

**U.S. Department of Commerce  
NOAA**



**Privacy Threshold Analysis  
for the  
NOAA8203 - National Weather Service (NWS) Performance  
Management System (N-PMS)**

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

### **DOC/NWS N-PMS**

**Unique Project Identifier: 006-48-01-12-02-3118-00**

**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:** NOAA8203, referred to as “NWS Performance Management System (N-PMS),” measures the accuracy and timeliness of National Weather Service warnings and forecasts issued for the public, aviation, marine, fire weather, and emergency management communities. Additionally, N-PMS is the NWS source for all Government Performance and Results Act (GPRA) Modernization Act of 2010 metrics.

The FIPS 199 classification for N-PMS is Low. N-PMS is considered a General Support System and interconnects with NOAA8850 NWS Enterprise Mission Enabling System for basic network connectivity to NOAA and the internet.

The legal authority for civil service employment is 5 U.S.C. 301, Departmental Regulations (see COMMERCE/DEPT-18 System of Records Notice). For the data provider information, 5 U.S.C. 301 and 15 U.S.C. 1512, Powers and duties of Department [of Commerce], are applicable (see COMMERCE/NOAA-11 System of Records Notice).

NWS employees to monitor forecast and warning performance at their forecast office predominantly use the N-PMS website. A subset of these users also accesses the Performance Management website to conduct some data entry interactions for programs such as Storm Data and the NWS Outreach and Education Event System. No one is allowed access to the data without logging in to the Performance Management website with a valid user account. System administrators must approve each user account request before access is granted.

Occasionally external partners from other government agencies or academic institutions (i.e., non-NOAA entities) will work with the NWS on data analysis projects and require access to the Performance Management website. All users must have a valid e-mail address. In these situations, the Performance Management website administrators initiate the account registration process with these partners by sending an account registration form via email. The external

partners fill out the form with their contact information, including a statement on why they need access to the website, and submit the form back to the administrators. Only after the website administrators review the contact information and access statement and approve access will the external user be granted an account to log in.

In order to provide the users with a customized experience on the website, including ensuring the entry of Storm Data and the NWS Outreach and Education Event System data is correctly attributed to their duty station, general information such as the user's email address, duty station, and contact information are collected during the account registration process.

Information entered will be validated to make sure it is an accurate entry (i.e. format, maximum, minimum length and data type). Once it passes, the system uses a stored procedure to check that the user has entered a unique username. Otherwise, the system displays an invalid username message to the user. Next, the system adds the user to the database after validating all fields. Once the registration is successful, an email alert is sent to the N-PMS system administrator and a notification email is sent to the user.

### 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.*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
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.*

\_\_\_X\_\_\_ 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 N-PMS 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 N-PMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Adam Yates, ISSO

Signature of ISSO or SO: YATES.ADAM.J.1363025087  Digitally signed by YATES.ADAM.J.1363025087  
Date: 2019.05.01 12:19:23 -04'00' Date: \_\_\_\_\_


Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349  Digitally signed by BROWNE.ANDREW.PATRICK.1472149349  
Date: 2019.05.02 09:48:12 -04'00' Date: \_\_\_\_\_

Name of Authorizing Official (AO): John Murphy

Signature of AO: WOODS.CINDY.P.1120659797  Digitally signed by WOODS.CINDY.P.1120659797  
Date: 2019.05.02 12:01:09 -04'00' Date: \_\_\_\_\_

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

Signature of BCPO: GRAFF.MARK.HYRUM.151447892  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: 2019.05.02 12:34:00 Date: \_\_\_\_\_