



**2020 CENSUS PROGRAM MEMORANDUM SERIES: 2017.12**

**Date:** June 6, 2017

**MEMORANDUM FOR:** The Record

**From:** Lisa M. Blumerman  
Associate Director, Decennial Census Programs

**Subject:** The 2020 Census Detailed Operational Plan for the Security, Privacy, and Confidentiality operation (SPC)

**Contact:** Pamela Mosley  
Assistant Division Chief, Data Management and Testing  
301-763-5007  
Pamela.D.Mosley@census.gov

This memorandum documents the review of The 2020 Census Detailed Operational Plan for the Security, Privacy, and Confidentiality operation (SPC). The document baselines the overall 2020 Census SPC process and provides specific details for the SPC operation.

The SPC operation ensures that all operations and systems used in the 2020 Census adhere to appropriate systems and data security, respondent and employee privacy and confidentiality policies, and regulations.

**The 2020 Census Memorandum Series**

The 2020 Census Memorandum Series documents significant decisions, actions, and accomplishments of the 2020 Census Program for the purpose of informing stakeholders, coordinating interdivisional efforts, and documenting important historical changes.

A memorandum generally will be added to this series for any decision or documentation that meets the following criteria:

1. A major program level decision that will affect the overall design or have significant effect on the 2020 Census operations or systems.
2. A major policy decision or change that will affect the overall design or significantly impact the 2020 Census operations or systems.
3. A report that documents the research and testing for the 2020 Census operations or systems.

Visit 2020 Census on [Census.gov](https://www.census.gov) to access the Memorandum Series, the 2020 Operational Plan and other information about preparations for the 2020 Census.

# 2020 Census Detailed Operational Plan for: 3. Security, Privacy, and Confidentiality Operation (SPC)

---

*A New Design for the 21st Century*

Issued: June 6, 2017

Version: 1.0

Prepared by: Decennial Census Management Division



[Page intentionally left blank.]

## Approvals

This SPC Detailed Operational Plan has been reviewed and approved for use.

<u>Electronically Approved</u> Pamela Mosley IPT Lead	<u>3/20/17</u> Date Signed
<u>Electronically Approved</u> Mary Butler Branch Chief	<u>3/20/17</u> Date Signed
<u>Electronically Approved</u> Pamela Mosley IPT Program Manager	<u>3/20/17</u> Date Signed
<u>Electronically Approved</u> Deborah M. Stempowski Chief, Decennial Census Management Division	<u>4/27/17</u> Date Signed
<u>Electronically Approved by Atri Kalluri</u> Lisa M. Blumerman Associate Director for Decennial Census Programs Chair, Portfolio Management Governing Board	<u>6/5/17</u> Date Signed

## Document Change History

Revision #	Version	Date	Description
1	v0.01	December 19, 2016	Initial Shell Version from 2020 Census DOP template
2	v0.02b	January 23, 2017	Initial Working DRAFT Version from Shell – with updates to Section 2
3	v0.03	February 16, 2017	Updated Working DRAFT Version – with additional updates to Section 2
4	V1.0	March 20, 2017	Final Document

Note: Edit the fields below to update the Document Version, Date and Status in the Page Footers throughout the document.

### Document Footer Information Control Table

Field Name	Version, Date and Status
DocVersion:	Version 1.0
DocDate:	March 20, 2017
DocStatus:	Final

## Table of Contents

<b>1. Document Purpose.....</b>	<b>1</b>
<b>2. Operational Overview .....</b>	<b>2</b>
2.1 Operation Purpose .....	2
2.2 Background .....	2
2.3 Detailed Operational Plan Scope.....	3
2.3.1 SPC Activity Areas .....	3
2.3.2 SPC Operational Context.....	4
2.3.2.1 SPC Operational Inputs .....	6
2.3.2.2 SPC Operational Controls .....	7
2.3.2.3 SPC Operational Outputs.....	8
2.3.2.4 SPC Operational Mechanisms .....	10
<b>3. SPC Operation Detailed Process Description – Security [SPC 3-1] .....</b>	<b>13</b>
3.1 Leadership & Organization [SPC 3-1.1].....	14
3.1.1 IT Security Responsibilities [SPC 3-1.1.1].....	15
3.1.2 IT Security Road Map [SPC 3-1.1.2].....	17
3.1.3 IT Security Governance [SPC 3-1.1.3].....	17
3.1.4 IT Security Planning [SPC 3-1.1.4] .....	18
3.1.5 IT Security Law & Regulations [SPC 3-1.1.5].....	18
3.1.6 IT Security Policy [SPC 3-1.1.6] .....	19
3.2 Security Risk Management [SPC 3-1.2] .....	19
3.2.1 Risk Management Framework (RMF) [SPC 3-1.2.1].....	20
3.2.2 Security Categorization of Systems [SPC 3-1.2.2].....	21
3.2.3 Security & Privacy Control Selection [SPC 3-1.2.3].....	22
3.2.4 Security Test & Evaluation [SPC 3-1.2.4].....	22
3.2.5 Vulnerability/Red Team Assessment [SPC 3-1.2.5].....	24
3.2.6 Risk/Issue Identification & Tracking [SPC 3-1.2.6].....	24
3.2.7 System Security Plans (SSP) [SPC 3-1.2.7] .....	25
3.2.8 Plans of Action & Milestones (POA&Ms) [SPC 3-1.2.8].....	25
3.3 Engineering & Information Security [SPC 3-1.3].....	26

