Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
NOAA5006
NESDIS Administrative Local Area Network (NESDIS Admin LAN)

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: 2023.11.16 14:02:50 -05'00' 11/16/2023

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NESDIS/NESDIS Admin LAN

Unique Project Identifier: NOAA5006

Introduction: System Description

Provide a brief description of the information system.

NESDIS Administrative LAN (NOAA5006) operates under the authority of the NESDIS Assistant Chief Information Officer and provides the Local Area Network (LAN) and Windows administrative support and services for several NESDIS office locations. NOAA5006 provides access to automated programs and systems supporting administrative programs such as budget and financial management, personnel management, procurement, building operation and management, interagency programs, IT planning, and IT security. The system also supports access to the Internet and supports web pages providing NOAA information and data to the public.

Address the following elements:

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

NOAA5006 is a general support system provided by the National Environmental Satellite, Data, and Information Service (NESDIS) Assistant Chief Information Officer – Satellites (ACIO-S) to most of the NESDIS offices.

(b) System location

- NESDIS Headquarters facility in Silver Spring Metro (SSMC) Center I and III
- NOAA Joint Polar Satellite System (JPSS) Office (NJO) located at GreenTec4 (GT4) building of the NASA Goddard Space Flight Center (GSFC), Lanham MD
- National Centers for Environmental Information offices located in Maryland, Mississippi, Colorado, and North Carolina
- Center for Satellite Applications and Research (STAR) in College Park, Maryland
- NOAA Satellite Operations Facility (NSOF) in Suitland, MD
- Wallops Control and Data Acquisition Station (WCDAS) in Wallops Island, Virginia
- Fairbanks Control and Data Acquisition Station (FCDAS) in Fairbanks, Alaska

NOAA5006 houses domain administration, local network infrastructure, file sharing services and support for NESDIS Admin LAN workstations and laptops at these locations.

NOAA5006 also supports the Office of Space and Commerce (OSC) located in the Herbert C. Hoover Building located at 1401 Constitution Avenue Washington, DC. NOAA5006 does not provide LAN or VoIP services to OSC.

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

NOAA5006 is a Moderate-level system which maintains interconnects with:

- NOAA (NOAA0100, NOAA0201, NOAA0550) for shared services (VPN, Internet, McAfee, ArcSight, SOC, etc.)
- NOAA (NOAA1200) for National Service Desk
- NOAA1101 for MARS Application
- NASA G-RASS for accounting coordination
- NASA at JPSS for SharePoint
- NOAA5009 for mission system connection
- NOAA5011 for mission system connection
- NOAA5018 for mission system connection
- NOAA5040 for mission system connection
- NOAA5044 for mission system connection
- NOAA5045 for mission system connection

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

NOAA5006 maintains a hardware stack (pod) at each location which hosts virtual servers that provide services needed by that site. Workstations connect to the pod via Cisco switches, and pods interconnect with each other over N-WAVE. The Boulder and NSOF locations provide services used by multiple locations and contain backups of all data from all other pod sites.

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

Users retrieve information from the system by using their Government Furnished Equipment (GFE) accessing files on their local file server, or on a remote file server (via VPN) in some cases. They also access websites using HTTP or HTTPS (internal as well as external) and Commerce applications. Network printers allow users to print when necessary.

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

Information to and from the system is transmitted primarily using HTTPS and SFTP. NOAA5006 maintains local Admin LAN infrastructure. Remote/telework users must use NOAA5006 ERAV VPN connection or access a Citrix VHS workstation in order to use NOAA5006 resources. Information to and from the Internet is evaluated via NOAA5006 IPS and NOAA NCSC.

(g) Any information sharing

NOAA5006 shares information including sensitive and non-sensitive PII to and from NOAA FISMA systems, DOC bureaus, other Federal agencies; State, local, tribal gov't agencies, and foreign entities on a case by case basis. The PII shared are names and other personal identifiers used in background investigations sent via kiteworks. It is not stored on NOAA5006. The BII are business identities.

