Version Number: 01-2019

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

Privacy Impact Assessment
for the
480-01 MEP Enterprise Information System (MEIS)

Reviewed by: Matt Wilkinson, Acting 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

Jennifer Goode 03/09/2021

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

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

Unique Project Identifier: 480-01

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.

(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 way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(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

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
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; Washington, District of Columbia; Chicago, Illinois; and Dallas/Ft. Worth, Texas.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
MEIS: (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 way the system operates to achieve the purpose(s) identified in Section 4
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.

e) 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.

f) 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.

g) Any information sharing conducted by the system
Information sharing internally with other NIST business units is by export of data that is analyzed by MEP Staff and reports or statistics are provided. There may also be some users from other NIST business units that have an account and can run reports or search for information. There are no automated interconnections to retrieve data.

h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information.
The National Institute of Standards and Technology Act, as amended, 15 U.S.C. 271 et seq. (which includes Title 15 U.S.C. 272) and section 12 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended, 15 U.S.C. 3710a. 15 U.S.C. 290; 15 U.S.C. 7301 et seq.; 42 U.S.C. 15441-15453.

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system is **Moderate.**

Section 1: Status of the Information System

1.1 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).

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

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated.

Identifying Numbers (IN)
Employee ID
File/Case ID
Other identifying numbers
Other identifying numbers:

NAICS and DUNS (Dunn & Bradstreet)
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

General Personal Data (GPD)
Name
Home Address
Telephone Number
Email Address
Other General Personal Data
Other general personal data:
Identifying Number, DUNS (Dunn & Bradstreet)

Work-Related Data (WRD)
Job Title
Work Address
Work Telephone Number
Work Email Address
Business Associates
Other work-related data:

Distinguishing Features/Biometrics (DFB)
Other distinguishing features/biometrics:

System Administration/Audit Data (SAAD)
User ID
IP Address
Date/Time of Access
Queries Run
Other system administration/audit data
Other system administration/audit data:
Queries/reports run are logged in MEIS.

Other Information

2.2 Indicate sources of the PII/BII in the system.

Directly from Individual about Whom the Information Pertains
Telephone
Hard Copy - Mail/Fax
Online
Other
Other:
MEP Survey can allow for backup mail/fax method of submitting a survey, but normal modes are web and telephone.

Government Sources

Other:

Non-government Sources
Public Organizations **Private Sector** **Commercial Data Brokers**
Other:

2.3 Describe how the accuracy of the information in the system is ensured.

Data is validated and summarized by the MEP Centers and reviewed and analyzed by the MEP staff. Integrity controls have been assessed as defined in NIST Special Publication 800-53.

2.4 Is the information covered by the Paperwork Reduction Act?

Yes, the information is covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:
OMB Control No. 0693-0032 (MEIS) **OMB Control No. 0693-0021 (MEP Survey)**

2.5 Is there any technology used that contain PII/BII in ways that have not been previously deployed?

No

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)
Other:

Section 3: System Supported Activities

3.1 Are there any IT system supported activities which raise privacy risks/concerns?

No

The IT system supported activities which raise privacy risks/concerns.

Activities
Other:

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.

Purpose
For administrative matters **For employee or customer satisfaction**

Other:

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 MEP Survey collects information to evaluate the performance of the MEP Centers and the MEP Program.

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.)

The potential privacy threats to the information includes the insider threat. The insider threat is addressed through segregation of duties and role-based access.

Section 6: Information Sharing and Access

6.1 Will the PII/BII in the system be shared?

Yes, the PII/BII in the system will be shared

The recipients the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

Bulk Transfer - DOC bureaus **Case-by-Case - DOC bureaus** **Case-by-Case – Within the bureau**
Other:

6.2 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.
The name of the IT system and description of the technical controls which prevent PII/BII leakage:
NIST 188-01, Platform Services System, Customer Relationship Management (CRM) Component (MEP Center Owned) **Dunn & Bradstreet (Selectory Database Web Services)** **Technical controls include those identified as FIPS-199 moderate for confidentiality.**

6.3 Identify the class of users who will have access to the IT system and the PII/BII.

Class of Users
Government Employees **Contractors** **Other (specify)**
Other:
MEP Centers who have a Cooperative Agreement with NIST MEP to provide services to U.S. Small Manufacturers.

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.