3.3.1	Integration of InfoSec into SDLC [SPC 3-1.3.1].....	26
3.3.2	Management Controls Implementation [SPC 3-1.3.2] .....	27
3.3.3	Operational Controls Implementation [SPC 3-1.3.3] .....	27
3.3.4	Technical Controls Implementation [SPC 3-1.3.4].....	28
3.3.5	Privacy Controls Implementation [SPC 3-1.3.5] .....	28
3.3.6	IT Security Procedures [SPC 3-1.3.6].....	29
3.3.7	Best Practices Guidance Implementation [SPC 3-1.3.7] .....	29
3.3.8	Authorization To Operate (ATO) [SPC 3-1.3.8] .....	30
3.3.9	Continuous Monitoring & Remediation [SPC 3-1.3.9] .....	31
3.4	Incident Response (IR) [SPC 3-1.4].....	31
3.4.1	Computer Security Operations Center (CSOC) Functions [SPC 3-1.4.1] .....	31
3.4.2	Incident Response Procedures [SPC 3-1.4.2] .....	31
3.4.3	External Agency Partnership [SPC 3-1.4.3] .....	32
3.4.4	IR Capability Testing/Training [SPC 3-1.4.4].....	32
3.5	Security Training & Awareness [SPC 3-1.5].....	32
3.5.1	General User Annual Training & Awareness [SPC 3-1.5.1] .....	33
3.5.2	Technical Staff Development [SPC 3-1.5.2] .....	33
3.5.3	Training & Awareness Communications [SPC 3-1.5.3].....	34
<b>4.</b>	<b>SPC Operation Detailed Process Description – Privacy and Confidentiality [SPC 3-2].....</b>	<b>35</b>
4.1	Leadership & Organization [SPC 3-2.1].....	36
4.1.1	Privacy Program Governance [SPC 3-2.1.1] .....	36
4.1.2	Privacy Program Management [SPC 3-2.1.2].....	37
4.2	Privacy Risk Management [SPC 3-2.2] .....	37
4.2.1	PII Inventory, Categorization and Minimization [SPC 3-2.2.1].....	38
4.2.2	Privacy Risk & Impact Assessment Maintenance [SPC 3-2.2.2].....	38
4.2.3	System of Record Notice (SORN) Maintenance [SPC 3-2.2.3] .....	39
4.2.4	Privacy Act Statement (PAS) Activities [SPC 3-2.2.4].....	39
4.2.5	Data Quality and Integrity Activities [SPC 3-2.2.5].....	39
4.2.6	PII Retention, Disposition, and Destruction [SPC 3-2.2.6] .....	39

4.2.7	FOIA Requests [SPC 3-2.2.7].....	39
4.2.8	Controlled Sharing of Information [SPC 3-2.2.8] .....	40
4.2.9	Privacy and Social Media [SPC 3-2.2.9] .....	41
4.2.10	Government Privacy Change Monitoring [SPC 3-2.2.10].....	41
4.2.11	Privacy Risk and Issue Tracking [SPC 3-2.2.11] .....	41
4.3	Engineering and Information Security [SPC 3-2.3].....	42
4.3.1	Cybersecurity Coordination [SPC 3-2.3.1].....	42
4.3.2	Authority to Operate (ATO) and Authority to Connect (ATU) Analysis [SPC 3-2.3.2] 42	
4.4	Incident Response (IR) [SPC 3-2.4].....	42
4.4.1	Privacy and Confidentiality Incident Management [SPC 3-2.4.1] .....	43
4.4.2	Incident Notification & Reporting [SPC 3-2.4.2].....	43
4.4.3	High-Impact Privacy Incident Response Team Activities [SPC 3-2.4.3].....	43
4.5	Transparency and Redress [SPC 3-2.5].....	44
4.5.1	Privacy Notice Maintenance Activities [SPC 3-2.5.1] .....	44
4.5.2	Managing Complaints and Inquiries [SPC 3-2.5.2].....	44
4.5.3	Individual Access, Amendment, Correction, Redress, and Accounting of Disclosures [SPC 3-2.2.3].....	44
4.6	Privacy Training & Awareness [SPC 3-2.6] .....	45
4.6.1	Workforce Training [SPC 3-2.6.1] .....	45
4.6.2	Internal Online Presence [SPC 3-2.6.2].....	46
4.7	Accountability [SPC 3-2.7].....	46
4.7.1	Rules of Behavior Acknowledgement [SPC 3-2.7.1] .....	46
4.7.2	Internal & External Reporting [SPC 3-2.7.2] .....	47
4.7.3	Privacy Monitoring and Auditing [SPC 3-2.7.3] .....	47
4.7.4	Incorporating Lessons Learned [SPC 3-2.7.4].....	47

**5. Cost Factors.....48**  
**6. Measures of Success.....49**  
**Appendix A – Acronyms and Terminology .....50**  
**Appendix B – References.....58**  
**Appendix C – Activity Tree for Security, Privacy, and Confidentiality  
Operation (SPC) .....59**

**List of Figures**

Figure 1: Security, Privacy, and Confidentiality Operation (SPC) Context Diagram ..... 5  
Figure 2: Security [SPC 3-1] Constituent Activities..... 14  
Figure 3: U.S. Census Bureau RMF Methodology Mapped to the NIST RMF ..... 20  
Figure 4: Privacy and Confidentiality [SPC 3-2] Constituent Activities..... 36