(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.)**
Contact Information for the Public	NOAA-11	5 U.S.C. 301, Departmental Regulations
		15 U.S.C. 1512, Powers and duties of Department
FOIA & Privacy Act Requests	COMMERCE/DEPT-5	5 U.S.C. 552, Freedom of Information Act
		5 U.S.C. 552a, Privacy Act of 1974 as amended
		5 U.S.C. 301
		44 U.S.C. 3101
Travel Records	COMMERCE/DEPT-9	Budget and Accounting Act of 1921
		Accounting and Auditing Act of 1950
		Federal Claim Collection Act of 1966
		FPMR 101-7
		5 U.S.C. 5701-09
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
Litigation	COMMERCE/DEPT-14	5 U.S.C. 301
		28 U.S.C. 533-535 and 1346(b)
		44 U.S.C. 3101

Personnel Actions Including Training	COMMERCE/DEPT-18	44 U.S.C. 3101
		Executive Orders 12107, 13164,
		41 U.S.C. 433(d)
		5 U.S.C. 5379
		5 CFR Part 537
		Executive Order 12564
		Public Law 100-71
		Executive Order 11246
		26 U.S.C. 3402
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
Public Health Emergency Info & Reasonable Accommodation	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
System for Award Management (SAM)	GSA-GOVT-9	2 CFR, Subtitle A, Chapter I, and Part 25
		40 U.S.C. 121(c); FAR Subparts 9.4 and 28.2
		Executive Order 12549 (February 18, 1986
		Executive Order 12689 (August 16, 1989)
Federal Acquisition Regulation (FAR) Data Collection System	GSA-GOVT-10	E-Government Act of 2002 (Pub. L. 107–347) Section 204

		Davis-Bacon and Related Acts
		40 U.S.C. 3141–3148
		40 U.S.C. 276a
		29 CFR parts 1, 3, 5, 6 and 7
		Section 5 of the Digital Accountability and Transparency Act (DATA Act), Public Law 113–101
Collection & Use of SSN	OPM/GOVT-1	Executive Orders 9397, as amended by 13478, 9830, and 12107
Recruiting, Examining, and Placement Records	OPM/GOVT-5	5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533
		Executive Order 9397

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

The FIPS 199 security impact category for the system is 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.
__X__ 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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Interface Control Document (ICD) for NOAA5045 added.					

____ 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	X	f. Driver's License	X	j. Financial Account	
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	X
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID	X				
n. Other identifying numbers (specify):					
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: The Social Security Numbers for NESDIS Admin LAN contractors and government employees are viewed and input into non-NOAA systems for the sole purpose of conducting background investigations and on I-9 forms for hiring in accordance with 10 U.S.C. 133 and E.O. 9397. Storage and processing of such PII does not occur on NOAA5006. This information is only viewed on screen as it is reviewed and entered into non-NOAA systems for personnel actions. NOAA5006 uses kiteworks for receipt. The authorities are those in COMMERCE/DEPT-18.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	
f. Race/Ethnicity		m. Education	X	t. Mother's Maiden Name	
g. Citizenship	X	n. Religion			
u. Other general personal data (specify): The OGE Form 450 is required annually for purchase agent and COR, for conflict of interest information only.					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	X
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	X
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	X*	h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs	X**	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): * These are recordings of meetings or training sessions in support of NOAA's mission. **Employees and contractors sign permission forms before being photographed. See Section 5.1.					

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

Other Information (specify)	Google Meet hosts may record meeting audio with consent of participants. This must be cleared with Privacy and does not occur frequently.

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	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign	X		
Other (specify): European Organization for the Exploitation of Meteorological Satellites (EUMETSAT) uses SharePoint hosted by NOAA5006.					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify): The NCEI Mississippi location provides the PII it views to the Mississippi State University for badging purposes.					

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

NOAA5006 views PII from 3rd parties in order to input into background investigations or send to responsible parties for badge processing. (Note that NOAA5006 does not control any facility in which our system is located; we partner with the site owner and must send them badge and visitor requests.) The information that is stored is collected directly from an individual via secure email transmission (kiteworks), encrypted disks or in person. The entity providing the information validates that the information provided is accurate. The Commercial Remote Sensing Regulatory Affairs (CRSRA) office uses BII to issue private remote sensing licenses using a specially configured, isolated laptop computer.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0648-0174, 0648-0227
	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	X
Video surveillance		Electronic purchase transactions	
Other (specify): Building entry badge readers are not on NOAA5006, however at Stennis we must relay some PII to Stennis' badging office for them to configure entry readers. NOAA5006 then deletes the PII without storing.			

