Version Number: 01-2021

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

Privacy Threshold Analysis for the
NOAA8885
National Weather Service (NWS) Western Region General Support System

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Weather Service (NWS) Western Region General Support System (NOAA8885)

Unique Project Identifier: NOAA8885

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:

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).

NOAA8885 data and products assist in the formation of a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community. NOAA8885 also provides administrative functions as well as scientific & technical research support for the NWS Western Region Headquarters (WRHQ) and all offices within the NWS Western Region (WR) boundary.

Address the following elements:

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

The NOAA8885 System is a General Support System (GSS) which is designed and used to collect, process, and disseminate supplemental weather data that supports warning and forecast products for the protection of life, property, and the enhancement of the national economy.

b) System location

The NOAA8885 system is distributed over eight states and provides computing resources and networks for personnel at the following offices: NWS Western Region Headquarters (WRHQ), 24 Weather Forecast Offices (WFOs), four Central Weather Service Units (CWSUs), three River Forecast Centers (RFCs), and two Port Meteorological Offices (PMOs):

NWS Western Region Headquarters (WRHQ) Salt Lake City, UT

Weather Forecast Offices (WFOs)

- WFO BOI Boise, ID
- WFO BYZ Billings, MT

- WFO EKA Eureka, CA
- WFO FGZ Bellemont, AZ
- WFO GGW Glasgow, MT
- WFO HNX Hanford, CA
- WFO LKN Elko, NV
- WFO LOX Oxnard, CA
- WFO MFR Medford, OR
- WFO MSO Missoula, MT
- WFO MTR Monterey, CA
- WFO OTX Spokane, WA
- WFO PDT Pendleton, OR
- WFO PIH Pocatello, ID
- WFO PQR Portland, OR
- WFO PSR Phoenix, AZ
- WFO REV Reno, NV
- WFO SEW Seattle, WA
- WFO SGX San Diego, CA
- WFO SLC Salt Lake City, UT
- WFO STO Sacramento, CA
- WFO TFX Great Falls, MT
- WFO TWC Tucson, AZ
- WFO VEF Las Vegas, NV

River Forecast Centers (RFCs)

- RFC PTR NWRFC Portland, OR
- RFC RSA CNRFC Sacramento, CA
- RFC STR CBRFC Salt Lake City, UT

Central Weather Service Units (CWSUs)

- CWSU ZLA Palmdale, CA
- CWSU ZLC Salt Lake City, UT
- CWSU ZOA Fremont, CA
- CWSU ZSE Auburn, WA

Port Meteorological Officer (PMO)

- PMO Long Beach, CA
- PMO Seattle, WA

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

Although there are a variety of hardware and operating systems, several of the activities are interconnected. NOAA8885 provides direct and indirect mission support for the NWS as a Government agency. NOAA8885 primarily interconnects with federal and state governmental

agencies:

- NOAA8106 Upper Air Observing System - The UAOS provides the NWS with environmental sounding measurements from balloon borne radiosondes launched twice daily.
- NOAA8104 Weather Surveillance Radar 88D (WSR-88D) - Facilitates the transfer of WSR-88D data to the NWS Level II Collection and Dissemination System which is collected at Western Region Weather Forecast Offices (WFOs).
- NOAA8107 Advanced Weather Interactive Processing System (AWIPS) - AWIPS is an interactive system that integrates meteorological, hydrological, satellite, and radar data that enables the forecaster to prepare and issue forecasts and warnings.
- NOAA8860 Weather and Climate Computing Infrastructure Services (WCCIS) - Wide Area Network (WAN) services for interconnecting WRH, all WFOs, and RFCs.
- NOAA0100 NOAA Cyber Security Center - The NOAA Cyber Security Center (NCSC) is a functional body of technologies, processes, and practices designed to support the NCSC mission to protect NOAA networks, computers, programs, and data from cyber-attack, damage, and unauthorized access.
- NOAA0201 Web Operation Center (WOC) - The WOC provides a wide range of information technology services and functions. The core services are the 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).
- NOAA8850 Enterprise Mission Enabling System (EMES) - EMES operates a group of servers throughout the National Weather Service (NWS) that include Active Directory (AD) domain controllers, Enterprise Continuous Monitoring Operations (ECMO) relays, and McAfee ePolicy Orchestrator (McAfee ePO) servers.
- NOAA0550 NOAA Science Network - N-Wave is a general-purpose shared network consisting of a private carrier class network backbone that supports the NOAA's scientific mission by providing high speed networking services to NOAA customer sites, programs, line offices, and research facilities.
- California Dept. Of Water Resources – Enables the collection, analysis and display of meteorological data collected throughout the Western United States.

