Version Number: 01-2017

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

Privacy Threshold Analysis
for the
Space Weather Prediction Center
NOAA8864

July 24, 2019

U.S. Department of Commerce Privacy Threshold Analysis

National Oceanic and Atmospheric Administration
National Weather Service/Space Weather Prediction Center (NOAA8864)

Unique Project Identifier: 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 and its purpose:
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 Air Force Weather Agency (AFWA) 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.

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).

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 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. *Please describe the activities which may raise privacy concerns.*
__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 about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
__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 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.

4c. 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, and/or 4c 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 Space Weather Prediction 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 Space Weather Prediction 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): Christopher John Ortiz (CISSP, CAP)_____

Signature of ISSO: ORTIZ.CHRISTOPHER.J.1154749175 Digitally signed by ORTIZ.CHRISTOPHER.J.1154749175 Date: 2019.08.12 14:12:15 -06'00' Date: _____

Name of Information Technology Security Officer (ITSO): Andrew Browne_____ _____

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2019.08.23 09:34:56 -04'00' Date: _____

Name of Authorizing Official (AO): Robert Maxson_____

Signature of AO: MAXSON.ROBERT.W.1079535326 Digitally signed by MAXSON.ROBERT.W.1079535326 Date: 2019.08.22 09:47:27 -04'00' Date: _____

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2019.09.05 17:21:16 -04'00' Date: _____