Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA Research & Development High Performance Computing System (R&D HPCS) – NOAA0500

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

08/30/2019

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA Research & Development High Performance Computing System (R&D HPCS) – NOAA0500

Unique Project Identifier: NOAA0500

Introduction: System Description

NOAA0500 system provides research and development weather models in support of NOAA's operational mission. The R&D HPCS operates large scale, extreme computing environments that encompass multiple geographic sites, and heterogeneous supercomputing architectures. This system supports NOAA's mission by providing cutting edge technology for weather and climate model developers. These models eventually form the basis for NOAA's daily weather forecasts, storm warnings, and climate change forecasts. System users include scientists from multiple NOAA Line Offices, and their research collaborators, including some foreign nationals.

NOAA's R&D HPC system (R&D HPCS) provides four fundamental HPC functions:

1. Large-scale computing provides computing for development, testing, and production integrations of NOAA environmental models. The workload that runs on this subsystem is characterized by computer-intensive codes with I/O characterized by regular snapshots of diagnostic fields.
2. Analysis and interactive computing provides computing for the post-processing of data from production runs and the analysis of post-processed data, code development, and debugging. The workload that runs on this subsystem is characterized by data-intensive codes requiring high I/O bandwidth.
3. Data archiving provides long-term storage of post-processed model runs and analyses.
4. Networking links these subsystems together.

The users of the system are primarily, but not exclusively, NOAA employees who represent the following offices:

1. NOAA/ESRL Global Systems Division, Boulder, Colorado
2. NOAA National Weather Service (NWS), National Centers for Environmental Prediction

(NCEP), Environmental Modeling Center (EMC), Camp Springs, Maryland

3. NOAA Geophysical Fluid Dynamics Laboratory (GFDL), Princeton, New Jersey

These users access the system and submit weather or climate modeling application program runs via job scheduling software. These models contain parallelized code to take advantage of the large scale, highly parallelized environment offered by the HPCS. This is necessary to support the science. Modeling jobs can be extremely large (e.g., 1200 processors required), because they incorporate different local, regional, or global atmospheric and ocean models to create an

ensemble model program. The scheduling software automatically identifies and collects the necessary processors to run the job, and controls its execution. Therefore, the user never has any direct interaction with the compute nodes of the system.

In accordance with applicable security controls, users of the R&D HPCS must first request an account prior to access approvals. Those users who would like an account must supply the requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators.

The user-supplied data is used only for identification and creation of unique accounts as well as for contact purposes if there should be a problem with the account. The user base consists of

Federal employees, contractors and foreign nationals.

Weather and climate data is collected from a variety of sources and fed into the system by the user community. All of this data is vetted by the NOAA scientific community through processes outside of this system, to guarantee its authenticity and integrity. Once entered into the R&D

HPCS, the system security controls are designed to guarantee the integrity of this data.

The current configuration of the R&D HPCS is architected along organizational lines. Largescale computing, analysis computing, and storage, at the following locations, are within the boundaries of NOAA0500. The other functions at these locations are not within the NOAA0500 boundaries.

1. NOAA Earth System Research Laboratory (ESRL). David Skaggs Research Center

(DSRC325 N. Broadway Street, Boulder, Colorado 80305,

2. NOAA Geophysical Fluid Dynamics Laboratory (GFDL), Princeton University Forrestal

Campus, 201 Forrestal Road, Princeton, New Jersey 08450,

3. NOAA Environmental, Security Computing Center (NESCC), 1000 Galliher Drive,

Fairmont, WV 26554.

The R&D HPCS has Interconnection Security Agreements with ORNL, N-Wave, NCEP, GFDL, and ESRL. These organizations provide general support and services such a LAN/WAN connectivity, authentication and identification controls, DNS, WEB and other IT infrastructure support.

