5

Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: eCommerce Suite
Bureau: Department of Energy
Project Unique ID:
Date:

A. CONTACT INFORMATION

1. Who is the person completing this document?

Peter Robinson
Pacific Northwest National Laboratory
eCommerce Project Lead
PO Box 999
MS: K7-50
Richland, WA 99352
509-375-5947
pete.robinson@pnl.gov

2. Who is the system owner?

Suzanne Davidson
Pacific Northwest National Laboratory
Manager, Financial Operations
PO Box 999
MS: J1-11
Richland, WA 99352
509-371-7500
sm.davidson@pnl.gov

3. Who is the system manager for this system or application?

Peter Robinson
Pacific Northwest National Laboratory
eCommerce Project Lead
PO Box 999
MS: K7-50
Richland, WA 99352
509-375-5947
pete.robinson@pnl.gov

4. Who is the IT Security Manager who reviewed this document?

Andrew Korson
Pacific Northwest National Laboratory

✓

Cyber Security Program Manager
PO Box 999
MS: K9-16
Richland, WA 99352
509-372-6968
andrew.korson@pnl.gov

5. Who is the Privacy Act Officer who reviewed this document?

Michael Talbot
Pacific Northwest Site Office
509-372-4365
michael.talbot@pnl.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

1. Does this system contain any information about individuals?

Yes.

a. Is this information identifiable to the individual? [1]

Yes. The following information will be collected from the individual: client's business address, phone number, email address, and billing address (when different from the business address). Additional types of information are not collected by this system.

b. Is the information about individual members of the public?

Yes.

c. Is the information about DOE or contractor employees?

Yes, in certain cases where employees make online purchases from PNNL.

2. What is the purpose of the system/application?

In this document, the term 'site' means a specific database/web interface. All of the sites and the system infrastructure are referred to collectively as the eCommerce Suite. The term 'system' is used synonymously with the term eCommerce Suite. The purpose of this system is to host a variety of web based eCommerce sites for

[1] "Identifiable Form" - According to the OMB Memo M-02-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptor).

numerous organizations throughout Pacific Northwest National Laboratory (PNNL) located in Richland, Washington. Each eCommerce site will conduct credit card transactions for a specific purpose such as recouping administrative fees and collecting registration fees as appropriate. Requests for new eCommerce sites follow a documented process that requires approval by the appropriate control owners.

3. What legal authority authorizes the purchase or development of this system/application?

All activities will be within the authority provided by the PNNL contract (DE-AC05-76RL01830) with collections being consistent with the guidelines set forth in the DOE Accounting Handbook, Chapter 13.

C. DATA IN THE SYSTEM

1. What categories of individuals are covered in the system?

All individuals that interact with any eCommerce site on this system and attempt to conduct a credit card transaction or make a purchase.

2. What are the sources of information in the system?

a. Is the source of the information from the individual or is it taken from another source?

The sole source of information is the individual making the purchase attempt.

b. What Federal agencies are providing data for use in the system?

None.

c. What tribal, state, and local agencies are providing data for use in the system?

None.

d. From what other third party sources will data be collected?

None.

e. What information will be collected from the individual and the public?

The following information will be collected from the individual:
Business address
Business phone number
Business email address
Credit card information (to include the billing address when different from the business address).

3. Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOE records be verified for accuracy?

Credit card information (the credit card number, name on the credit card, billing address and expiration date) will be immediately encrypted, transmitted and verified by PNNL's credit card processor at the time of purchase.

b. How will data be checked for completeness?

For required data, field validation is implemented via an automated process to ensure completeness. All required data is clearly marked as being required and any purchase attempt will be rejected until all required data has been entered and validated.

c. Are the data current? What steps or procedures are taken to ensure the data are current and not out-of-date?

Yes, all credit card data is current at the time of purchase. PNNL's credit card processor verifies that the purchaser has entered the correct credit card number, expiration date, name on the credit card and billing address.

d. Are the data elements described in detail and documented?

For each eCommerce site on this system a data dictionary is maintained.

D. ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No.

3. Will the new data be placed in the individual's record?

Temporary individuals' records are maintained for thirty days. No sensitive information is maintained.

4. Can the system make determinations about employees/the public that would not be possible without the new data?

No.

5. **How will the new data be verified for relevance and accuracy?**

   See Section C.3

6. **If the data are being consolidated, what controls are in place to protect the data from unauthorized access or use?**

   Not applicable, the data are not being consolidated.

7. **If processes are being consolidated, do the proper controls remain in place to protect the data and prevent unauthorized access?**

   Not applicable, the data are not being consolidated.

8. **How will data be retrieved? Does a personal identifier retrieve the data? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**

   All databases for each eCommerce site are encrypted with 1024-bit RSA encryption that requires a user account on the PNNL network, a unique identification file (Lotus Notes ID) and password as well as a private key to access any data. This data will only be available on PNNL's internal network to authorized individuals with approval by the site owner. Each site is limited to viewing data from their site only.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

   Reports containing an individuals' information can be created internally by PNNL staff; however, no sensitive information is included in these reports. The reports provide statistical information about individuals using the system.

10. **What opportunities do individuals have to decline to provide information (e.g., where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**

    Any individual that does not want to provide any required information can contact the eCommerce site's point of contact who will put them in contact with the appropriate individual to arrange alternate methods of payment.

E. <u>Maintenance and Administrative Controls</u>

1. **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

   Not applicable, the system will only operate at PNNL Richland campus.

2. **What are the retention periods of data in the system?**

The data will be stored for thirty days after the purchase to allow for any customer disputes and to allow PNNL's financial specialists to reconcile all transactions. The credit card number will be stored in the following format: 1234-56XX-XXXX-7890. This is the preferred manner of storage outlined by the Payment Card Industry (PCI) Data Security Standard dated September 2006 (Section 3.3). After thirty days, all credit card data for each transaction will be overwritten. When the purchase involves registration for a conference, symposium or other type of meeting, the data will be stored for thirty days after the close of the meeting. After that thirty day period, the data will be overwritten and appear in the following format: XXXX-XXXX-XXXX-XXXX so that it is not available for viewing. No additional credit card data will be stored on this system.

3. **What are the procedures for disposition of the data at the end of the retention period?**

The procedures for data retention and disposition are outlined in the system's security plan. These procedures reflect the standards outlined in the Payment Card Industry (PCI) Data Security Standard dated September 2006. Essentially the procedures implemented in this system are designed to protect against exposure and compromise of all sensitive data during the storage, processing and transmission of this data. Reports based upon the stored data are available as long as the data remains in the system. See Section E.2 regarding the details of the data storage.

4. **Is the system using technologies in ways that DOE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No.

5. **How does the use of this technology affect public/employee privacy?**

With appropriate security protections, use of this technology does not affect public/employee privacy. The information collected is not shared with anyone beyond the support staff for each particular site, except as otherwise required by law.

6. **Will this system provide the capability to identify, locate, and monitor individuals?**

No.

7. **What kinds of information are collected as a function of the monitoring of individuals?**

- the Internet Protocol (IP) address of the domain from which the individual accessed the Internet (e.g., 123.123.123.123), whether individually or provided as a proxy by the individual's Internet Service Provider (ISP)
- the date and time the individual accessed the site.
- the pages that the individual visited (recorded by the text and graphics files that compose that page.)

- the Internet address of the web site from which the individual linked directly to the site.

8. What controls will be used to prevent unauthorized monitoring?

Numerous automated controls are in place to detect any unauthorized browsing or monitoring on both the internal and external servers. If such an event occurs, an automated email alerts the appropriate individuals of the event immediately. The details of these controls are outlined below.

Unauthorized monitoring is prohibited by requiring all transmissions between the users and the eCommerce system to be conducted via encrypted communication. For users of the internal and external web sites, this is accomplished via Secure Sockets Layer (SSL). SSL prevents eavesdropping, tampering, and message forgery by encrypting all communication with 128-bit encryption. All other communication with the eCommerce servers is routed via the Notes Remote Procedure Call (NRPC) service that encrypts all transmissions to prevent all eavesdropping and monitoring. This encryption occurs at the application layer of the protocol and is independent of all other forms of encryption.