	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	X	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)	X	For web measurement and customization technologies (multi-session)	
Other (specify): NOAA5006 views but does not process PII for onboarding (background, badging) purposes. If it must be stored for a brief period (while accomplishing the indicated activities) it is stored with full disk encryption. CRSRA utilizes an offline laptop specifically configured and maintained for its license issuance responsibilities.			

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).

NJO collects Employment Eligibility Verification Form I-9, government issued ID and has requestors sign a non-disclosure agreement to be granted access to International Traffic in Arms Regulations (ITAR) data, which may contain BII.

Social Security Numbers are viewd on NESDIS Admin LAN Federal employees and contractors for the purposes of conducting background investigations. The I-9 and background investigation information may be stored electronically and on paper in locked cabinets.

NOAA5006 may collect audio or video recordings from meetings, or to record training sessions for later playback.

NJO asset tracking system information collected by Management Operation Division contains such information as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular Federal employee or contractor or small, well-defined group of people. This information includes work telephone numbers and work mobile number.

JPSS stores BII contract support information about its contractors on its shared drives for contract related deliverables.

CRSRA collects and maintains license application data about businesses that apply for and operate private earth remote sensing space systems. The information collected includes the name, street address and mailing address, telephone number of the applicant as well as any affiliates or subsidiaries, each foreign lender and amount of debt, as well as a copy of the charter or other authorizing instrument certified by the jurisdiction in which the applicant is incorporated or organized and authorized to do business. CRSRA collects BII, not PII.

The ACIO-S stores NESDIS Federal and contractor employee passport information when necessary for tracking and records purposes regarding international travel. ACIO-S also stores information related to background investigations for new and recent employees. Information is stored on shared drives.

ACIO-S also stores copies of Freedom of Information Act (FOIA) requests in an external cloud-based Software as a Service system called FOIA Xpress. Information contained in these requests includes but is not limited to requesters' and their attorneys' or representatives' names, addresses, e- mail, telephone numbers, and FOIA case numbers; office telephone numbers, names, telephone numbers, and addresses of the submitter of the information requested; unique case identifier; social security number (if provided by the requesting party). Information stored within FOIA Xpress application is not the original data. ACIO-S will only use the FOIA Xpress system to process redactions of sensitive information from requests and to collaborate with the FOIA lawyer. The system will not use be used to collect any forms of payments from requesters nor will it be used as a repository for storing FOIA request information. All copies of information stored in FOIA Xpress is encrypted at rest. Access to such information is controlled via access control list. This information is related to Federal employees and contractors, business entities and members of the general public and is not kept on NOAA5006 computers.

STAR personnel collect the following Work-Related-Data (WRD) from all STAR personnel: Name, Work Email address, Job Title, Work Address, Work Telephone Number. This data is used to maintain a roster of STAR personnel. STAR personnel store Vendor BII in proposals and contracts and grants documents which is used for the administration of contracts and grants. The information includes data on Federal employees, contractors and businesses.

NCEI Maryland (MD), Asheville (NC), Boulder (CO) and Stennis (MS) store WRD such as Name, Work Email address, Job Title, Work Address, Work Telephone Number dates for periods of performance Title series and grades. These sites also collect personal email, personal phone number, photographs for internal use (voluntarily posted to the intranet for recognition purpose) from all from all employees and contractors to maintain a roster, and for Occupancy Emergency preparedness.

NCEI-MS is located on a NASA site, in the Mississippi State University (MSU) and is a tenant of MSU. Both NASA and MSU require badges for access: NASA for facility access and MSU for building access. NCEI MS collects Federal and contractor employee information which includes pictures for NASA and Mississippi State Universality (MSU) badging. The pictures are stored on Admin LAN until the System Owners send them to MSU.

The information collected by the NCEI MS System Owner is removed from the network within 15-30 business days after information is provided to NASA and MSU. All users sign permission forms prior to releasing their information used for these purposes. The form is included with this PIA.

NSOF collects contractor and Federal employee information such as SSN, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone Number, Email Address, Salary Information, Military Service, Occupation, Job Title, Work Address, Telephone Number, and Work History. In addition, the system stores Onboarding forms, training forms (SF-182). NSOF also stores procurement and contractual information. The NSOF information is maintained on the NOAA5044 network. NSOF users can download information from the shared drives to their NOAA5006 laptop PC. While the users have the ability to copy data from their shared drives to the local PC, NSOF users migrated to the NOAA5006 network do not have access to any data on NOAA5006 shared drives. All NSOF user data is maintained on their network, managed by the NSOF support Staff and is also covered under the NSOF PIA reference: NOAA5044 FY18 PIA SAOP approved. NOAA5006 has full disk encryption on its laptops that encrypts data at rest when copied to the local host.