**List of Tables**

Table 1: SPC Operational Inputs ..... 6  
Table 2: SPC Operational Controls..... 7  
Table 3: SPC Operational Outputs..... 9  
Table 4: Staff Resources used within SPC Operational Activities ..... 10  
Table 5: Infrastructure Sites for SPC Operational Activities..... 11  
Table 6: Systems used within SPC Operational Activities..... 12  
Table 7: Acronyms and Abbreviations List ..... 50  
Table 8: Glossary of Terms..... 54

## 1. Document Purpose

The 2020 Census Detailed Operational Plan for the Security, Privacy, and Confidentiality operation (SPC) is intended for use by U.S. Census Bureau managers, staff, contractors, and other internal and external stakeholders working on the 2020 Census. The document provides a high level description of the production support processes for the 2020 Census SPC operation and includes a summary of the operational processes involved, their inputs, outputs and controls, and the basic mechanisms employed to conduct the operational work.

Anticipated uses of this document include the following:

- Communication – Documents operational design details for internal and external stakeholders.
- Planning – Documents planning assumptions and key milestones.
- Staffing – Documents staffing needs and strategies.

This document complements the 2020 Census Operational Plan, which presents the 2020 Census operational design and covers all operations required to execute the 2020 Census, starting with precensus address and geographic feature updates and ending once census data products are disseminated and coverage and quality are measured.

This document will be updated over time to reflect changes in strategies that result from 2020 Census planning, research, and testing activities.

## **2. Operational Overview**

### **2.1 Operation Purpose**

The SPC operation ensures that all operations and systems used in the 2020 Census adhere to the following policies and regulations:

- Appropriate systems and data security.
- Respondent and employee privacy and confidentiality.

### **2.2 Background**

In order to ensure that all 2020 Census operations and systems adhere to the appropriate systems and data security standards and perform the required privacy and confidentiality functions, the Security, Privacy, and Confidentiality (SPC) operation includes support activities for the following requirements:

#### *Security*

- IT Security Program Policy Compliance.
- Data Stewardship Policies Compliance.
- Mission and Legal Requirements Compliance.
- Authority to Operate (ATO) Process.
- Information System Security Officer (ISSO) Functions.
- Risk Management Framework.
- Suitability Screening Processes.

#### *Privacy and Confidentiality*

- Privacy Impact Assessments.
- Privacy Threshold Analyses.
- System of Record Notices.
- Accreditation Process.
- Special Sworn Status Certification for Title 13 and Title 26 Materials Handling.
- Personally Identifiable Information (PII) Incident Handling Processes.

Key innovations planned for the 2020 Census SPC operation include:

- Implement an IT Security Program Risk Management Framework in accordance with National Institute of Standards and Technology guidelines.
- Hire a 2020 Census Chief IT Security Engineer to support application development, mobile computing, and enterprise systems.

- Increase staff in the Census Bureau Office of Information Security to provide penetration testing services and more extensive scanning for vulnerabilities and configuration management.
- Align all Privacy Impact Assessments and Privacy Threshold Assessments to the System Security Plans.

## 2.3 Detailed Operational Plan Scope

The discussions of Security, Privacy and Confidentiality activities in this document focus on the run-time Operation and Maintenance (O&M) functions for IT Security components and Privacy and Confidentiality components during the conduct of the 2020 Census. The IT Security planning activities and the Privacy and Confidentiality planning activities are described elsewhere.

The SPC process discussion below employs a descriptive framework used to characterize the scope of the SPC O&M functions. This framework is based on functional analysis of both the Security domain and the Privacy and Confidentiality domain as they relate to the key operational activity areas used to support the conduct of 2020 Census.

### 2.3.1 SPC Activity Areas

The SPC operation for the 2020 Census includes two major operational activity areas:

- Security.
- Privacy and Confidentiality.

Each of these major activity areas is summarized below. Together, these activities represent the complete set of work that needs to be performed by this operation during the conduct of the 2020 Census.

#### *Security*

The top-level Security activity areas are:

- **Leadership & Organization:** Organizational support for security program priorities and initiatives.
- **Security Risk Management:** Methods and process used to identify, assess, prioritize, and manage security risk.
- **Engineering & Information Security:** Incorporating security into the enterprise systems engineering approach and integrating with privacy and confidentiality.
- **Incident Response:** Management of and response to security incidents, including breaches.

- **Security Training & Awareness:** Establishment of workforce training and a culture of security awareness.

### *Privacy and Confidentiality*

The top-level Privacy and Confidentiality activity areas are:

- **Leadership & Organization:** Organizational support for privacy and confidentiality program priorities and initiatives.
- **Privacy Risk Management:** Methods and process used to identify, assess, prioritize, and manage privacy risk.
- **Engineering & Information Security:** Incorporating privacy and confidentiality into the enterprise systems engineering approach and integrating with security.
- **Incident Response:** Management of and response to privacy incidents, including breaches.
- **Transparency & Redress:** Visibility into the information about the public that the agency collects and uses as well as the ability to address inquiries and complaints.
- **Privacy Training & Awareness:** Establishment of workforce training and a culture of privacy and confidentiality awareness.
- **Accountability:** Responsibility of the workforce to implement privacy principles and requirements and answerability of the agency to the public.

