Template Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
Network D

Reviewed by: Maria D. Dumas, 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

Jennifer Goode

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

01/07/2022

Date

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary / Network D

Unique Project Identifier: 2591

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.

The Network D is a threat management system which was purposefully designed to maintain and analyze records that reflect and support mission related and functions related to identifying, assessing, and/or managing access, use, and safeguarding of classified national security information.

(a) Whether it is a general support system, major application, or other type of system
General Support System

(b) System location
HCHB

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
Network D is a standalone system and information will not be shared with anyone unless an imminent threat is identified.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
Network D requires information from various sources to perform its mission to safeguard DOC resources and information assets. The Network D derives information for analysis from multiple sources within the Department, including network and system audit logs, information assurance, security and counterintelligence, human resources, and law enforcement files and reports, including from open-source information. OCRM uses automated computer monitoring data, IT audit logs, facility physical access control records, security files (to include personnel security file information, records of violations, infractions, and incidents, and security clearance information), counterintelligence information, personnel files containing information about misconduct and adverse actions, and law enforcement investigatory data.

(e) How information in the system is retrieved by the user
The information is retrieved by user via classified national security system.

(f) How information is transmitted to and from the system

The information is encrypted and transmitted via classified national security data lines.

(g) Any information sharing conducted by the system

When a threat is identified, and it is determined classified information was disclosed in an unauthorized manner to a foreign power or an agent of a foreign power, DOC is required by 50 U.S.C. § 3381(e) to notify the Federal Bureau of Investigation (FBI) and provide access to any DOC records needed for investigative purposes. If other misconduct that raises law enforcement or other national security concerns is uncovered, the misconduct is referred to the appropriate investigative agency at the federal, state, or local level.

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

Executive Order 13587: "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information".

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

Cumulative Impact Level:
Confidentiality -High
Integrity - High
Availability – High
FIPS 199 Categorization – High

Network D is categorized in accordance with CNSS 1253 Instruction for NSS.

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.

____ 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 01-2017).

_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 01-2019 or later).

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*	X	f. Driver's License	X	j. Financial Account	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration	X	l. Vehicle Identifier	X
d. Employee ID	X	i. Credit Card	X	m. Medical Record	
e. File/Case ID	X				
n. Other identifying numbers (specify): **CAC or building access card numbers; visa numbers; license and permit numbers; criminal history and arrest records; FBI numbers.**					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: **SSN may be used to identify a linked record.**					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	X
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	X
e. Age	X	l. Email Address	X	s. Physical Characteristics	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	X
g. Citizenship	X	n. Religion	X		
u. Other general personal data (specify): T**ravel history, records related to drug and alcohol use, names of spouses/relatives/references/affiliations/personal associates, activities, Internet data and items posted to social networking sites.**					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	f. Scars, Marks, Tattoos	X	k. Signatures	
b. Palm Prints	X	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	X	j. Weight		o. Dental Profile	
p. 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	X	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify):
Commerce/DEPT-27

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	
Telephone		Email	X		
Other (specify):					

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

Non-government Sources					
Public Organizations	X	Private Sector		Commercial Data Brokers	X
Third Party Website or Application			X		
Other (specify): **Unknown via anonymous reporting or referrals.**					

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

By informing system users about security measures, explaining potential threats, and implementing security measures. Gathering information necessary to maintain security and establishing functioning external barriers such as firewalls and other security measures. Also, by defining, creating, and maintaining the documentation for certification and accreditation of the information system in accordance with government requirements. By assessing the impacts on system modifications and technological advances. Additionally, by monitoring the system and conducting security scans to identify potential security issues or weaknesses and recommending improvements to amend vulnerabilities, implement changes and document upgrades.

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		For employee or customer satisfaction	
For web measurement and customization technologies (single session)		For web measurement and customization technologies (multi-session)	
Other (specify): **To protect national security information.**			

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 about a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

PII/BII that is collected, maintained, or disseminated will be used: This system is used by authorized personnel to maintain records that reflect, and support, mission-related functions and safeguarding of classified national security information. Any federal employees, contractors, members of the public, foreign nationals, or visitors who use our systems may be subject to collection.

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

The following mandatory training for users: **- Cyber Awareness Challenge for the Intelligence Community** **- Derivative Classification**

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	X		
Federal agencies	X		
State, local, tribal gov't agencies	X		
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?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	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: **Systems A,B,C & Department' s unclassified systems**
	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.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	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: **Privacy Act of 1974** - https://osec.doc.gov/opog/PrivacyAct/PrivacyAct.html	
X	Yes, notice is provided by other means.	Specify how: **Commerce/DEPT-27** **Investigation and Threat Management Records**
	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: **Exempt under 5 U.S.C. 552a(e)(3).**

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: **Exempt under 5 U.S.C. 552a(e)(3).**

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: **Exempt under 5 U.S.C. 552a(e)(3).**

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: **Protection of classified national security information.**
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): **12/21/2021** ☐ 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).
X	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.
	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).*

Data at rest will be protected by encryption software.

Section 9: Privacy Act

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

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

____ 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."

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/DEPT-18 - Employees Personnel Files Not Covered by Notice of Other Agencies** **Commerce/DEPT-27 - Investigation and Threat Management Records** **Commerce/DEPT-25 - Access Control and Identity Management System**
	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: **General Records Schedule 5.6 - Security Records**
	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	X
Degaussing	X	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.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	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: **Uniquely and indirectly identifies specific individuals.**
X	Quantity of PII	Provide explanation: **Identifies number of data points.**
X	Data Field Sensitivity	Provide explanation: **Combined fields depict more sensitive data.**
X	Context of Use	Provide explanation: **Protection of classified data.**
X	Obligation to Protect Confidentiality	Provide explanation: **CNSS, 0MB, NIST, and D0C require protection of PII.**

	Access to and Location of PII	Provide explanation:
	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 regarding the type or quantity of information collected and the sources providing the information 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.)

No potential threats to privacy have been identified.

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.