Version Number: 01-2015

U.S. Department of Commerce
National Oceanic and Atmospheric Administration
National Weather Service

Privacy Impact Assessment
for the
National Weather Service Headquarters Local Area Network (NWSHQNet) NOAA8205

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 D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.03.09 15:53:26 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA8205

Unique Project Identifier: 006-000351104 00-48-02-00-02-00

Introduction: System Description

NWSHQNet is in the operational phase of the system development life cycle.

The National Weather Service (NWS) Headquarters Local Area Network, NOAA8205, is a general support system consisting of domain controllers, servers, desktop/workstation, laptops, printers and network infrastructure components. NOAA8205 is located within the Silver Spring Metro Complex Building 2 (SSMC-2), providing Local Area Network (LAN) support for NWS Headquarters, supporting approximately 800 users and 1,500 network devices.

NOAA8205 provides network infrastructure support, management and connectivity services for administrative functions to include: Service Desk support, Active Directory, file and print, file backup and restoration, storage, Dynamic Host Configuration Protocol, Windows Internet Name Services, Domain Name Service, IP address space allocation, application distribution and patch management, backup and disaster recovery to the desktop and server customers within the NOAA8205 accreditation boundary. In addition, it provides system-level support for servers, desktops/workstations, and laptops and a test lab mimicking the production environment for systems and network engineers to develop and test new technologies. Lastly, the NOAA8205 active directory user base receives electronic mail and calendar services from the NOAA Messaging Operations Center.

Multi Year Planning System (MYPS)

The Multi Year Planning System (MYPS) is comprised of three General Services Systems (GSS) and includes 20 servers (CFO1 servers). The GSS are the MYPS Labor Projection Model, Management Analysis and Reporting System Business Intelligence (BI) Maintenance Platform (MARS), and the General Forecaster Vacancy System. The Labor Projection Model and the General Forecaster Vacancy System are operational production systems. MARS BI Maintenance Platform is used only for maintenance efforts related to the production and pre-production MARS systems which are housed at the NOAA Information Technology Center.

The MYPS Labor Projection Model is a tool used to compute the multi-year total NWS labor model (5 years) using a detailed site-by-site, bottom-up cost approach. It calculates labor costs by site by position with the impact of changes in staffing levels. The model applies a labor lapse, calculates FTE, benefits, premium pay (shift differential), overtime, locality pay, cost of living allowance (COLA), special IT pay, awards, and annual pay raises. Costs are calculated using

OPM-published salary and rates tables. All costs are categorized by Accounting Classification Code Structure (ACCS), cost category, funding source, and portfolio. In addition, the model is used in "what-if" analyses to answer questions about proposed changes in labor such as lapse, labor rates, inflation, and table of organization changes. The resulting five year answer sets are used to answer detailed questions about labor planning for NWS, NOAA, DOC, OMB, and Congressional requests without any PII data. The labor data contained in the model's database is the master authorized (funded) position data for NWS. The model has its own user logon system and is accessed by its sole Federal user and its maintenance support contractor staff via the NOAA Silver Spring Metro Campus (SSMC) trusted campus network. The MYPS system retains user name, job title, and budgeted salary information for the purposes of budget forecast modeling.

MARS is a NOAA enterprise system that provides a common Business Intelligence (BI) platform to all NOAA Line Offices for financial reporting and querying, budget planning and commitment tracking. It consists of two modules, Reporting and Querying and Data Entry. The Data Entry module is not supported by MYPS. The MARS Reporting and Querying module is a business intelligence maintenance environment used for ongoing design, creation and testing of new reports; new extract, transform and load (ETL) jobs; and software patches and upgrades for eventual deployment to the Reporting and Querying module of MARS. MARS BI Maintenance Platform is accessible only via the NOAA Silver Spring Metro Campus (SSMC) trusted campus network. PII related information is collected solely for regression testing purposes within the MARS system. Once testing has been completed, the sample data will be retained for a time, and deleted within 3 years or sooner. Our mandate is to make sure any revisions to our processes operate correctly and produce correct answers on the MARS reports before promoting the revisions forward to TEST where yet another testing cycle occurs. Once the Federal client approves the system fix(es) on TEST, the final solution is only then migrated to PROD, with another final confirmation things worked in PROD before closing our Software Design Request (SDR) ticket.

We extract sample data from production to use during various development cycles that include previous fiscal year (FY) data and the current FY data. We ultimately compare the resultant differences between DEV or TEST to the PROD environment to prove the expected system modifications actually repaired the process or MARS report.

If we were to implement dummy data, we would still have to extract live data, but then systematically revise it to substitute real values for dummy values across multiple fiscal years and multiple database tables many of which enforce primary/foreign key relational constraints. After this exercise, we would still need to map backwards to the original data for direct comparison to our production system data or reports for validation of the changes. These steps would be costly in team resources with multiple developers working on multiple SDRs, but yet allowing correlated comparison of before and after change modification to the operational

MARS production system as proof of task completion. Since the Government doesn't want to pay for these steps in time or dollars, we added the additional developer, system, and user controls on all MARS developers and users giving them the responsibility to protect data from all unauthorized disclosures (e.g. NDAs mentioned previously above).

