U.S. Department of Commerce
U.S. Census Bureau

Privacy Threshold Analysis
for the
DATA COMMUNICATIONS
U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau Data Communications

Unique Project Identifier: [Number]

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

General Support System

(b) System location

- U.S., Census Bureau, Suitland, MD
- U.S., Census Bureau, Bowie, MD
- AWS GovCloud, AWS Region US-East, VA
- Microsoft Azure Commercial (O365), Azure Region East US, VA
- National Processing Center (NPC), Jeffersonville, IN

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

Data Communications is a core system at the Census Bureau that provides secured access to services such as internet, e-mail services, file access, printing services and other information system services and interconnects with all of the IT systems at the Census Bureau. Data Communications Systems receive PII from the Human Resources Applications system named CAMPIN and the Commerce Business Systems, in a one-way pull, for the creation of new employee accounts.

The NPC Call Center video screen captures and audio recordings will be stored on servers within...
the Network Services System and accessed only by authorized individuals (call center supervisors and call center managers) for the purpose of quality assurance and call center employee training.

(d) The purpose that the system is designed to serve

The Data Communications IT system serves as the medium to interconnect the various Census Bureau information systems that are deployed in addition to providing services such as authentication for internal and external customers, network security, LAN/WAN, e-mail, Internet access, remote access, and voice and video teleconferencing services.

This system also contains a digitized “Likeness and Profile Release” form within a Microsoft 0365 application for identification and consent purposes in addition to Call Center Monitoring functionalities used to support quality assurance and call center training.

(e) The way the system operates to achieve the purpose

Data Communications General Support System serves as the transport system utilized by data collection/dissemination systems, and is therefore not a data collection/dissemination system itself but utilizes PII for the purpose of administrative matters. This system serves as the medium to interconnect the various Census Bureau information systems that are deployed. These information systems provide services such as authentication for internal and external customers, network security, LAN/WAN, e-mail, Internet access, remote access, mobile devices, and voice and video teleconferencing services. The personally identifiable information (PII) maintained by the IT system is account information (such as user ID, name, and email address) for federal employees, contractors, and external users; in order to access Census Bureau resources.

The Data Communications System contains a Microsoft O365 application, the digitized “Likeness and Profile Release” form, that will be used to establish the identity of an individual and capture the consent from the public, regarding photographs taken at Census Bureau events. At Census Bureau events, photographs of event attendees may be captured but will only be used if the individual identifies themselves and provides consent. If the event goer chooses to consent to their photograph being used by the U.S. Census Bureau, they will be handed a Census Bureau device with a copy of the digitized Likeness and Release form open and required to input their name and confirm that they are over the age of 18. Once they input their name and confirm they are over 18, the app will require them to take a selfie for purposes of identifying the signer, followed by the provision of a signature; an image capture of their signature will be saved for consent purposes. If the individual is under the age of 18, the app will require parental name, email address consent and signature. This information will be securely exported to the Enterprise Applications. Each individual’s consent form will be assigned a unique identifier and will not be searchable by PII.
Another purpose of the Data Communications System is for quality assurance and call-center agent training via the National Processing Center (NPC) Call Center Monitoring; The Call Center monitoring is a client application that is installed on NPC Call Center Agents’ Computers and when it detects an incoming call, it starts to capture the agent’s computer screen and call audio; this could include assisting an individual in completing a survey. This is intended to support quality assurance as well as to document incidents warranting dismissal. This data can be used by the Census Bureau for personnel enforcement. An assortment of PII may be captured via the video screen recordings and audio recordings depending on the nature of the call as members of the public opt to complete surveys via the call center. Although Title 13 information may be incidentally captured in the screen capture recordings and audio recordings, the purpose is not for Title 13 survey processing, but solely for quality assurance and call-center agent training. Incidental Title 13 screen capture recordings are deleted after 90 days and audio recordings are deleted after 180 days. No PII/BII captured via the screen capture recordings is searchable by personal identifier.

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

For authentication for internal and external customers, network security, LAN/WAN, e-mail, Internet access, remote access, and voice and video teleconferencing services, the PII collected is account information such as userID, name, telephone and email address and is from federal employees and contractors who use internal email systems and the general public who sign up to external web sites. The information used is to allow users the ability to authenticate to Census Bureau systems.

In regard to Call Center Monitoring functionalities used to support quality assurance and call center training; an assortment of PII may be captured via the agent screen recording and audio recordings. Title 13 PII may be incidentally collected from the public if they opt to complete their survey via the call center.

