Template Version Number: 01-2021

U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Impact Assessment
for the
Legal Document Management System-Cloud (LDMS-C)

Reviewed by: Henry J. Holcombe, 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

Holcombe Jr, Jamie approved on 2025-07-25T20:56:16.9456625____7/25/2025 8:56:00 PM_
Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
USPTO Legal Document Management System-Cloud (LDMS-C)

Unique Project Identifier: EBPL-LT-02-00

Introduction: System Description

Provide a brief description of the information system.

The Legal Document Management System-Cloud (LDMS-C) is a commercial Software as a Service (SaaS) implemented with Federal Risk and Authorization Management Program (FedRAMP)- authorized NetDocuments software. This SaaS will support the Office of General Counsel's (OGC) document management requirements as they provide advice to USPTO clients on the full range of federal agency legal issues: fiscal, procurement, rulemaking, administrative law, labor and employment, and information law. The system provides a centralized repository for easy storage, search, and retrieval of documents relating to legal matters.

Address the following elements:

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

LDMS-C is FedRAMP-authorized commercial SaaS and minor application.

(b) System location

LDMS-C is SaaS hosted in NetDocuments Cloud in Microsoft Azure U.S. Government (Richmond, Virginia and San Antonio, Texas).

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

LDMS-C is hosted in the NetDocuments Cloud in Microsoft Azure U.S. Government Cloud and accessed by users via a web browser. It interconnects with the following systems:

Identity, Credential, and Access Management-Identity as a Service (ICAM-IDaaS): ICAM-IDaaS is the USPTO system by which users are authenticated to enable single sign-on (SSO) to LDMS-C.

Network and Security Infrastructure System (NSI) - The NSI is an Infrastructure information system, and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications.

Security and Compliance Services (SCS) - SCS provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response.

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

LDMS-C is an application located within the NetDocuments Cloud hosted in Microsoft Azure Cloud that will be accessible to the OGC to develop a centralized repository of USPTO documents pertaining to legal advice and guidance in support of the USPTO mission. It will enable for efficient document storage, retrieval, search, redaction, versioning, sharing, and knowledge management.

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

LDMS-C is a web application that allows authorized users to access and view information in the system using a web browser.

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

LDMS-C users use a web browser to make a Hypertext Transfer Protocol Secure (HTTPS) connection to the web application.

(g) Any information sharing

LDMS-C does not share any information outside of the USPTO.

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

LDMS-C supports OGC. OGC provides advice and written legal opinions on areas concerning the administration and management of the USPTO. The OGC also represents USPTO in various administrative proceedings. As such, there are several authorizing statutes including but not limited to 5 U.S.C. 301, Federal Rules of Civil Procedures, Freedom of Information Act, Privacy Act, Administrative Procedures Act, Principles of Federal Appropriations Law (Red Book), Federal Advisory Committee Act, Merit System Principles, E.O. 10450, E.O. 11478, E.O. 12107, and E.O. 12564.

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

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☐ This is a new information system.

☐ 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):					

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

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*	☒	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	☒	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☒				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

The LDMS-C is a document repository comprised of emails containing legal advice and attachments from the Office of General Law. The marked categories identified above and below may be included in this system, by virtue of being included in email correspondence, or attached document, that is saved to LDMS-C. The Social Security Number would be incidentally a piece of a record. We estimate that it is rare for any of this private information to be included, but in light of OGC operations that involve employee matters, it is possible.

This system is not used as a primary means for collecting, maintaining, or disseminating any of the data listed in 2.1. The PII/BII that is incidentally contained in these emails is in reference to federal employees, contractors and members of the public

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

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☒
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☐	o. Dental Profile	☐
p. Other distinguishing features/biometrics (specify): The advice and information in the system is more general in nature and does not include any Distinguishing Features/Biometrics identified above, except perhaps a wet signature that may be shown on a document.					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☒
b. IP Address	☒	f. Queries Run	☐	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	□	Hard Copy: Mail/Fax	□	Online	□
Telephone	□	Email	☒		
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 system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.

