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

Privacy Impact Assessment
for the
NOAA3090
National Severe Storms Laboratory (NSSL)
Scientific Computing Facility

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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2024.04.29 09:20:17 -04'00'

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

Template Version Number: 01-2021

U.S. Department of Commerce Privacy Impact Assessment
National Oceanic & Atmospheric Administration (NOAA)/
Oceanic & Atmospheric Research (OAR)/
National Severe Storms Laboratory (NSSL)

Unique Project Identifier: NOAA3090

Introduction: System Description

NOAA3090 is the information system for the National Severe Storms Laboratory (NSSL). It provides resources for NSSL to meet its mission to enhance NOAA's capabilities to provide accurate and timely forecasts and warnings of hazardous weather events. NSSL accomplishes this mission through research to advance the understanding of weather processes, research to improve forecasting and warning techniques, and development of operational applications. The NSSL studies severe and hazardous weather processes and develops tools to help National Weather Service forecasters, as well as federal, university and private sector partners to use weather information more effectively.

NSSL is introducing PII and BII within its security boundary (NOAA3090) to support mission requirements. NOAA3090 collects, processes and transmits security background forms via the National Background Investigation Services by the NSSL Trusted Agent.

New PII: Logical access to NOAA3090 is restricted to authorized users. In addition to a Federal workforce, NSSL has a strategic research partnership with the University of Oklahoma's Cooperative Institute for Severe and High-Impact Weather Research and Operations (CIWRO). The user base also includes private industry partners and foreign national guests. Authorization to non-Federal employees is accomplished through human resource and administrative processes performed by NSSL administrative support staff. These processes require the collection of PII from non-Federal employees to conduct background investigations by the Department of Commerce Office of Security. NSSL is introducing an internal web-based system to assist in the collection, notification and processing of contract employees, and is outlined in section 1.1(j) below.

New BII: NSSL is providing collaborative research under a Cooperative Research & Development Agreement (CRADA Identification Number CR-000163) with Climavision. NOAA considers all data received by Climavision to be ‘proprietary business information.’ The data is processed by an internal web application produced by NSSL and CIWRO researchers. Once processed, the product data is classified as jointly created, and NOAA/NSSL is responsible for retaining the original copy and supplying access to Climavision. NSSL restricts access to all CRADA data to those researchers with direct involvement in the project and with Climavision.

Address the following elements:

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

The National Severe Storms Laboratory Scientific Computing Facility (NOAA3090) is a general support system for weather research.

(b) System location

The system's primary location is the National Weather Center in Norman, OK. A secondary facility is located at the National Weather Radar Testbed in Norman, OK.

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

NOAA3090 has the following connection agreements in place

- Interconnection Security Agreement (ISA) with National Weather Service Storm Prediction Center (NOAA8868) to provide file services for accessing research data.
- Memorandum of Agreement (MOA) with NOAA Enterprise Network (N-Wave/NOAA0550) to supply external networking to the N-Wave network and Internet access for NSSL.
- Service Level Agreement (SLA) with the University of Oklahoma Information Technology for internal network layer-1/2 infrastructure and network configurations.
- NOAA0100 covers Arcsight, Bigfix, and FireEye services
- NOAA0900 Covers Google Suite, NOAA MaaS360 MDM, Smartsheets, ArcGIS

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

NOAA3090 comprises networked servers and storage systems designed to meet individual project requirements. Servers are accessible through NSSL secured workstations and laptops within a local area network, and an externally accessible virtual private network. All external data is securely transmitted through N-Wave's Trusted Internet Connection and restricted by an enterprise firewall. The majority of data transmitted, stored, and processed within the NOAA3090 boundary is based on data collected from weather-related observation. Sources include radars and field instruments developed by NSSL researchers, or from other NOAA agencies, partnering universities, and private companies. Real-time data is primarily transmitted via Local Data Manager (LDM) protocol and restricted to authorized senders or recipients.

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

Personal Identifiable Information (PII) is stored in a dedicated network storage volume with restricted access limited to the NSSL Trusted Agent and Admin Support Specialist. The network share is secured through network-level and file system level permissions based on user account and host IP.

General data access is restricted to business use cases and ultimately the responsibility of the respective data owner. NOAA3090 utilizes centralized role-based access control based on least privilege. Projects may request data to be shared with external partners based on project requirements, restricted by firewall access control lists. Data may also be publicly shared through various protocols such as LDM, secure file transfer protocol (SFTP), or hypertext transfer protocol secure (HTTPS).

