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

Privacy Impact Assessment for the NOAA8860

Weather and Climate Computing Infrastructure Services (WCCIS)

Reviewed by: Mark H. 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

GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2024.04.29 07:30:59 -07'00' 29 April 2024

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

U.S. Department of Commerce Privacy Impact Assessment NOAA/NWS/Weather and Climate Computing Infrastructure Services (WCCIS)

Unique Project Identifier: NOAA8860

Introduction: System Description

Provide a brief description of the information system.

NOAA8860 is an integral part of the National Centers for Environmental Prediction (NCEP) that helps in providing timely, accurate and continually improving worldwide forecast guidance products.

Address the following elements:

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

NOAA8860 is a general support system that supports four Major Operational Functions: Integrated Dissemination Program (IDP), OneNWSNet, the Weather and Climate Operational Supercomputing System (WCOSS), and NCEP center support. Additionally, NOAA8860 supports data centers in Kansas City, MO, and Silver Spring, MD, which host weather.gov, while this function is being migrated to IDP.

(b) System location

Weather and Climate Computing Infrastructure Services (WCCIS; NOAA8860) is comprised of six National Centers for Environmental Prediction (NCEP) centers. These are:

- NCEP Central Operations (**NCO**)
- Weather Prediction Center (**WPC**)
- Ocean Prediction Center **(OPC**)
- Environmental Modeling Center (**EMC**)
- Climate Prediction Center (**CPC**), and
- National Hurricane Center (**NHC**)

All of the centers are located in College Park, MD, (CP), except NHC which is located in Miami, Florida. NOAA8860 operates a high availability backup location in Boulder, CO, (BLDR), and Kansas City, MO, (KC), which act as alternate processing sites for the aforementioned functions. Additionally, NOAA8860 has a minimal presence in Silver Spring, MD, to support telecommunications for various customers.

WCOSS systems require high availability and thus have identical primary and failover sites. These sites are located in Phoenix, AZ, and Manassas, VA.

OneNWSNet is an enterprise wide area network supporting field offices and forecast centers across the country. As such, OneNWSNet has physical presence in the form of networking gear (routers, firewalls, switches) in every Weather Forecast Office (WFO) and Regional center.

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

any other systems to which it interconnects)

External	System Name	Owner	Interface Type	Transfer Method	Transfer Type	Classification
No	NOAA0201 – Web Operation Center (H)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA0500 – NOAA Research & Development High Performance Computing System (R&D HPCS)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA0550 - NOAA Enterprise Network	NOAA	Active	Via Network	Both	Unclassified
No	NOAA3065 - NOAA Profiler Network Central Facility (FSL Demonstration Division) (NPN)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA5045 – NOAA Environmental Satellite Processing Center	NOAA	Active	Via Network	Both	Sensitive But Unclassified
No	NOAA8104 - WSR-88D Weather Radar (NEXRAD)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8106 - Upper Air Observing System (UAOS)	NOAA	Active	Via Network	Receive	Unclassified
No	NOAA8107 – Advanced Weather Interactive Processing System	NOAA	Active	Via Network	Send	Unclassified
No	NOAA8202 - Office of Water Prediction	NOAA	Active	Via Network	Both	Sensitive But Unclassified
No	NOAA8212 - Terminal Doppler Weather Radar - Supplemental Product Generator	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8501 - NWS Cloud Infrastructure System (NCIS)	NOAA	Active	Via Network	Send	Unclassified
No	NOAA8850 – NWS Enterprise Mission Enabling System	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8861 – Aviation Weather Center	NOAA	Active	Via Network	Send	Unclassified
No	NOAA8864 – Space Weather Prediction Center	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8865 – NOAA Tsunami Warning System (NTWS)	NOAA	Active	Via Network	Both	Sensitive But Unclassified

No	NOAA8868 – Storm Prediction Center	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8872 - Meteorological Development Lab Network	NOAA	Passive	Via Network	Both	Unclassified
No	NOAA8873 - National Data Buoy Center	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8881 – Central Region	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8882 - ER Bohemia	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8883 - Pacific Region	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8884 – Southern Region	NOAA	Active	Via Network	Both	Unclassified
Yes	US Coast Guard International Ice Patrol	CDR William C. Woityr	Active	Via Network	Both	Unclassified

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

NOAA8860 provides application servers, database servers, web servers, file servers, FTP servers, and client workstations to achieve its purpose.

(e) How information in the system is retrieved by the user

NOAA/NWS users login physically to workstations or remotely via 2-factor enforced VPN. External users access information via publicly accessible web sites.

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

IDP is built on the concept of shared data and virtual machines. This allows applications with different software design paradigms and computing needs to co-exist and run at peak performance. Input datasets exist on shared storage and can be accessed by many projects, simplifying the data ingest process, conserving bandwidth, and accelerating the onboarding process through common networking services, common data acquisition, storage and a common source control system.