The full hierarchy of activities for the SPC operation is provided in Appendix C in the form of an activity tree. In the activity tree, each major operational activity area listed above is numbered and then decomposed into a numbered set of subactivities, some of which are further decomposed into more detailed numbered subactivities or steps.

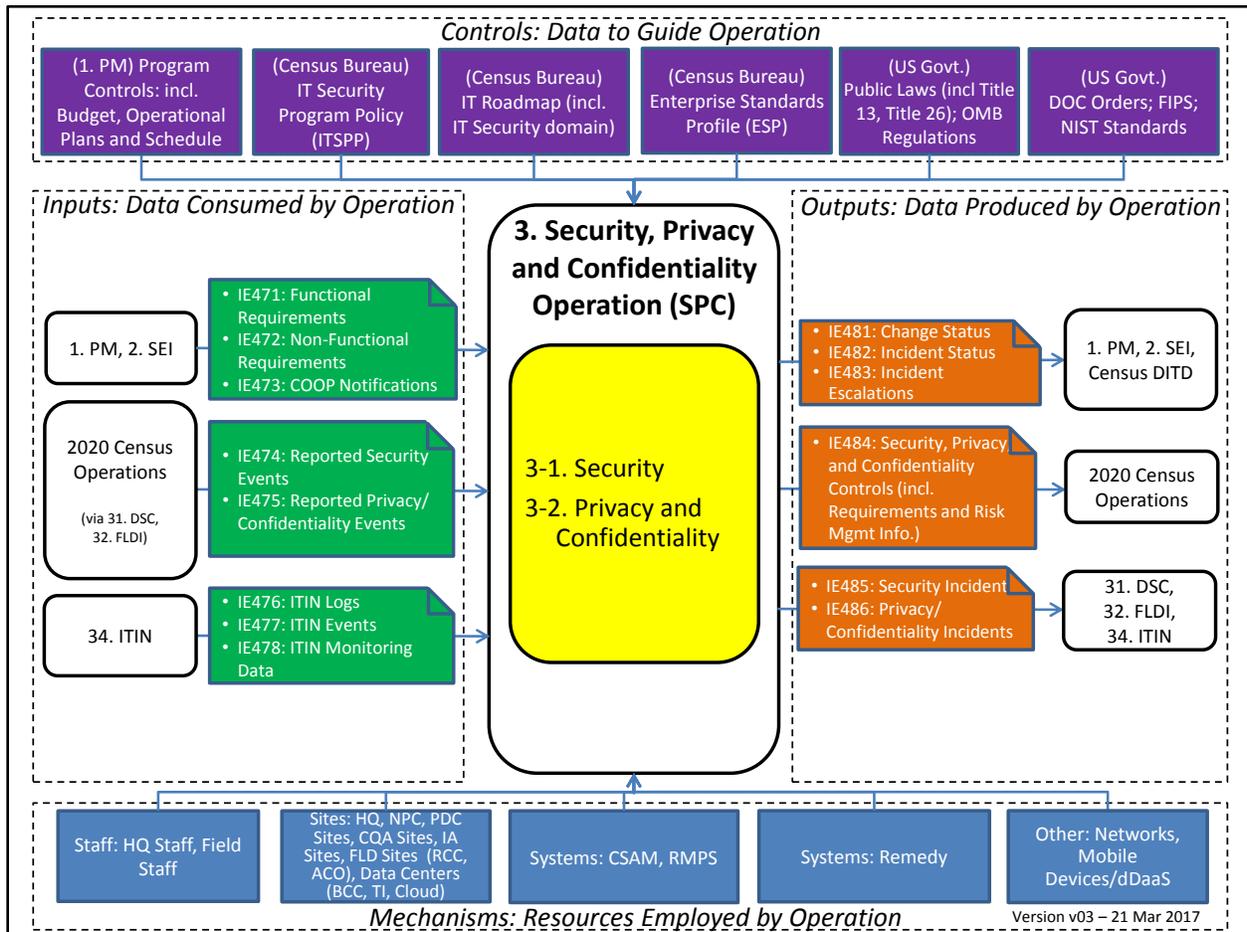
For a full description of the operational subactivities that comprise the SPC operation, see the Detailed Process Description discussions in Section 3 (Security) and Section 4 (Privacy and Confidentiality) below.

### **2.3.2 SPC Operational Context**

The SPC operational activities described above are conducted within the context of other 2020 Census operations and other programs or data sources that are external to the 2020 Census Program. One way to depict an operational context is by using a “Context Diagram,” which shows the boundary of the operational process, the operational activities it contains, and the information exchanged with its neighbor operations (or other entities), as well as the resources (mechanisms) needed to conduct the operational work.

Figure 1 is a top-level context diagram for the SPC operation represented as an Integrated Definition, Level 0 (IDEF0) model. An IDEF0 model of a process (or operation) shows the Inputs, Controls, Outputs and Mechanisms of the process. These IDEF0 model elements are summarized below and described further in the sections that follow.

The yellow box in the center of the IDEF0 model lists the major operational activity areas for the operation, numbered as given in the SPC operation Activity Tree in Appendix C. Specific Information Exchanges (IE) are shown in different colored boxes to represent the Inputs (green boxes on left side), Outputs (orange boxes on right side), Controls (purple boxes on top) and Mechanisms (blue boxes on the bottom). Boxes to the left of the Inputs indicate the *Provider* of the inputs to the operation (typically another 2020 Census operation or an external source). The Provider of the Controls is noted in the box itself. Boxes to the right of the Outputs indicate the *Receiver* of the outputs (typically another 2020 Census operation or external entity). Each Information Exchange has a name and a unique number for identification purposes.



