Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
NOAA8881
CR LAN/WAN

U.S. Department of Commerce Privacy Threshold Analysis

NOAA8881 CR LAN/WAN

Unique Project Identifier: NOAA8881

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).

The National Weather Service (NWS) is a general support system that provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community. Issuance of warnings and forecasts is dependent on a complex interaction of many information resources. The system is designed and used to collect, process, and disseminate supplemental weather data which supports warning and forecast products. It also supports the supporting and administrative functions and supports the scientific & technical research and innovations activities of all offices within the Central Region including the regional headquarters.

Although there are a variety of hardware and operating systems, several of the activities are interconnected. The system provides direct and indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems and client-server systems. The system supports a variety of users, functions, and applications. Supported applications include word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

Security cameras have been deployed for many years in NOAA8881, however, the information wasn't previously added to the privacy documentation.

Address the following elements:

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

General Support System

b) *System location*

NOAA8881 CRHQ Kansas City, Missouri

Warning Decision Training Branch Norman, OK

2 River Forecast Centers

5 Center Weather Service Units

38 Weather Forecast Offices

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

NOAA8881 interconnects with the following FISMA systems (ALL internal to NOAA):

NOAA8102 – Automated Surface Observation System
NOAA8104 – WSR-88D Radar Operations Center
NOAA8106 – Upper Air Observing System
NOAA8107 – Advanced Weather Interactive Processing System
NOAA8850 – Enterprise Mission Enabling System
NOAA8860 – Weather and Climate Computing Infrastructure Services

Other (non-FISMA):

Big Sioux River Flood Forecasting Center
Bureau of Reclamation – Billings Area Office
Bureau of Reclamation – Great Plains Regional Office
Colorado State University (CIRA)
Iowa Flood Center
North Dakota State Agricultural Communications
University of Northern Colorado – School of Earth Sciences and Physics
University of Wisconsin – Madison
USACE – Northwestern Division – Omaha
USACE – St. Louis Office
USACE – St. Paul District
USACE _ Rock Island
USGS – Illinois Water Science Center
*Internet
*Articulate 360 SAAS

**Note: These are not new, simply overlooked previous PTA.*

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

The system provides direct or indirect mission support for the NWS as a Government agency. Mission

Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems and client-server systems. The system supports a variety of users, functions, and applications, including word processing, budget and requisition information, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development, and collaboration.

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

The NWS Central Region (CR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees and volunteers who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports, and performing other related administrative tasks. In addition, Weather Forecast Office (WFO)/River Forecast Centers (RFC) maintain local databases that contain information on volunteers who provide weather reports to them. NOAA8881 site WFO Louisville, KY recently acquired a Mavic 2 Enterprise drone that will be used to collect hydrologic data along with post storm damage surveys.

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

Network (WAN)/Local Area Network (LAN) databases, consist of basic identifying information (name, phone number, address) about employees and volunteers who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports, and performing other related administrative tasks. NOAA881 site WFO Louisville, KY will use an Unmanned Aircraft System (UAS) for hydrologic surveys and post storm damage surveys. The UAS is used strictly over hydrologic resources and areas of storm damage. Any privacy data that is inadvertently collected will be immediately deleted.

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

Federal Employees and contractors working on behalf of NOAA8881. These individuals must have a need to know and access is part of their duties. Currently the UAS is non-operational but only UAS operators will have access to the data and they will scrub all PII data before distribution.

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

Information is retrieved using Government Funded Equipment while at the official duty station and both GFE and Personally Owned Equipment while teleworking. CAC usage is enforced while at the duty station and when using the VPN from the teleworking location. Data on the UAS is captured on internal drive or SD card. It uses AES-265 encryption and is password protected. The UAS is operated in a way (altitude/ hydrologic locations) where the capturing of PII is unlikely. As soon as the data has been transferred to a local PC, the UAS footage is reviewed and any PII that was captured is deleted.

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

Only authorized personnel can transmit to and from NOAA8881 using secure methods. NOAA8881 uses OneNet which is a Trusted Internet Connection Access Provider. If PII needs to be emailed, NOAA8881 uses KiteWorks for encrypted transport. UAS data is transferred directly to a dedicated PC for PII review/deletion.

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.

X 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.

____ 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		Building entry readers	X
Video surveillance	X	Electronic purchase transactions	
Other (specify): Although the UAS has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. The UAS is operated in mainly remote locations and is always in the line of sight of the operator. Security cameras are in place at all offices. Data is recorded but the data does not include any sensitive PII. Data is only captured outside facility entries and other locations around like parking lots and upper air facilities where present. These cameras have been in use for many years but just now being included in the privacy documents.			

____ 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
____ 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 NOAA8881 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 NOAA8881 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: Darrel Smith Office: NWS Central Region Headquarters Phone: 816-268-3150 Email: Darrel.Smith@noaa.gov Signature: SMITH.DARREL.RAY.1103479017 Digitally signed by SMITH.DARREL.RAY.1103479017 Date: 2022.11.04 06:14:56 -05'00' Date signed: ________________	**Information Technology Security Officer** Name: Andrew Browne Office: NWS OCIO Phone: 301-427-9034 Email: Andrew.Browne@noaa.gov Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2022.11.07 09:08:15 -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: 2022.11.09 14:45:30 -05'00' Date signed: ________________	**Authorizing Official** Name: Kenneth Harding Office: NWS Central Region Headquarters Phone: 816-268-3130 Email: Signature: HARDING.KENNETH.WALLACE.1139815765 Digitally signed by HARDING.KENNETH.WALLACE.1139815765 Date: 2022.11.07 07:55:23 -06'00' Date signed: ________________
Bureau Chief Privacy Officer Name: Mark Graff Office: NOCC OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.12.08 16:13:46 -05'00' Date signed: ________________	