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.** **Yes, notice is provided by other means.**
The Privacy Act statement and/or privacy policy can be found at:
The Privacy Act statement and/or privacy policy can be found at: **https://www.nist.gov/public_affairs/privacy.cfm and** **https://meis.nist.gov/_layouts/MEIS/Public/MEPLogin.aspx?ReturnUrl=%2f**
The reason why notice is/is not provided:
For MEIS, Centers are provided with the NIST MEP Reporting Guidelines which includes information about how the collection is maintained and disseminated.

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.
The reason why individuals can/cannot decline to provide PII/BII:
For MEIS, MEP Centers have opportunity to decline inputting information pertaining to their Center. However, doing so may affect the outreach conducted by the Center and associated Center performance metrics. **For MEP Connect, individuals have opportunity to decline to provide information by not registering and thus will not have access to MEP resources that support the mission.** **For MEP Survey, the company representative has opportunity to decline participation in the survey by choosing not to participate when they receive an invitation.**

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.
The reason why individuals can/cannot consent to particular uses of their PII/BII:
For MEIS, Center representatives can comment on the collection process at the annual MEP National Conference and through meetings with user groups. **For MEP Connect, Center representatives can comment on the collection process at the annual MEP National Conference and through meetings with user groups.** **For MEP Survey, Center representatives can comment on the collection process at the annual MEP National Conference and through meetings with user groups.**

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.
The reason why individuals can/cannot review/update PII/BII:
For MEIS, MEP Centers have opportunity to review information pertaining to their Center. Center representatives have accounts in the system and can make changes to some data at any time. Client company data is reviewed quarterly before each survey is administered and corrections are made at that time by the Center. **For MEP Connect, MEP Centers can review information pertaining to their Center. Center representatives have accounts in the system and can make changes to some data at any time. Client company data is reviewed quarterly before each survey is administered and corrections are made at that time by the Center.** **For MEP Survey, data is only changed by MEP staff when sufficient documentation from a center is presented to justify a change in a client's response and submitted to MEP Help Line, 301-975-4778 or mepinfo@nist.gov. This is done to preserve the integrity of the survey process and the answers given by clients.**

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

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.** **The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.**

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 supporting 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 ownership rights over data including PII/BII.

Reason why access to the PII/BII is being monitored, tracked, or recorded:

Access logs are kept and reviewed for anomalies on an as needed basis.

The information is secured in accordance with FISMA requirements.

Is this a new system? No
Below is the date of the most recent Assessment and Authorization (A&A).
04/01/2020

Other administrative and technological controls for the system:

8.2 General description of the technologies used to protect PII/BII on the IT system. *(Includes data encryption in transit and/or at rest, if applicable).*

Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for anomalies on an as needed basis. The MEIS and MEP Connect components are located at the NIST Gaithersburg, Maryland facility within the continental United States. The MEP Survey component utilizes assessed storage services in Arlington, Virginia; Washington, District of Columbia; Chicago, Illinois; and Dallas/Ft. Worth, Texas.

For information sharing, the data transmitted utilizes secure web services using the Transport Layer Security (TLS) protocol, which encrypts communications.

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.

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).

SORN name, number, and link:
COMMERCE/NIST-6: Participants in Experiments, Studies, and Surveys
SORN submission date to the Department:

Section 10: Retention of Information

10.1 Are these records are covered by an approved records control schedule and monitored for compliance?

Yes, there is an approved record control schedule.
Name of the record control schedule:
NIST Records Schedule N1-167-97-1: Manufacturing Extension Partnership (MEP) Program Records
The stage in which the project is in developing and submitting a records control schedule:
Yes, retention is monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:

10.2 Indicate the disposal method of the PII/BII.

Disposal
Shredding **Overwriting** **Deleting**
Other disposal method of the PII/BII:

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.

11.2 The factors that were used to determine the above PII confidentiality impact levels.

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Identifiability **Quantity of PII** **Data Field Sensitivity**	**The data types that are collected and maintained can be used to identify specific individuals and businesses.** **There exists a large volume of Work-Related Data pertaining to Center customers.** **Information collected is work-Related Data**

	about businesses, General Personal Data collected is deemed non-sensitive PII.

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.)

The information collected is about businesses, and contains minimal information about individuals, both of which are non-sensitive. Therefore, threats to privacy is minimal.

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

No, the conduct of this PIA does not result in any required business process changes.
Explanation

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

No, the conduct of this PIA does not result in any required technology changes.
Explanation