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

All external traffic to and from NOAA3090 is transmitted using a Trusted Internet Connection through N-Wave. Network traffic is controlled and monitored through a NOAA3090-managed firewall. NSSL coordinates with external sources to restrict data incoming/outgoing by public IP address. NSSL employs least functionality on externally accessible systems to limit exposure and risk from unauthorized sources.

Security forms are provided by prospective employees to the Admin Support Specialist either in hard copy or electronically via the NOAA email system (NOAA0900). Hard copy forms are electronically scanned to a secured network share. The full security package is uploaded by the Trusted Agent to the National Background Investigation Services (NBIS) via encrypted web transmission. A hard copy of the individual's fingerprint card is transmitted by commercial courier to the Office of Security (OSY) by the Admin Support Specialist.

(g) Any information sharing

NSSL's research is conducted in collaboration with CIWRO, one of NOAA's cooperative institute (CI) partners. CI personnel data is only shared to the extent necessary to support administrative onboarding processes between the parent organization and OSY. The information is required for background investigations, and follows the same guidelines outlined in the onboarding process in the PTA/PIA.

NOAA's information security policy requires the transmission of system audit logs to the NOAA Cybersecurity Center (NCSC). System security logs containing System Administration/Audit Data (SAAD) are centrally collected within NOAA3090 and transmitted to NOAA0100.

Data received and classified as PII/BII is restricted to personnel with a need to know in support of their approved mission functions. Any additional information sharing with external entities requires pre-approval from the original owning organization.

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

	Type of Information Collected (Introduction h.)	**Applicable SORNs (Section 9.2)**	**Programmatic Authorities (Introduction h.)**
1.	Security Investigations (Security Clearance actions)	COMMERCE/DEPT-13	Executive Orders 10450, 11478
			5 U.S.C. 7531-332
			28 U.S.C. 533-535
			Equal Employment Act of 1972
2.	Emergency Preparedness/COOP	COMMERCE/DEPT-18	Executive Order 12656

			Federal Preparedness Circular (FPC) 65, July 26, 1999
3.	Building Entry/Access & Surveillance	COMMERCE/DEPT-25	5 USC 301
			Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
4.	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
5.	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-1	31 U.S.C. 66a
			44 U.S.C. 3101, 3309
		COMMERCE/DEPT-2	28 U.S.C. 3101-3105
			Debt Collection Act of 1982 (PL 97-365)
		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)
		COMMERCE/DEPT-25	5 USC 301
			Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for

			Federal Employees and Contractors
6.	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

NOAA3090 is currently classified as a low system in accordance with the Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

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): New PII: NSSL is designing a new onboarding system which will provide custom workflows for					

authorizing and tracking new personnel requests. The system will use a secure web form to create a personal contact record with the following information:

- Name
- Email
- Phone
- Position title
- Hiring authority (federal, CI, or contractor)
- Citizenship (i.e. verification they are/are not U.S. citizen)
- General locality (i.e. the employee be processed remotely or onsite).

The information will be provided to the Admin Support Specialist who will follow existing processes to complete an OSY security package. The full list of categories identified in section 2.1 of the PIA is applicable to the data collection process of the Admin Support Specialist. Sensitive PII is not transmitted within the onboarding tracking system; however, the electronic copies uploaded to NBIS are retained on a restricted network file system until OSY confirms the initial screening is complete. OSY will complete section C of the CD-591 and return it via e-mail to the Admin Support Specialist indicating they are eligible to be processed for a PIV card. Once they have been approved, the previously submitted security forms containing all sensitive PII is purged from the NOAA3090 system.

New BII: NSSL established a Cooperative Research and Development Agreement (CRADA) with Climavision for specific data ingested into the Multi-Radar, Multi-Sensing (MRMS) system. NOAA considers all data received under this CRADA to be 'proprietary business information.' NSSL cannot redistribute any data without Climavision's express permission. NSSL restricts access to the data via network segmentation to those researchers with direct involvement in the project.

____ 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.

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: SSN, driver's license, and/or passport documents are required to initiate a background screening process through OSY. This information is gathered by the Administrative Support Specialist responsible for submitting a security package on behalf of NSSL. Electronic copies are uploaded to NBIS retained on a restricted network file system with access restricted to the Support Specialist and Trusted Agent (for					

Trusted Agent Sponsorship System approval). Once the initial screening is approved by OSY, the previously submitted security forms containing all sensitive PII are purged from NOAA3090's network file system.