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.
☒	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):			

☒	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): Click or tap here to enter text.			

☒	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	☒	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).

The LDMS-C is a document repository comprised of emails containing legal advice and attachments from the OGC.

The PII/BII that is incidentally contained in these emails is in reference to federal employees, contractors and members of the public.

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.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

In addition to policies and training, this system may be accessed only by a very limited number of individuals that include attorneys, paralegals, information technology (IT) support staff, and a small number of administrative support staff. This population is highly experienced in accessing and protecting private/confidential information in light of the sensitive matters with which OGC regularly works.

LDMS-C has put certain security controls in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

<u>Section 6</u>: 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	☒	☐	☐
DOC bureaus	☐	☐	☐
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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

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

☒	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: LDMS-C connects with ICAM-IdaaS, which provides authentication and authorization services to all enterprise USPTO applications and information systems. PTONet provides the common network that connects all USPTO applications and network access for employees, contractors, Public Search Room visitors to applications and systems in IT-East and IT-West data centers. LDMS-C has put certain security controls in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public	☐	Government Employees	☒
Contractors	☒		
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: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: This system will consist of attorney and paralegal work product that may incidentally contain BII/PII. Any PII and/or BII contained in this system is initially collected and stored in other systems. If and when that happens, employees receive notice of the collection upon collection (through Privacy Act and Paperwork Reduction Act notices).
☐	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: The system is not set up to collect PII/BII directly from individuals. Any changes required would be the responsibility of the source system.

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The system is not set up to collect PII/BII directly from individuals. Opportunity to consent would be the responsibility of the source system.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☐	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: The system does not collect PII/BII directly from individuals. Any changes required would be the responsibility of the source system.

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.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: System logs users and what they have accessed.
☒	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): 9/17/2024 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 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).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	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).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST and FedRAMP requirements. Such management controls include the life cycle review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorize personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

Section 9: Privacy Act

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

☒ 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."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: Commerce/Dept-5, Freedom of Information Act and Privacy Act Request Records Commerce/Dept-14, Litigation, Claims, and Administrative Proceeding Records Commerce/Dept-18, Employees Personnel Files Not Covered by Notices of Other Agencies
□	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.)*

General Records Schedules (GRS) | National Archives

☒	There is an approved record control schedule. Provide the name of the record control schedule: GRS 2.5, item 030, Records Documenting Capture of Institutional and Specialized Knowledge N1-241-05-1, 2a, Routine Administrative Law Files, Internal Management
□	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
□	Yes, retention is monitored for compliance to the schedule.
□	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding	□	Overwriting	□
Degaussing	□	Deleting	☒
Other (specify):			

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

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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

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

☒	Identifiability	Provide explanation: The system contains identifying numbers including sensitive PII; extensive general personal data and work-related data; several distinguishing features/biometrics; and system administration and audit data.
☒	Quantity of PII	Provide explanation: The quantity of PII will be determined by the amount of legal correspondence that employees determine appropriate for transfer into LDMS-C (as duplicates). PII is incidental and will not be the norm for most of the records in LDMS-C. We estimate that the quantity of records that contain PII will be low and intend to minimize the collection of PII in the system.
☒	Data Field Sensitivity	Provide explanation: LDMS-C may inadvertently contain PII/BII data. The combination of the data in the fields identified in section 2.1 could together make the data fields more sensitive.
☒	Context of Use	Provide explanation: LDMS-C is a document repository for exclusive OGC use to disseminate legal guidance and advice regarding the USPTO mission to other OGC colleagues.
☒	Obligation to Protect Confidentiality	Provide explanation: NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security controls for protecting PII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M); Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: The data is stored in the Microsoft Azure U.S. Government cloud and is protected by FedRAMP privacy and security controls.
☐	Other:	Provide explanation:

<u>Section 12</u>: 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.)

System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zones within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

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:
☒	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:
☒	No, the conduct of this PIA does not result in any required technology changes.