Version Number: 01-2017

U.S. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA)

Privacy Impact Assessment
for the
NESDIS Headquarters Information System NOAA5006

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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.04.19 15:52:17 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA NESDIS HQ NOAA5006

Unique Project Identifier: [Number]

Introduction: System Description

NESDIS Assistant Chief Information Officer –Satellites (ACIO-S), located in NOAA/NESDIS Headquarters. NOAA5006 provides the Local Area Network (LAN) and Windows administrative support and services for the following offices and locations
NESDIS Headquarters facility in the Silver Spring Metro Center (SSMC) Building 1 and Building 3, the NOAA Joint-Polar Satellite System (JPSS) Office (NJO) located in the Aerospace building and GreenTec4 [GT4] building of the NASA Goddard Space Flight Center (GSFC), Lanham, Maryland, National Centers for Environmental Information (NCEI) offices located in Maryland, Mississippi, Colorado, and North Carolina,
Center for Satellite Applications and Research (STAR) in College Park, Maryland and the NOAA Satellite Operations Facility (NSOF).

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. The purpose of NOAA5006 is to provide mission support and resources for IT management functions and overall office automation support for the programs, offices, and staff of the offices listed above. NOAA5006 servers are located in each of the physical locations and managed by NOAA5006 Support Staff at the specified locations.

Information Sharing

The PII/BII information collected by NOAA5006 may be shared with other systems on a case-by-case basis. The type of information that may be shared includes but is not limited to passport data (shared with the State Department for issuance and renewal purposes), employment history and verification (shared with other agencies should an employee transfer to another line office with in NOAA or another DOC bureau or another agency) as well as information related to background checks of existing and new employees (shared with OPM, other government agencies and Universities to initiate the investigation process). Employee information may also be shared with DOC and other Federal agencies in the case of a breach.

Legal Authorities to collect PII and BII

This information is collected under the authority of 5 U.SC., including Section 301. In addition, Title 31 U.S.C. 66a, 492, Title 44 U.S.D. 3101, 3309 and the Federal Collection Claim Act of 1966 apply. Additional authorities include E-Government Act of 2002 (Pub. L. 107–347) Section 204 and Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR,

Subtitle A, Chapter I, and Part 25.
From NOAA-11: 5 U.S.C. 301, Departmental Regulations and 15 U.S.C. 1512, Powers and duties of Department.

From DEPT-9: Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.

From DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531–332; 15 U.S.C. 1501 *et seq.*; 28 U.S.C. 533–535; 44 U.S.C. 3101; Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.

From DEPT-18: Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

From GSA/GOVT-9: For the Entity Management functional area of SAM, the authorities for collecting the information and maintaining the system are the Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c). For the exclusions portion of the Performance Information functional area, the authorities for collecting the information and maintaining the system are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).

From GSA/GOVT-10: E-Government Act of 2002, 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.

From OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

From 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, and Executive Order 9397.

NOAA5006 is a Federal Information Processing Standard (FIPS) 199 moderate security impact category 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.
__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	X	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): Addition of users from NCEI, STAR and NSOF systems.					

____ 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.

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	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X**	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: : The Social Security Numbers are collected on NESDIS HQ LAN contractors and government employees for the purposes of conducting background investigations and on I-9 forms for hiring. The processing of such information does not occur on NOAA5006. This information is only collected and in some cases may be stored electronically on the internal shared drives as well as in hard copies that are stored in locked file cabinets.

The authorities are those in DEPT-18.

** Government-issued passport.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X

b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates	X		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	X*	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

*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	d. Queries Run		f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify): Financial information in contract-related documents.

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		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify): The NCEI Mississippi location provides the PII collected to the Mississippi State university for badging purposes.					

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

NOAA5006 does not process PII information and only stores the information. The information that is stored is collected directly from the individual via secure email transmission or in person. The individual providing the information validates that the information provided is accurate.

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, Licensing of Private Remote-Sensing Space Systems This is the only portion of the information that is covered by the PRA.
	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	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)		For web measurement and customization technologies (multi-session)	
Other (specify):			

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 and stores 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 collected on NESDIS HQ LAN contractors and government employees for the purposes of conducting background investigation

The I-9 and background investigation information may be stored electronically and on paper in locked cabinets. NESDIS local area network users must delete from NESDIS local drives, removable media, and shared drives all copies of Human Resource documents, which include but are not limited to I-9 forms, OF-306 forms, and eQIP submissions, within 30 days after verification of accurate information or when no longer needed for administrative, legal, audit, or other operational purposes.

The above information PII/BII is collected on Federal employees and contractors.