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

U.S. Census Bureau employees and contractors

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

Information is retrieved by the specific network device or application console by Census Bureau Telecommunications Office (TCO) administrators. For the digitized Likeness and Release form, information is retrieved upon by date and/or unique identifier.

No PII/BII captured is searchable by personal identifier.
(i) How information is transmitted to and from the system

Information in the Data Communications System varies based on the technology. All data is securely communicated through Secure Message Transfer Protocol (SMTP), Transport Layer Security (TLS) 1.2, and Secure Shell (SSH).

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.

__X__ This is an existing information system with changes that create new privacy risks.  Complete chart below, continue to answer questions, and complete certification.

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
<tr>
<td>d. Significant Merging</td>
</tr>
<tr>
<td>e. New Public Access</td>
</tr>
<tr>
<td>f. Commercial Sources</td>
</tr>
<tr>
<td>g. New Interagency Uses</td>
</tr>
<tr>
<td>h. Internal Flow or Collection</td>
</tr>
<tr>
<td>i. Alteration in Character of Data</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify): Adding a new screen capture recording/audio recording component</td>
</tr>
</tbody>
</table>

____ 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 or 01-2017).  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 01-2019 or later).  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.

__X__ 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.

_[X_] Yes.  *(Check all that apply.)*

<table>
<thead>
<tr>
<th>Activities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio recordings</td>
<td>X</td>
</tr>
<tr>
<td>Video surveillance</td>
<td></td>
</tr>
<tr>
<td>Other (specify): Video Screen Capture Recording and image capture of signatures</td>
<td></td>
</tr>
</tbody>
</table>

____ 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.

_[X_] 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_] Contractors working on behalf of DOC

_[X_] Other Federal Government personnel

_[X_] 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 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 Data Communications system 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.

<table>
<thead>
<tr>
<th>System Owner</th>
<th>Chief Information Security Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Kenneth Harrison</td>
<td>Name: Beau Houser</td>
</tr>
<tr>
<td>Office: Division Chief of Telecommunications Office</td>
<td>Office: Office of Information Security</td>
</tr>
<tr>
<td>Phone: (301) 763-5561</td>
<td>Phone: (301) 763-1235</td>
</tr>
<tr>
<td>Email: <a href="mailto:kenneth.r.harrison@census.gov">kenneth.r.harrison@census.gov</a></td>
<td>Email: <a href="mailto:beau.houser@census.gov">beau.houser@census.gov</a></td>
</tr>
</tbody>
</table>

Signature: KENNETH HARRISON
Date signed: 2021.07.02 07:34:18 -04'00'

Signature: BEAU Houser
Date signed: 2021.07.06 09:55:42 -04'00'

<table>
<thead>
<tr>
<th>Privacy Act Officer</th>
<th>Agency Authorizing Official</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Byron Crenshaw</td>
<td>Name: Luis Cano</td>
</tr>
<tr>
<td>Office: Policy Coordination Office (PCO)</td>
<td>Office: Chief Information Office</td>
</tr>
<tr>
<td>Phone: (301) 763-7997</td>
<td>Phone: (301) 763-3968</td>
</tr>
<tr>
<td>Email: <a href="mailto:byron.crenshaw@census.gov">byron.crenshaw@census.gov</a></td>
<td>Email: <a href="mailto:luis.j.cano@census.gov">luis.j.cano@census.gov</a></td>
</tr>
</tbody>
</table>

Signature: BYRON CRENSHAW
Date signed: 2021.06.16 14:21:22 -04'00'

Signature: LUIS CANO
Date signed: 2021.07.09 12:42:00 -04'00'

<table>
<thead>
<tr>
<th>Bureau Chief Privacy Officer</th>
<th>Business Authorizing Official</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Byron Crenshaw</td>
<td>Name:</td>
</tr>
<tr>
<td>Office: Policy Coordination Office (PCO)</td>
<td>Office:</td>
</tr>
<tr>
<td>Phone: (301) 763-7997</td>
<td>Phone:</td>
</tr>
<tr>
<td>Email: <a href="mailto:byron.crenshaw@census.gov">byron.crenshaw@census.gov</a></td>
<td>Email:</td>
</tr>
</tbody>
</table>

Signature: BYRON CRENShAW
Date signed: 2021.08.16 14:21:50 -04'00'

Signature: N/A
Date signed: N/A