Template Version Number: 01-2021

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/Comprizon Suite (C. Suite)

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: *Provide a brief description of the information system.*

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).

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 on Internet Explorer, Firefox, and Chrome and with J2EE Web/application with an Oracle database. C.Suite consists of two integrated modules. These modules function independently but 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

• Comprizon.Award – provides automated preparation and management of purchase requests, solicitations, amendments, contracts, and modifications.

DOC has successfully deployed C.Suite in five of the six bureaus that warrant delegated procurement authority. These include Enterprise Services-Acquisition (ES-A); FirstNet; 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 are part of the Commerce Business Environment (CBE) suite of procurement applications.

DOC operates and manages C.Suite in two locations. DOC currently houses the ES-A, FirstNet, NOAA and Census C.Suite installations at the Department of Transportation's Enterprise Service Center (DOTESC) in Oklahoma City, Oklahoma. The Commerce Service Center (CSC) provides C.Suite application-level support and DOTESC provides the required hosting environment support through a Service Level Agreement (SLA) with CSC. NIST operates and maintains a separate instance of C.Suite at their Gaithersburg, Maryland facility.

Address the following elements:

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 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 exchanges data with the Commerce Financial System (CFS) installations at NOAA, NIST, 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, are part of the Commerce Business Environment (CBE) suite of procurement applications. C. Suite also sends data in an XML (Extensible Markup Language) file to the Federal Procurement Data System-Next Generation (FPDS-NG) for public reporting requirements.

DOC operates and manages C. Suite in two locations. DOC currently houses the Enterprise Services/Acquisition, FirstNet , NOAA, and Census C. Suite installations at the Department of Transportation's Enterprise Service Center (ESC) in Oklahoma City, Oklahoma. The Commerce Service Center (CSC) provides C. Suite application-level support and ESC provides the required hosting environment support through a Service Level Agreement (SLA) with CSC. NIST operates and maintains a separate instance of C. Suite at their Gaithersburg, Maryland facility.

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, used, 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

Employees and contractors 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. 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.*

____ 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. *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.

____ 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):			

____ 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.

____ 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

____ 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__ The criteria implied by one or more of the questions above **apply** to the C. Suite and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the C. Suite and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information Technology Security Officer Name: Eduardo Macalanda Office: DOC OFMS Phone: 301-355-5987 Email: emacalanda@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: EDUARDO MACALANDA Digitally signed by EDUARDO MACALANDA Date: 2022.07.25 15:57:52 -04'00' Date signed: _____	**Chief Information Security Officer** Name: Densmore Bartley Office: OS OCIO Phone: 202-482-3186 Email: dbartley@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: DENSMORE BARTLY Digitally signed by DENSMORE BARTLY Date: 2022.08.03 10:15:49 -04'00' Date signed: _____
System Owner Name: Teresa Coppolino Office: DOC OFMS Phone: 301-355-5501 Email: tcoppolino@doc.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: TERESA COPPOLINO Digitally signed by TERESA COPPOLINO Date: 2022.07.26 08:29:42 -04'00' Date signed: _____	**Authorizing Official** Name: Dr. Lawrence W. Anderson Office: OS OCIO Phone: 202-482-2626 Email: landerson@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2022.08.03 14:33:41 -04'00' Date signed: _____
Authorizing Official Name: Stephen M. Kunze Office: Office of Financial Management Phone: 202-482-3709 Email: skunze@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: STEPHEN KUNZE Digitally signed by STEPHEN KUNZE Date: 2022.07.27 11:41:18 -04'00' Date signed: _____	**Privacy Act Officer** Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: tmurphy2@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Tahira Murphy Digitally signed by Tahira Murphy Date: 2022.08.24 21:11:50 -04'00' Date signed: _____

Section intentionally left blank.	**Bureau Chief Privacy Officer** Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: tmurphy2@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Tahira Murphy Digitally signed by Tahira Murphy Date: 2022.08.24 21:12:17 -04'00' Date signed: