Version Number: 01-2021

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

Privacy Threshold Analysis
for the
NOAA8860
Weather and Climate Computing Infrastructure Services (WCCIS)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NWS/ Weather and Climate Computing Infrastructure Services

Unique Project Identifier: NOAA8860

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: *Provide a brief description of the information system.*
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).

NOAA8860 is an integral part of the National Centers for Environmental Prediction (NCEP) that helps in providing timely, accurate and continually improving worldwide forecast guidance products.

Address the following elements:

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

NOAA8860 is a general support system that supports four Major Operational Functions: Integrated Dissemination Program (IDP), OneNWSNet, the Weather and Climate Operational Supercomputing System (WCOSS), and NCEP center support. Additionally, NOAA8860 supports data centers in Kansas City, MO, and Silver Spring, MD, which host weather.gov, while this function is being migrated to IDP.

b) *System location*

Weather and Climate Computing Infrastructure Services (WCCIS; NOAA8860) is comprised of six National Centers for Environmental Prediction (NCEP) centers. These are NCEP Central Operations (**NCO**), Weather Prediction Center (**WPC**), Ocean Prediction Center (**OPC**), Environmental Modeling Center (**EMC**), Climate Prediction Center (**CPC**), and the National Hurricane Center (**NHC**), All of the centers are located in College Park, Maryland except NHC which is located in Miami, Florida. NOAA8860 operates a high availability backup location in Boulder, CO, which acts as an alternate processing site for the aforementioned functions. Additionally, NOAA8860 has a minimal presence in Silver Spring, MD, to support telecommunications for various customers.

WCOSS systems require high availability and thus have identical primary and failover sites. These sites are located in Reston, VA, and Orlando, FL.

OneNWSNet is an enterprise wide area network supporting field offices and forecast centers across the country. As such, OneNWSNet has physical presence in the form of networking gear (routers, firewalls, switches) in every Weather Forecast Office and Regional center.

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

One of the major functions of NOAA8860 is to provide an enterprise wide area network. As such, NOAA8860 interconnects with many other NOAA FISMA systems at the network boundary. These include the following:

External	System Name	Owner	Interface Type	Transfer Method	Transfer Type	Classification
No	NOAA0201 - Web Operation Center (H)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA0500 – NOAA Research & Development High Performance Computing System (R&D HPCS)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA3065 - NOAA Profiler Network Central Facility (FSL Demonstration Division)(NPN)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA5045 - NOAA Environmental Satellite Processing Center	NOAA	Active	Via Network	Both	Sensitive But Unclassified
No	NOAA8104 - WSR-88D Weather Radar (NEXRAD)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8106 - Upper Air Observing System (UAOS)	NOAA	Active	Via Network	Receive	Unclassified
No	NOAA8107 - Advanced Weather Interactive Processing System	NOAA	Active	Via Network	Send	Unclassified
No	NOAA8202 - Office of Water Prediction	NOAA	Active	Via Network	Both	Sensitive But Unclassified

No	NOAA8212 - Terminal Doppler Weather Radar - Supplemental Product Generator	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8850 - NWS Enterprise Mission Enabling System	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8861 - Aviation Weather Center	NOAA	Active	Via Network	Send	Unclassified
No	NOAA8864 - Space Weather Prediction Center	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8865 - NOAA Tsunami Warning System (NTWS)	NOAA	Active	Via Network	Both	Sensitive But Unclassified
No	NOAA8868 - Storm Prediction Center	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8872 - Meteorological Development Lab Network	NOAA	Passive	Via Network	Both	Unclassified
No	NOAA8873 - National Data Buoy Center	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8877 – ROC LAN	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8881 – Central Region	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8882 - ER Bohemia	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8883 - Pacific Region	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8884 – Southern Region	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8885 – Western Region	NOAA	Active	Via Network	Both	Unclassified
Yes	US Coast Guard International Ice Patrol	CDR William C. Woityra	Active	Via Network	Receive	Unclassified

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

To support four Major Operational Functions Integrated Dissemination Program (IDP), OneNWSNet, the Weather and Climate Operational Supercomputing System (WCOSS), and local center support. Additionally, NOAA8860 supports data centers in Kansas City and Silver Spring, which host weather.gov, while this function is being migrated to IDP.

