

U.S. Department of Commerce NOAA



Privacy Impact Assessment for NOAA0201 Web Operations Center (WOC)

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: 2017.01.09 12:16:20 -05'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA0201 Web Operations Center (WOC)

Unique Project Identifier: 006-000351100 00-48-03-17-01-00

Introduction: System Description

The Web Operations Center (WOC) is a diverse information technology services provider to Line and Staff Offices within NOAA. The WOC provide a wide range of information technology services and functions which include high availability, scalability, redundancy, clustering, and high performance computing to replicate and distributed general information as well as critical time sensitive life and property information to the general public and meteorology community.

The services and functions of the information system technology have been broken down into five (5) core services and functions: WOC Domain Name System Services (WOCDNSS), WOC Information Sharing Services (WOCISS), WOC Adoptive System Framework (WOCASF), WOC NOAA Enterprise Message System (WOCNEMS) and WOC Collaboration Services (WOCCS). These services and functions make up the subsystems within NOAA0201.

NOAA WOC NOAA Enterprise Message System (WOCNEMS): The WOC NOAA Enterprise Message System (former MOC) provides top-level Directory Service, as part of NOAA's distributed Unified Messaging System. This includes maintaining the Master Directory, and replication of directory information to approximately 11 second to tier II level Consumers Directory Servers. WOCNEMS was recently merged into the WOC.

The WOCNEMS systems are physically located at 3 NOAA datacenters (W1: Silver Spring, Maryland W2: Largo, Maryland and W4: Boulder, Colorado).

As part of the distributed NEMS system, a redundant Master Directory Service is hosted at NOAA3400 (outside of NOAA0201 boundary) in Boulder, Colorado. This provides fault-tolerance. Directory services continue to operate despite failure of either location. All master directory replication traffic is encrypted using Secure Sockets Layer (SSL).

In addition to the top-level Directory services described above, there are consumers Directory Servers that provide local directory service to the departmental users. All directory synchronization traffic between Master and Consumer directory servers is encrypted using SSL.

WOCNEMS has also retained a limited portion of its Message Transfer Agent (MTA) server for mailing capability. There are a limited number of LDAP group accounts, ship's user accounts and trusted NOAA wide application servers that rely on the MTA for SMTP mail transfers. These accounts are allowed access if the sender is an authenticated LDAP user or the sending host machine is "Trusted hosts" on the MTA servers.

A typical transaction is LDAP verification and SMTP forwarding.

The WOC has now absorbed NOAA0300, Messaging Operations Center(MOC). The MOC services included servicing LDAP directories for all of NOAA. The information collected includes:

- Name
- Work address
- Work phone numbers
- Work e-mail addresses
- Organization name

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

Information sharing – The information is shared only within the bureau.

The WOCNEMS is one of five subsystems which comprise NOAA0201 Web Operations Center (WOC). Taken together, NOAA0201 has a FIPS 199 security input category of “High”.

Individually the five subsystems are evaluated as follows:

SC (NOAA0201 Domain Name System Service) = (Low, High, High)

SC (NOAA0201 Information Sharing Services) = (Low, High, High)

SC (NOAA0201 Adoptive System Framework) = (Low, Low, Moderate)

SC (NOAA0201 Collaboration Services) = (Low, Low, Low)

SC (NOAA0201 NOAA Enterprise Message System) = (Low, Medium, Low)

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

General Personal Data (GPD)			
a. Name	X	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	X
b. Job Title		e. Email Address	X
c. Work Address	X	f. Business Associates	
g. Salary			
h. Work History			
i. Other work-related data (specify): X Organization Name			

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): None			

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

Other Information (specify)

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	<input checked="" type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online
Telephone	<input type="checkbox"/>	Email	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Other (specify):				

Government Sources				
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify)				

Non-government Sources				
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers
Third Party Website or Application	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):				

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):				

<input checked="" type="checkbox"/>	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):			

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).

The information which is subject to this PIA is not private and is not sensitive. The information is used for IT administration and for LDAP verification (federal 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):			

<input type="checkbox"/>	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.

<input type="checkbox"/>	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:
X	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.	
<input type="checkbox"/>	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: Notice is provided as part of employee enrollment,

		and on the staff directory warning banner.
	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 individual may decline but would not have access to the NOAA IT network.
	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: There is only one use, which is explained during employee orientation.
	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: Individuals may view their info online and make a request for a change.
	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.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u> 1/12/2016 </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 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.

Only NOAA personnel with authenticated access would be able to change or delete information.
--

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 SORN
	Yes, a SORN has been submitted to the Department for approval on (date).
	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. “Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use.” from http://www.corporateservices.noaa.gov/audit/records_management/schedules/index.html , Chapter 200-12.
	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.
	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		Overwriting	
Degaussing		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.

X	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.)*

X	Identifiability	Provide explanation: Minimal admin information for IT work identity
X	Quantity of PII	Provide explanation: Minimal work contact information
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields.
X	Context of Use	Provide explanation: Minimal data for IT user identification
	Obligation to Protect Confidentiality	Provide explanation:
	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. 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.