Privacy Impact Assessment
for the
Eighth Day Design Facilities Management System (FMS)

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

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer 12/08/2021
U.S. Department of Commerce Privacy Impact Assessment
USPTO Eighth Day Design Facilities Management System (FMS)

Unique Project Identifier:  PTOC-028-00

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.

Facilities Management System (FMS) is a web-based application information system. The FM:Systems suite of Digital Workplace Solutions automates workflows, streamlines employee interactions, encourages collaboration, enhances productivity and delivers strategic insight on opportunities for the organization to grow and adapt. FMS:Workplace is the foundation of the digital workplace with extensive options for strategic planning, comprehensive space and move management and robust capabilities for facility maintenance. Eighth Day Design (EDD) is the prime contractor hired by USPTO to provide a facilities management solution. EDD leverages the application and hosting services of FM:Systems, Inc. who provides a SaaS model for hosting the FM:Interact application.

FM:Interact features an intuitive interface to provide quick and easy access to key facilities information such as floor plans, reports, employee information and critical documents. Through this tool, USPTO users can:

- Access property information with a simple point and click map-based interface
- Run live reports, view floor plans, search archived drawing, and critical documents
- Share facility data with management, partners, and internal customers via corporate intranet
- Dynamically search for employees and related information
- Streamline the helpdesk, work order, and move processes

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

(b) System location
FMS is located at 99 TW Alexander Drive, Morrisville, NC 27560 (primary)

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
FMS connects to Network and Security Infrastructure System (NSI). 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 United States Patent and Trademark Office (USPTO) IT applications.
(d) The way the system operates to achieve the purpose(s) identified in Section 4
FMS is a web-based application that resides at the FM:Systems Hosting Facility. Access to the application is by HTTPS protocol.

(e) How information in the system is retrieved by the user
Access to the application is through a web-based interface that utilizes the HTTPS protocol and encryption and authentication is done using the TLS/SSL protocol.

(f) How information is transmitted to and from the system
The import files for data feeds are delivered through secure FTP, limited to designated users. The typical DBMS configuration is a shared instance which is isolated by a logical database per Client.

(g) Any information sharing conducted by the system
USPTO users can access the information on the system for use to review property information with a simple point and click map-based interface. It is also used to share facility data with management, USPTO contractors, and internal customers via the intranet.

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

(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.)

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
<tr>
<td>d. Significant Merging</td>
</tr>
<tr>
<td>e. New Public Access</td>
</tr>
<tr>
<td>f. Commercial Sources</td>
</tr>
<tr>
<td>g. New Interagency Uses</td>
</tr>
<tr>
<td>h. Internal Flow or Collection</td>
</tr>
<tr>
<td>i. Alteration in Character of Data</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify):</td>
</tr>
</tbody>
</table>
☐ 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.)*

<table>
<thead>
<tr>
<th>Identifying Numbers (IN)</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>b. Taxpayer ID</td>
<td>☐</td>
<td>g. Passport</td>
<td>☐</td>
<td>k. Financial Transaction</td>
<td>☐</td>
</tr>
<tr>
<td>c. Employer ID</td>
<td>☐</td>
<td>h. Alien Registration</td>
<td>☐</td>
<td>l. Vehicle Identifier</td>
<td>☐</td>
</tr>
<tr>
<td>d. Employee ID</td>
<td>☒</td>
<td>i. Credit Card</td>
<td>☐</td>
<td>m. Medical Record</td>
<td>☐</td>
</tr>
<tr>
<td>e. File/Case ID</td>
<td>☐</td>
<td>n. Other identifying numbers (specify):</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n. Other identifying numbers (specify):</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

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

<table>
<thead>
<tr>
<th>Work-Related Data (WRD)</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Occupation</td>
<td>☐</td>
<td>e. Work Email Address</td>
<td>☒</td>
<td>i. Business Associates</td>
<td>☐</td>
</tr>
<tr>
<td>b. Job Title</td>
<td>☐</td>
<td>f. Salary</td>
<td>☐</td>
<td>j. Proprietary or Business Information</td>
<td>☒</td>
</tr>
</tbody>
</table>
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. UserID ☒
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**

<table>
<thead>
<tr>
<th>In Person</th>
<th>Hard Copy: Mail/Fax</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Telephone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

| Other(specify): |

**Government Sources**

<table>
<thead>
<tr>
<th>Within the Bureau</th>
<th>Other DOC Bureaus</th>
<th>Other Federal Agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>☒</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State, Local, Tribal</th>
<th>Foreign</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

Other (specify): Source files received from PALM system and HR systems with limited information and placed in secured folder. Source plans received from contractors.

**Non-government Sources**

<table>
<thead>
<tr>
<th>Public Organizations</th>
<th>Private Sector</th>
<th>Commercial Data Brokers</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>
2.3 Describe how the accuracy of the information in the system is ensured.

