Template Version Number: 01-2021

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

Privacy Threshold Analysis for the
Space Weather Prediction Center
NOAA8864

Template Version Number: 01-2021

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/ National Weather Service/Space Weather Prediction Center (NOAA8864)

Unique Project Identifier: NOAA8864 SWPC **006-48-01-13-01-3504-00-108-023**

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).

The Space Weather Prediction Center (SWPC) located in Boulder, Colorado, provides real-time monitoring and forecasting of solar and geomagnetic events, conducts research in solar-terrestrial physics, and develops techniques for forecasting solar and geophysical disturbances.

The Space Weather Prediction Center (SWPC) has been designated a National Critical Infrastructure system. Its components ingest, process, create, and disseminate critical real-time space weather data, information, and products used directly by National Oceanic and Atmospheric Administration (NOAA)/SWPC Forecast Operations Center, other government agencies, international organizations, private industry, research, academic and other public sector interests to help reduce the impact of space weather disturbances and protect life and property. Critical users, including the NOAA National Geophysical Data Center (NGDC), United States Air Force (USAF), National Aeronautics and Space Administration (NASA) and the Federal Aviation Administration (FAA), satellite and communication operators, the power and airlines' industries, and a developing space weather industry, rely on the data and products made available 24 X 7 through Forecast Operations Center, which is staffed jointly by SWPC and 557th Air Force Weather Wing personnel.

SWPC functions as a national and international center for space environment and geophysical services and supporting research. SWPC provides a diverse spectrum of military, government, private industry and general public users with information on the state of the space environment, forecasts of solar-terrestrial conditions, alerts and warnings of expected disturbances in space weather, and analyses of user problems. These products help users take action to reduce the impact of space weather and to plan activities sensitive to solar-terrestrial conditions. Space weather forecasts and real-time information are of vital importance to users and owners of satellites, communications, navigation, power and pipelines, and high altitude / high latitude aircraft. Customers range from NASA's Space Radiation Analysis Group who uses this information to assess crew (and payload) radiation levels during NASA Space Shuttle missions, to satellite operators who need advisories of severe space weather which may harm their spacecraft's, to radio operators who use space weather indices for predicting radio propagation.

SWPC also serves as a Regional Warning Center (RWC) and the World Warning Agency (WWA) of the International Space Environment Services (ISES). The ten Regional Warning Centers of the ISES are responsible for providing real-time monitoring and prediction of space weather for their localized section of the world. SWPC, as RWC Boulder, serves the Western Hemisphere. As WWA, SWPC acquires and exchanges data between all the RWCs, and plays a major role in planning and executing international space weather campaigns.

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

Boulder, Colorado
Ashburn, Virginia

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

NOAA0100 – NOAA Cyber Security Center (NCSC)
NOAA5011 – National Geophysical Data Center Data Archive Management and User System
NOAA0550 - NOAA Enterprise Network (NWAVE)
NOAA5050 - Geostationary Environmental Operational Satellite Series-R Ground System
NOAA8860 - Weather and Climate Computing Infrastructure Services (WCCIS)

d) The purpose that the system is designed to serve

The Space Weather Prediction Center (SWPC) provides real-time monitoring and forecasting of solar and geomagnetic events, conducts research in solar-terrestrial physics, and develops techniques for forecasting solar and geophysical disturbances. SWPC's parent organization is the National Oceanic and Atmospheric Administration (NOAA).

e) The way the system operates to achieve the purpose

Information is gathered in order for individuals to subscribe to receive alerts produced by SWPC through the https://pss.swpc.noaa.gov/.

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

For the Product Subscription Service this website collects the following information:

- Email Address

- Name of user
- Name of company/entity/organization (optional)

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

Database administrators, IT support staff administrators

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

Users must authenticate to obtain their user account data. SWPC does not store the passwords that are created by the users. Once inside the website, a user can update their personal data.

i) How information is transmitted to and from the system

Emails are distributed to users that subscribe to the alerts from SWPC.

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.*

_X_ 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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): NOAA5049 COSMIC is decommissioned. NOAA5050 GOES-R Ground System replaces NOAA5003 - GOES Ground System. NOAA8107 – AWIPS no longer interconnects with SWPC.					

____ 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.*

____ 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 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
____ 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 NOAA8864 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 NOAA8864 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: Steve Michnick Office: NWS/NCEP/SPC Phone: (816) 708-1835 Email: Steve.M.Michnick@noaa.gov Signature: MICHNICK.STEVEN.MICHAEL.1383826469 Digitally signed by MICHNICK.STEVEN.MICHAEL.1383826469 Date: 2023.11.15 10:57:19 -06'00' Date signed: November 15, 2023	**Information Technology Security Officer** Name: Andrew Browne Office: NWS ACIO Phone: 301-427-9033 Email: andrew.browne@noaa.gov Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2023.11.16 15:16:15 -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: 2023.11.20 14:58:18 -05'00' Date signed: 11/20/2023	**Authorizing Official** Name: Michael Farrar Office: NWS/NCEP Phone: 301-683-1315 Email: michael.farrar@noaa.gov Signature: FARRAR.MICHAEL.RAY.1106463960 Digitally signed by FARRAR.MICHAEL.RAY.1106463960 Date: 2023.11.17 16:41:36 -05'00' 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: 2023.12.07 14:59:22 -05'00' Date signed: 12/7/23	