Version Number: 01-2017

U.S. Department of Commerce
Bureau of Industry and Security

Privacy Threshold Analysis
for the
Chemical Weapons Convention (CWC) System

U.S. Department of Commerce Privacy Threshold Analysis

Bureau of Industry and Security
Chemical Weapons Convention (CWC) System

Unique Project Identifier: 000550200

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).

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

The CWC System consists of three applications BIS employees use CWC IMS for internal processing and validating of declarations and reports received from industry, whether paper or Internet submissions. The IMS also generates the final U.S. Industrial CWC Declaration that the USG submitted to the Organization for the Prohibition of Chemical Weapons (OPCW), in accordance with OPCW requirements in both paper and Extensible Markup Language (XML) formats. The CWC IMS is only accessible through the CWC Local Area Network (LAN) and is further restricted by user access privileges. The CWC User Management application allows internal users with the proper access rights to administer and assign user ids and passwords for industry's use of Web-DESI.

b) *System location*

The CWC System is subsystem of TCD-Net, a Major Application that consists of two subsystems: a Major Application (referred to in this document as CWC) and a General Support System (Office Automation Local Area Network (OA LAN), which is physically housed in the consolidated server room of the Department of Commerce's Herbert C. Hoover Building (HCHB).

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

The CWC System is a standalone system consisting of the following: 1) Web Data Entry Software for industry (Web-DESI), 2) CWC Information Management System (IMS), and 3) User Management application, as well as other tools to support collecting, processing, and storing of CWC related data. The system does not connect with any other systems.

d) The purpose that the system is designed to serve

The purpose of the CWC system is to allow the secure collection, validation and reporting of information required under the Chemical Weapons Convention Treaty. The system facilitates the process of collecting information from industry and submitting it through the National Authority to the Organization of the Prohibition of Chemical Weapons (OPCW).

e) The way the system operates to achieve the purpose

The CWC System consists of three applications. Web-DESI allows industry to submit declarations through a secure web portal. It allows the system to comply with the Government Paperwork Elimination Act. The CWC User Management application allows internal users with the proper access rights to administer and assign user ids and passwords for industry's use of Web-DESI. Information Management System is used by BIS employees for the internal processing and validation of declarations and reports received from industry, whether paper or electronic (internet) submissions. The IMS also generates the final U.S. industrial CWC Declaration that is submitted through the Department of State, and National Authority to the Organization for the Prohibition of Chemical Weapons (OPCW), in accordance with Chemical Weapons Convention Treaty Regulatory, and OPCW requirements in both paper and Extensible Markup Language (XML) formats.

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

The information collected is used to the support the United States international treaty obligation to: 1) Report data on certain chemical activities by the U.S. chemical facilities and trading companies; 2) Impose certain trade controls; 3) Permit the inspection of certain U.S. chemical facilities by international inspection teams from the Organization of the Prohibition of Chemical Weapons (OPCW). Some examples of the business identifiable information collected are name, telephone number, work address, email address, and job title.

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

Although information is shared with the Department of State, the U.S. National Authority to the Chemical Weapons Convention and the international organization responsible for implementing the Convention, the Organization for the Prohibition of Chemical Weapons (OPCW), only CWC personnel have direct access to the system. Through Web-DESI, individuals authorized by the respective company and the Treaty Compliance Division (TCD) have access to the information that pertains to their company's plant sites. In certain instances, information may be shared, upon request, with States Parties to the Convention as provided for under the Convention.

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

The Web-DESI application is accessible via the Internet through an external web portal that is protected by a firewall and is encrypted via Secure Socket Layers (SSL). Information cannot be retrieved without multiple credentials.

i) How information is transmitted to and from the system

U.S. chemical facilities and tracing companies submit data either via paper submissions which the data is manually entered into the Information Management System (IMS), or electronically through the web based Web-Data Entry System (Web-DESI). Once all relevant data has been received and processed, the United States declaration is compiled and exported in hard-copy format as well as in XML file format (on CD), both of which are transmitted to the State Department, the U.S. National Authority, for submission to the Technical Secretariat of the Organization for the Prohibition of Chemical Weapons (OPCW).

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 an 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.*

_X___ This is an existing information system in which no changes have been made to 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.

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

The BII/PII being collected is accessible for administrative matters, litigation, civil, criminal law enforcement and intelligence activities and to promote information sharing.

____ 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.)."

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

X___ Companies
X___ 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..."

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

____ DOC employees
____ Contractors working on behalf of DOC
X___ 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?

X___ 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.

X___ 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 CUESS and as a consequence of this applicability, I will perform and document a PIA for this system.

____ I certify the criteria implied by the questions above do not apply to the CUESS and as a consequence of this non-applicability, a PIA for this system is not necessary.

Name of Information Systems Security Officer (ISSO): Jawayne Davis

Signature of ISSO: Jawayne D Date: 10/16/2017

Name of System Owner: Aleck Che-Mponda

Signature of System Owner: Aleck Che-Mponda Date: 10/16/2017

Name of Authorizing Official (AO): Roger Clark

Signature of AO: R L Clark Date: 10/17/2017