Government stakeholders need the MARS Financial Data Warehouse and they imposed the best possible security measures given the exigent trade-offs and limited available resources available (CPU speed, disk space, contract dollars, time, and staff).

The General Forecaster Vacancy System is a notification application that is used by regional workforce managers to make regional meteorological (met) interns (Met Interns) aware of upcoming general forecaster vacancies at NWS Weather Forecast Offices (WFOs), per an agreement between NWS management and the National Weather Service Employees Organization (NWSEO). The system contains a database of all the Met Interns in the regions. The data base is maintained by the regional workforce managers using a web application which is accessed using LDAP authentication. Prior to posting a vacancy for a general forecaster (meteorologist) at a WFO, the workforce manager in the region uses the system too automatically send an email to all the met interns listed in the database. An intern who is interested in the listed vacancy clicks on an HTML hyperlink imbedded in the email to express their interest. The system counts the responses and a determination is made at the regional level, based on the number of responses, whether the vacancy will be advertised to status candidates only or to all hiring sources (USAJOBS, etc.). The web portal uses session cookies to time-out any open workforce manager sessions within five minutes to maintain security of the process. PII in the form of user name and email address is collected and retained as part of the application process.

The NOAA8205 Trusted Agent collects and stores Form CD591 (PIV request form) for government issued IDs, LDAP and Active Directory. The Trusted Agent processes security and badging forms for contractors only, not federal employees. The processing package includes fingerprints and a photograph, both taken by the badging office (but not stored in NOAA8205), driver's license and passport number. Once the Eastern Region Security Office approves a contractor for a CAC, it returns the CD-591s for the sponsored contractors and they are stored electronically. OF306 Declaration for Federal Employment, which contains SSNs, is stored temporarily when the form needs to be scanned and saved to a drive prior to uploading into Accellion Secure File transfer to send to the Security Office. *Contractors are advised to remove the form from their desktops after the transfer, but there is no current way to check this. The system is investigating courses of action to discover PII data within NOAA8205, including user terminals, but in the meantime, we are changing the confidentiality level to 'High' based on possible SSN retention on desktops.* A paper copy of the Security Coversheet/Request for Investigation Coversheet is also stored after removing Birth Date and SSN.

No PII is shared outside of the Department of Commerce (DOC). Only PII directly related to an individual's clearance is shared with DOC.

Authorities

U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

15 U.S.C. § 1512, which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.

Federal Information Security Management Act (Pub. L. 107– 296, Sec. 3544).

E-Government Act (Pub. L. 107–347, Sec. 203).

Homeland Security Presidential Directive 12 (HSPD–12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

Federal Property and Administrative Services Act of 1949, as amended.

This system has been classified as FIPS 199 moderate level.

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):					

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: *For MARS testing: We use a three tier approach (DEV, TEST, PROD) so any new bug fixes or new developments are moved forward to TEST tier first, run in mock production setting on TEST, then once all regression testing has been validated and approvals given from Federal agent, the "code" is migrated into production. During testing periods, the TEST tier has PROD data to assure everything works as though it were in production. Afterwards we do housecleaning on TEST until the next testing cycle.

There is also temporary storage of the OF306, containing the SSN, before transmitting to the security office. *In some cases, the information may not have been removed after transmission. The system is working on addressing this issue.*

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender	x	j. Telephone Number	x	p. Military Service	x
e. Age	x	k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity	x	l. Education	x	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	
c. Work Address	x	f. Business Associates			
i. 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):					

* For badging purposes only

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	x	f. Contents of Files	
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	x	Online	
Telephone		Email			
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):					

2.3 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	x	Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	x
Other (specify):			

	There are not any technologies used containing PII/BII in anyway not 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			
To determine eligibility		For administering human resources programs	x
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	x	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).

The NOAA8205 Trusted Agent collects and stores Form CD591 (PIV request form) for government issued IDs, LDAP and Active Directory. The Trusted Agent processes security and badging forms for contractors only, not federal employees. The processing package includes fingerprints and a photograph, both taken by the badging office (but not stored in NOAA8205), driver's license and passport number. Once the Security Office approves a contractor for a CAC, it returns the CD-591 for the sponsored contractors and they are stored electronically.

OF306 Declaration for Federal Employment, containing the SSN,is stored temporarily when the form needs to be scanned and saved to a drive prior to uploading into Accellion Secure File transfer to send to the Security Office. *Contractors are advised to remove the form from their desktops after the transfer, but there is no current way to check this. The system is investigating courses of action to discover PII data within NOAA8205, including user terminals, but in the meantime, we are changing the confidentiality level to 'High' based on possible SSN retention on desktops.* A paper copy of the Security Coversheet/Request for Investigation Coversheet is also stored after removing Birth Date and SSN.