The National Centers for Environmental Prediction (NCEP) utilize data acquired from commercial, other U.S Government and International sources to execute NCEP mission. A subset of this data, referred to as "restricted data" is made available to NCEP with restrictions on further dissemination.* As a direct or indirect party to the agreements governing the use of this Restricted Data, NCEP is charged with protecting restricted data during use and identifying restricted data to managers, users, staff and partners supporting NCEP mission. Authority for collection of information: 5 U.S.C. 301 5 U.S.C. 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

*NOAA has agreements with ships and planes, which collect local weather data while at sea/in the air and share with NOAA. The data includes the positions of those ships and planes, because the two types of information cannot be separated. The location data is considered proprietary.

Information sharing: The PII in the system will not be shared outside of the bureau except in case of a breach. The BII (restricted data). NCEP receives and shares with RDHPCS.

R&D HPCS FIPS 199 Impact Level: MODERATE

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.

__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 newer).

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		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

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		f. Business Associates			
i. Other work-related data (specify):					

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	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
NWS NCEP proprietary and restricted data (locations of ships and planes providing weather data).

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	X
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): NWS NCEP program owns the data and is responsible for its distribution.					

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.

Restricted data stored is protected by setting each file containing restricted data as readable only by users in the RSTPROD group. With the file / directory setting as read-only, the integrity of the file can be maintained. RSTPROD data is a copy of data provided to our storage system for the purposes of longer-term storage and access. We do not own the RSTPROD data. NCEP does. The NCEP copy process will ultimately ensure accuracy. Inaccurate data would disrupt mission and would immediately be identifiable. NCEP explicitly grants access to restricted data to NCEP staff and associates whose work utilizes these data. This access is granted through each system's account approval process on R&D HPCS.

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	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Archive and Storage only – no dissemination or processing within the R&D HPCS environment.			

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 National Centers for Environmental Prediction (NCEP) utilize data acquired from commercial, other U.S Government and International sources to execute NCEP mission. A subset of this data, referred to as "restricted data" is made available to NCEP with restrictions on further dissemination. As a direct or indirect party to the agreements governing the use of this Restricted Data, NCEP is charged with protecting restricted data during use and identifying restricted data to managers, users, staff and partners supporting NCEP mission.

NCEP Restricted Data Storage Locations
Restricted data can be found in the following locations:

- System networks [transitory]
- Long-term scratch file system in the path /tbd/tbd [transitory]
- Fast scratch file system in the path /tbd/tbd [stored]
- NCEP-Authorized user home file systems [stored]
- Backup media holding NCEP files [stored]

NCEP Restricted Data Protection
Restricted data stored is protected by setting each file containing restricted data as readable only by users in the RSTPROD group.

Authorized Users
NCEP explicitly grants access to restricted data to NCEP staff and associates whose work utilizes these data. This access is granted through each system's account approval process on R&D HPCS.

Privileged Users
Privileged users include staff that supports the systems, storage, and networks utilized to accomplish NCEP work. Privileged access includes access to a systems administrator or root account on a system, privileged access to network devices, and other than general user access to system storage devices, including data archiving or backup equipment. A privileged user has access to restricted data as a result of their privileged access to these systems.

Limitations on Privileged Users
Privileged users are notified that any of the following actions may be taken only with NCEP Management and Site Manager approval:

- Copying or moving restricted data to a location not identified as an NCEP Restricted Data Storage Location
- Making restricted data available by any means to a user that is not identified by NCEP Management as authorized to access restricted data
- Making restricted data available by any means to the public such as through an internet-connected server or public portal

In accordance with applicable security controls, users of the R&D HPCS must first request an account prior to access approvals. Those users who would like an account must supply the requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators. The user-supplied data is used only for identification and creation of unique

accounts as well as for contact purposes if there should be a problem with the account. The user base consists of Federal employees, contractors and foreign nationals.

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.)

All users who interact with NCEP RSTPROD data must read and agree to/acknowledge Terms and Conditions regarding the nature and protections associated with RSTPROD prior to obtaining access. Approvals for access to RSTPROD are solely at the discretion of an NCEP Federal Employee. R&D HPCS refers to the role this individual performs as, "Principle Investigator (PI)."

