Template Version Number: 01-2020

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

Privacy Threshold Analysis
for the
Eighth Day Design Facilities Management System (FMS)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Eighth Day Design Facilities Management System (FMS)

Unique Project Identifier: PTOC-028-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 purpose that the system is designed to serve

FMS features an intuitive interface to provide quick and easy access to key facilities information such as floor plans, reports, employee information, and critical data.

e) The way the system operates to achieve the purpose

FMS is a web-based application that resides at the FM: Systems Hosting Facility. Access to the application is by HTTPS protocol.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

FMS provides information such as floor plans, reports, employee information and critical documents.

g) Identify individuals who have access to information on the system

USPTO staff are assigned roles based on their duty in order to support the system's mission.

h) 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.

i) 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☐ This is a new information system. *Continue to answer questions and complete certification.*

☒ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

☐ 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). *Continue to answer questions and complete certification.*

☐ 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). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☐ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☒ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to

those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☒ Yes, the IT system collects, maintains, or disseminates BII.

☐ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- ☒ DOC employees
- ☒ Contractors working on behalf of DOC
- ☐ Other Federal Government personnel
- ☐ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☒ Yes, use will cause the assignment of a higher PII confidentiality impact level.

☐ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the **Eighth Day Design Facilities Management System (FMS)** and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the **Eighth Day Design Facilities Management System (FMS)** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Melissa Fatni Office: Office of Administrative Services (C/OAS) Phone: (571) 270-5234 Email: Melissa.Fatni@uspto.gov Signature: Users, Fatni, Melissa Digitally signed by Users, Fatni, Melissa Date: 2021.11.10 13:49:27 -05'00' 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 Signature: DON R Watson Digitally signed by DON R Watson Date: 2021.11.10 21:48:08 -05'00' Date signed: _____
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (G/GLO) Phone: (571) 270-1557 Email: ezequiel.berdichevsky@uspto.gov Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2021.11.03 15:49:50 -04'00' 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 Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2021.11.12 17:14:09 -05'00' 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 Signature: Users, Steckler, Frederick W. Digitally signed by Users, Steckler, Frederick W. Date: 2021.11.16 17:53:19 -05'00' Date signed: _____	