Version Number: 01-2019

U.S. Department of Commerce

National Oceanic and Atmospheric Administration

Privacy Threshold Analysis
for the
Aviation Weather Center
NOAA8861

U.S. Department of Commerce Privacy Threshold Analysis

National Oceanic and Atmospheric Administration
National Weather Service/Aviation Weather Center (NOAA8861)

Unique Project Identifier: 006-48-01-17-01-3113-00

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: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

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

The Aviation Weather Center (AWC) is a general support system.

b) System location

The Aviation Weather Center is located in 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)

The Aviation Weather Center interconnects with Air Force Weather Agency (AFWA), Air Force Weather Agency (AFWA), and NOAA8860 - Weather and Climate Computing Infrastructure Services

(WCCIS).

d) The purpose that the system is designed to serve

The Aviation Weather Center, enhances aviation safety by issuing accurate warnings, forecasts and analyses of hazardous weather for aviation interests. The Center identifies existing or imminent weather hazards to aircraft in flight and creates warnings for transmission to the aviation community. The Center also originates operational forecasts of weather conditions predicted to affect domestic and international aviation interests during the next 24 hours.

e) The way the system operates to achieve the purpose

AWC ingests data into the operations network servers using DBNET and LDM. Once data is ingested it is processed by the AWC data processing servers and stored on the storage servers for use by the Linux Forecaster workstations and Development Linux Workstations. All ingested data enters through the local site router and/or firewalls. All incoming data is restricted and controlled.

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

The AWC collaborates with universities, governmental research laboratories, Federal Aviation Administration facilities, international meteorological watch offices and other National Weather Service components to maintain a leading edge in aviation meteorology hazards training, operations and forecast technique development.

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

Universities, governmental research laboratories, Federal Aviation Administration facilities, international meteorological watch offices and other National Weather Service components

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

Forecasters are able to retrieve and render the data on demand, display the data for analysis, and develop the AWC suite of products, e.g., scheduled guidance and outlook products and event driven watch and special products. These products cover a time period from a few days to within a few minutes. With such a time range and a mixture of important and routine products, it is important for AWC to have multiple distribution pathways. The AWC distribution pathway from highest preference to lowest preference is:

1. PDS to the AWC local PDS server.
2. PDS to any other National Center PDS.
3. AWC local access to the NWS Gateway via the redundant socket servers.
4. AWC PDS servers which in turn places text products into the AWIPS environment via AWIPS firewall for distribution to the AWIPS WAN.

i) How information is transmitted to and from the system.

The AWC ingests data into the operations network servers using DBNET and LDM. Once data is ingested it is processed by the AWC data processing servers and stored on the storage servers for use by the Linux Forecaster workstations and Development Linux Workstations. All ingested data enters through the local site router and/or firewalls. All incoming data is restricted and controlled.

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.*

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). *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 01-2017 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. *(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.)*

____ DOC employees
____ National Institute of Standards and Technology Associates
____ Contractors working on behalf of DOC
____ 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 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 NOAA8861 Aviation Weather Center 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 NOAA8861 Aviation Weather Center 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):

Hugo Del Rio (AWC ISSO)

Signature of ISSO or SO: DEL RIO.HUGO.ENRIQUE.1182167980 Digitally signed by DEL RIO.HUGO.ENRIQUE.1182167980 Date: 2020.05.18 11:00:15 -06'00' Date: 5/18/2020

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

Signature of ITSO: BROWNE.ANDREW.PATRICK .1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2020.05.18 13:19:42 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.05.26 12:02:12 -04'00' Date: _____

Name of Authorizing Official (AO): Dr. Grant Cooper

Signature of AO: COOPER.GRANT.ALEXANDER.10476893 99 Digitally signed by COOPER.GRANT.ALEXANDER.1047689399 Date: 2020.05.26 08:52:37 -06'00' Date: _____

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2020.06.30 09:30:55 -04'00' Date: _____