As an additional security precaution against monitoring, the external eCommerce server is maintained in the Extranet Secure Web Zone. The Extranet Secure Web Zone employs the NetContinuum Web Application Firewall which provides a layer of security at the application level that is inserted between the perimeter firewall and the web application server. All traffic to and from the internet must pass through and is filtered by Webfarm16 before being transmitted to the eCommerce system.

With regards to directory browsing, by default, Lotus Notes is configured to prevent any directory browsing. Attempts to browse any directory results in the following error message being displayed, "Unable to process request, directory browsing is not allowed." This action triggers an automated email notification to the system administrator and site developer. This email message as well as the database log record the day and time of the incident and what action was attempted. The database log also records the IP address of the computer attempting the unauthorized access.

Where anonymous access is permitted (to allow one to make purchases), only those portions of the database that are required for the customer to initiate and make the purchase are accessible. To prevent unauthorized browsing or use of all other portions of each web site/database, an Access Control List (ACL) restricts access to the database, the design elements and any stored documents. Access requires a username, password and a Lotus Notes identification file (also known as a Notes ID file.) Any unauthorized access attempt immediately forwards the individual or process to an error page. This error page triggers an automated email notification to the system administrator and site developer. This email message as well as the database log record the day and time of the incident and what was attempted. The database log also records the IP address of the computer attempting the unauthorized access.

The eCommerce system is also configured to prohibit indexing by search engines such as Google. By employing the robot.txt file at the root of the system's web directory, search engines are not allowed to index the contents of any database/web site. If a search engine were to attempt to index the eCommerce system, access would be denied by the database's ACL and would trigger an automated email notification to the system administrator and site developer. This email message as well as the database log record the day and time of the incident and what was attempted. The database log also records the IP address of the computer attempting the unauthorized access.

To ensure uniformity throughout the entire eCommerce system, an automated code generator was developed to create all eCommerce sites and to ensure that all of the processes described above are incorporated into each eCommerce site.

9. Under which PA system of records notice does the system operate?

In accordance with clause H-15 of the PNNL contract (DE-AC05-76RL01830), this system is not covered by an applicable Privacy Act system of records.

10. If the system is being modified, will the PA system of records notice require amendment or revision?

No.

F. ACCESS TO DATA

1. Who will have access to the data in the system?

All credit card data is immediately encrypted and transmitted to PNNL's credit card processor at the time of purchase. Regardless of whether the transaction is approved or rejected, no one at PNNL has access to the complete credit card number at any time. Once the transaction has been completed, a "masked" version of the credit card number is stored in the system (ie 1234-56XX-XXXX-7890 - as described in E.2). This is the only credit card data stored on the system. Only eCommerce developers and select finance personnel have access to this particular data. Authorized privileged users will have access to all other types of data such as the customer's name, contact information, purchase information (to include type of license purchased, license price, quantity of licenses purchased, license expiration date, etc.)

2. How is access to the data by a user determined?

External users (i.e. customers) are able to access sites on the system anonymously. Internal privileged users access is managed by the database access control list.

3. **Will users have access to all data on the system or will the user's access be restricted?**

   External users have no access to site data. Internal privileged users are restricted to viewing data from their sites only. The eCommerce system administrators have access to all sites data.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

   All access to data is password protected. These passwords are changed frequently and comply with strict security policies. Access by external users is prevented by internal database access control lists.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were PA contract clauses included in their contracts and other regulatory measures addressed?**

   Other than PNNL, no subcontractor will be involved with the design, development or maintenance of the system.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**

   No.

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   Suzanne Davidson, the system owner.

8. **Will other agencies share data or have access to the data in this system?**

   No.

9. **How will the data be used by the other agency?**

   Not applicable.

10. **Who is responsible for assuring proper use of the data?**

    Suzanne Davidson, the system owner, will be responsible for assuring proper use of this data.

PIA Approval Signatures

Original copy signed and on file with the DOE Privacy Office.