FCDAS uses information in the system for various tracking, compliance, and reporting uses to meet the following requirements:

- Maintain a current employee list and organizational chart
- Maintain an emergency contact listing
- Maintain a current phone listing with room assignment
- Track security and facilities related matters (keys, badges, key cards, etc)
- Financial reporting for COR (OGE form 450) and qualifications for federal purchase card/travel card/warrants
- Track Foreign National visitors
- Track training completion
- Track authorized drivers of government vehicles
- Respond to facilities and other HQ data calls
- Track and maintain employee vacation and work schedules
- Comply with Department Administrative Order 207-12 and Technology Controls and Foreign National Access 207-12 of the Foreign National Visitor and Guest Access Program
- Comply with Executive Order 10450 – Security Requirements for Government employment FCDAS collects the PII/BII information from both contractors and Federal employees and Foreign National visitors to the facility.

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.)

NOAA5006 does not have a system in place that electronically processes any PII/BII on its network. NOAA5006 users use external systems to process such information i.e. NOAA HR system, NOAA Travel system, DOD Defense Enrollment Eligibility Reporting System (DEERS) etc. NOAA5006 only stores PII/BII information on its network. All NOAA5006 users are required to take the NOAA annual awareness training. Also, all users have access to the NOAA PII training posted on the NOAA website and can take the training at any time as many times as they wish. There is a small risk of insider threat and potential compromise by shared-agency PII (e.g., passport renewal information Department of State). The continuously monitored and implemented controls, leveraged to ensure data is handled, retained and disposed of properly, relates to designated roles required to comply with DOC ITSBP; i.e., Incident Responders and ISSOs. Both roles have successfully met and maintained the credential / training requirement via qualified certifying organization and the associated Continuing Professional Education (CPE) programs, which sustain a working knowledge of industry standard and best practices. These controls help reduce any potential insider threat.

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	X		
Other (specify): Shared with NASA and MSU for building access badges; with Dept. of State for passport renewal information sharing.	X		

	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: • NOAA (NOAA0100, NOAA0201, NOAA0550) for shared services (VPN, Internet, McAfee, ArcSight, SOC, etc.) • NOAA (NOAA1200) for National Service Desk • NOAA1101 for MARS Application • NASA G-RASS for accounting coordination • NASA at JPSS for SharePoint • NOAA5009 for mission system connection • NOAA5011 for mission system connection • NOAA5018 for mission system connection • NOAA5040 for mission system connection • NOAA5044 for mission system connection • NOAA5045 for mission system connection The interconnects with NOAA5009, 5010, 5011, 5018, 5040, 5044 and 5045 exist to allow access to mission systems from NOAA5006 laptops and workstations using mission specific VPN. Users accessing mission systems are unable to access PII on NOAA5006 (different VPNs). SharePoint allows EUMETSAT users to access only the EUMETSAT documents on SharePoint. SharePoint does not contain any PII/BII, and allows NOAA5006 employees to use the NASA transport to connect back to NOAA5006; no PII is exchanged with NASA. The other interconnects are for network services provided by NOAA to allow NESDIS daily operations.
	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	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.noaa.gov/protecting-your-privacy .	
X	Yes, notice is provided by other means.	Specify how: Written notice is provided on all personnel forms that NESDIS Admin LAN employees complete. BII related data notices are given in the request for proposal or the request for information. CAC applications provide notice for the CAC process.
	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: A background investigation is a NESDIS job requirement. Providing the information is voluntary, but choosing not to provide the required information will result in not meeting the requirements of the job and not being considered further in the application/hiring process. Active employees may opt not to provide PII/BII for DOC personnel data at the time of the request, and in writing to the personnel administration representative who is assisting them - but this information is needed for processing awards. Performance information is part of the official personnel record for DOC employees and information is added to the eOPF in conjunction with the employee mid-year and annual reviews. Employees are asked permission in writing by their supervisors when collecting the applicable information for COOP or emergency recall and may decline at that time. This information is not required. Solicitation or RFI respondents may decline to provide information in responses; by doing so, they may lose eligibility to be awarded or employed on that contract.
	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: Consent is included on all personnel forms that employees complete, and consent to the uses explained on the forms is implied by completion of the forms. DOC personnel data is only used for performance evaluations/awards. Employee consents by participating in the performance evaluation, and