WCOSS ingests, processes, and produces multiple types of data, including observational input data, operational forecast model output data, and development forecast model output data. Most data is moved using the infrastructure within IDP, but some data sets (such as radar data) are ingested directly into WCOSS. Direct access to WCOSS is limited to authorized users involved in the development and support of the models. External systems do not directly interact with WCOSS - it is not public facing.

WCOSS also ingests some business sensitive information including geolocation data of NOAA ships and aircrafts, as well as proprietary weather data from private commercial sources. These data are considered restricted, and only necessary personnel have access, which is controlled on a per user basis.

(g) Any information sharing conducted by the system

NOAA8860 shares information with many Weather Service and NOAA internal systems. This information consists of weather-related models and forecasts. This data is shared with NWS, NOAA, DOC, and other Government agencies. Additionally, weather data is shared with external systems and the public.

Proprietary weather data is only accessible from specific personnel and not disseminated outside of NOAA8860.

Human Resources (HR) related personal information is not shared outside of the organization.

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

Type of Information Collected	Applicable SORNS	Programmatic Authorities
Collection & Use of SSN	COMMERCE/DEPT-18	44 U.S.C. 3101
		Executive Order 12107
	OPM/GOVT-1	Executive Orders 9397, as amended by 13478, 9830, and 12107
	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
Badging & CAC Issuance	COMMERCE/DEPT-18	Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		5 U.S.C. 301
	GSA/GOVT-7	5 U.S.C. 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
		Federal Information Security Management Act of 2002 (44 U.S.C. 3554)
		E-Government Act of 2002 (Pub. L. 107–347, Sec. 203)
Employee Performance Info	OPM/GOVT-2	Executive Order 12107
		5 U.S.C. Sections 1104, 3321, 4305, and 5405

System Administration/Audit Data (SAAD)	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
		Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		28 U.S.C. 533-535
Managing Access Accounts and Login Names	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
		Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		28 U.S.C. 533-535
Public Health Emergency Info & Reasonable Accommodation	COMMERCE/DEPT-18	Executive Order 13164
	COMMERCE/DEPT-31	Rehabilitation Act, 29 U.S.C. 701 et. seq
		Americans with Disabilities Act of 1990, as amended, 102(d), 42 U.S.C. 12112(d)
		29 CFR parts 1602, 1630, 1904, 1910, and 1960
		29 USC chapter 15 (e.g., 29 U.S.C. 668)
		Executive Order 12196
		5 U.S.C. 7902
	OPM/GOVT-1	5 U.S.C. 1302, 3301
Foreign National Information	COMMERCE/DEPT-27	28 U.S.C. 533-535
		44 U.S.C. 3101
		5 U.S.C. 301
		Executive Orders 13526, 12968, 13356, 13587
		Public Law 108-458 (Intelligence Reform and Terrorism Prevention Act of 2004)
		Intelligence Authorization Act for FY 2010, Public Law 111-259
		31 U.S.C. 951-953
		8 U.S.C. 1324a
		15 Code of Federal Regulations (CFR) Parts 730-774, Export Administration Regulations
		NOAA Administrative Order (NAO) 207-12 “Technology Controls and Foreign National Access”
		Department Administrative Order (DAO) 207-12 Version Number: 01-2017 “Foreign National Visitor and Guest Access Program

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

NOAA8860 is a FIPS199 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):					

_____ 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.

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* **	**x**	f. Driver's License	x	j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration	x	l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	X**
e. File/Case ID					
n. Other identifying numbers (specify): ** Reasonable Accommodation records related to COVID-19.					

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

PII is collected for facilitating completion of required business processes and administrative tasks. SSNs are only collected for purposes of issuing a Common Access Card (CAC). Only trusted agents have access to this data.

Alien Registration cards are only collected from Non-US citizens who require access to the NOAA8860 information system, or the National Center for Climate and Weather Prediction, and is used by HR to issue access badges.

General Personal Data (GPD)					
a. Name	x	h. Date of Birth	x	o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	x	q. Military Service	x
d. Gender	x	k. Telephone Number	x	r. Criminal Record	
e. Age		l. Email Address	x	s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship	x	n. Religion	x*		
u. Other general personal data (specify): * Reasonable Accommodation records related to COVID-19.					

Work-Related Data (WRD)					
a. Occupation	x	e. Work Email Address	x	i. Business Associates	
b. Job Title	x	f. Salary		j. Proprietary or Business Information	x
c. Work Address	x	g. Work History	x	k. Procurement /contracting records	
d. Work Telephone Number	x	h. Employment Performance Ratings or other Performance Information	x		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. 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)

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	x	Hard Copy: Mail/Fax	x	Online	
Telephone		Email	x		
Other (specify):					

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

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

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

Any Human Resource related information is verified when it is collected.

