Template Version Number: 01-2020

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

## Privacy Impact Assessment
## for the
## VASTEC Data Conversion System (DCS)

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

Lisa Martin
for Dr. Jennifer Goode 06/28/2021

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

# U.S. Department of Commerce Privacy Impact Assessment
# USPTO VASTEC Data Conversion System (DCS)

**Unique Project Identifier: PTOC-012-00**

**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.*

The VASTEC Data Conversion System (DCS) has been implemented in support of the Continuous Data Conversion (CDC) and Backfile/Pre-1971 Patent Conversion projects. The purpose of the system is to transform electronic Tagged Image File Format (TIFF) images of patent application documents to Extensible Markup Language (XML) documents based on a predefined XML schema. The files in the new XML format allow patent examiners to search, manage, and manipulate different document types, using examination tools under development.

VASTEC receives a USPTO bundle of document files for batch process in the Tampa VASTEC DCS through Secured File Transfer Protocol (SFTP). After the conversion is performed the output is returned to USPTO in a VASTEC bundle. A bundle is the basic unit of recovery point objective in case of failure. The recovery of interrupted processing starts with the last USPTO bundle received, if it is intact. Otherwise the USPTO bundle is retrieved from USPTO.

***(a) Whether it is a general support system, major application, or other type of system***
VASTEC Data Conversion System (DCS) is a Major Application.

***(b) System location***
VASTEC Data Conversion System (DCS) is located at 1101 Channelside Drive, Suite 100 Tampa, Florida

***(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)***
VASTEC Data Conversion System (DCS) is an external contractor system that has been implemented in support of the Continuous Data Conversion (CDC)

***(d) The way the system operates to achieve the purpose(s) identified in Section 4***
The purpose of the system is to transform electronic Tagged Image File Format (TIFF) images of patent application documents into Extensible Markup Language (XML) documents based on a predefined XML schema.

***(e) How information in the system is retrieved by the user***
The files in the new XML format allow patent examiners to search, manage, and manipulate different document types, using examination tools under development.

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

VASTEC Data Conversion System (DCS) receives patent applications directly from the United States Patent and Trademark Office (USPTO). Data transfer between DCS and USPTO is done via a secure transport system. The transfers take place over public internet, from DCS to USPTO through their TIC (trusted internet connection).

***(g) Any information sharing conducted by the system***
DCS shares information within the agency and the private sector. The information provided by USPTO is used by DCS for authorized data conversion activities performed by internal personnel only.

***(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information***
The PII and BII data collected by the USPTO in the patent applications is to enable identification of the inventory and facilitate the patent application process. It is provided to DCS so that data conversion activities can be performed on the collected patent application. The legal authority to collect PII and/or BII derives from 35 U.S.C. 1, 2, 6, and 115; 5 U.S.C. 301 (SORN COMMERCE/PAT-TM-7).

***(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system***
The Federal Information Processing Standard (FIPS) 199 security impact category for the system is 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 (version 01-2015 or

01-2017).

☒ 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 01-2019 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 | ☐ | 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: | | | | | |

| **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. Gender | ☐ | k. Telephone Number | ☒ | r. Criminal Record | ☐ |
| e. Age | ☐ | l. Email Address | ☒ | s. Physical Characteristics | ☐ |
| 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): | | | | | |

| **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.

| |
|---|
| VASTEC Data Conversion System (DCS) receives patent applications directly from the United States Patent and Trademark Office (USPTO). Data transfer between DCS and USPTO is done via a secure transport system. The transfers take place over public internet, from DCS to USPTO through their TIC (trusted internet connection). The connectivity is automated via folders that were established on both ends. When establishing the transfer mechanism, a user account/password was established on both sides as well as an SSL certificate exchange. Therefore, DCS will only accept connections from PTO that come from the proper IP address, have the correct username/password, and provides the proper certificate. The same exists for traffic coming from DCS to PTO. |

2.4 Is the information covered by the Paperwork Reduction Act?

| | |
|---|---|
| ☒ | Yes, the information is covered by the Paperwork Reduction Act.<br>Provide the OMB control number and the agency number for the collection.<br>0651-0031 Patent Processing<br>0651-0032 Initial Patent Application |
| ☐ | 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): | | | |

| | |
|---|---|
| ☒ | 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).

This PII and BII data is collected by the USPTO to enable identification of the inventory and facilitate the patent application process. VASTEC DCS does not store any data after processing and it is directly transmitted back to USPTO. The PII/BII comes from persons applying for patents through the USPTO. This could include federal employees, contractors, members of the public or foreign nationals.