The MYPS system retains user name, job title and budgeted salary information for the purposes of budget forecast models.

The Forecaster Vacancy system retains name and email only for federal employees.

The MARS system retains sample PII for testing purposes only.

Additionally; NOAA provides mandatory annual IT Security Awareness training, which includes the handling of PII/BII. This training advises the users not to store any PII/BII, but if it is stored, they are advised to remove the PII/BII information prior to storing the documentation.

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.

	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.	
	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:

		Form CD591, the DOC PIV request form, provides notice in that the request for information comes from the sponsor and registrar. The information comes from the applicant, who completes the form and provides it to the sponsor. https://mars.rdc.noaa.gov/docs/forms/NOAA_MARS_Rules_of_Behavior.pdf https://mars.rdc.noaa.gov/docs/forms/DOC_NOAA_MARS_NDA_v2.pdf Form OF306 states that the Office of Personnel Management is authorized to request this information under sections 1302, 3301, 3304, 3328, and 8716 of title 5, U. S. Code and addresses and Routine Uses. The MYPS, Forecaster Vacancy System, and MARS: Federal workers sign a privacy release pursuant to the Privacy Act of 1974 during on-boarding with NOAA/NWS; see https://www.justice.gov/opcl/privacy-act-1974 ; Conditions of disclosure; "For routine uses within a U.S. government agency" and "Other administrative purposes." Additionally; NOAA provides mandatory annual IT Security Awareness training, which includes the handling of PII/BII. This training advises the users not to store any PII/BII, but if it is stored, they are advised to remove the PII/BII information prior to storing the documentation.
	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 can decline by not providing requested information to receive NOAA ID. However, without a NOAA ID, they cannot work at NOAA as a Federal Employee or Contractor. The information collected Forecaster Vacancy System is provided only if the service is desired. The information collected by MYPS is solely for budget purposes (no opt out) and MARS collects information solely for testing applications (no opt out).
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: If no consent is granted, no ID will be issued as in 7.2 above. This is the only purpose for this information. There is only one use for each of these: MYPS (budget) and MARS (testing)

		Forecaster Vacancy is voluntary for job openings and solely consists of user name and email address. There is only one use of the information.
	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: Users are informed in person or in writing by their supervisors at time of onboarding, that they can update PII/information via NOAA LDAP or NOAA Locator. https://nsd.rdc.noaa.gov/ Forecaster Vacancy user name, email address and MYPS information updates are not applicable for the individual. However, updates may be implemented by HQ and FMC administrators at an individual's request in writing to one or the other. MARS PII is used solely for testing and thus the individual does not need to review/update PII/BII pertaining to them.
	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: MARS has built-in auditor for who accessed what report and when.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 5/20/2016 ☐ 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 and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
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.
x	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.

User name, Office location, and Telephone Number of NOAA employees and contractors are collected and maintained in NOAA8205 Active Directory and LDAP. NOAA8205 Administrators can access or alter this information; the Active Directory is not publicly accessible and has internal boundary controls in place to include firewall and Access Control Lists (ACLs). The NWS HQ Trusted agent (TA) collects and maintains CD591information. This information is stored by the TA in a locked secure location; after three months, the information is shredded in accordance with NOAA Records Management schedule. (Contains name, phone number and email address.) The MYPS and MARS information is maintained in encrypted files and protected through Role Based Access Controls (RBAC). Additionally; NOAA provides mandatory annual IT Security Awareness training, which includes the handling of PII/BII. This training advises the users not to store any PII/BII, but if it is stored, they are advised to remove the PII/BII information prior to storing the documentation.

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 and number *(list all that apply)*: DEPT-18, Employees Information Not Covered by Notices of Other Agencies; DEPT-25, Access Control and Identity Management System, GSA./GOVT-7, Personal Identity Verification Identity Management System
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

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 Series Chapter: 900 904-01Building Identification Credential Files NOAA Chapter 100: Enterprise-Wide Functions Electronic Records schedule: NARA General Records Schedule 20, Electronic 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	x	Overwriting	
Degaussing		Deleting	
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

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.

	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.
x	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.)*

	Identifiability	Provide explanation:
x	Quantity of PII	Provide explanation: No access for average MARS user; limited access for MARS power users as needed to do their job function; and more access for top level managers who require access for those they manage.
x	Data Field Sensitivity	Provide explanation: *In some cases, the CD306 containing a contractor SSN may not have been removed from a desktop. The system is working on addressing this issue.*
x	Context of Use	Provide explanation: MARS links some PII data using natural keys for SQL table joins which report users cannot see.
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: The information collected for badging purposes contains two forms of personal identification (ie Passport, Driver's license, etc.) which, if exposed during the course of collection and verification, could have an adverse impact to user confidentiality.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: The possibility of retention of the SSN, as stored electronically in the OF306, caused us to change our confidentiality rating from “moderate” to “high”.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 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.