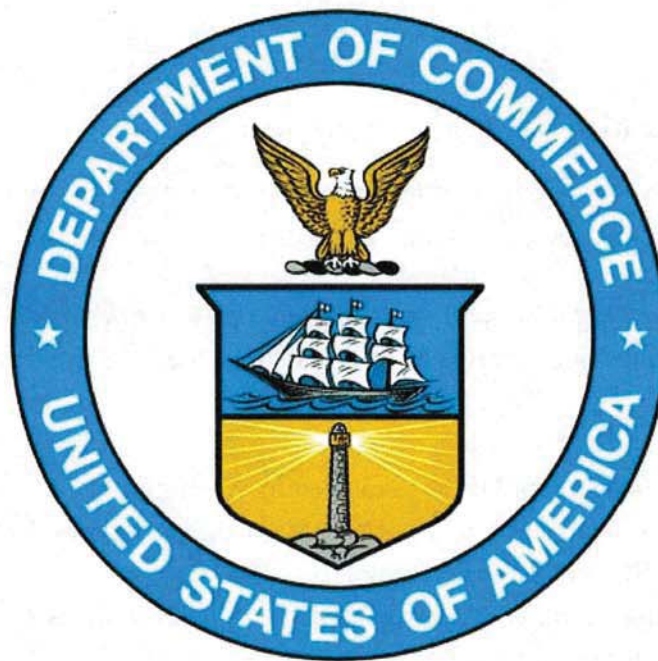


**U.S. Department of Commerce
Office of Acquisition Management**



**Privacy Threshold Analysis
for the
C.Suite Application**

U.S. Department of Commerce Privacy Threshold Analysis

Office of Acquisition Management/ComprizonSuite (C.Suite)

Unique Project Identifier: OS010 - Comprizon Suite

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:

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*
 - C.Suite is a Minor System; it is a child system of the EAS application system boundary.
- b) *System location*
 - The C.Suite Management Office is located in Washington, DC. Application infrastructure is located at the Department of Transportation – Enterprise Services Center (DOTESC) in Oklahoma City.
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
 - C.Suite is a child system to the DOC Enterprise Application System.
- d) *The purpose that the system is designed to serve*
 - The application represents the standard procurement business practice for all Commerce agencies except PTO.
- e) *The way the system operates to achieve the purpose*
 - C.Suite provides an environment to create, route, track and report all procurement activity for Commerce. This includes small purchase requirements as well as complex contract activities. The program is designed to provide consistent automated support to all Commerce procurement offices and offer aggregate procurement reporting information and analysis capabilities to operating unit and departmental management.

- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- The application collects taxpayer ID numbers, personal data such as name and address, and work related contact information.
- g) *Identify individuals who have access to information on the system*
- Individuals within the DOC bureaus and Federal agencies involved in the federal acquisition process for services, goods, and materials provided by the vendor community to the Federal Government will have access to the information.
- h) *How information in the system is retrieved by the user*
- Data is retrieved by authorized access users through a secured data extract point from the System for Award Management.
- i) *How information is transmitted to and from the system*
- Information is transmitted to and from C.Suite through the System for Award Management, which consolidates several existing Federal government wide procurement and award support systems into a single database and single entry point.

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 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. *Please describe the activities which may raise privacy concerns.*

☐ 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 about: *(Check all that apply.)*

☐ Companies

☐ Other business entities

☐ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

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

☐ DOC employees

☐ Contractors working on behalf of DOC

_____ 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 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.

4c. 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.

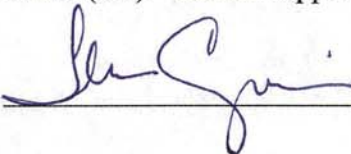
If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to C.Suite 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 CARTS/Version Manager and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Teresa Coppolino

Signature of SO: 

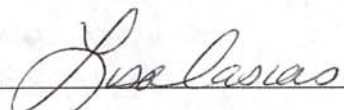
Date: 4/19/18

Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO:  Digitally signed by JUN KIM
DN: cn=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=JUN KIM,
0.9.2342.19200300.100.1.1=13001001483988
Date: 2018.04.23 08:39:05 -04'00'

Date: 4/23/2018

Name of Authorizing Official (AO): Lisa Casias

Signature of AO: 

Date: 4/30/18

Name of Bureau Chief Privacy Officer (BCPO): Kathleen Gioffre

Signature of BCPO: **KATHLEEN GIOFFRE**  Digitally signed by KATHLEEN GIOFFRE
DN: cn=US, o=U.S. Government, ou=Department of Commerce,
ou=Office of the Secretary, cn=KATHLEEN GIOFFRE,
0.9.2342.19200300.100.1.1=1300100075444
Date: 2018.04.24 07:34:01 -04'00'

Date: _____