Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the

NESDIS Center for Satellite Applications and Research (STAR) LAN
NOAA5018

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

11/29/2019

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

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

Unique Project Identifiers: 006-48-01-16-01-3201-00 and 006-48-01-16-01-3202-00

Introduction: System Description

NOAA5018 is the main scientific IT system for the NESDIS Center for Satellite Applications and Research (STAR).

STAR is the science arm of the National Environmental Satellite, Data, and Information Service (NESDIS), which acquires and manages the nation's environmental satellites for the National Oceanic and Atmospheric Administration (NOAA). STAR research activities, integral to the implementation of NOAA's research priorities, are aligned with and carried out in direct support of NOAA and NESDIS programs, strategic goals, and performance objectives.

STAR's mission is to accelerate the transfer of satellite observations of the land, atmosphere, ocean, and climate from scientific research and development into routine operations, and offer state-of-the-art data, products and services to decision-makers.

NOAA5018 consists of approximately 400 CentOS Linux workstations and servers, connected to Cisco/IOS switches and a Cisco ASA firewall. NOAA5018 also contains one Oracle Solaris server, a few OpenBSD systems, a few Apple Mac OS-X systems, a large amount of disk storage systems from Dell, NetApp, and Supermicro, and VMware ESXi hypervisors.

NOAA5018 resides on a private firewalled network, located at the NOAA Center for Weather and Climate Prediction (NCWCP), in College Park, MD 20740.

NOAA5018 is primarily used for scientific research and development. In this respect, it primarily contains scientific data, code, documentation, publications, etc. NOAA5018 does not facilitate e-commerce or other similar transactions. Rather, typical NOAA5018 "transactions" include scientific processes, and scientific data input, output, and production.

The type of data processed, stored, and transmitted by STAR includes scientific, remote-sensing observations of the land, atmosphere, ocean, and climate, provided by Earth-orbiting satellite observing systems and in-situ readings.

The Security Categorization of NOAA5018 has been determined to be moderate using the guidance in FIPS 199 and NIST SP 800-60.

Relevant to this PIA, NOAA5018 hosts the following:

- PII in the form of a basic personnel roster available to the public via the STAR Web site.
- System Administration/Audit Data (SAAD) of STAR employees to facilitate IT administration, and especially IT Security administration.

Information sharing

NOAA5018 does not share PII/BII except within the bureau, in the form of a roster on a public Web site, and in case of a law enforcement incident, to applicable DOC and federal bureaus.

Authorities

Statute 5 U.S.C 301 authorizes the collection, for civil employment, of employee personnel information. In addition: 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.

For 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; and Equal Employment Act of 1972.

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):					

_X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	

m. Other identifying numbers (specify):
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:

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

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number		g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify): ResearcherID (if available), STAR Division, STAR Branch, and Employment Type (Government, Contractor, Visitor/PostDoc).					

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

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

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax	X	Online	
Telephone		Email	X		
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):					

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

The Work-Related Data maintained within the NOAA5018 system is the basic STAR Staff Directory maintained on the main STAR web site. The information in that staff directory is gathered via STAR account activation form, and established when personnel are on-boarded, and updated via STAR account activation/deactivation form, when personnel leave STAR. Part of the processing of that form is updating the STAR roster.

The System Administration/Audit Data is maintained by the operating systems of the computers upon which it is generated.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): To provide a basic roster of STAR personnel.			

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).

WRD: The following Work-Related-Data (WRD) from all STAR personnel (federal employees and contractors) is collected for maintenance of a basic roster of STAR personnel, available to the public via the STAR Web site:

Name, ResearcherID (if available), NOAA Email Address, STAR Division, STAR Branch, and Employment Type (Government, Contractor, Visitor/PostDoc).

SAAD: The following System Administration/Audit Data (SAAD) from all STAR personnel (federal employees and contractors) is used by STAR IT personnel while administering the system, and especially the IT Security aspects of the system:

User ID, IP Address, Date/Time of Access, and File Contents.

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.)

There are no significant potential threats to privacy as a result of STAR's use of the information.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			Basic STAR roster available via STAR Web site
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	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.)*

	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:	
X	Yes, notice is provided by other means.	Specify how: • WRD: Personnel (federal employees and contractors) are notified, via a privacy act statement on the STAR IT account request form, of the basic STAR staff roster on the STAR Web site containing their WRD. Only the resulting roster is within the system boundary. • SAAD: Logon banners warn all IT users that their SAAD and system use is subject to monitoring.
	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: • WRD: Personnel (federal employees and contractors) are notified, via a privacy act statement on the STAR IT account request form, of the basic STAR staff roster on the STAR Web site containing their WRD. Only the resulting roster is within the system boundary. Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent the individual from being employed by NOAA/NESDIS/STAR. • SAAD: Logon banners warn all IT users that their SAAD and system use is subject to monitoring. Users can decline to proceed with the use of STAR IT, however, that will prevent them from being employed by STAR, since they must use STAR IT to perform their jobs.

	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: • WRD: Personnel (federal employees and contractors) are notified, via a privacy act statement on the STAR IT account request form, of the basic STAR staff roster on the STAR Web site containing their WRD. Only the resulting roster is within the system boundary. There is only one use for the roster. Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent the individual from being employed by NOAA/NESDIS/STAR. • SAAD: Logon banners prompt users that their use of the NOAA5018 IT System requires and implies their consent to monitoring, which they give by continuing the logon process.
	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: • WRD is maintained to maintain a basic roster of STAR personnel. The roster is maintained on the STAR Web site, and is accessible by all STAR employees. They can request updates via their supervisor and the STAR webmaster.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: • SAAD is used by STAR IT personnel while administering the system, and especially the IT Security aspects of the system. This information is necessary to maintain the security of the system, and it cannot be updated, other than the contents of their files, of course.

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.
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: There is no sensitive PII. SAAD: User ID, IP Address, Date/Time of Access, File Contents These are protected by files system permissions. User ID and IP address tables are readable only by users of the system. Date/Time of Access information is kept in logs readable only by IT administrators of the system. File Contents are only readable to the file owner, IT administrators, and any other system user only if the file owner sets the file permissions to allow that access.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization(A&A): 12/06/2018 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is moderate of 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).*

WRD in the STAR roster is already publicly available via the STAR Web site.
SAAD is available only to privileged STAR IT administrators, and the SAAD owners.

Section 9: Privacy Act

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: DEPT-13, Investigative and Security Records DEPT-18: Employees Personnel Files Not Covered By Notices of Other Agencies (EPFNCBNOOA)
	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: System Access Records, the disposition authority is DAA-GRS- 2013-0006-003. Disposition instruction: Temporary. Destroy when business need ceases.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing		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.)*

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: The PII discussed in this PIA is maintained in the roster on the STAR Web site and is already publicly available.
X	Quantity of PII	Provide explanation: The PII discussed in this PIA consists of only a few elements for each user, and is already publicly available in the roster on the

		STAR web site.
X	Data Field Sensitivity	Provide explanation: NOAA5018 maintains no PII/BII above a low sensitivity level.
X	Context of Use	Provide explanation: The PII discussed in this PIA consists of only a few elements for each user, and is already publicly available in the roster on the STAR web site.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: The PII discussed in this PIA is maintained in the roster on the STAR Web site and is already publicly available.
	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.)

There are no significant potential threats to privacy in light of the information collected or the sources from which the information is collected.

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.