Template Version Number: 01-2021

U.S. Department of Commerce
National Telecommunication and Information Administration (NTIA)

Privacy Impact Assessment
for the
EL-CID Online (Green) – NTIA038

Reviewed by: _____Arthur Baylor_____, 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

ARTHUR BAYLOR Digitally signed by ARTHUR BAYLOR
Date: 2024.01.16 11:03:39 -05'00' 7/31/2023

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

U.S. Department of Commerce Privacy Impact Assessment
NTIA/EL-CID Online (Green)

Unique Project Identifier: NTIA038

Introduction: System Description

Provide a brief description of the information system.

The purpose of the NTIA038 EL-CID Online Green Major Application (MA), which is a web application with a browser-based user interface is to improve NTIA spectrum certification data quality, reduce system review effort, and provide data dictionary-compliant automation to support spectrum certification data management in an unclassified environment.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
Major Application

(b) System location
EL-CID Online Green and its component equipment are physically located in the Consolidated Server Room (CSR), Room 61018 office complex of the Herbert C. Hoover Building (HCHB), in Washington DC and is not open to the public.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
EL-CID Online Green is a standalone system composed of three Windows hosts: a DMZ web proxy, a front-end application server, and a backend database server. All are connected by a virtual switch. The computing platform for NTIA038 is entirely virtual Windows Server 2019 hosts. It has the following two interconnections:

NTIA038 connects using TLS version 1.2 to an Active Directory endpoint for the purpose of synchronizing user information such as password and email. This is a read-only arrangement over secure LDAP.

Interconnection between EL-CID Online Green and DISA E2ESS by a logical access link between DISA E2ESS application on NIPRNet and the NTIA EL-CID Online Green system on the DOC Unclassified Network. Data is encrypted via TLS over this link and connections will be limited to specific IP Addresses and certificates via firewall rules on both ends of the link. The servers and firewalls at each endpoint are located in Federally-owned and controlled facilities, guarded twenty-four (24) hours a day.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
EL-CID Online provides NTIA with a highly available tool to manage the Spectrum Certification application and approval process. It is an internal web application with all persistent storage in its database server.

(e) How information in the system is retrieved by the user
Information retrieval is conducted only on the internal ECO Workflow application. In most cases, information is retrieved through a web interface, however DoD data is retrieved through their E2ESS system.

(f) How information is transmitted to and from the system
Information is exchanged with the user-base through secure, encrypted connections whether connecting through the web interface or interconnected through secure channel with DoD. Information is transmitted over a secure connection using HTTPS using TLS version 1.2.

(g) Any information sharing
Users of EL-CID Online are internal NTIA staff, DoD and external agencies. The external system hosted on the DMZ server is accessible to the public and does not require any credentials or authentication.

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

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

General Personal Data (GPD)					
a. Name		h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address		i. Business Associates	

b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		f. Queries Run		f. Contents of Files	
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		Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign			
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 data entered is compared to the NTIA red book requirements. If data is not conformant, it is rejected back to the submitter. The data is also reviewed by various members of NTIA and Systems Review Branch (SRB).

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		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
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).

Agencies submit certification requests containing equipment and frequency information for approval. This certification request is reviewed by NTIA and SRB.

5.2 Describe any potential threats to privacy, such as insider threat, 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.)

Since federal employees are the only individuals with access to the internal system and possible BII stored in the database there is a potential insider threat to the information. Using the SAAR & ROB process, all users with access to the internal system are required to complete the annual security & privacy awareness training provided by their agency within agency designated timeframes

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			
Foreign governments			
Foreign entities			
Other (specify):			

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

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: DOD's End-to-End Spectrum Supportability (E2ESS) is a Defense Information Systems Agency (DISA) system that provides a data collection tool and database for spectrum supportability business processes. E2ESS and EL-CID Online have an electronic data exchange (via secure web services) for processing spectrum certification requests. Data is encrypted via TLS over a logical access link and connections are limited to specific IP addresses and certificates via firewall rules on both ends of the link. The servers and firewalls at each endpoint are located in Federally-owned and controlled facilities, guarded twenty-four (24) hours a day.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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):			

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.)*

	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:
X	No, notice is not provided.	Specify why not: Federal agency users, not NTIA, are the ones that enter data into the EL-CID Online system. It is unknown if those users inform business

		individuals what information is collected, maintained, or disseminated by the system

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: Businesses can provide any information to their federal customers that they like. The Federal agencies decide what information to put into the EL-CID Online system. If they choose to not enter required information that happens to be proprietary then the agencies will need to work through the Spectrum Planning Subcommittee of the IRAC in order to get their system certified.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: While business individuals may have the opportunity to provide consent to their Federal agency partners, they do not provide consent to NTIA. The Federal agency users decide what to enter into EL-CID. If a business user generates their own records using the external editor then they acknowledge the following: You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all Government-furnished computers connected to this network, and 4) all Government-furnished devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this

		information system at any time and for any lawful Government purpose, the Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. Accessing and using this system indicate your understanding of this warning.

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

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Business individuals do not have access to the EL-CID Online internal system; therefore, they have no mechanism to review any data pertaining to them. They can, however, ask their agency partner for this information and the agency partner can provide the information for review if they wish. They can request that the federal agency partner update data, but again it's up to that agency to determine if the updates will be made or not.

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:
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 8 April 2022_____ ☐ 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).
	A security assessment report has been reviewed for the 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 DOC 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).*

Users are authenticated and must be authorized to use the system. The data is encrypted in transit using HTTPS/SSL.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

____ Yes, the PII/BII is searchable by a personal identifier.

_X___ No, the PII/BII is not searchable by a personal identifier.

9.2 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."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).

X	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: Office of Spectrum Management, N1-417-10-2, was approved by NARA on February 22, 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):			

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, and does not have to be 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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: We do not collect uniquely identifiable information, such as EIN, pertaining to any business.
X	Quantity of PII	Provide explanation: The collection of corporate proprietary information is the exception, rather than the norm.
X	Data Field Sensitivity	Provide explanation: Sensitive data is stored only in the internal system and the entire database is encrypted at rest.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: The protection of sensitive BII that the ELCID Online maintains is governed by the E-Government Act of 2002.
X	Access to and Location of PII	Provide explanation: The BII in the EL-CID Online is stored in an encrypted database with Access Controls that allow only federal users to access the information. Database Administrators are the only others with access to the actual data
X	Other:	Provide explanation: This system contains BII. No PII is contained in the system

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.)

There are no potential threats to personal privacy existing based on the information collected. Threats related to the collection of BII concerning company proprietary information are mitigated by limiting access to BII to only federal staff so that competitors cannot view the sensitive information. The potential for insider threats is mitigated through training provided to federal employees and application logging

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.