U.S. Department of Commerce (DOC)
Office of the Secretary (OS)

Privacy Threshold Analysis for the System B General Support System (GSS)

U.S. Department of Commerce Privacy Threshold Analysis

National Security Solution and Services (NS3) System B GSS

Unique Project Identifier: System B GSS

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*

System B is a General Support System (GSS).

b) *System location*

System B is located at the Department of Commerce (DOC) Herbert C. Hoover Building (HCHB) in Washington DC.

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

System B a GSS provides support for the Office of the Secretary (OS)/Office of Security (OSY) and is a law enforcement system used by the Department of Commerce (DOC), Office of Security (OSY).

d) The purpose that the system is designed to serve

The purpose of this system is to provide the network access, email services, file and print storage, workstation management and support services, and utility packages critical to the mission of the Counter Intelligence (CI) division of OSY and is classified up to Top Secret.

e) The way the system operates to achieve the purpose

Connectivity between the room is provided by armored 62.5 MM fiber optic cabling and is terminated on NSA approved KG-175D TACLANE encryption devices. All IT equipment is owned and operated by the National Security Solutions and Services (NS3). The data processed within the System B GSS environment is transmitted via the TACLANE encrypted devices to protect the data from being read and or intercepted while in transit

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

System B GSS allows the OSY to conduct investigations and analyses to identify and/or assess critical threats to the Department's mission, operations, or activities; prevent or mitigate such threats from adversely affecting Department personnel, facilities, property, or assets through strategic and tactical approaches; and collaborate with other national security and law enforcement entities as appropriate.

System B GSS manages all matters relating to the storage, facilitation and enabling of documentation of activities associated with proactive and reactive assessments, complaints, inquiries, and investigations; process and house information and intelligence; identify risks, vulnerabilities, and threats to Department and information assets and activities; and track referrals of potential interest to internal and external partners. It provides a basis for the development and recommendation of solutions to deter, detect, and/or mitigate potential risks, vulnerabilities, and threats identified, provide statistical reports of OSY actions, and meet other reporting requirements.

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

System B GSS access is on a restricted network. This network to those authorized users with authorized access with a need to know only.

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

System B GSS users log into the network using two factor authentications: UserID and password. Electronic access via individual-specific logon credentials will retrieve cases assigned to the user logged in. Searches may be performed by search criteria that include case numbers, date range, priority level, category, status organizations, and other key word search variations.

i) How information is transmitted to and from the system

The data processed within the System B GSS environment is transmitted via the TACLANE encrypted devices to protect the data from being read and or intercepted while in transit.

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.*

__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 01-2015). *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 01-2017 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raiseprivacy 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.

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

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

____ 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.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

X___ 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.)*

_X__ DOC employees

_X__ National Institute of Standards and Technology Associates

_X__ Contractors working on behalf of DOC

____ Other Federal Government personnel

____ 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?

__X__ 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.

SSNs are part of law enforcement and subject records (both received and created) as one piece of data used to positively identify people.

Provide the legal authority which permits the collection of SSNs, including truncated form.
ITMS legal authorities to collect and maintain Privacy Act information contained in this system of records:
15 U.S.C. 1501 et. seq.; 28 U.S.C. 533–535; 44 U.S.C. 3101; 5 U.S.C. 301 (Management of Executive Agencies); 5 U.S.C. 7311 (Suitability, Security, and Conduct); 5 U.S.C. 7531-33 (Adverse Actions, Suspension and Removal, and Effect on Other Statutes); 18 U.S.C. 111 (Crimes and Criminal Procedures) (Assaulting, resisting, or impeding certain officers or employees); 18 U.S.C. 201 (Bribery of public officials and witnesses); 18 U.S.C. 202 (Bribery, Graft, and Conflicts of Interest-Definitions); 18 U.S.C. 1114 (Protection of officers and employees of the U.S.); Executive Order 10450 (Security requirements for government employment); Executive Order 13526 and its predecessor orders (Classified National Security Information); Executive Order 12968 (Access to Classified Information); HSPD-12, 8/27/04 (Homeland Security Presidential Directive); Executive Order 13356, 8/27/04 (Strengthening the Sharing of Terrorism Information to Protect Americans); Executive Order 13587 (Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information), P.L. 108-458 (Sect. 1016), 12/17/04 (Intelligence Reform and Terrorism Prevention Act of 2004).

____ 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 System B GSS 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 notnecessary.

Name of Information System Owner (SO): Jerome Nash

Signature of SO: JEROME NASH Digitally signed by JEROME NASH Date: 2020.09.03 22:51:21 -04'00' Date: ___________

Name of Information Technology Security Officer (ITSO): Eric Cline

Signature of ITSO: ERIC CLINE Digitally signed by ERIC CLINE Date: 2020.09.08 12:01:05 -04'00' Date: ___________

Name of Privacy Act Officer (PAO): Lisa J. Martin

Signature of PAO: LISA MARTIN Digitally signed by LISA MARTIN Date: 2020.09.28 18:00:55 -04'00' Date: ___________

Name of Authorizing Official (AO): Lawrence W. Anderson

Signature of AO: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2020.09.08 15:02:14 -04'00' Date: ___________

Name of Bureau Chief Privacy Officer (BCPO): Maria Dumas

Signature of BCPO: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2020.09.28 22:54:02 -04'00' Date: ___________