Template Version Number: 01-2021

U.S. Department of Commerce
National Oceanic & Atmospheric Administration

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

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/ NWS/ Performance Management System (N-PMS)

Unique Project Identifier: NOAA8203 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: 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.

NWS employees 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.

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).

Address the following elements:

a) *Whether it is a general support system, major application, or other type of system*

NOAA8203 is a General Support System.

b) *System location*

Silver Spring, MD
Kansas City, MO

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

Interconnects with NOAA8850 for basic network connectivity to NOAA and the internet and NOAA0100 for use of NOAA enterprise security tools.

d) *The purpose that the system is designed to serve*

NOAA8203 measures the accuracy and timeliness of NWS 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.

e) *The way the system operates to achieve the purpose*

Users access the Performance Management website to conduct data entry interactions for programs such as Storm Data and the NWS Outreach and Education Event System.

f) *A general description of the type of information collected, maintained, used, or disseminated by the system*

Data that measures the accuracy and timeliness of NWS 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.

g) Identify individuals who have access to information on the system

Only users that are approved by system administrators once registered.

h) How information in the system is retrieved by the user

Through the secure website using their authorized user account.

i) How information is transmitted to and from the system

Data is submitted securely through the website and stored in an encrypted Microsoft SQL database. It is backed up onto Google Drive regularly.

Questionnaire:

1. Status of the Information System

1a. 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.*

_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. *Continue to answer questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X__ No. This is not a new information system.

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 tothose 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. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X 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.

X No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

X DOC employees
X Contractors working on behalf of DOC
X Other Federal Government personnel
X 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 Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

_X__ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

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

_X__ 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.

4d. 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.

_X__ 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, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ The criteria implied by one or more of the questions above **apply** to the NOAA8203 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the NOAAXXXX and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Mike Sowko Office: NWS/OCOO Phone: 301-233-9258 Email: mike.sowko@noaa.gov I certify that this PTA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: SOWKO.ARTHUR.MICHAEL.1365859864 Digitally signed by SOWKO.ARTHUR.MICHAEL.1365859864 Date: 2023.06.26 17:29:09 -04'00' Date signed: __________	**Information Technology Security Officer** Name: Andrew Browne Office: NWS/OACIO Phone: 301-427-9033 Email: Andrew.browne@noaa.gov I certify that this PTA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2023.06.26 16:39:06 -04'00' Date signed: __________
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov I certify that this PTA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.06.27 13:49:31 -04'00' Date signed: __________	**Authorizing Official** Name: Mike Coyne Office: NWS/OCOO Phone: 817-978-1000 Email:mike.coyne@noaa.gov I certify that this PTA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: HARDING.KENNETH.WALLACE.1139815765 Digitally signed by HARDING.KENNETH.WALLACE.1139815765 Date: 2023.06.27 10:20:03 -05'00' Date signed:
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov I certify that this PTA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2023.06.27 14:09:18 -04'00' Date signed: 6/27/23	