General Personal Data (GPD)					
a. Name	✓	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	✓	r. Criminal Record	
e. Age		l. Email Address	✓	s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship	✓	n. Religion			
u. Other general personal data (specify): Contractor background information contains the items listed above for background investigation.					

Work-Related Data (WRD)					
a. Occupation	✓	e. Work Email Address	✓	i. Business Associates	
b. Job Title	✓	f. Salary		j. Proprietary or Business Information	*✓
c. Work Address	✓	g. Work History	✓	k. Procurement/contracting records	
d. Work Telephone Number	✓	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify): *CRADA data provided by Climavision into the MRMS web application is proprietary to their radars and classified as BII.					

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): *Blank fingerprint cards are provided by the Administrative Support Specialist to the employee to be completed by a law enforcement agency. Once completed, the cards are returned and mailed via courier to OSY. No copies are scanned or retained locally.					

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): NOAA3090 requires all devices connected to the internal network to send logs to a central logging system. The data is transferred to the NOAA Security Operations Center for archiving audit data per audit control policies.					

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	✓
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): *Climavision is a private sector data source of BII.					

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

Personally identifiable information is recorded directly on PDF forms provided by OSY. The accuracy of information is determined by cross-referencing information on an OF-306 submitted by the applicant and/or verified in person by the applicant prior to submission.

Proprietary business information is restricted to originate from pre-authorized source IP addresses. Incoming data is then filtered and transmitted to a segmented local area network which is restricted to authorized personnel.

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. 3206-0182, OF-306, Declaration for Federal Employment
	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):			

✓	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):			
✓	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	✓
For litigation		For criminal law enforcement activities	
For civil enforcement activities		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): *The application incorporating PII into the NOAA3090 security boundary is to improve business processes by ensuring consistent, accurate, and timely processing of personnel. It accomplishes these goals by providing standard workflow with secure tracking and notification throughout the onboarding process including pending tasks by external agencies. Work-related data also supports business continuity and IT security functions through COOP integration based on employee roles and organizational account reviews for access requirements.			

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).

NOAA3090 utilizes data categorized as PII/BII for the purpose of administrative functions or in use of specific NSSL developed applications.

- Authentication and information access is recorded through system logs that are generated on individual network systems and forwarded to a central log system. This information enables the protection of information assets within NOAA3090 by auditing system events which contain:
  - Username
  - IP Addresses
  - Access Timestamps
  - Data directories/files accessed

- PII data is collected from individuals (federal, cooperative institute and contract employees) during the onboarding process for employment. An internal secure web form is used to gather and store the following preliminary employee information from an employee's sponsor:
  - Full name
  - E-mail address
  - Phone number
  - Citizenship (Identifying only if the person is/is not a U.S. citizen)
  - Hiring authority (Federal, CI, or contracted company)
  - Position title
  - General locality (i.e. employee processed remotely or onsite)

  The information will be provided to the Admin Support Specialist who will follow existing processes to complete an OSY security package. The following forms comprise an OSY security package which are collected and uploaded to NBIS by NSSL's designated Trusted Agent. Additionally, a hard copy fingerprint card (processed by an OSY authorized source such as local police department) is collected and sent by commercial courier to OSY by the Administrative Support Specialist.

  Trusted Agent and Admin Support Specialist processed forms:
  - DOC OSY Coversheet (completed by Admin Support Specialist)
  - OF-306 (provided by employee)
  - CD-591 (completed by Admin Support Specialist)

- Position Designation Record (completed by Admin Support Specialist)
- Employee Resume (provided by employee)

These forms collect the following categories:

- Full legal name and aliases
- SSN
- Date of birth
- Place of birth
- Address
- E-mail address
- Phone number
- Entrance on duty date
- Citizenship
- Employer (for contract employees)
- Investigation type
- Position title
- Driver's license
- Passport number

If a background investigation is approved, the employee contact information (phone, address, and e-mail) collected from the onboarding form will be retained within a central database by NSSL for emergency contact/COOP plans. The information would be maintained and accessible by the appropriate division manager (Federal). Personnel would have the ability to review and modify information as needed. Information that would be retained will include:

