Version Number: 01-2019

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

Privacy Threshold Analysis for the
SYSTEM A General Support System
(GSS)

U.S. Department of Commerce Privacy Threshold Analysis

National Security Solution and Services (NS3) System A

Unique Project Identifier: SYSTEM A

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 A is a General Support System (GSS).

b) System location

System A GSS 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 A GSS hosts various major applications used by DOC Bureaus charged with missions that support the National Essential Functions. The System A GSS network is used by the Office of the Secretary, Office of Security, the Bureau of Industry and Security, the International Trade Administration, the National Institute of Standards and Technology, the National Oceanic and Atmospheric Administration, the National Telecommunication and Information Administration, the U.S. Patent and Trademark Office and the Office of the Chief Information Officer.

d) The purpose that the system is designed to serve

The purpose of System A GSS is for the hosting applications to be able to transmit, receive, and store classified information up to the Secret level.

e) The way the system operates to achieve the purpose

The System A GSS obtains its external connectivity from Department of Defense (DoD) Defense Information Systems Agency (DISA) Federal Demilitarized Zone (FED DMZ) Secret Internet Protocol Router Network (SIPRNet) to transmits classified information.

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

The type of information collected, maintained, use or disseminated by System A GSS are as follows:
- International Affairs & Commerce
- Critical Infrastructure Security
- Workforce Management
- Economic Development
- Regulatory Development and Compliance Inspection
- Risk Management and Mitigation
- Planning and Budgeting
- System and Network Monitoring
- Help Desk Services
- Information and Technology Management
- IT Infrastructure Maintenance
- Security Management

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

System A GSS access is on a restricted network. This network is for users with authorized and authenticated access with a need to know only.

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

System A GSS users retrieve information via classified web browser and/or email.

i) How information is transmitted to and from the system

System A GSS users transmit information via classified web browser and/or email.

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	X	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.*

____ 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.*

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

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):			

____ 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."

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?

____ 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.

X 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 A 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 not necessary.

Name of Information System Owner (SO): Jerome Nash

Signature of SO: JEROME NASH Digitally signed by JEROME NASH Date: 2020.09.03 22:05:58 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Shawn Yuthsakdidecho

Signature of ITSO SHAWN YUTHSAKDIDECHO Digitally signed by SHAWN YUTHSAKDIDECHO DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=SHAWN YUTHSAKDIDECHO, 0.9.2342.19200300.100.1.1=13001000970422 Date: 2020.09.04 01:06:56 -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 17:35:40 -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 15:04:03 -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 22:52:33 -04'00' Date: _____