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

Privacy Threshold Analysis
For the
IRACNET

U.S. Department of Commerce Privacy Threshold Analysis
NTIA/IRACNET (Green)

Unique Project Identifier: 006-60-01-29-02-7319-00

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).

The objective of the IRACNET application is to provide document management, agenda management, collaboration, and documentation of proceedings of the IRAC and sub committees in support of the Federal Government's use of the radio frequency spectrum.

The IRACNET allows user to retrieve and post documents, check announcement, review the schedule of meetings, look up contact information for committee representatives. It also provides access to a full text search capability of the Inter-department Radio Advisory Committee (IRAC) and subcommittee documents current and historical.

The IRACNET system utilized a role based security model to allow segmentation of information based on specific user needs and roles.

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

The NTIA006 IRACNET Green is a Major Application (MA) that provides the following core functions:

- Access to documents under consideration by the IRAC and its subcommittees
- Access to metadata about those documents
- Access to upcoming and past subcommittee meeting agendas
- Access to a searchable archive of the documents, metadata, and dispositions
- Controlled access to the above

(b) System location

The IRACNET and its component equipment is located within the DOC consolidated server facility within the National Capital Region 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)

There is no interconnection between IRACNET and other systems. However, NTIA HQs General Support System (NTIA005) provides hosting environment for IRACNET and provides no interconnections for data.

(d) The purpose that the system is designed to serve

The objective of the IRACNET application is to provide document management, agenda management, collaboration, and documentation of proceedings of the IRAC and sub committees in support of the Federal Government's use of the radio frequency spectrum.

The IRACNET allows user to retrieve and post documents, check announcement, review the schedule of meetings, look up contact information for committee representatives. It also provides access to a full text search capability of the Inter-department Radio Advisory Committee (IRAC) and subcommittee documents current and historical.

(e) *The way the system operates to achieve the purpose*

The IRACNET application provides document management, agenda management, collaboration, and documents proceedings of the IRAC and sub committees in support of the Federal Government's use of the radio frequency spectrum. IRACNET is a highly available tool to improve the management of the IRAC and its subcommittees by facilitating the distribution of documents under consideration and the logging of the bodies' decisions on those documents as well as providing a searchable archive of those documents and the decision process. It is an internal web application with all persistent storage of data and documents as well as users, user profiles, and logs of user actions in a database server.

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

The IRACNET application stores both structured and unstructured information related to the proceedings of the IRAC and sub committees in support of the Federal Government's use of the radio frequency spectrum. Unstructured data includes documents that describe radio systems and policies and procedures of the IRAC and its subcommittees. Structured information includes data related to status updates of federal frequency assignments and descriptions of radio systems requesting certification of spectrum support.

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

The user-base is comprised of NTIA staff, as well as, IRAC members' federal staff and contractors from 19 federal agencies.

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

IRACNET facilitates the distribution of documents under consideration of the IRAC and logs the bodies' decisions on those documents, as well as, providing a searchable archive of those documents and the decision process. It is an internal web application with all persistent storage of data and documents as well as users, user profiles, and logs of user actions in a database server. IRACNET data is retrieved via agency name, document number, document title, submission date, and data classification.

(i) *How information is transmitted to and from the system*

IRACNET maintains and disseminates information related to the management of federal spectrum usage and the policies and procedures that the federal government plans and implements for spectrum management. This information is primarily unstructured data stored in documents such as MS-Word, Adobe PDF, etc.

Some structured information is disseminated through IRACNET, such as status information related to frequency assignments and system description information related to the certification of spectrum support. Information is exchanged with the user-base through a web interface via secure encrypted connections.

IRACNET is categorized as a FISMA Moderate system. Information is posted and retrieved by the user base through a web interface via secure encrypted connections using the HTTPS protocol.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

_X__ 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 Characterof Data	X
j. Other changes that create new privacy risks (specify): New function added to the IRACNET system aggregates data type business identifiable information (BII). The data consists of property business and competitive sensitive information.					

____ This is an existing information system in which changes do not create new privacyrisks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answerquestions 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 or01-2017). *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 01-2019 orlater). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X__ No. This is not a new information system.

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."

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

____ DOC employees
____ Contractors working on behalf of DOC
____ Other Federal Government personnel
____ Members of the public

_X__ 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.

____ 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?

____ 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.

____ 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 SAOP 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 IRACNET (Green) NTIA006 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 IRACNET (Green) NTIA006 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Soma Chary Office: OPCM Phone: 202-482-5965 Email: schary@ntia.gov SOMA CHARY Digitally signed by SOMA CHARY Date: 2021.07.02 10:17:31 -04'00' Signature: ________________ Date signed: ________________	**Information Technology Security Officer** Name: Shine Kang Office: OPCM Phone: 202-482-1752 Email: skang@ntia.gov SHINE KANG Digitally signed by SHINE KANG Date: 2021.07.02 12:02:17 -04'00' Signature: ________________ Date signed: ________________
Privacy Act Officer Name: Dr. Catrina D. Purvis Office: OPCM Phone: 240-672-4974 Email: cpurvis@ntia.gov SHINE KANG Digitally signed by SHINE KANG Date: 2021.07.02 12:05:38 -04'00' Signature: ________________ Date signed: ________________	**Authorizing Official** Name: Dr. Catrina D. Purvis Office: OPCM Phone: 240-672-4974 Email: cpurvis@ntia.gov SHINE KANG Digitally signed by SHINE KANG Date: 2021.07.02 12:06:16 -04'00' Signature: ________________ Date signed: ________________
Bureau Chief Privacy Officer Name: Dr. Catrina D. Purvis Office: OPCM Phone: 240-672-4974 Email: cpurvis@ntia.gov SHINE KANG Digitally signed by SHINE KANG Date: 2021.07.02 12:05:00 -04'00' Signature:________________ Date signed: ________________	