- Name
- Home address
- Telephone number
- Email address

- The NSSL MRMS system ingests proprietary weather data from a commercial organization (collaborator). This data is filtered by the source IP address and routed to a segmented network for ingest into the MRMS system via LDM protocol. The raw data feed is restricted by LDM rulesets to not be redistributed outside of the MRMS system. The data is processed in real-time and the generated research products are considered joint property of NSSL and the collaborator once processed by MRMS servers. The network is isolated to a limited number of personnel (both Federal and CI) for use within specific research projects. NSSL and associated CI partners will not share the collaborator's data with any other third party without explicit written permission from the collaborator.
    - Per the SoW in (CR-000163):
        - "NSSL and associated CI partners will not share Climavision's data with any other third party without explicit written permission from Climavision."

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.)

The threat to privacy can result from the unintentional disclosure of information due to a number of factors. Insider threats such as human error, sabotage, or system misconfiguration are potential threats to the system. All users are required to complete annual security awareness and privacy training which includes proper information handling. Additional training is augmented by the bureau through records management training. Cyber security training commensurate with system administrator roles are also required annually to enforce IT security principles.

Mitigating controls implemented from the access control family and identification and authentication control family ensure access is granted appropriately. Additionally, auditing is enforced to record valid and unauthorized access to information. Auditing also verifies change management controls are appropriately followed and limits inadvertent leaks of information. The system must also conduct vulnerability assessments and maintain regular system patches to prevent newly discovered 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	✓		
DOC bureaus	**✓		
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
*Other (specify):			***✓

*BII is not shared outside the NOAA3090 boundary, only ingested.

**PII is shared with DOC OSY through the NBIS web application, and the NOAA Cybersecurity Division through the Arcsight logging system.

***The University of Oklahoma Information Technology provides layer 1 & 2 network infrastructure to NSSL which provides access to SAAD information (date/time, IP address, MAC address). This service is provided under a service level agreement through the National Weather Center rental lease.

□	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?

	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.

* Based on NSSL's CRADA agreement with Climavision (external entity). There are no restrictions placed on Climavision regarding the use of their data. PII is only shared internally with the Department (OSY and NCSC), so option three appears the most appropriate selection for that category.

6.3 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: NOAA0900 is authorized to store and transmit PII, and used by the Admin Support Specialist to communicate with pending employees to gather required OSY forms. NOAA0100 is authorized to collect system log information for monitoring cyber security events. System logs generated by NOAA3090 are transferred via Arcsight for archiving of audit records and contain SAAD categories from section 2.1. NOAA8868 is classified as a FIPS high system. Access to NOAA3090 data is restricted to specific systems which do not store or process PII/BII, and controlled by firewall policies and centralized role-based access control lists. NOAA0550 provides external network connectivity for NOAA3090. All network traffic is controlled through NOAA3090 firewall policies to restrict data flows and external access. NOAA3090 uses the University of Oklahoma Information Technology infrastructure for internal network switching. NOAA3090 networks are segmented by virtual LANs, and restricted by NOAA3090 through central firewall policies to control all PII/BII data flows.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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	✓
Contractors	✓		
Other (specify): *CIWRO (cooperative institute) employees are categorized under the general public.			

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.)*

✓	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
✓	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.noaa.gov/protecting-your-privacy .	
✓	Yes, notice is provided by other means.	Specify how: PAS statement is on the OF306 filled out by the employee. DOC also requires the use of specific login banners prior to granting end user access to systems. This message provides the notice of the government's right to protect communications within its electronic resources.
	No, notice is not provided.	Specify why not:

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

✓	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: BII provided for research projects within NSSL are at the discretion of the owning organization and detailed in a CRADA agreement. For OSY background investigations, an individual may request to decline to provide PII, however they will not be granted logical access to systems and restricted from physical access to NOAA space without a NOAA escort.
	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.

✓	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Yes, proprietary business data may be restricted from redistribution and sharing at the discretion of the owning organization. For onboarding employees and contractors, the data collected is required per OSY as a condition for employment; however, they may request personal data not be retained or used for NSSL emergency contact/COOP purposes.
	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.