The accuracy is ensured by validating with floor walks, moves, department administration and working with HR and PALM administrators. From an administrative perspective, the FMS application has administrative and support staff that function as points of contact whereby users may directly contact for the administration of information accuracy. From a technical implementation, USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information.

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.)

<table>
<thead>
<tr>
<th>Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Cards □</td>
</tr>
<tr>
<td>Biometrics □</td>
</tr>
<tr>
<td>Caller-ID □</td>
</tr>
<tr>
<td>Personal Identity Verification (PIV) Cards □</td>
</tr>
<tr>
<td>Other (specify):</td>
</tr>
</tbody>
</table>

☒ 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.)

<table>
<thead>
<tr>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio recordings □</td>
</tr>
<tr>
<td>Building entry readers □</td>
</tr>
<tr>
<td>Video surveillance □</td>
</tr>
<tr>
<td>Electronic purchase transactions □</td>
</tr>
<tr>
<td>Other (specify):</td>
</tr>
</tbody>
</table>
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.)

<table>
<thead>
<tr>
<th>Purpose</th>
<th></th>
<th>Purpose</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>For a Computer Matching Program</td>
<td></td>
<td>For administering human resources programs</td>
<td></td>
</tr>
<tr>
<td>For administrative matters</td>
<td></td>
<td>To promote information sharing initiatives</td>
<td></td>
</tr>
<tr>
<td>For litigation</td>
<td>☒</td>
<td>For criminal law enforcement activities</td>
<td></td>
</tr>
<tr>
<td>For civil enforcement activities</td>
<td></td>
<td>For intelligence activities</td>
<td></td>
</tr>
<tr>
<td>To improve Federal services online</td>
<td></td>
<td>For employee or customer satisfaction</td>
<td>☒</td>
</tr>
<tr>
<td>For web measurement and customization technologies (single-session)</td>
<td></td>
<td>For web measurement and customization technologies (multi-session)</td>
<td></td>
</tr>
<tr>
<td>Other (specify):</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 information in the system is about PTO employees and contractors. Information is transmitted to the system through a secured file transfer protocol to the hosted server. The application bases personnel information table relations on the Employee ID, which is used in restricted views and reports based on Roles. USPTO users can access the information on the system for use to review property information with a simple point and click map-based interface. It is also used to share facility data with management, partners, and internal customers via the intranet. The services provided by FMS help the facility management crew act on service request faster and more efficiently thereby increasing employee satisfaction and comfort.

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.)

Information is maintained for only active personnel at USPTO. All system users undergo annual IT security training. Foreign entities, adversarial entities and insider threats are the threats to privacy within this system. Inadvertent private information exposure is a risk and USPTO has policies, procedures, and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires Annual Security Awareness Training for all employees as well as policies and procedures documented in the Cybersecurity Baseline Policy. All USPTO offices adhere to USPTO Records Management Office’s Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

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.)

<table>
<thead>
<tr>
<th>Recipient</th>
<th>How Information will be Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Case-by-Case</td>
</tr>
<tr>
<td>Within the bureau</td>
<td>☒</td>
</tr>
<tr>
<td>DOC bureaus</td>
<td></td>
</tr>
<tr>
<td>Federal agencies</td>
<td></td>
</tr>
<tr>
<td>State, local, tribal gov’t agencies</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Private sector</td>
<td></td>
</tr>
<tr>
<td>Foreign governments</td>
<td></td>
</tr>
<tr>
<td>Foreign entities</td>
<td></td>
</tr>
<tr>
<td>Other (specify):</td>
<td></td>
</tr>
</tbody>
</table>

☐ 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:

☒ 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.)

<table>
<thead>
<tr>
<th>Class of Users</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>General Public</td>
<td>☐</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government Employees</td>
<td></td>
<td>☒</td>
<td></td>
</tr>
<tr>
<td>Contractors</td>
<td></td>
<td>☒</td>
<td></td>
</tr>
<tr>
<td>Other (specify):</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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: ___See Appendix A: Warning Banner___________.

☐ Yes, notice is provided by other means. Specify how:

☐ 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: Any opportunity to decline would be provided by the source systems of HR and PALM that initially collect the PII/BII. PII Data is then disseminated by HR and
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: Any opportunity to consent to particular uses of PII/BII would be provided by the source systems of HR and PALM that initially collect the PII/BII. PII/BII data is collected and maintained by HR and PALM and then disseminated to FMInteract via exported reports.

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: Any opportunity to review/update PII/BII would be provided by the source systems of HR and PALM that initially collect the PII/BII. PII/BII data is collected and maintained by HR and PALM and then disseminated to FMInteract via exported reports.

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: Audit logs.

☒ 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): 05/14/2021

☐ 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).*

The following functions are used to protect PII/BII on the IT system: SFTP, encryption of any password used with UserID, firewalls, and Group Policy security on File Folders maintaining the source files.