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

NOAA8860 provides application servers, database servers, web servers, file servers, FTP servers, and client workstations to achieve its purpose.

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

The majority of information collected, maintained, and disseminated by NOAA8860 is publicly available weather data used to develop and enhance weather models, forecasts, and alerts that are ultimately provided to the public for important decision-making and weather-ready awareness.

WCOSS also ingests some business sensitive information including geolocation data of NOAA ships and aircrafts, as well as proprietary weather data from private commercial sources. These data are considered restricted and only necessary personnel have access, which is controlled on a per user basis.

Finally, trusted agents have access to forms CD591, which is used for government issued identification cards. Senior management personnel also have access to employee performance reviews.

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

Number of Users	**Type of User**	**User Location**
30	System Administrators	AK, CP, BLDR, KC, NHC, Reston, Orlando
20	Network Administrators	CP, BLDR, NHC, KC, HI
5	Security Engineers	CP
675	Meteorologists, Hydrologists, Oceanographers	CP
80	Programmers	CP, KC, Remote
20	Office Administrators	CP
40	Managers	CP
40	Physical Scientists	CP
15	Support Scientists	CP
15	Program Managers & Task Leaders	CP
20	Clerical Support	CP

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

NOAA/NWS users login physically to workstations or remotely via 2-factor enforced VPN. External users access information via publicly accessible web sites.

i) How information is transmitted to and from the system

IDP is built on the concept of shared data and virtual machines. This allows applications with different software design paradigms and computing needs to co-exist and run at peak performance. Input datasets exist on shared storage and can be accessed by many projects, simplifying the data ingest process, conserving bandwidth, and accelerating the onboarding process through common networking services, common data acquisition, storage and a common source control system.

WCOSS ingests, processes, and produces multiple types of data, including observational input data, operational forecast model output data, and development forecast model output data. Most data is moved using the infrastructure within IDP, but some data sets (such as Radar data) are ingested directly into WCOSS. Direct access to WCOSS is limited to authorized users involved in the development and support of the models. External systems do not directly interact with WCOSS - it is not public facing.

WCOSS also ingests some business sensitive information including geolocation data of NOAA ships and aircrafts, as well as proprietary weather data from private commercial sources. These data are considered restricted, and only necessary personnel have access, which is controlled on a per user basis.

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. *Skip 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 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.)."

X Yes, the IT system collects, maintains, or disseminates BII.

____ 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
____ Other Federal Government personnel
____ 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?

X 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.

PII is collected for facilitating completion of required business processes and administrative tasks. SSNs are only collected for purposes of issuing a Common Access Card (CAC). Only trusted agents have access to this data.

Provide the legal authority which permits the collection of SSNs, including truncated form.

Legal authority for collection of PII: 5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

____ 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 Weather and Climate Computing Infrastructure Services 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 Weather and Climate Computing Infrastructure Services and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer Name: Scott Tieperman Office: NWS Phone: 301-683-3869 Email: scott.tieperman@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: TIEPERMAN.SCOTT.M.1293905289 Digitally signed by TIEPERMAN.SCOTT.M.1293905289 Date: 2022.03.31 16:53:10 -04'00' Date signed: 03/31/2022	**Information Technology Security Officer** Name: Chris Ortiz Office: NWS Phone: 303-497-3930 Email: chris.ortiz@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ORTIZ.CHRISTOPHER.J.1154749175 Digitally signed by ORTIZ.CHRISTOPHER.J.1154749175 Date: 2022.04.01 16:09:16 -04'00' Date signed: 4/1/2022
Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 240-577-2372 Email: Adrienne.Thomas@noaa.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2022.04.07 10:57:11 -04'00' Date signed:	**Authorizing Official** Name: Michael Farrar Office: NOAA NCEP Phone: 301-683-1315 Email: michael.farrar@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: FARRAR.MICHAEL.RAY.1106463960 Digitally signed by FARRAR.MICHAEL.RAY.1106463960 Date: 2022.04.05 12:38:41 -04'00' Date signed: 4/5/2022
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.04.13 11:43:52 -04'00' Date signed: 4.13.22	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.