Version Number: 01-2019

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

Privacy Impact Assessment
for the
Space Weather Prediction Center
NOAA8864

Reviewed by: MARK GRAFF, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 03/18/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
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: System Description

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 577th 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.

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

General Support System

(b) System location

David Skaggs Research Center
325 Broadway
Boulder, CO 80305

(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)
NOAA0550 – NOAA Enterprise Network (NWAVE)
NOAA5003 – Geostationary Operational Environmental Satellite Ground System (GOES)
NOAA5011 – National Geophysical Data Center Data Archive Management and User System
NOAA5049 – Constellation Observing System for Meteorology Ionosphere and Climate Product Generation and Distribution (COSMIC)
NOAA8107 – Advanced Weather Interactive Processing System (AWIPS)
NOAA8860 – Weather and Climate Computing Infrastructure Services (WCCIS)

(d) The way the system operates to achieve the purpose(s) identified in Section 4

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

(e) 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.

(f) How information is transmitted to and from the system

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

(g) Any information sharing conducted by the system

Name and contact information is shared with other agencies in order to allow notification of space weather activities.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

5 U.S.C. § 301, Departmental regulations and 15 U.S.C. 1512, Powers and duties of Department. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared only among Department staff for work-related purposes. U.S. Government regulations restrict the distribution of customer information.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

High

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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.

_____ 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).

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 01-2017 or later).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): Telephone Number and e-mail collected maybe either General Personal Data (GPD) or Work-Related Data (WRD) depending on customer input.					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History			
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
k. Other work-related data (specify): Telephone Number and e-mail collected maybe either General Personal Data (GPD) or Work-Related Data (WRD) depending on customer input.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online https://pss.swpc.noaa.gov/	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Information accuracy is ensured by employing proper handling techniques and storage methods as well as utilizing access control methods that restrict access to only authorized individuals. Access controls enable data consistency, accuracy, trustworthiness and on a need to know basis.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities, which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities, which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	

To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The purpose of collection of PII is to promote customer service activities.

E-Mail is collected as the only method used for communicating with the customer. The various products subscribed are all delivered to end customers via e-mail. Contact information (Name and Phone Number) is used to contact individual customers if there is a problem with the product subscription service (PSS).

Additionally the use of the requested and provided information is used for statistical purposes to determine the customer base and general interest to products (emergency managers, researchers, specific industry sectors, etc.)

The information identified in section 1.1 of this document is in reference to anyone wishing to receive e-mail information for the various products of interest. Therefore, this would be members of the general public.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats to privacy information are primarily the inadvertent disclosure of the information due to unauthorized access to the system, unintentional disclosure, insider threat, and the accidental dissemination of contact information by 3rd party systems. Mitigations include the use of system security safeguards, which limits access to the information as well as monitors the access to the information system. Access to information is granted on a "need to know" basis and the least privilege principle. Users undergo the NOAA annual mandatory IT Security Awareness and Privacy Training, which includes the proper handling of information. Users acknowledge the rules of behavior to ensure they understand their responsibilities.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		

Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: • NOAA0100 – NOAA Cyber Security Center (NCSC) • NOAA0550 – NOAA Enterprise Network (NWAVE) • NOAA5003 – Geostationary Operational Environmental Satellite Ground System (GOES) • NOAA5011 – National Geophysical Data Center Data Archive Management and User System • NOAA5049 – Constellation Observing System for Meteorology Ionosphere and Climate Product • Generation and Distribution (COSMIC) • NOAA8107 – Advanced Weather Interactive Processing System (AWIPS) • NOAA8860 – Weather and Climate Computing Infrastructure Services (WCCIS) The Space Weather Prediction Center prevents the accidental leakage of the PII information by storing it in a database that is password protected. Only the database administrators, one forecaster and one software developer have access to this database password.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
	Other (specify):		

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at https://pss.swpc.noaa.gov/.	
X	Yes, notice is provided by other means.	Specify how: Notice is provided on the subscription web page. https://www.swpc.noaa.gov/content/subscription-services

	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals have the opportunity to decline to provide PII/BII. However, since the various products subscribed are all delivered to end customers via e-mail, and contact information (Name, Address, Phone Number, e-mail) are mandatory fields which are used to contact individual customers if there is a problem with the product subscription service (PSS), declining to provide the mandatory information will result in the services by email not being received.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Users have the option of subscribing to SWPC alerts and warnings through the product subscription service and can receive the data through other means (via SWPC Web Page, etc.).
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: When customers enter their e-mail address and password, they can update the information collected including product preferences.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: On a monthly basis, a report is generated demonstrating the usage of the subscription platform. Limited personnel within NOAA8864 have the capability to view this information.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 10/2/2020 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.

X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The information collected is stored within the operational database at the Space Weather Prediction Center. Protections include separation of the operations networks from other areas, stand-alone active directory access to the Database server for operations only, limited number of individuals with database access to review information. Passwords that are generated are only stored as a hash value. Data collection is done over an encrypted channel via HTTPS protocols.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: NOAA-11 - NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission Dept-18 - DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies Dept-25 - DEPT-25, Access Control and Identity Management System OPM/Govt-1 – OPM GOVT-1, General Personnel Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: DAA-GRS-2013-0006-003. Disposition Instruction: Temporary. Destroy when business need ceases.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: E-mail address and phone number
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: There is no sensitive data
X	Context of Use	Provide explanation: Data is only used to create an account with contact information if there was a problem (e-mail, phone number)
	Obligation to Protect Confidentiality	Provide explanation:

X	Access to and Location of PII	Provide explanation: PII is collected via an external website (HTTPS) and stored in a database that is not publicly accessible.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

SWPC collects only the minimum required information necessary for the purpose in which it is intended. In addition, SWPC participates in a mandated annual Assessment and Authorization (A&A) exercise that evaluates, test, and examine security controls to ensure they are implemented in a way to adequately mitigate risk to the unauthorized information disclosure.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes.
	Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.