Management Controls:
- The USPTO uses the Life Cycle review process to ensure that management controls are in place for FMS. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address the management, operational and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency checks on all personnel, including contractor staff.

Operational Controls:
- Automated operational controls include securing all hardware associated with IDSS in the USPTO Data Center. The Data Center is controlled by access card entry and is manned by a uniformed guard service to restrict access to the servers, their Operating Systems and databases. Contingency planning has been prepared for the data. Backups are performed on the processing databases. Backups are stored on tape and are secured off-site. Additional operation controls include (1) Logical edit checks to ensure proper sequence of actions; (2) Physical terminal identification; (3) Database User ID; (4) Restricted data display, as required; and (5) Restricted access.
- Manual procedures shall be followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:
  - Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.
  - Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased and that this activity is recorded on the log.
  - Obtain management concurrence in the log, if an extract aged over 90 days is still required.
  - Store all PII data extracts maintained on a USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private network (VPN).
  - Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

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):* 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.)*

| ☑ | There is an approved record control schedule. Provide the name of the record control schedule: GRS 5.4: items 010, 020, 030, 040, 050, 051, 060, 070, 071 Facility, Equipment, Vehicle, Property, and Supply Records. GRS 5.8 items 010. Administrative Help Desk 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: Discovery |
| ☑ | 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.)*

<table>
<thead>
<tr>
<th>Disposal</th>
<th>Shredding</th>
<th>☐</th>
<th>Overwriting</th>
<th>☑</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degaussing</td>
<td>☐</td>
<td>Deleting</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Other(specify):</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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: FMS collects, maintains, or disseminates PII about DOC employees and contractors. The types of information collected, maintained, used or disseminated by the system include FMS employee ID, USPTO email, phone number, department information and a location for USPTO personnel. When combined, this large data set uniquely and directly identifies individuals.

- **Quantity of PII**
  
  Provide explanation: The quantity of data could be as large as 10,000 to include all employees imported from PALM if tied to a seat on campus. Although the data set collected is large, the number of data items collected is limited to government and government contractors within the bureau. If loss, theft, or compromise, there would be limited collective harm to individuals, the organization, or cost to the organization in addressing the breach.

- **Data Field Sensitivity**
  
  Provide explanation: The data includes limited PII which when combined will not make the data fields more sensitive.

- **Context of Use**
  
  Provide explanation: Data is related to key facilities information such as floor plans, reports, employee information, and critical data. Disclosure of PII itself is unlikely to result in harm to the individual or organization.

- **Obligation to Protect Confidentiality**
  
  Provide explanation: Based on the data collected, USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974 and USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance with NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. These government-wide privacy laws, regulations and mandates that have been put in place to protect the individual and the organization.

- **Access to and Location of PII**
  
  Provide explanation: Access to FMS is limited only to the identified and authenticated users.
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.)

In addition to insider threats, activity which may raise privacy concerns include the collection, maintenance, and dissemination of PII in the form of name and personal and work name, telephone number and email address as well as user ID and date/time access. USPTO mitigates such threats through mandatory training for system users regarding appropriate handling of information and automatic purging of information in accordance with the retention schedule.

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.
Appendix A: Warning Banner

This is a government computer system and is intended for official and other authorized use only. Unauthorized access or use of the system is prohibited and subject to administrative action, civil, and criminal prosecution under 18 USC 1030. All data contained on this information system may be monitored, intercepted, recorded, read, copied, or captured and disclosed by and to authorized personnel for official purposes, including criminal prosecution. You have no expectations of privacy regarding monitoring of this system. Any use of this computer system signifies consent to monitoring and recording, and compliance with USPTO policies and their terms.

FM: Systems Privacy Policy
## USPTO Points of Contact and Signatures

### System Owner
Name: Melissa Fatni  
Office: Office of Administrative Services (C/OAS)  
Phone: (571) 270-5234  
Email: Melissa.Fatni@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

**Signature:**  
**Date signed:**

### Chief Information Security Officer
Name: Don Watson  
Office: Office of the Chief Information Officer (OCIO)  
Phone: (571) 272-8130  
Email: Don.Watson@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

**Signature:**  
**Date signed:**

### Privacy Act Officer
Name: Ezequiel Berdichevsky  
Office: Office of General Law (G/GLO)  
Phone: (571) 270-1557  
Email: ezequiel.berdichevsky@uspto.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

**Signature:**  
**Date signed:**

### Bureau Chief Privacy Officer and Co-Authorizing Official
Name: Henry J. Holcombe  
Office: Office of the Chief Information Officer (OCIO)  
Phone: (571) 272-9400  
Email: Jamie.Holcombe@uspto.gov

I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.

**Signature:**  
**Date signed:**

### Co-Authorizing Official
Name: Frederick W. Steckler  
Office: Office of the Chief Administrative Officer (OCAO)  
Phone: (571) 272-9600  
Email: Frederick.Steckler@uspto.gov

I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.

**Signature:**  
**Date signed:**

---

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.