**Figure 1: Security, Privacy, and Confidentiality Operation (SPC) Context Diagram**

For detailed descriptions of the Inputs, Controls, Outputs, and Mechanisms used by the SPC operation, see the sections that follow.

### 2.3.2.1 SPC Operational Inputs

Inputs are the data that are consumed by the operation. The inputs define the amount of operational work that needs to be performed.

Table 1 lists the inputs to the SPC operation.

**Table 1: SPC Operational Inputs**

<b>Provider</b>	<b>Information Exchange</b>	<b>Description</b>
1. Program Management (PM) Operation  2. Systems Engineering and Integration (SEI) Operation	<ul style="list-style-type: none"> <li>• IE471: Functional Requirements</li> <li>• IE472: Nonfunctional Requirements</li> <li>• IE473: COOP Notifications</li> </ul>	Functional and nonfunctional requirements relating to SPC operation.  Notification of COOP decisions from 2020 Census Program Management.  Used to identify required operational behaviors and characteristics and plan for COOP events.
2020 Census Operations  (incl. 31. DSC, 32. FLDI)	<ul style="list-style-type: none"> <li>• IE474: Security Event Reports</li> <li>• IE475: Privacy/Confidentiality Event Reports</li> </ul>	Event Reports relating to suspected or ongoing Security Incidents or Privacy/Confidentiality Incidents.  Used to inform SPC staff of ongoing conditions regarding Security and Privacy/ Confidentiality.
34. ITIN	<ul style="list-style-type: none"> <li>• IE476: ITIN Logs</li> <li>• IE477: ITIN Events</li> <li>• IE478: ITIN Monitoring Data</li> </ul>	Logs, events and monitoring data provided to the SPC operation relating to security, privacy, and confidentiality conditions within the IT Infrastructure environment.

### 2.3.2.2 SPC Operational Controls

Controls are the data that guide the behavior of the operation. They are not consumed by the operation, but rather they provide guidance, models, limits, criteria, cutoff dates, or other information that controls the way in which the operational work is performed.

Table 2 lists the controls for the SPC operation.

**Table 2: SPC Operational Controls**

Provider	Information Exchange	Description
1. PM Operation	Program Controls	Program Control information including: <ul style="list-style-type: none"> <li>• Budget</li> <li>• Operational Plans and Schedule</li> </ul>
Census Bureau	Census Bureau IT Security Program Policy (ITSPP)  Census Bureau IT Roadmap (including IT Security domain)  Census Bureau Enterprise Standards Profile (ESP)	Census Bureau Process, Standards, Planning and Control Documentation.  Used to inform SPC Management staff of expected actions and behaviors and provide information needed in the formulation of SPC operational procedures.

U.S. Government	Public Laws (including Title 13, Title 26)  Office of Management and Budget (OMB) Regulations  Department of Commerce (DOC) Orders  Federal Information Processing Standards (FIPS)  National Institute of Standards and Technology (NIST) Standards	Applicable U.S. Federal Government Laws, Regulations and Standards.
-----------------	--	---

**2.3.2.3 SPC Operational Outputs**

Outputs are the data produced by the operation. The outputs constitute the results of operational work that has been performed. Outputs produced may be used as inputs or controls to other operations.

Table 3 lists the outputs from the SPC operation.

**Table 3: SPC Operational Outputs**

Consumer	Information Exchange	Description
<p>1. Program Management Operation (PM)</p> <p>2. Systems Engineering and Integration Operation (SEI)</p> <p>Decennial IT Division (DITD)</p>	<ul style="list-style-type: none"> <li>• IE481: Change Status</li> <li>• IE482: Incident Status</li> <li>• IE483: Incident Escalations</li> </ul>	<p>Documentation provided by SPC Management staff to inform the 2020 Census Program (PM and SEI) and Decennial IT Division (DITD) of routine SPC status updates/changes and SPC problem/incident status.</p>
<p>2020 Census Operations</p>	<ul style="list-style-type: none"> <li>• IE484: Security, Privacy and Confidentiality Controls (including Requirements and Risk Management Information)</li> </ul>	<p>Laws, policies, regulations, and guidelines related to physical security, IT security, data security and privacy and confidentiality impacts, analyses, and processes. These include but are not limited to Title 13, Title 26, and other laws and policies related to protection of personally identifiable information.</p> <p>This information includes the common controls in place or planned for meeting applicable security, privacy and confidentiality requirements and managing security, privacy and confidentiality risks (e.g. Physical Security Controls).</p>
<p>31. DSC</p> <p>32. FLDI</p> <p>34. ITIN</p>	<ul style="list-style-type: none"> <li>• IE485: Security Events</li> <li>• IE486: Privacy/ Confidentiality Events</li> </ul>	<p>Notifications of ongoing Security Incident or Privacy/Confidentiality Incident status.</p> <p>Used to inform IT Management staff of ongoing conditions regarding Security and Privacy/ Confidentiality.</p>

### 2.3.2.4 SPC Operational Mechanisms

Mechanisms are the resources (people, places, and things) that are used to perform the operational processes. They include Staff Resources, Infrastructure Sites, and Systems and other Technology Infrastructure.

