Version Number: 01-2017

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

Privacy Impact Assessment
for the
Chemical Weapons Convention (CWC) System

Reviewed by: Carol Rose, 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
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.01.30 16:45:29 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment

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

Unique Project Identifier: 000550200

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
The CWC System consists of three applications; 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 way the system operates to achieve the purpose(s) identified in Section 4
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) 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.

(f) 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).

(g) Any information sharing conducted by 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.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

Chemical Weapons Convention Implementation Act of 1998 (P.L.105-277, 22 U.S.C. 6701 et. seq.)

Executive Order 13128 of June 25, 1999 (64 Fed Reg. 34703) (authorizing the Department of Commerce to issue regulations necessary to implement the Act and U.S. obligations under Article VI and related provisions of the Convention).

The Chemical Weapons Convention Regulations (CWCR), 15 CFR Parts 710 through 721.

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

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 no changes have been made to create new privacy risks, and there is a SAOP approved Privacy Impact Assessment on file (version 2015).

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		g. Passport		k. Financial Transaction	
d. Employee ID	x	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: N/A					

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		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

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			
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	x
b. IP Address		d. Queries Run	x	f. Contents of Files	x
g. Other system administration/audit data (specify):					

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		Email	x		
Other (specify):					

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

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

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

The accuracy of the information is ensured by reviewing IAW the records review schedule and upon the destruction of the paper declarations

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
x	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	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): To determine eligibility and POCs on declared facilities and trading companies subject to the CWC.			

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 information collected is used in support of the United States international treaty obligations to;

1.Report data on certain chemical activities by U.S. Companies
2.Impose certain trade controls
3.Permit the inspection of certain U.S. facilities by international inspection teams from the OPCW.

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.)

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. Information may be shared, but upon request only with States Parties to the Convention as provided for under the Convention.

CWC personnel undergo annual refresher training hosted by the Department.

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		
DOC bureaus			
Federal agencies		x	
State, local, tribal gov't agencies			
Public			
Private sector	x		
Foreign governments		x	
Foreign entities			
Other (specify): OPCW & States Parties & Congress		x	

	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.

	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:
x	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	x	Government Employees	x
Contractors	x		
Other (specify):			

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.	
	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:	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

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.	Specify how:
x	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Information is required for US to implement its treaty obligations. If a company wants special consideration for release of PII/BII, they can request additional consideration of release of their information in the event a FOIA request is received.

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: Prior to release of certain collected information determined to be in the "national interest" to disclose, the USG must inform a person 30 days before the release of the information; See Section 404 (c)(2)(A) and (B) or the CWC Implementation Act.
	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: Per Sect. 7.3 above, the individual would be notified of the specific information to be released.
	No, individuals do not have an opportunity to review/update PII/BII	Specify why not:

	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 to the Web-DESI, User Manager applications and the Information Management System tracks the individual by login/password
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): The ATO is dated February 1, 2017 ☐ 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. Moderate
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). Yes
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.
x	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).*

1. The CWC Web-DESI web application requires a secure https connection that uses VeriSign FIPS 140-2 certificates.

2. CWC Web-DESI uses Open SSL to implement the SSLv3 encryption protocol.

3. CWC Web-DESI user activity is stored in a log where the PII/BII is encrypted with FIPS 140-2 specified algorithms AES and SHA-1.

4. CWC Web-DESI and its companion User Manager Application encrypt all CWC Web-DESI passwords whether in transmission or storage.

5.TCD uses MD5 hashes for file comparisons when transmitting XML to the OPCW.

6.Oracle uses the AES algorithm to encrypt Oracle passwords TCD users require for the CWC IMS application.

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/BIS-1 **[Docket No. 150903817–5817–01] Document Number: 2015-30860** https://www.federalregister.gov/documents/2015/12/08/2015-30860/privacy-act-of-1974-amended-system-of-records
	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: Treaty Compliance Division of the Office of Nonproliferation and Treaty Compliance of the Bureau of Industry and Security has a records schedule #N1–476-11-1 approved by National Archivist on June 18, 2012.
	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	
Degaussing		Deleting	x
Other (specify): No information has been deleted from the IMS at this stage of implementation of the Convention; however, submitted paper declarations have been destroyed since the information is contained in the IMS.			

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.)*

x	Identifiability	Provide explanation: Employee names, titles, telephone numbers, alternate phone numbers (e.g., cell or home numbers) and email addresses
x	Quantity of PII	Provide explanation: Approximately 56, 000 pieces of PII have been collected at September 28, 2017.
x	Data Field Sensitivity	Provide explanation: This PII is not specifically protected from release under FOIA as provided under the CWC Implementation Act or the CWC Regulations.
x	Context of Use	Provide explanation: To implement U.S. treaty obligations from a domestic implementation perspective.
x	Obligation to Protect Confidentiality	Provide explanation: BIS tries to protect confidentially of PII but since it is not protected information under the CWC Implementation Act, it is releasable under FOIA.
x	Access to and Location of PII	Provide explanation: PII is maintained in the Web-DESI application, the User Manager application and the Information Management System.
	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 this is a systems that only persons with a need to know have access to there is always that chance of insider threat. Or when sharing information with State Parties across a firewall that is encrypted. However, even with multiple credential, the approved shared information is only accessible by persons of that particular company. This is done to limit access to unwarranted information.

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.

x	Yes, the conduct of this PIA results in required technology changes. Explanation: Enabled internal access of employee log in with PIV
	No, the conduct of this PIA does not result in any required technology changes.