		may opt out at the time of the request in writing to administrative personnel. COOP or emergency recall data use is implied by voluntarily providing information for that intended use. Solicitation and RFI respondents may opt not to consent to use – review and consideration for award – but denying consent will affect their eligibility for award consideration.
	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: Information is reviewed and updates can be made by updating CRSRA licensing information or contact information where applicable. An employee may update information on personnel forms at any time by contacting their HR representative. Unless there is need-to-know, employees may not review Emergency and COOP information because it contains other staff's PII. They may request their information be updated. An employee may update information used for their DOD-issued CAC by contacting the NOAA Trusted Agent and DOD DEERS Office. Solicitation and RFP offerors may submit updated information.
	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: Select individuals access PII/BII from controlled sources (i.e. badging, personnel systems, e-QIP). CRSRA utilizes a purpose built computer for monitoring, tracking and recording licenses containing BII.
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): **6/24/2023** ☐ 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.
	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/BII data stored in our system is located on our internal network and only for enough time to use the data for a specified work requirement. NOAA5006 has boundary protection devices such as firewalls and Intrusion detection/prevention systems in place to protect this data. Authorized users who access PII data in our system are required to use CAC authentication which uniquely identifies and authenticates them before they access any PII data. All PII/BII is encrypted in transit using the DOC Secure File sharing system (Kiteworks) or HTTPS /SSL. All NOAA5006 Laptops have full disk encryption protected with CAC/pin. NOAA5006 prohibits the use of USB drives on laptops and workstations and only permits limited use of FIPS-140-2 encrypted devices by explicit permission to Tier 2 support staff and CRSRA. NOAA5006 uses approved DOD sanitization software to ensure no data remains on NOAA5006 media. NOAA5006 utilizes an encrypted Amazon S3 bucket in their virtual tape backup solution.

Section 9: Privacy Act

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

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

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

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. (list all that apply): NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission COMMERCE/DEPT-5, Freedom of Information Act and Privacy Act Request Records COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons COMMERCE/DEPT-13, Investigative and Security Records COMMERCE/DEPT-14, Litigation, Claims, and Administrative Proceeding Records COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-25, Access Control and Identity Management System COMMERCE/DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations. GSA/GOVT-9, System for Award Management GSA/GOVT-10, Federal Acquisition Regulation (FAR) Data Collection System OPM/GOVT-1, General Personnel Records OPM/GOVT-5, Recruiting, Examining, and Placement Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule: Chapter 100-General 100.11 Program Correspondence Subject Files 100.12 Program and Correspondence Subject Files 100-19 Interagency Cooperative Documents/ Agreements Chapter 200-Administrative 200-03 Transitory Records 200-04 Library Records 200-06 Non-Recordkeeping Copies of Electronic Records. 200-05 Technical Reference Materials Chapter 1400 – Satellites and Data Centers 1401-02 Original Non-disclosure Agreement (NDA) (DAA-370-2012-0001) 1402 International and Interagency Affairs Office
	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	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 information can directly identify government and contractor employees. Only authorized personnel have access to this information.
X	Quantity of PII	Provide explanation: NOAA5006 views and temporarily stores a significant quantity of PII for personnel security, COOP and badging use.
X	Data Field Sensitivity	Provide explanation: In some cases, the information contained in the data field may be the government or contractors' SSNs. Such data is not publicly available and is located on our internal network.
X	Context of Use	Provide explanation: Performance plans/evaluations/records for NOAA staff limited to supervisor and admin. Foreign national information is restricted to NOAA staff only.
X	Obligation to Protect Confidentiality	Provide explanation: BII for private remote sensing licenses is kept confident but license issuance is public.
X	Access to and Location of PII	Provide explanation: Performance plans/evaluations/records for NOAA staff limited to

		supervisor and admin. Foreign national information is restricted to NOAA staff only.
	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.)

NOAA5006 support staff collects only minimum PII/BII data needed to complete a specific task. This data is collected directly from the identified person or business by systems NOAA5006 does not control (except for CRSRA) and its accuracy is validated by the persons/business submitting the information.

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.