Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
Southern Region General Support System (GSS)
(NOAA8884)

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

Jennifer Goode 03/18/2021

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

U.S. Department of Commerce Privacy Impact Assessment
Southern Region General Support System (GSS)
(NOAA8884)

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

General Support System

The National Weather Service (NWS) Southern Region provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including forecasts and warning is dependent on a complex interaction of many information resources and systems. This system is designed and used to support the collection, processing, and dissemination of data that supports the mission of the organization. It also supports the administrative functions and the scientific & technical research and innovations activities of employees within the organization.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems; client-server and web- based server systems. The system supports a variety of users, functions, and applications; including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development and collaboration.

(b) System location

The system is located in Fort Worth TX, but the WAN extends across 11 states which support 32 Weather Forecast Offices, 4 River Forecast Center's, 7 Center Weather Service Unit's, and 4 Port Marine Office's.

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

The SR GSS is a system with interconnections only to trusted NWS-NOAA internal systems with no direct interconnections to the outside. Although there are a variety of hardware and operating systems, all the operational activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems, and client-server systems. The system supports a variety of users, functions, and applications, including word processing, employee data, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development, and collaboration.

The following systems interconnect internally with NOAA8884:

NOAA0201 - Web Operation Center (H)
NOAA0900 – Consolidated Cloud Applications
NOAA1101 - Information Technology Center (M)
NOAA8106 - Upper Air Observing System (UAOS)
NOAA8107 - Advanced Weather Interactive Processing System
NOAA8850 - NWS Enterprise Mission Enabling System

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

The National Weather Service (NWS) Southern Region provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including forecasts and warning is dependent on a complex interaction of many information resources and systems. The NOAA8884 General Support System (GSS) is designed and used to support the collection, processing, and dissemination of data that supports the mission of the organization. It also supports the administrative functions alongside the scientific and technical research and innovation activities of employees within the organization.

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

MARS Data:
Authorized users log into MARS via interconnection with NOAA1101. This data does not reside within 8884.

Volunteer Observer Data:
Access to the data is done manually and resides within each of the 32 Weather Forecast Offices on workstation hard drives or centralized network attached storage devices.

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

All data is transmitted and received via NWSOneNet cloud. All internal NWS data is on the Internal cloud network and all Internet connectivity is supplied through the NOAA TIC sites.

MARS Data:
All access to the MARS reports are done via web browser, all data transmission is one way, from MARS to the SR Portal and then the users pull their set of data for restricted internal use.

Volunteer Observer Data:
There is no PII information transmitted to and from the system.

(g) Any information sharing conducted by the system

MARS Data:
Management Analysis and Reporting System (MARS) is a NOAA enterprise system within the NOAA1101 GSS accreditation boundary that provides a common source for business information and financial transactions for all NOAA line offices. NOAA8884 extracts non-sensitive employee, business, and financial data and stores it on encrypted centralized servers, authorized employee workstations, and in authorized Google Account for Government (GAfG) cloud environments. The data is then used by authorized agency employees and contractors within the NOAA organization in the performance of their official duties.

Volunteer Observer Data:
There is no information sharing within or outside of the system.

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

Authorities from DEPT-11: 5 U.S.C. 301, Departmental Regulations and 15 U.S.C. 1512, Powers and duties of Department.

Authorities from DEPT-18: Authorities from DEPT-18: 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.

Authorities from DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

OPM GOVT-1: General Personal Records. 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Order 9397 as amended by E.O.13478, E.O.9830, and E.O.12107

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

NOAA8884 is a Moderate categorized 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		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): * Trusted Agent data is removed from the system.					

____ 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 (version 01-2015).

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
Volunteer Observer Data: Volunteer data consists of Name, Address, Phone number and email address. No additional PII is collected.					

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

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

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	X
b. IP Address	X	d. Queries Run	X	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	X	Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify): **Volunteer Observer Data collected in person**					

Government Sources					
Within the Bureau	X	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.

MARS Data:
There is no data change when we read in data from the MARS system. Users only have read-only privilege.

Volunteer Observer Data: All of this PII information is directly received from the user when accounts are created. It is manually input into the local office DB and only the OPL (Observation Program Leader) has access to make changes to the data.

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 no new 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 technologies used that contain PII/BII in ways that have not been previously deployed.

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	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

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).

Volunteer Observer Data: NOAA8884 collects, stores, and uses volunteer observer general

personal data who provide daily climate and weather reports. The data resides within each of the 32 Weather Forecast Offices on workstation hard drives or centralized network attached storage devices. The contact information is used by NWS staff members responsible for providing meteorological, hydrological, and climatological data collection oversight as part of their official duties.

Volunteer observer PII data collected and stored within the NOAA8884 accreditation boundary is limited to general personal data including name, home address, email address, and telephone number. A limited amount of contact information is retained in the local office for quick access to contact the volunteer observer in case of equipment outages.

The volunteer observer has the right to opt-out of the program at any time. Once collected the information is stored on workstation or network attached storage device and also entered into a NOAA database called the Station Information System (SIS) located and maintained by NWS Office of Observations. Once the volunteer opts out of the program the PII is purged from the system.

Volunteer Observer Data and is not shared outside the National Weather Service.

MARS Data: This data is used by authorized agency employees, and contractors within NOAA8884's accreditation boundary in the performance of their official duties. Uses include decisions related to agency staffing, budgeting, acquisitions, finance, and mission delivery.

Employee data consists of the name of the employee, the email address of the employee, CBS employee number, job title, employee grade, step, series, org code, project-task, employee salary, employee benefits, FLSA code, and BUS code.