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.)

| |
|---|
| Foreign entities and insider threats are the predominant threats to the system. DCS connects to the USPTO File Transfer system which is a part of the NSI Master System. In accordance with the USPTO Privacy Policy guidelines, the DCS system is designed and administered to ensure the confidentiality of PII provided to DCS by USPTO. Specific safeguards that are employed by the DCS system to protect the patent applications include: • The DCS system and its facility are physically secured and closely monitored. Only individuals authorized by DCS to access USPTO data are granted logical access to the system. • All patent information is encrypted when transferred between DCS and USPTO using secure electronic methods. • Technical, operational, and management security controls are in place at DCS and are verified regularly. • Periodic security testing is conducted on the DCS system to help assure than any new security vulnerabilities are discovered and fixed. • All DCS personnel are trained to securely handle patent information, insider threats and to understand their responsibilities for protecting patents |

## 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 | ☐ | ☒ | ☐ |
| 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.<br>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:<br><br>DCS connects to the USPTO File Transfer system which is a part of the NSI Master System.<br><br>In accordance with the USPTO Privacy Policy guidelines, the DCS system is designed and administered to ensure the confidentiality of PII provided to DCS by USPTO. Specific safeguards that are employed by the DCS system to protect the patent applications include: • The DCS system and its facility are physically secured and closely monitored. Only individuals authorized by DCS to access USPTO data are granted logical access to the system. • All patent information is encrypted when transferred between DCS and USPTO using secure electronic methods. • Technical, operational, and management security controls are in place at DCS and are verified regularly. • Periodic security testing is conducted on the DCS system to help assure than any new security vulnerabilities are discovered and fixed. • All DCS personnel are trained to securely handle patent information and to understand their responsibilities for protecting patents |
| ☐ | 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: _____. | |
| ☒ | Yes, notice is provided by other means. | Specify how:<br>Notice is provided at the time of collection by the patent front – end systems. |

| | | |
|---|---|---|
| ☐ | 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: Individuals may have the opportunity to decline to provide their PII/BII within the DCS system; however, the information is needed for successful processing of the patent application. That option would be offered by the primary patent application ingress system, which is covered under the system of records at USPTO: COMMERCE/PAT/TM-7 |

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: Individuals may have the opportunity to consent to particular uses of their PII/BII within the DCS system. That option would be offered by the primary patent application ingress system, which is covered under the system of records at USPTO: COMMERCE/PAT/TM-7, Patent Application Files. That information is volunteered by individuals as a part of the patent application process. The PII/BII contained in this information is needed for successful processing of the patent application |

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: Individuals have an opportunity to review/updated PII/BII pertaining to them up to and before the Patent application is published and finalized. That option would be offered by the primary patent application ingress system, which is covered under the system of records at USPTO: COMMERCE/PAT/TM-7, Patent Application Files. |
| ☐ | 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. |
| ☒ | 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.<br>Explanation: Audit records are reviewed daily as part of the daily system log review. |
| ☒ | The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.<br>Provide date of most recent Assessment and Authorization (A&A): 9/30/2020_____<br>☐ 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 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). |
| ☒ | 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).*

| |
|---|
| Access to the system and data are limited to system administrators and software developers. Data is received, processed, and returned. This is usually within four hours. All transfers of data between DCS and USPTO occur over a FIPS 140-2 certified secure file transport system |

## 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).<br>Provide the SORN name, number, and link. *(list all that apply)*:<br><br>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (list all that apply):<br><br>Patent Application Files. (Note: This notice is broken down, where indicated, into three subsystems relating to the status of the files: a. Pending; b. Abandoned; and c. Patented.).COMMERCE/PAT/TM-7 |
| ☐ | 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.)*

| | |
|---|---|
| ☒ | There is an approved record control schedule.<br>Provide the name of the record control schedule:<br>Patent Granting and Maintenance (N1-241-10-1) |
| ☐ | No, there is not an approved record control schedule.<br>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: Occupation, name, title, address, phone number, & email address are all non-sensitive identifiers. |
| ☒ | Quantity of PII | Provide explanation: PII is only on the system for the time it takes to process and return to USPTO. The amount of PII is very minimal. |
| ☒ | Data Field Sensitivity | Provide explanation: Non Sensitive. Items listed in the Identifiability section are all publically available information. |
| ☒ | Context of Use | Provide explanation: Information is for identifying and tracking patent applicants/applications |
| ☒ | Obligation to Protect Confidentiality | Provide explanation: Data Privacy Act of 1974 |
| ☒ | Access to and Location of PII | Provide explanation: The information containing PII must be transmitted outside of the USPTO environment, there is an added need to ensure the confidentiality of information during transmission. |
| ☐ | 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.)

| |
|---|
| Insider threats and Adversarial entities are the predominant threat to the information system. In accordance with the USPTO Privacy Policy guidelines, the DCS system is designed and administered to ensure the confidentiality of PII provided to DCS by USPTO. Specific safeguards to mitigate threats to privacy that are employed by the DCS system to protect the patent applications include: The DCS system and its facility are physically secured and closely monitored. Only individuals authorized by DCS to access USPTO data are granted logical access to the system. All patent information is encrypted when transferred between DCS and USPTO using secure electronic methods. Technical, operational, and management security controls are in place at DCS and are verified regularly. Periodic security testing is conducted on the DCS system to help assure than any new security vulnerabilities are discovered and fixed. All DCS personnel are trained to securely handle patent information, insider threats and to understand their responsibilities for protecting patents. The type or quantity of information collected and the sources providing the information is done prior to DCS involvement. DCS converts the information given to them by USPTO and is not privy to the decision making process within USPTO regarding information collected. |

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

| | |
|---|---|
| ☐ | Yes, the conduct of this PIA results in required business process changes.<br>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.<br>Explanation: |
| ☒ | No, the conduct of this PIA does not result in any required technology changes. |