Version Number: 01-2019

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

Privacy Threshold Analysis
for the
480-01 MEP Enterprise Information System (MEIS)

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 (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).

a) Whether it is a general support system, major application, or other type of system
b) System location
c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
d) The purpose that the system is designed to serve
e) The way the system operates to achieve the purpose
f) A general description of the type of information collected, maintained, use, or disseminated by the system
g) Identify individuals who have access to information on the system
h) How information in the system is retrieved by the user
i) How information is transmitted to and from the system

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 or topic area groups) 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 facility within the continental United States.
1. **The MEP Survey component utilizes storage services in Arlington, Virginia; Rockville, Maryland; Chicago, Illinois; and Dallas/Ft. Worth, Texas.**
2. **The MEIS and MEP Connect components are located at the NIST Gaithersburg, 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 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 web services using provided Application Programming Interface (API) calls. These are periodic connections that exists only to extract specific data elements into MEIS at predefined times throughout the year. It is only possible to collect specific predefined data elements from these systems. The MEIS to MEP Survey is an export/import of data in and out of both systems.

MEP Connect is a standalone system.

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. The status of this information system:
   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 01-2017 or later).
   (Skip questions and complete certification).

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks:

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.

Activities
Other activities which may raise privacy concerns:

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.)."

4. Personally Identifiable Information (PII)

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

   The IT system collects, maintains, or disseminates PII about:

   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?

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.

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

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.

Is a PIA Required?	**Yes**

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 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 480-01 MEP Enterprise Information System (MEIS) 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 480-01 MEP Enterprise Information System (MEIS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Chancy Lyford

Signature of SO: JOHN LYFORD Digitally signed by JOHN LYFORD Date: 2021.01.25 10:21:14 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Blair Heiserman

Signature of ITSO: _____ Digitally signed by BLAIR HEISERMAN Date: 2021.01.25 14:23:14 -05'00' Date: _____

Name of Privacy Act Officer (PAO):

Catherine Fletcher

Signature of PAO: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2021.01.19 08:56:50 -05'00' Date: _____

Name of Co-Authorizing Official (Co-AO):

Robert Ivester

Signature of Co-AO: ROBERT IVESTER Digitally signed by ROBERT IVESTER Date: 2021.01.22 18:38:57 -05'00' Date: _____

Name of Co-Authorizing Official (Co-AO):

Chandan Sastry

Signature of Co-AO: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2021.01.16 12:55:44 -05'00' Date: _____

Name of Acting Bureau Chief Privacy Officer (BCPO):

Matt Wilkinson

Signature of Acting BCPO: MATTHEW WILKINSON Digitally signed by MATTHEW WILKINSON Date: 2021.01.26 09:24:56 -05'00' Date: _____