

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



**Privacy Threshold Analysis  
for the  
Web Operation Center (WOC; NOAA0201)  
October 21, 2019**

## U.S. Department of Commerce Privacy Threshold Analysis

### NOAA/Web Operation Center

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

**Introduction:** This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

**Description of the information system and its purpose:**

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 Transport Layer Security (TLS).

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 TLS.

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

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, High, High)
- SC (NOAA0201 NOAA Enterprise Message System) = (Low, Moderate, Low)
- SC (NOAA0201 Collaboration Services) = (Low, Low, Moderate)

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

**Questionnaire:**

## 1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

- This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*
- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

## 2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

- Yes. *Please describe the activities which may raise privacy concerns.*
- No.

## 3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information 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.)."

- Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*
- Companies
- Other business entities
- No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: (*Check all that apply.*)

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

*If the answer is "yes" to question 4a, please respond to the following questions.*

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

***If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.***

### CERTIFICATION

X  I certify the criteria implied by one or more of the questions above **apply** to the NOAA0201 Web Operation Center (WOC) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the NOAA0201 Web Operation Center (WOC) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO): William C. Beck

**BECK.WILLIAM.CHRISTIAN.1406165791**  
Digitally signed by BECK.WILLIAM.CHRISTIAN.1406165791  
Date: 2019.10.21 16:11:55 -04'00'

Signature of ISSO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Information Technology Security Officer (ITSO): Charles Obenschain

**OBENSCHAIN.CHARLES.THOMAS.1506347293**  
Digitally signed by OBENSCHAIN.CHARLES.THOMAS.1506347293  
Date: 2019.10.22 14:21:26 -04'00'

Signature of ITSO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Authorizing Official (AO): Douglas A. Perry

**PERRY.DOUGLAS.A.1365847270**  
Digitally signed by PERRY.DOUGLAS.A.1365847270  
Date: 2019.10.24 16:47:50 -04'00'

Signature of AO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Bureau Chief Privacy Officer (BCPO): Mark H. Graff

**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: 2019.10.21 10:29:27 -04'00'

Signature of BCPO: \_\_\_\_\_ Date: \_\_\_\_\_