Version Number: 01-2019

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

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

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 (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

This system is one of three subsystems (major applications) that reside on TCD-NET. The Chemical Weapons Convention (CWC) Information Management System (IMS) for internal processing by BIS employees 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 submits to the Organization for the Prohibition of Chemical Weapons (OPCW), in accordance with OPCW requirements in both paper and Extensible Markup Language (XML) format. The CWC IMS is only accessible through the CWC Local Area Network (LAN) and is further restricted by user access privileges.

b) System location

The CWC system is a 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 interconnects with 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.

d) The purpose that the system is designed to serve

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 the Web-DESI. Web-DESI allows industry users to submit and modify declarations and reports via the Internet, as required by the Government Paperwork Elimination Act.

e) The way the system operates to achieve the purpose

Internal users administer access to industry users to input declaration/report information into Web-DESI application. USG personnel input declaration/report information into the IMS application.
Declaration/report data contains proprietary information on chemical production, processing, consumption, import/export of subject chemicals; trade report information on aggregate import/export data on subject chemicals from chemical facilities and trading companies. The IMS system generates declaration information into OPCW format and aggregates all information into aggregate national data in paper and XML format.

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

The CWC system collects and validates information from industry as required under Chemical Weapons Convention Treaty. The System generates declaration information into OPCW format and aggregates all information into aggregate national data in paper and XML format.

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

The 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), and then certain information is shared, upon request, with States Parties to the Convention as provided for under the Convention. When users no longer need access, their accounts are disabled in active directory and they no longer have access to any information on TCD-NET.

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

A web-based interface allows industry to safely log on to the CWC web application using user-names and passwords over Secure Socket Layers (SSL) and TLS connections, Internal users to TCD-NET user multi-factor authentication to log on to TCD-NET. The Web-DESI application is accessible via the Internet through an external web portal that is protected by a firewall and is encrypted via SSL.

i) How information is transmitted to and from the system

Information is transmitted via DOC HCHB firewall to the segmented TCD-NET network for the purposes of OA LAN functions and CWC declaration business.

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). *Continue to answer questions and complete certification.*

__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 (version 01-2017 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.

_____ Yes. *(Check all that apply.)*

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

_X__ 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.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate 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."

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

____ DOC employees
____ National Institute of Standards and Technology Associates
____ Contractors working on behalf of DOC
____ Other Federal Government personnel
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 Social Security numbers (SSNs), including truncated form?

___Yes, the IT system collects, maintains, or disseminates 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.

____X No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

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.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ 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, 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 Chemical Weapons Convention (CWC) Information Management System (IMS) 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 [IT SYSTEM NAME] 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):

_____

Signature of ISSO or SO: JAWAYNE DAVIS Digitally signed by JAWAYNE DAVIS Date: 2020.10.14 13:11:46 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: IDA MIX Digitally signed by IDA MIX Date: 2020.10.14 14:38:23 -04'00' Date: _____

Name of Privacy Act Officer (PAO): _____

Signature of PAO: TIFFANY DANIEL Digitally signed by TIFFANY DANIEL Date: 2020.10.14 15:49:30 -04'00' Date: _____

Name of Authorizing Official (AO): G. Nagesh Rao

Signature of AO: G. Nagesh Rao Date: 14 October 2020

Name of Bureau Chief Privacy Officer (BCPO): Carlos LaCosta II (on behalf of Carol M. Rose)

Signature of BCPO: CARLOS LACOSTA Digitally signed by CARLOS LACOSTA Date: 2020.10.19 13:22:18 -04'00' Date: _____