#### *Staff Resources*

Table 4 identifies the Staff Resources employed for the SPC operation.

**Table 4: Staff Resources used within SPC Operational Activities**

<b>Staff Resources</b>	<b>Description/Role</b>
Headquarters (HQ) Staff	HQ Staff to manage overall SPC Production operation and coordinate activities with other sites for 2020 Census Security activities and Privacy and Confidentiality activities. HQ Staff to conduct monitoring, analysis, and ongoing SPC Incident Management support, O&M and planning work.
Field Staff	Field Staff to manage SPC Production operation within Field sites and coordinate activities with other sites for 2020 Census Security activities and Privacy and Confidentiality activities. Field Staff to conduct monitoring, analysis and ongoing SPC Incident Management support, O&M and planning work.

***Infrastructure Sites***

Table 5 identifies the Infrastructure Sites employed for the SPC operation.

**Table 5: Infrastructure Sites for SPC Operational Activities**

<b>Infrastructure Site</b>	<b>Description/Role</b>
HQ	HQ Sites for SPC monitoring, analysis, and planning work.
NPC	National Processing Center site used for 2020 Census Production operational work.
Paper Data Capture (PDC) Center Sites	PDC Center sites hosting Census IT assets used for 2020 Census Production operational work. Note: One of the PDC Center sites is located at the NPC.
Census Questionnaire Assistance (CQA) Center Sites	CQA Center sites hosting Census IT assets used for 2020 Census Production operational work.
Island Areas (IA) Sites	IA sites (e.g. IA ACOs) hosting Census IT assets used for 2020 Census Production operational work.
Field Sites (Regional Census Center (RCC), Area Census Office (ACO))	Field sites (RCCs and ACOs) hosting Census IT assets used for 2020 Census Production operational work.
Data Centers (Bowie Computer Center (BCC), TI, Cloud)	Data Center sites hosting Census (BCC), TI, or Cloud-based IT assets used for 2020 Census Production operational work.

### *Systems and other Technology Infrastructure*

Table 6 identifies the Systems employed for the SPC operation.

**Table 6: Systems used within SPC Operational Activities**

<b>System</b>	<b>Description</b>
Cyber Security Asset Management Tool (CSAM)	A centralized identification and tracking tool used to store system information, POA&Ms, and system security authorization packages. Also used to create and update System Security Plans. Also used along with RMPS as a FISMA system inventory tool to support system tracking, management, and reporting.
Risk Management Program System (RMPS)	A risk profiling tool used to document the security control baseline for a system. Also used along with CSAM as a FISMA system inventory tool to support system tracking, management, and reporting.
Remedy (Trouble Ticketing Tool)	A commercial trouble ticketing tool used for used for Incident Reporting and Incident Response tracking. For incident notification, all reported incidents go through the Help Desk staff, where Remedy tickets are created for tracking the resolution of incidents.

Other Technology Infrastructure employed for the SPC operation includes:

- Networks.
- Mobile Devices/dDaaS.

### **3. SPC Operation Detailed Process Description – Security [SPC 3-1]**

IT Security at the U.S. Census Bureau continues to evolve to combat today’s dynamic threat landscape. The Census Bureau seeks to mitigate threats and vulnerabilities by addressing IT security through the dedication of people, robust technology, well-defined procedure, best practices, and written policy. Risk management, automation, and security assessment are key security focus areas that are used to ensure enterprise and 2020 Census systems remain operationally secure and effective in support of the general public.

The security discussion in this section focuses on the Operation and Maintenance (O&M) of the IT Security components of the 2020 Census. The IT Security planning activities are described elsewhere.

The Security Activity Area of the SPC operation [SPC 3-1] is subdivided into the following constituent Activities (See Figure 2).

- Leadership & Organization [SPC 3-1.1].
- Security Risk Management [SPC 3-1.2].
- Engineering & Information Security [SPC 3-1.3].
- Incident Response (IR) [SPC 3-1.4].
- Security Training & Awareness [SPC 3-1.5].



**Figure 2: Security [SPC 3-1] Constituent Activities**

The business processes for each of these Security activity areas are discussed along with their inputs and outputs in the following subsections.

### **3.1 Leadership & Organization [SPC 3-1.1]**

The Leadership & Organization activity area is subdivided into the following operational subactivities.

- IT Security Responsibilities [SPC 3-1.1.1].
- IT Security Road Map [SPC 3-1.1.2].
- IT Security Governance [SPC 3-1.1.3].
- IT Security Planning [SPC 3-1.1.4].
- IT Security Law & Regulations [SPC 3-1.1.5].
- IT Security Policy [SPC 3-1.1.6].

Subsequent sections describe the Leadership & Organization operational subactivities.

### **3.1.1 IT Security Responsibilities [SPC 3-1.1.1]**

The U.S. Census Bureau has identified and established IT security roles to coordinate security activities, assign responsibility, and mitigate risk to both Census Bureau and 2020 Census data and systems. The *Census Bureau IT Security Program Policy (ITSPP)* [November 2015], Section 3.3, has identified a number of established roles. Key IT security roles have been highlighted here for brevity. Please refer to the ITSPP for a comprehensive list of Census Bureau roles. These key roles include, but are not limited to:

#### ***Census Bureau Director***

The Director of the Census Bureau is accountable to the Department of Commerce (DOC) for developing and implementing the Census Bureau's IT security program. The Director performs a number of key IT security duties including:

- Ensuring that the Census Bureau has an established IT security program to protect its IT systems.
- Communicating the importance of IT security in the Census Bureau's mission to all Census Bureau employees.
- Assigning management of IT systems to responsible program officials.

