NSCS.
	No, the conduct of this PIA does not result in any required technology changes.