✓	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: PII stored for emergency contact/COOP may be requested for review by an individual to their division leads and modified as needed. BII is controlled through LDM, which is restricted at the hosting side. The owning organization may restrict access to specific products by modifying an allow list to restrict access.
	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.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
✓	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
✓	Access to the PII/BII is restricted to authorized personnel only.
✓	Access to the PII/BII is being monitored, tracked, or recorded. **Explanation:** System and audit logs are stored in a central security information/event management system (SIEM).
✓	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): June 6, 2023 □ This is a new system. The A&A date will be provided when the A&A package is approved.
	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
✓	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).
✓	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
✓	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):

* Treatment of CRADA Data: "Climavision will retain the original copy of the CRADA data created solely by it. NOAA shall retain the original copy of all jointly created CRADA data; NOAA shall supply Collaborator with a copy of the original copy of jointly created CRADA data, and Collaborator shall have access to the original copy. NOAA and Collaborator shall each have the right to use all CRADA Data for their own purposes, consistent with their obligations under this CRADA."
Ownership of Research Products: "NOAA and the Collaborator agree to exchange samples of all Research Products. Research Products will be shared equally by the Parties. Subject to these sharing requirements, the Research Products created under this CRADA are the jointly owned property of the Parties. The Parties agree to make mutually acceptable arrangements for the disposition of unique or hard-to-replace Research Products."

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).*

External network traffic is protected and monitored using the N-Wave TIC infrastructure. Internal systems used to store data are protected with role-based access controls maintained in an Active Directory system. Systems are also segmented and protected by firewall rulesets which provides an additional layer of least privilege enforcement. All systems are monitored using a centralized SIEM which provides customized alerting to events. All public web applications enforce HTTPS protocol to protect data in transit.

<u>Section 9</u>: Privacy Act

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

✓ 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."

✓	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-13, Investigative and Security Records COMMERCE/DEPT-25, Access Control and Identity Management System OPM/GOVT-1, General Personnel Records COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons COMMERCE/DEPT-2, Accounts Receivable GSA/GOVT-7, HSPD-12 USAccess COMMERCE/DEPT-27, Investigation and Threat Management 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.

<u>Section 10</u>: 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.)*

✓	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Control Schedule Chapter 205-14: Personally Identifiable Information Extracts NOAA Records Control Schedule Chapter 1200-06: Data Request Records NOAA Records Control Schedule Chapter 2400-03: System Access Records If data is referenced in a scientific journal publication, NOAA3090 is subject to FOIA and data requests pertaining to data referenced. Any source data that has been processed and modified by NSSL systems is determined to be property of NSSL, and must be controlled according to these schedules.
	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:
✓	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	✓
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.
✓	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.)*

✓	Identifiability	Provide explanation: Individuals can be identified using the information collected. The purpose of the collection of PII is to facilitate background investigations so identifiability is inherently high.
✓	Quantity of PII	Provide explanation: The quantity of records is considered low since it is for new contract and CI employees.

✓	Data Field Sensitivity	Provide explanation: Data collected through the internal onboarding forms and retained for COOP purposes are considered low-impact fields. Sensitive PII (i.e. SSN, Driver's License, Passport, DOB) are used only for background investigations.
✓	Context of Use	Provide explanation: The PII is necessary for the proper conduct of a background check.
✓	Obligation to Protect Confidentiality	Provide explanation: Department and bureau privacy policies require the protection of PII.
✓	Access to and Location of PII	Provide explanation: Data collected for the submission to OSY is gathered both electronically and physically. The entire collection of data that would pose a significant risk of exposure would remain in hard copy form. Documents remain under the physical protection of the Admin Support Specialist in a locked cabinet within their office. Additional physical controls including cameras and electronic door locks provide detective controls.
✓	Other: Time of retention	Provide explanation: Data is only retained on an as-needed basis for emergency contact purposes (name, phone, address, email), and ultimately at the discretion of the employee.

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.)

NSSL only gathers and retains information required per NOAA policy. NOAA requires background screening of all personnel prior to providing logical access to information systems. NSSL complies with this requirement by submitting a security package to OSY through the NBIS. A security package includes a DOC/OSY coversheet, OF-306, CD-591, position designation record form, and employee resume. Per CD-591 requirements, the Administrative Support Specialist must verify two forms of valid identification exist for an individual, but are not required for submission to OSY.

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: NOAA3090 is reviewing existing security controls according to its assessment and authorization schedule to determine control gaps and associated risk. NOAA3090's authorizing officials will determine if the current FIPS level is adequate based on the risk assessment and recommendations of the ATO briefing.
	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: NSSL is implementing a web application to support the onboarding process. The creation of the application has triggered the creation of this PIA.
	No, the conduct of this PIA does not result in any required technology changes.