Version Number: 01-2017

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

Privacy Impact Assessment
for the
Manufacturing Extension Partnership (MEP) Enterprise Information System (480-01)

Reviewed by: Susannah Schiller, 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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
Date: 2019.08.13 17:27:45 -04'00'

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.

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; 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 periodic connections.

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

MEPConnect is a standalone system. MEP Survey 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

The MEIS shares information with other internal NIST business units.

(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 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.)*

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.
__X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

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.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID	X	i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID	X	g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: NAICS and DUNS for client companies.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X*	o. Medical Information	

d. Gender		j. Telephone Number	X*	p. Military Service	
e. Age		k. Email Address	X*	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					
*Only collected if Sole Proprietor.					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates	X		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run	X	f. Contents of Files	
g. Other system administration/audit data (specify): Queries/reports run are logged in MEIS.					

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					
In Person		Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email			
Other (specify): MEP Survey can allow for backup mail/fax method of submitting a survey, but normal modes are web and telephone.					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	X
Third Party Website or Application					
Other (specify):					

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 per those controls defined in NIST Special Publication 800-53.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0693-0032, Expiration Date: 10-31-2021 (MEIS) OMB Control No. 0693-0021, Expiration Date: 10-31-2020 (MEP Survey)
	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.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	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.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.

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.)*

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

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 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 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.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			

Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	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: • NIST 188-01, Business Logistics System Customer Relationship Management (CRM) Component (MEP Center Owned) • Dunn & Bradstreet (Selectory Database Web Services)
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): 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. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	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: https://www.nist.gov/public_affairs/privacy.cfm and https://meis.nist.gov/_layouts/MEIS/Public/MEPLogin.aspx?ReturnUrl=%2f	
X	Yes, notice is provided by other means.	Specify how: For MEIS, Centers are provided with the NIST MEP Reporting Guidelines which includes information about how the collection is maintained and disseminated.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: 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 to participate.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For MEIS, collection of data from MEP Centers is mandatory and required by terms defined in Cooperative Agreements.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: 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.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: 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.
	No, individuals do not have an	Specify why not:

	opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access logs are kept and reviewed for anomalies on an as needed basis.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): **04/1/2019** ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	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).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish 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).*

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 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."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/NIST-6: Participants in Experiments, Studies, and Surveys
	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.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NIST Records Schedule N1-167-97-1: Manufacturing Extension Partnership (MEP) Program 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:
X	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.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

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 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.
X	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 levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: The MEP Survey respondents are notified that NIST will take reasonable precautions to protect their information.
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

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.)

Because the information collected is about businesses, not individuals, minimal PII is collected, and none of it is sensitive. Therefore, threats to privacy are commensurately minimal.

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