#### ***Chief Information Officer (CIO)***

The CIO performs a number of IT-security related functions. Some key responsibilities include:

- Coordinating with DOC and Census Bureau staff.
- Managing the Census Bureau IT Security Program.
- Appointing a Census Bureau Chief Information Security Officer (CISO) to implement the IT Security Program.
- Ensuring that Census Bureau IT Security Policy is developed, approved and maintained.
- Providing overall leadership and direction of the IT Security Program.
- Ensuring the IT Security Program complies with FISMA and other federal government guidance.
- Approval of system ATO packages.
- Ensuring that IT Security Planning is performed throughout the system development life cycle.
- Providing training opportunities to those staff with significant IT security responsibilities.

### ***Chief Information Security Officer (CISO)***

The Census Bureau CISO is the Senior Agency Information Security Officer (SAISO) appointed by the Census Bureau CIO. The Census Bureau CISO/SAISO reports to the DOC CISO/SAISO, through the Census Bureau CIO. The Census Bureau CISO/SAISO serves as the principal adviser to the Authorizing Official (AO), System Owners (SO), and DOC CISO/SAISO on strategic IT Security matters involving Census Bureau IT systems. Some key CISO functions include:

- Developing and maintaining an overall Census Bureau Cybersecurity Strategy.
- Influencing the development of the Census Bureau IT Security Policy, procedures, standards, and guidance consistent with departmental and federal requirements.
- Participating as a standing member of the Census Bureau Breach Notification Team.
- Review and approval of interagency and internal Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), Service Level Agreements (SLA) and Interconnection Security Agreements (ISA).

### ***Authorizing Official (AO)***

The AO assumes responsibility for operating an information system at an acceptable level of risk by issuing a risk-based, authorization decision, as well as terms and conditions for the authorization.

The authorization decision for the information system can take the form of an Authorization to Operate (ATO), Interim Authorization to Operate (IATO) or Denial of Authorization to Operate (DATO). The AO authorizes System Security Plans (SSPs), Continuous Monitoring Plans, ISAs, and MOAs and/or MOUs.

### ***Information System Security Officer (ISSO)***

The responsibility of each Census Bureau ISSO is to ensure the appropriate operational security posture for an information system or program is maintained. The ISSO also serves as the principal advisor to the CISO/SAISO and System Owner (SO) on all security matters for the information system.

ISSOs perform an active role in developing and updating System Security Plans (SSP), addressing Plans of Action & Milestones (POA&M), managing and controlling changes to the system, and assessing the security impact of those changes. ISSOs are typically assigned to a particular Cen(Census)Plan, which may include multiple systems. ISSOs are assigned to systems once the ATO has been granted.

### **3.1.2 IT Security Road Map [SPC 3-1.1.2]**

The Census Bureau has an established IT Road Map that incorporates the IT Security domain. The IT Road Map articulates 26 Technology Areas mapped across the ESP, a framework for Enterprise Architecture standards. Road Map Technology Areas were based on an understanding of the Census IT environment. For each Technology Area, the current state and the future state are defined.

The IT Security domain technology areas include:

- Network Infrastructure Security Services.
- Remote Access Management Services.
- Identity and Access Management Services.
- End-Point Security Services.
- Filtering Services.
- Public Key Infrastructure Services.
- Cyber Forensic Services.

### **3.1.3 IT Security Governance [SPC 3-1.1.3]**

The IT Security Governance structure at the U.S. Census Bureau is defined in the *Census Bureau IT Security Program Policy (ITSP)*. The ITSP defines a number of standing working groups that oversee the direction of IT security and its support to the operational mission of the larger Bureau and 2020 Census. These groups include:

- Census IT Directorate Project Review Governance Board.
- Standards Working Group.
- Secure Configurations Working Group.
- Architecture Review Board.
- Data Stewardship Executive Policy Committee.
- IT Risk Review Board.
- IT Change Advisory Board.
- Systems Development Lifecycle Center of Excellence.
- IT Investment Review Board.
- IT Purchase Review Board.

### **3.1.4 IT Security Planning [SPC 3-1.1.4]**

The Census Bureau has composed a number of planning and procedures documents that provide guidance in the secure operation of IT systems, for both the Census Bureau and the 2020 Census. These include:

- Secure System Development Life Cycle Methodology.
- New System Security Control Assessment Standard Operating Procedure.
- Census Bureau Risk Management Framework Methodology.
- Risk Management Program System User Guide.

### **3.1.5 IT Security Law & Regulations [SPC 3-1.1.5]**

A number of laws and regulations shape the operations of the Census Bureau and 2020 Census. These include U.S. public laws, Office of Management and Budget (OMB) regulations, and DOC Administrative and Organization Orders. The Census Bureau ITSPP contains a comprehensive list of applicable laws and regulations. Some key laws and regulations include:

Public Laws:

- Title 13, United States Code, The Census Act.
- Title 26, United States Code, The Internal Revenue Code.
- Computer Fraud and Abuse Act.
- FISMA.

