

**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/C. Suite Application

Unique Project Identifier: An EAS OS-059 Application

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 Department of Commerce supports its acquisition mission and objectives by utilizing a Commercial Off-The-Shelf (COTS) product named ComprizonSuite (C.Suite). C.Suite integrates and streamlines the entire acquisition management process from requisition through contract/purchase to order closeout. C.Suite is platform independent and operates in multiple desktop environments and with J2EE Web/application/database server combinations. C.Suite consists of two integrated modules. These modules function independently; however, combine seamlessly to manage the entire acquisition process. The modules are Comprizon.Request and Comprizon.Award:

- Comprizon.Request – provides Web requisitioning, routing for review and approvals, support documentation, real-time status checks, and development of acquisition plans; and
- Comprizon.Award – provides automated preparation and management of purchase requests, acquisition plans, solicitations, amendments, contracts, and modifications.

DOC has successfully deployed C.Suite in four of the five bureaus that warrant delegated procurement authority. These include: Office of the Secretary (OS); Bureau of the Census and its Processing Office; National Institute of Standards and Technology (NIST); and field and Headquarter offices within the National Oceanic and Atmospheric Administration (NOAA). The Patent and Trademark Office (PTO) is using another COTS solution for their acquisition needs and does not plan to use C.Suite.

C.Suite exchanges data with the Commerce Financial System (CFS) installations at NOAA, NIST and Census, through the Obligation and Requisition System Interface (ORSI). ORSI uses Enterprise Application Interface (EAI) technology to standardize and transfer information among the systems. The CFS and elements of ORSI are part of the Commerce Business Systems (CBS) suite of financial applications, while C.Suite and remaining elements of ORSI, and are part of the Commerce Business Environment (CBE) suite of procurement applications

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. *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..."

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

 X ☐ DOC employees

 X ☐ 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.

 X No, the user ID is the only PII collected, maintained, or disseminated by the IT system. (*Name and user ID is only used to log into the application.*)

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.

 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, 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

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.

Name of System Owner (SO): Tammy Journet

Signature of SO: 

Date: 3-6-2017

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

Signature of ITSO: JUN KIM

Digitally signed by JUN KIM
DN: c=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: 2017.04.14 12:07:48 -04'00'

Date: 4/14/2017

Name of Authorizing Official (AO): Lisa Casias

Signature of AO: 

Date: 5/4/17

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

Signature of BCPO: KATHLEEN GIOFFRE

Digitally signed by KATHLEEN GIOFFRE
DN: c=US, o=U.S. Government, ou=Department of
Commerce, ou=Office of the Secretary, cn=KATHLEEN
GIOFFRE, 0.9.2342.19200300.100.1.1=13001000075444
Date: 2017.06.20 06:48:31 -04'00'

Date: _____