Checksums are used when provided to validate the accuracy of weather data received by internal and external entities.

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	x
For administrative matters	x	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)		For web measurement and customization technologies (multi-session)	
Other (specify): BII, including private weather data, is collected to improve accuracy and performance of certain weather models. These data are considered restricted and only necessary personnel have access.			

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)

Personally Identifiable Information (PII)

PII, to include drivers licenses and alien registration cards, is collected to support administrative functions. These functions include issuing badges, creating accounts, and verifying citizenship status before accounts can be created. Personnel-related forms of NOAA employees and contractors are only shared with NOAA HR on a case-by-case basis.

Similarly, employee performance evaluations are collected and maintained. These evaluations are only shared with employee's immediate supervisors, management team, and NOAA HR on a case-by-case basis.

Business Identifiable Information (BII)

WCOSS ingests two forms of business-sensitive information. The first is in the form of geolocation data of NOAA Ships and Aircraft. The second is private, proprietary weather data. Both are used to develop and improve forecasting and weather-related models. These data are ingested to a restricted area within WCOSS, and only essential personnel with need-to-know have access.

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.)

NOAA8860 employs least privilege access to data stored in the system. All information is stored within network-shared devices, and access control lists and file share permissions control who has access to specific information. WCOSS has a strict policy in place for account requests, and all account requests must have a sponsor and System Owner and Information System Security Officer approval. Access to WCOSS systems is only allowed via two-factor authentication. Similarly, any form of elevated access is clearly documented in the form of a ServiceNow Ticket request and must receive System Owner approval before being granted access.

The information would be subject to the potential of insider threats given that authorized individuals do have access to the PII within the system. Mandatory training is required for handling sensitive information as part of the annual security awareness course. Users are also required to sign rules of behavior to indicate they understand their responsibilities to protect the system and data within. This, along with the other NOAA privacy controls, work to mitigate the risk of threats.

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	x		
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

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

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

x	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: Yes, a list of interconnections is found below. Technical controls in place to prevent PII/BII leakage include: AC-1: Access Control Policy and Procedures AC-3: Access Enforcement AC-4: Information Flow Enforcement AC-5: Separation of Duties AC-6: Least Privilege AC-14: Permitted Actions Without Identification or Authentication AC-21: Information Sharing AC-22: Publicly Accessible Content AU-2: Audit Events AU-6: Audit Review, Analysis, And Reporting IA-4: Identifier Management IA-5: Authenticator Management IA-8: Identification And Authentication (Non-Organizational Users) SC-4: Information In Shared Resources SC-7: Boundary Protection SC-8: Transmission Confidentiality And Integrity
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

External	System Name	Owner	Interface Type	Transfer Method	Transfer Type	Classification
No	NOAA0201 – Web Operation Center (H)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA0500 – NOAA Research & Development High Performance Computing System (R&D HPCS)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA0550 - NOAA Enterprise Network	NOAA	Active	Via Network	Both	Unclassified
No	NOAA3065 - NOAA Profiler Network Central Facility (FSL Demonstration Division) (NPN)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA5045 – NOAA Environmental Satellite Processing Center	NOAA	Active	Via Network	Both	Sensitive But Unclassified
No	NOAA8104 - WSR-88D Weather Radar (NEXRAD)	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8106 - Upper Air Observing System (UAOS)	NOAA	Active	Via Network	Receive	Unclassified
No	NOAA8107 – Advanced Weather Interactive Processing System	NOAA	Active	Via Network	Send	Unclassified
No	NOAA8202 - Office of Water Prediction	NOAA	Active	Via Network	Both	Sensitive But Unclassified

No	NOAA8212 - Terminal Doppler Weather Radar - Supplemental Product Generator	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8501 - NWS Cloud Infrastructure System (NCIS)	NOAA	Active	Via Network	Send	Unclassified
No	NOAA8850 – NWS Enterprise Mission Enabling System	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8861 – Aviation Weather Center	NOAA	Active	Via Network	Send	Unclassified
No	NOAA8864 – Space Weather Prediction Center	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8865 – NOAA Tsunami Warning System (NTWS)	NOAA	Active	Via Network	Both	Sensitive But Unclassified
No	NOAA8868 – Storm Prediction Center	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8872 - Meteorological Development Lab Network	NOAA	Passive	Via Network	Both	Unclassified
No	NOAA8873 - National Data Buoy Center	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8881 – Central Region	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8882 - ER Bohemia	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8883 - Pacific Region	NOAA	Active	Via Network	Both	Unclassified
No	NOAA8884 – Southern Region	NOAA	Active	Via Network	Both	Unclassified
Yes	US Coast Guard International Ice Patrol	CDR William C. Woityr	Active	Via Network	Both	Unclassified

6.4 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://www.weather.gov/privacy.	
x	Yes, notice is provided by other means.	Specify how: Individuals are told verbally when the information is requested for administrative functions. Employees are informed either verbally or through email that performance reviews will be conducted. Business-sensitive information is provided by external parties and protected by Memorandum of Understanding (MOU).

