Version Number: 01-2017

U.S. Department of Commerce
NOAA

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

11/15/2019

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

U.S. Department of Commerce Privacy Impact Assessment
National Weather Service / Space Weather Prediction Center

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

Introduction: System Description

The Space Weather Prediction Center (SWPC) has been designated a National Critical Infrastructure system. The Space Weather Prediction Center's (SWPC) Product Subscription Service (PSS) is a web and e-mail based service that allows customers to register via the internet to receive SWPC products via e-mail. Data collected during the registration process is also used for statistical analysis of users. The data is stored on a virtual server which is located in our data center located in Boulder, Colorado. Even though it is a virtual server, the data physically rests in government controlled facility and a specific location. Specific products of interest, which are registered by the individual, are then delivered via e-mail until the subscription is cancelled or the e-mail address is determined to be invalid. A Privacy Act Statement is listed on the main page of the Product Subscription Service, which contains this text:

Privacy Act Statement

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations and 15 U.S.C. 1512, Powers and duties of Department.

Purpose: Name, email and address may be collected for those requesting data, so that they may open an account through which to receive the data. Addresses are used to send alerts, respond to questions and send information that SWPC considers of interest to our customers. The information provided on the registration form may be used by SWPC for statistical analysis of customers.

Routine Uses: 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. No customer information is made available to other customers, organizations, vendors or other government agencies. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent required contacts regarding provision of data and alerts.

The Service consists of a web interface where customers subscribe by entering personal information (name, email address, work or home telephone number, work or home address) and selecting the products they want, a Structured Query Language (SQL) secure clustered database that stores the information, and a Notify Service that distributes the products. Subscriber

information is stored in a high-availability, secure environment that safeguards subscriber privacy.

Customers manage their own accounts by:

- Initially registering by entering a valid e-mail address and a password of their own choosing
- Adding to or deleting subscription preferences
- Updating personal information
- Listing current subscription choices
- Temporarily suspending product subscriptions
- Reinstating suspended product subscriptions
- Deleting all products to which they are subscribed
- Canceling subscription

Currently, the only delivery method for all Subscription Service products is e-mail.
Using the web interface, customers can update contact information and subscriptions for SWPC products. Once the subscriptions have been selected, the customer will receive e-mail alerts based on preferences.

The Product Subscription Service does not share any PII/BII data with anyone, except within the bureau, with the Department and other federal agencies, in the case of security or privacy breach. The data collected is used for statistical analysis and to identify groups of individuals who may be interested in helping SWPC develop future products or to improve existing products and forecasts.

Current customers of the PSS system include all major airlines, drilling and oil exploration companies, satellite companies, transportation sector, emergency responders and public/private Researchers.

See Statutory Authorities: 5 U.S.C 301, Departmental Regulations and 15 USC 1512 - Sec. 1512,Powers and Duties of Department [of Commerce] and 15 U.S.C 1151, which covers collection of information from customers who wish to receive data.

FROM DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C.1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

This is a FIPS 199 HIGH impact system.

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):					

__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.

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

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X*	o. Medical Information	
d. Gender		j. Telephone Number	X*	p. Military Service	
e. Age		k. Email Address	X*	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): Telephone Number, Address 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		d. Telephone Number	X*	g. Salary	
b. Job Title		e. Email Address	X*	h. Work History	
c. Work Address	X*	f. Business Associates			
i. Other work-related data (specify): Telephone Number, Address 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): Name, email and address may be collected for those requesting data, so that they may open an account through which to receive the data.			

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, Address, 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 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 is primarily the inadvertent disclosure of the information due to unauthorized access to the system or unintentional disclosure. 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):			

*In case of breach

	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.

	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:

X	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.
	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.	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.	

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.	

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.	

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: All system logs are sent to the NOAA Enterprise ArcSight log management solution. The log files can be used to determine who has access to the PII/BII information.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): November 16, 2018 ☐ 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. (High)
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 supporting 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 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 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)*: Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. DEPT-13, Investigative and Security 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: System Access Records; the disposition authority is 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.

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	E-mail address and phone number (optional)
	Quantity of PII	
X	Data Field Sensitivity	There is no sensitive data
X	Context of Use	Data is only used to create an account with contact information if there was a problem (e-mail, phone number, etc.)
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	PII is collected via an external website (HTTPS) and stored in a database that is not publicly accessible.
	Other:	

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