d) The purpose that the system is designed to serve

NOAA8885 data and products assist in the formation of a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community. NOAA8885 also provides administrative functions as well as scientific & technical research support for the NWS Western Region Headquarters (WRHQ) and all offices within the NWS Western Region (WR) boundary.

e) The way the system operates to achieve the purpose

NOAA8885 employs an information security architecture that promotes segmentation, redundancy, and the elimination of single points of failure to the fullest extent possible,

which enables NOAA8885 to more effectively manage risk. In addition, NOAA8885 takes into consideration its mission/business programs and applications when considering new processes or services to help determine areas where shared resources can be leveraged or implemented. NOAA8885 strives to implement security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

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

The majority of information produced by the system is public information. Functional areas of NOAA8885 can be classified into six major areas:

- Observations – Meteorological/Hydrological Sensing systems
- Operations/Production – Operations/Production of Watches, Warnings, & Forecasts
- Dissemination – Systems used for the dissemination of NWS information
- Administration – Office Automation, Word Processing, Email, etc.
- Security – Systems supporting the security posture of the Enterprise
- Network – Networking/Transport Infrastructure

Weather related data (i.e., public data) within NOAA8885 for the most part is considered perishable information and is retained for as long as the information is useful or serves a legitimate purpose.

Video surveillance imagery is captured at points of ingress and egress at facilities to ensure safety and security.

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

The general public has access to publicly available information through a variety of dissemination methods that include the issuance of watches, warnings, and forecasts and public web sites. NOAA8885 employees and contractors have access to various internal NWS information based on their role and responsibilities within the organization to support the NWS mission.

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

Publically available information is retrieved using standard techniques and protocols (i.e., https). Access to and retrieval of internal information is controlled by the use of account permissions, firewall access lists, and two-factor authentication. Access is based on "need to have" and the least privilege principle.

i) How information is transmitted to and from the system

NOAA8885 implements managed interfaces for all devices through the uses of

intelligent network devices that use access groups and access control lists which limits access to only the essential functions and services. As noted above, much of the information transmitted is public information and utilizes standard techniques and protocols. Information deemed not to be public (i.e., internal), is transmitted using the underlying operating system and device capabilities which afford a level of protection commensurate with the information sensitivity.

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.

X Yes. *(Check all that apply.)*

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

____ 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
- ____ 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 NOAA8885 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 NOAA8885 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Sean Wink Office: NOAA NWS Western Region Phone: 385-419-3131 Email: sean.wink@noaa.gov Signature: WINK.SEAN.P.1365853270 Digitally signed by WINK.SEAN.P.1365853270 Date: 2023.02.12 14:09:12 -07'00' Date signed: _____	**Information Technology Security Officer** Name: Andrew Browne Office: NOAA NWS Office of the CIO Phone: 301-427-9033 Email: andrew.browne@noaa.gov Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2023.02.13 15:33:48 -05'00' Date signed: _____
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: robin.burress@noaa.gov Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.03.20 09:43:48 -04'00' Date signed: _____	**Authorizing Official** Name: Grant Cooper, Ph.D. Office: NOAA NWS Western Region Phone: 801-524-5122 Email: grant.cooper@noaa.gov Signature: COOPER.GRANT.ALEXANDER.1047689399 Digitally signed by COOPER.GRANT.ALEXANDER.1047689399 Date: 2023.02.13 07:56:19 -07'00' Date signed: _____
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2023.04.13 07:46:01 -04'00' Date signed: _____	