Users no longer requiring access are removed upon notification from the RSTPROD PI or when R&D HPCS access expires.

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.

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: NCEP. AC-1, 3, 4, 5, 6, 14, 21, 22; AU-2, 6; IA-4, 5, 8; and SC-4, 7, 8
	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: NCEP: (located above Clear Form button) http://www.nco.ncep.noaa.gov/sib/restricted_data/restricted_data_sib/register/ and R&D HPCS AIM:(located at bottom right / top line) https://aim.rdhpcs.noaa.gov/.	
X	Yes, notice is provided by other means.	Specify how: Notification and use is provided by NCEP on their rstprod web site: http://www.nco.ncep.noaa.gov/sib/restricted_data/restricted_data_sib/ Proprietary data is shared through NCEP agreements.
	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	Specify how: Proprietary data collected is provided through

	decline to provide PII/BII.	organizations with which NCEP has agreements for the use and dissemination of the data etc. Account users may decline to provide PII, by not providing it, but this will affect their ability to establish an account.
	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: Proprietary data is provided through agreements, for research purposes as agreed on. Account users: By providing information to establish an account, the user consents to its uses – access to the data and trouble-shooting any problems with the account.
	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: Account users may update their information at any time, and we ask them to update at least annually, using instructions on the Web site. This is N/A for the proprietary data.
	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.)*

X	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: Users who would like an account must supply the requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators. The usersupplied data is used only for identification and creation of unique accounts as well as for contact purposes if there should be a problem with the account.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 15 Mar 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.
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 NCEP data stored within the R&D HPCS and is only accessible to NCEP, which approves and provides access. Network accessibility to the storage and archive system is via internal connection (private circuits) and does not traverse the internet. Both NCEP and R&D HPCS users are required to login utilizing either 2-factor authentication and or CAC authentication. Overall system access is through secure bastions accessed over the internet with SSH encryption.

R&D HPCS has 24hr network and system monitoring and security logs weekly for suspicious activities, attempted logins etc. Data residing within the R&D HPCS system boundary remains within a data center which is also monitored 24x7, has CCTV, and armed guards. Access to the data center where the Storage and Archive resides is accessible via CAC/Badge reader to authorized and vetted NOAA personnel and contractors. Maintenance, and other personnel not previously vetted by NOAA are escorted and observed at all times within the data center.

In accordance with applicable security controls, users of the R&D HPCS must first request an account prior to access approvals. Those users who would like an account must supply the requested/required data on a web-based form. Those requests and associated data supplied by the user are stored in a database and only accessible by authorized privileged account administrators. The user-supplied data is used only for identification and creation of unique accounts as well as for contact purposes if there should be a problem with the account. The user base consists of Federal employees, contractors and foreign nationals.

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)*: DEPT-18, Employees Personnel Files not Covered by other Notices; COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. DEPT-13, Investigative and Security Files.
	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: This is governed by NOAA 1200-02, Research Notebooks and NOAA1200-6, Data Requests.
	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	X	Deleting	
Other (specify): The referenced data has a very long/perpetual life. Storage media that has potentially been used for this referenced data is degaussed once retired and prior to being removed from the system boundary.			

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 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: An individual may be identified from information in the accounts database.
X	Quantity of PII	Provide explanation: The only PII is account contact information.
X	Data Field Sensitivity	Provide explanation: There is no sensitive PII.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: AC-1, 3, 4, 5, 6, 14, 21, 22; AU-2, 6; IA-4, 5, 8; and SC-4, 7, 8
	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.)

R&D HPCS provides services for Archive and Storage only – no dissemination or processing within the R&D HPCS environment. It is outside the scope of R&D HPCS to determine type or quantity. R&D HPCS employs the required FISMA controls to protect the data stored within R&D HPCS.

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.