NOAA8884 uses MARS employee data in conjunction with directly related financial data to formulate and track labor costs by portfolio, project code, program code, assigned org code and physical location for the purposes of Financial Management Center (FMC) budget planning, oversight, forecasting, and execution. The FMC uses all specific data to accurately manage budget allocations, status, analyze variances and historical spending trends to support the formulation of future resource needs. Data is used to calculate, analyze, and track FTE, benefits, premium pay shift differential, overtime, locality pay, cost of living allowances, special IT pay, awards, and annual pay raises in a complex budget accounting environment that requires daily detailed analysis. Information is shared with managers and supervisors responsible and accountable for programmatic oversight of costing and controls. All associated accounting is categorized in accordance with the Accounting Classification Code Structure (ACCS), cost category, funding source, and in accordance with NWS' Appropriations Reference Manual.

NOAA8884 extracts non-sensitive employee, business, and financial data directly from MARS and stores it on encrypted centralized servers, employee workstations, and in authorized GAfG cloud environments. MARS PII data or derivatives of data originating from the MARS system is also received from agency officials outside our accreditation boundary using a variety of communication technologies (i.e., attachments to Email, DOC secure file sharing sites, Google cloud file sharing technologies, etc.) and in a variety of electronic formats and is stored on both centralized servers, employee workstations, and in authorized GAfG cloud environments.

MARS data and is not shared outside the Department of Commerce.

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.)

An insider threat is a malicious threat to an organization that comes from people within the organization. DOC and NOAA has put in place mandatory training for all its uses. The Security Awareness and Insider Threat is an annual requirement, intended to reduce the risk and minimize the impact of an authorized user intentionally or unintentionally disclosing data, and causing adverse impact to sensitive data and mission.

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			
State, local, tribal gov't agencies			
Public			
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.

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: NOAA0201 - Web Operation Center (H) NOAA0900 – Consolidated Cloud Applications NOAA1101 - Information Technology Center (M)

	NOAA8106 - Upper Air Observing System (UAOS) NOAA8107 - Advanced Weather Interactive Processing System NOAA8850 - NWS Enterprise Mission Enabling System Employee and financial data are extracted from NOAA1101 system by authorized users within NOAA8884 using standardized user interface tools every two (2) weeks corresponding with Federal pay schedules, or more frequently as needed by management. The reports are then saved as an .XLS file that is ingested to the SR SQL server, resides on the server for four (4) years. SQL server data at rest is encrypted, and only accessible to authorized users using CAC authentication. Once into the SR System, the users access the secure portal to retrieve their relevant data in HTML format. There is no sharing of PII/BII with any other NOAA systems; therefore, no controls are in place to prevent leakage.
	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 and/or privacy policy can be found at: Privacy Policy: https://www.weather.gov/privacy .	
X	Yes, notice is provided by other means.	Specify how: **Volunteer Observer Data:** Notice to volunteers is provided when information is collected, via the cooperative agreement form.
	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: **Volunteer Observer Data:** All of this information is voluntary, as part of the cooperative agreement to work with the NWS on providing observations. The only means of providing

		the PII is by completing and signing the cooperative agreement form. Declining to sign the agreement will void the observer the duties with NWS.
	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: **Volunteer Observer Data:** The volunteer observer information is for contact purposes only which is given as part of the signed agreement. No other uses are suggested or specified. The volunteer have an opportunity to consent or question the form's contents prior to signing with the local forecast office POC.
	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	

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: **Volunteer Observer Data:** The local manager visits each volunteer twice monthly to monitor equipment and answer questions. Updates can be made then, or emailed, as explained by the manager during orientation.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
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: System logging is enabled and all access is tracked
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): April 30, 2020 ☐ 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.
	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).*

Volunteer Observer Data: Access to the system maintaining the PII is controlled by access via Active Directory and the use of CAC (PIV) cards. Only employees with authority to maintain this database are allowed access to the information.

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). COMMERCE/NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission; COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; COMMERCE/DEPT-25, Access Control and Identity Management OPM GOVT-1: General Personal Records. 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Order 9397 as amended by E.O.13478, E.O.9830, and E.O.12107
	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: • NOAA Records Schedule, Chapter 1300, Weather, 1307-05, Service Locations Data Networks • NOAA Records Schedule, Chapter: 900, 904-01, Building Identification Credential Files • NOAA Records Schedule, Chapter 100, Enterprise-Wide Functions Electronic Records schedule • NOAA Records Schedule, Chapter 402, Employee Compensation and Benefits Records • NOAA Records Schedule, Chapter 403, Financial Management and Reporting Records • NARA General Records Schedule- 3.1, General Technology Management Records • NARA General Records Schedule- 3.2, Information Systems Security Records
	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 *	X
Degaussing		Deleting	X
Other (specify): * Over write is done with DoD disc wipe program DBAN, which is ruin at the high security level and overwrites disc 48 times with 1's and 0's.			

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.)*

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	An employee, contractor, or volunteer can be identified by name or contact information
X	Quantity of PII	Only name and contact information for volunteers, and names of employees, are in the system.
X	Data Field Sensitivity	No sensitive data is collected.
X	Context of Use	Voluntary submission of PII for internal use only
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Secured local database managed by limited Federal employees. Access is limited to the program manager who is in charge of the Co-Op program. The technical controls in place rely on the use of Active Directory and CAC authentication.
	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.)

Only the information that is required for the given financial reports is selected and downloaded from the MARS database. By selecting only certain fields and not the entire report we can ensure

that sensitive or private information is not included with the broader reports. Reports are also broken down by individual office ORG codes so only data for that particular office is included in the reports. This ensures that only data needed by that office is available for that office to view.

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.