	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 are told verbally when the information is requested for administrative functions. Employees then have the opportunity to decide if they want to provide PII. Employee performance reviews are only used by HR and the employee's direct supervisor. Performance review notices are sent via email. Business-sensitive information is provided by external parties and protected by an MOU.
	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: Individuals have the opportunity to decline consent verbally or in writing when the information is requested for administrative functions. If a request to collect PII is declined by an employee, then access to services may be limited or denied. By consenting to the collection of PII, the employee is agreeing with the intended use. Employee performance reviews are only used by HR and the employee's direct supervisor. Performance review notices are sent via email. Business-sensitive information is provided by external parties and protected by an MOU.
	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: Personnel may contact HR Staff or supervisors at any time to review or update their information, and this is discussed during new employee orientation. This includes information provided for administrative functions or performance reviews. Business-sensitive information is provided by external parties and protected by an MOU. The MOU can be reviewed or updated upon request from the 3rd party to NOAA8860 management.
	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: Access logs are recorded for restricted datasets.
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): July 7th, 2023 ☐ 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.
x	Contracts with customers establish DOC ownership rights over data including PII/BII.
x	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).*

Any PII or BII is segregated from general access and only appropriate personnel are given access.

Servers and data storage systems have limited access.
All mobile laptops are encrypted with FIPS 140-2 compliant algorithms and data is similarly encrypted while in transit and at rest.

NOAA8860 employs least privileged access to data stored in the system. All information is stored within network-shared devices, and access control lists and file share permissions control who has access to specific information. WCOSS has a strict policy in place for account requests, and all account requests must have a sponsor and System Owner and Information System Security Officer approval. Access to WCOSS systems is only allowed via 2-factor authentication. Similarly, any form of elevated access is clearly documented in the form of a ServiceNow ticket request and must receive System Owner approval before being granted access.

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)*: COMMERCE/DEPT-18, Employees' Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-25, Access Control and Identity Management System COMMERCE/DEPT-27, Investigation and Threat Management Records COMMERCE/DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations OPM/GOVT-1, General Personnel Records OPM/GOVT-2, Employee Performance File System Records GSA/GOVT-7, HSPD-12, USAccess
	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: NARA General Records Schedules: 2.1 Employee Acquisition Records 2.2 Employee Management Records 2.3 Employee Relations Records 2.4 Employee Compensation & Benefits Records 2.5 Employee Separation Records 2.6 Employee Training Records 2.7 Employee Health & Safety Records NOAA Record Schedules Chapter 300 302 General Personnel Program Files 303 Recruitment and Employment Files 304 Employee Performance, Utilization, and Training Files 305 Position Classification, Pay and Allowance Files 306 Attendance and Leave Files NOAA Records Schedule Chapter 1300, Weather
	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	x	Overwriting	x
Degaussing	x	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.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
x	**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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: The type of PII acquired could identify individuals.
X	Quantity of PII	Provide explanation: PII is used for administrative HR functions and is stored only for the period of time necessary to validate the information and obtain signatures on necessary forms.
X	Data Field Sensitivity	Provide explanation: Human Resource Information such as Name, GS level, Phone and SSN are collected. SSNand alien registration cards are only collected for the sole purpose of HR required processes.
X	Context of Use	Provide explanation: PII is used for administrative HR functions and is stored only for the period of time necessary to validate the information and obtain signatures on necessary forms.
X	Obligation to Protect Confidentiality	Provide explanation: Minimal sensitive BII collection requires confidentiality for Operations Security (OpsSec) and non-disclosure for general public use. Restricted lightning data is paid for by the NWS in agreement with two third parties. Geo-location of ship data is required to be confidential for the protection of OpSec of the vessels.
X	Access to and Location of PII	Provide explanation: PII is stored temporarily and only essential personnel have access to PII while it is stored.
	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.)

NOAA8860 purposely minimizes the collection and retention of PII and BII within the system. The data that is collected is limited to only data that is required for administrative functions, such as issuing badges and creating accounts. Similarly, only BII that is useful in enhancing models and forecasts is collected. In both cases, PII and BII are stored in controlled areas where only essential personnel have access. Once information is no longer needed, it is destroyed in compliance with NIST/DOC/NOAA requirements.

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.