Version Number: 01-2019

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
C.Suite Application

Reviewed by: Maria Dumas, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.05.13 09:52:19 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
ComprizonSuite (C.Suite)

Unique Project Identifier: Comprizon Suite (C. Suite) is an EAS OS-059 Application

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system

- C.Suite is a Minor System. It is the 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 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. 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, 1stNet, 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 way the system operates to achieve the purpose(s) identified in Section 4

- The Department of Commerce (DOC) 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; however, combine seamlessly to manage the entire acquisition process. The modules are Comprizon.Request and Comprizon.Award.

(e) How information in the system is retrieved by the user

- Data is retrieved daily by authorized data access users through a secured data extract point from the System for Award Management (SAM) and stored within C.Suite. The SAM is a government wide system operated and maintained by GSA on behalf of Federal Agencies who use it. SAM consolidates several existing Federal government wide procurement and award support systems into a single database and a single entry point.

(f) How information is transmitted to and from the system

- 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.

(g) Any information sharing conducted by the system

- DOC shares this data as required by the Federal Acquisition Regulation (FAR).

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

- The authority for the maintenance of the system is 28 U.S.C. 3101–3105, Debt Collection Act of 1982 (Pub. L. 97–365); 26 U.S.C. 6402(d); and 31 U.S.C. 3711.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

- C.Suite is classified as a Moderate system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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.

____ 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).

_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).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID	X	g. Passport		k. Financial Transaction	X
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	X
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: Although the Social Security number (SSN) is not collected by C.Suite, the taxpayer identification number may be in the form of an SSN for a sole proprietor.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address		s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History			
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance			

		Information			
k. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations	X	Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Data validation controls are in place in order to ensure the appropriate format is utilized. The Taxpayer Identification Number is stored within the SAM and validated by the IRS.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

Information is collected in the System for Award Management (SAM) and then passed to C. Suite for financial and business decisions. Any individual or company wishing to do business with the Federal Government must submit information into SAM to be considered for a contract or award. Any notification regarding use, collection, review, or updates to PII/BII is delivered by the SAM application. C.Suite is updated on a daily basis with the applicable data from SAM. No individual or company has access to their information in C. Suite. Information is required as part of the federal acquisition process for services, goods, and materials provided by the vendor community to the Federal Government. Having the correct Tax Identification Number (TIN) in System for Award Management (SAM) improves data collection by allowing a single point of data entry for any person or firm who wants to conduct business with the Federal Government. The SAM web application is used by various departments and bureaus across the Federal Government. Since October 1, 2003, it is federally mandated that any person or firm wishing to conduct business with the Federal Government under a FAR-based contract must be registered in SAM before being awarded a contract [Federal Acquisition Regulation (FAR) policy FAR 4.1102 (October 1, 2003), and Federal Acquisition Circular (FAC) 2001-16]. In addition, this information is used in the DoC's Core Financial System to make timely payments to these vendors for their services and materials. DOC uses the information for the acquisition of and payment for goods and services by NOAA, Census, OS and NIST to support their respective missions. DOC shares this data as required by the Federal Acquisition *Regulation (FAR).*

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate

handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Insider threat is possible. Annual Cybersecurity Awareness Training is conducted in order to communicate the appropriate procedures for handling and dispensing of information. All users and privileged users signed Rules of Behavior annually attesting to this as well.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: C.Suite receives the PII/BII information from the System for Award Management (SAM). 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. C. Suite also sends data in an XML file to the Federal Procurement Data System - Next Generation (FPDS-NG) for public reporting requirements.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _____.	
X	Yes, notice is provided by other means.	Specify how: Notice of the collection, maintenance and dissemination of PII/BII is provided when the users enter their information in System for Award Management (SAM). Every department of the Federal Government pulls information from this system for payment and awards. C. Suite uses the data received from SAM to process payments and awards. No individual/company wishing to conduct business with the Department of Commerce has access to their data in C. Suite. They are only able to access their data in SAM.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: If an individual company would choose to decline to provide PII/BII for SAM they would not be eligible for contract awards. It is Federally mandated that an individual/company wishing to conduct business with the Federal Government under a FAR based contract must be registered in SAM before being awarded the contract. No individual/company wishing to conduct business with the Department of Commerce has access to their data in C. Suite. They are only able to access their data in SAM.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their	Specify how:

	PII/BII.	
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The only use of PII/BII in C.Suite is to process contracts and awards.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: No individual/company wishing to conduct business with the Department of Commerce has access to their data in C.Suite. Any data that would need to be changed or updated must be updated in SAM.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to the PII/BII is restricted to those roles that require the information to support their job functionality.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 8/8/2019 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The servers are located at DOT/FAA/ESC is maintained by administrators that configure the servers to be in a secure state as part of the service level agreement (SLA) between DOC and DOT/FAA/ESC. In addition, servers are in a physically secure room by specific personnel access, to limit the possibility of unauthorized physical modification or damage.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT2- Accounts Receivable http://osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-2.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: General Records Schedule 20, Item 3
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII/BII does include SSN and financial information that could uniquely and directly identify individuals.
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: PII/BII does include SSN and financial information for individuals and business.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: PII/BII is only accessed through C.Suite by necessary individuals.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or

mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

No potential threats to privacy were discovered.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.