

**U.S. Department of Commerce
National Institute of Standards and Technology
(NIST)**



**Privacy Threshold Analysis
for the
Manufacturing Extension Partnership (MEP) Enterprise
Information System (480-01)**

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 480-01

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 of the information system in a way that a non-technical person can understand.*

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).

The Hollings Manufacturing Extension Partnership (MEP) is a nationwide network of not-for-profit Centers in multiple locations in all 50 states and Puerto Rico, whose purpose is to provide small and medium sized manufacturers with the help they need to succeed in today’s competitive world. Each Center works directly with area manufacturers to provide expertise and services tailored to their most critical needs. MEP’s mission is supported by the following components:

- The MEP Enterprise Information System (MEIS) accepts, processes, and reports on center performance, center activities, partners, financial management, and project management activities. The component contains information maintained for statistical research or reporting purposes.
- MEP Connect allows MEP to collaborate with the MEP Center system by accepting, processing, and providing Center knowledge sharing activities (communities of practice and MEP University) for MEP Centers and other partners.
- The MEP Survey component is used to perform mandated quarterly data collection from MEP client companies on the impacts of services received. The MEIS shares data with the MEP Survey, and all survey responses are imported back into MEIS and attributed to a specific center, client company, and project(s).

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

The MEP System is a general support system

b) *System location*

The MEIS and MEP Connect components are located at the NIST Gaithersburg, Maryland facility within the continental United States. The MEP Survey component utilizes storage

services in Arlington, Virginia, and Rockville, Maryland.

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

MEIS is a standalone system with interconnections: (1) An interconnection exists with Dunn & Bradstreet's database of U.S. manufacturing firms. This is covered under a Cooperative Agreement with State Science and Technology Institute (SSTI) with a sub-contract to Dunn & Bradstreet. (2) An interconnection exists with MEP Center's customer relationship management web services to allow the centers to electronically submit required reporting and survey data to NIST MEP quarterly. These are periodic connections.

MEP Connect is a standalone system.

MEP Survey is a standalone system.

Information is shared between MEIS and MEP Survey, but data is exported, securely transmitted, and imported between systems. See (f) below.

- d) *The purpose that the system is designed to serve*

MEP's purpose is to provide small and medium sized manufacturers with the help they need to succeed in today's competitive world. Each Center works directly with area manufacturers to provide expertise and services tailored to their most critical needs. All systems support MEP's mission.

- e) *The way the system operates to achieve the purpose*

MEIS: Information is entered or provided by the MEP Centers electronically via the internet. Additional information is entered or provided by the MEP Program staff. Data is validated and summarized by the system and reviewed and analyzed by the MEP Program staff. Summaries and reports are made available to the MEP Centers and MEP Program staff.

MEP Connect: MEP Centers and other partners access the portal to share or obtain knowledge and best practices, or to participate in training.

MEP Survey: Data is collected through a web survey, either entered directly by the respondent or by a telephone interviewer if the respondent chooses this method.

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

The type of information is manufacturing technology focused. Additional types of information include: identifying numbers, general personal data, work related data, and system administration/audit data.

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

MEIS and MEP Survey: Only authorized NIST users and MEP Centers have access to the information.

MEP Connect: MEP Centers and other partners access the portal to share or obtain knowledge and best practices, or to participate in training.

h) *How information in the system is retrieved by the user*

MEIS: Some information is retrieved by searching, some by menu/navigation. Summaries and reports are made available to the MEP Centers and MEP Program staff.

MEP Connect: Information is retrieved by menu/navigation and search.

MEP Survey: Some information is retrieved by searching, some by menu/navigation. Summaries and reports are made available to the MEP Centers and MEP Program staff.

i) *How information is transmitted to and from the system*

MEIS and MEP Survey: NIST’s secure file transfer service (nfiles.nist.gov) is used for encryption of ad hoc data that is transferred by email to MEP Centers, Survey Contractors.

Questionnaire:

1. 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 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 later).
Skip questions and complete certification.

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. *Please describe the activities which may raise privacy concerns.*

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 about: *(Check all that apply.)*

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

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

DOC employees

Contractors working on behalf of DOC

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 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.

4c. 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, the context of 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, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the **Manufacturing Extension Partnership (MEP) Enterprise Information System** 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 **Manufacturing Extension Partnership (MEP) Enterprise Information System** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

Chancy Lyford

Signature of SO: JOHN LYFORD Digitally signed by JOHN LYFORD
Date: 2019.05.30 13:12:49 -04'00' Date: 5/30/2019

Name of Information Technology Security Officer (ITSO):

K. Robert Glenn

Signature of ITSO: KENNETH GLENN Digitally signed by KENNETH GLENN
Date: 2019.06.13 10:29:48 -04'00' Date: 6/13/2019

Name of Co-Authorizing Official (AO):

Carroll A. Thomas

Signature of AO: CARROLL THOMAS Digitally signed by CARROLL THOMAS
Date: 2019.06.11 09:06:55 -04'00' Date: _____

Name of Co-Authorizing Official (AO)/Bureau Chief Privacy Officer (BCPO):

Susannah Schiller, Acting SUSANNAH

Signature of AO/BCPO: SCHILLER Digitally signed by SUSANNAH
SCHILLER Date: 2019.06.13 12:56:10 -04'00' Date: 6/13/2019