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 person or small,

well-defined group of people as well as work telephone numbers and work mobile number. The above information PII/BII is collected on Federal employees, and contractors

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

The above information BII is collected on contractors.

CRSRA collects and maintains license application data about businesses that apply for and operate private earth remote sensing space systems. This information collected includes but is not limited to 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.

The above BII information is collected on businesses.

The ACIO-S stores, on its shared drive, NESDIS employee passport information for tracking and records purposes regarding international travel. ACIO-s also stores information related to background investigations for new and recent employees on the shared drive.

The above PII is collected on Federal employees.

STAR personnel collect the following Work-Related-Data (WRD) from all STAR personnel and is maintained to simply maintain a roster of STAR personnel:
Name, Work Email address, Job Title, Work Address, Work Telephone Number.
STAR personnel store Vendor BII in proposals and contracts and grants is used for the administration of contracts and grants.

The above BII information is collected on businesses
The above PII is collected on Federal/Contractor employees.

NCEI Maryland (MD), Asheville (NC), Boulder (CO) and Stennis (MS) store work related data, 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 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 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.*
The above PII is collected on Federal/Contractor employees.

NSOF collects employee information such as SSN, Passport, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone Number, Email Address, Financial 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.

The above PII/BII information is collected on both contractors and Federal employees

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

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.

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):Universities			

*Shared with NASA and MSU for building access badges.

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

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.

X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement for CRSRA and/or privacy policy can be found at: https://docs.google.com/a/noaa.gov/forms/d/1STEt0B6EUweGMmk1QyXAoo1KZAnQ1G8JJcnsuifO1SA/viewform?edit_requested=true _____as well as printed on the badging information permission form. All federal government–wide forms have Privacy Act Statements._____.	
	Yes, notice is provided by other means.	Specify how: Written notice is provided on all personnel forms that NESDIS HQ LAN employees complete. For BII related data notices is given in the request for proposal or the request for information.
	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 have an opportunity to decline during on-boarding and applicable processes. An individual can decline by not submitting the applicable forms, if individuals do not submit the forms, or data is not accurate and complete, the individual is not granted physical or logical access. Businesses providing information for licensing may decline to provide BII by not submitting a request, but will not receive a license.
	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 an opportunity to consent to particular uses of BII/PII in their employment terms and agreements as well as the contract/license terms and The Authorization to share PII with non-Department of Commerce entities, included with this PIA.
	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 their individual licensing information or contact information where applicable. Updates to licensing information must be submitted in writing to the NOAA NESDIS HQ office. Also, personnel can contact the HR department manager and provide any updates or changes to their information.
	No, individuals do not have an opportunity to review/update PII/BII	Specify why not:

	pertaining to them.	

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: NOAA5006 Only stores PII and does not process any PII/BII. NOAA5006 does not have any databases stored on our network that house PII/BII information. We monitor our network devices using Solar Winds and our user accounts are monitored using Active Administrator.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 06/19/2017_____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

All PII/BII data stored in our system is located on our internal network. NOAA5006 has boundary protection devices such as firewalls and Intrusion detection/prevention systems in place to protect this data. Also all 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/BBI is encrypted in transit using the DOC Secure File sharing system. All NOAA5006 Laptops have full disk encryption, The NOAA5006 Removable media policy requires that any removable media i.e. USB drives external hard drives must be FIPS140-2 validated using hardware encryption. NOAA5006 uses approved DOD sanitization software to ensure no data remains on NOAA5006 media. Lastly NOAA5006 encrypts all data that is stored on its back up to type drives.

Section 9: Privacy Act

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission, DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons and DEPT-13, Investigative and Security Records. Also, DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; GSA/GOVT-9, System for Award Management and 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** **100-22 Electronic Records** **100-24 Information Technology Operations & Management** **100-27 Records of the Chief Information Officer** **Chapter 200-Administrative** **200-03- Budget Background Records** **200-04 Budget Estimate and Narrative Statement Records** **200-06 Agency-wide Budget Projection Records** **200-30 Technical Reference Materials** **Chapter 1400 – Satellites and Data Centers** **1401Original 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:

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		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 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 levels. *(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 and must access PII data in our system using their CAC authentication which uniquely identifies and authenticates them before they access any PII data.
X	Quantity of PII	Provide explanation: There is a significant quantity of PII.
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 publically available and is located on our internal network. NOAA5006 has boundary protection devices such as firewalls and Intrusion detection/prevention systems in place to protect this data. Also all 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.

	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	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 only collects minimum PII/BII data needed to complete a specific task. This data is collected directly from the persons or company 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.