OMB Regulations:

- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources.
- OMB Circular A-127 Revised, Financial Management Systems.

Department of Commerce Administrative and Organization Orders:

- Department Administrative Order 207-1, Security Programs.

The Census Bureau is also required to comply with all Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST) standards. Some of these include:

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.
- SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*.
- SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

### 3.1.6 IT Security Policy [SPC 3-1.1.6]

A number of laws and regulations have shaped organizational policy at the Census Bureau. Some key security policies include:

- **IT Scanning Policy:** This document identifies the requirements for vulnerability and compliance scans, remediation time frames, and external party scanning.
- **Patch Management Policy:** The Patch Management Policy enumerates responsibilities, procedures, and time frames for addressing security vulnerabilities.
- **Secure Configuration Policy:** This document establishes the policy for the development of, and compliance with, Enterprise Secure Configuration Benchmarks for core Information Technology (IT) components at the U.S. Census Bureau. The policy enumerates several requirements including: the identification of IT components for benchmarks; development of benchmarks; compliance with benchmarks; and security assessment against established benchmarks.
- **Incident Response Policy:** The purpose of this policy is to ensure that the Census Bureau appropriately handles confirmed or suspected computer security incidents and data security breaches. The policy identifies and assigns incident response roles, responsibilities, and reporting requirements.

## 3.2 Security Risk Management [SPC 3-1.2]

The U.S. Census Bureau has applied the NIST Risk Management Framework to information systems within its organizational boundary. The Risk Management Framework supersedes the legacy Assessment and Authorization (A&A) process with a more dynamic and comprehensive approach to risk management. Please refer to the *Census Bureau RMF Methodology* for a comprehensive treatment of each of the topical areas present in this section.

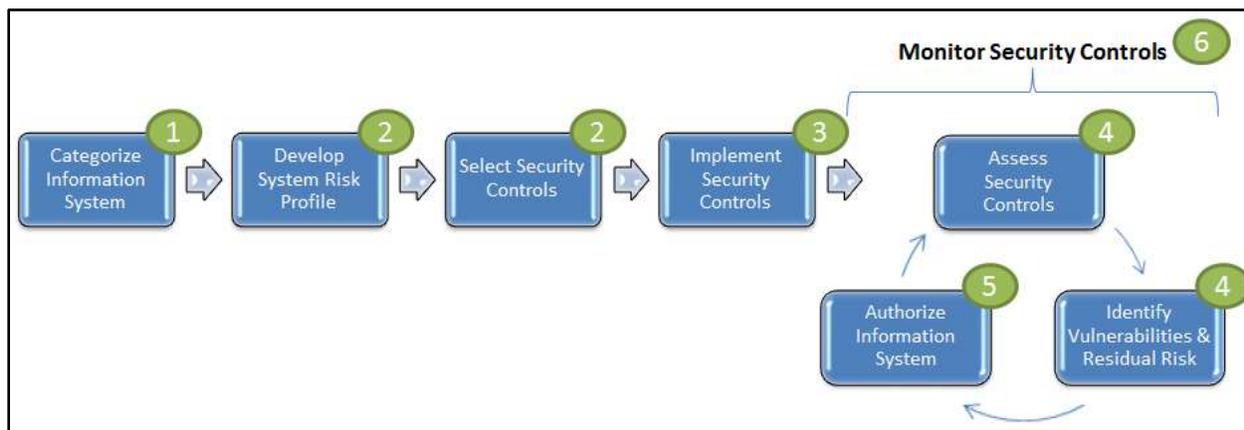
The Security Risk Management activity area is subdivided into the following operational subactivities.

- Risk Management Framework (RMF) [SPC 3-1.2.1].
- Security Categorization of Systems [SPC 3-1.2.2].
- Security & Privacy Control Selection [SPC 3-1.2.3].
- Security Test & Evaluation [SPC 3-1.2.4].
- Vulnerability/Red Team Assessment [SPC 3-1.2.5].
- Risk/Issue Identification & Tracking [SPC 3-1.2.6].
- System Security Plans (SSP) [SPC 3-1.2.7].
- Plans of Action & Milestones (POA&Ms) [SPC 3-1.2.8].

Subsequent sections describe the Security Risk Management operational subactivities.

### 3.2.1 Risk Management Framework (RMF) [SPC 3-1.2.1]

The Census Bureau has developed an RMF Methodology that aligns with the RMF in NIST SP 800-37. This process has been documented in the *Census Bureau Risk Management Framework Methodology* [September 2016]. Figure 3 illustrates the mapping between Census Bureau RMF Methodology and the NIST RMF.



**Figure 3: U.S. Census Bureau RMF Methodology Mapped to the NIST RMF**

The Census Bureau RMF Methodology also incorporates three significant enhancements into the NIST RMF:

- **Risk Profiling:** Business process and technology factors are used to develop an information system's Risk Profile. The Risk Profile helps to identify appropriate security controls as well as determine the level of risk for each control.
- **Continuous Monitoring Plan:** The selection of security controls for ongoing assessments, as well as the frequency for assessments, are prioritized based on the Risk Profile of the information system along with other factors.
- **Automated Assessments:** Secure configuration standards are developed for major platforms, and tools are configured to perform automated assessments of information systems against the established standards.

Please refer to the *Census Bureau RMF Methodology* for a comprehensive treatment of each of the steps.

### 3.2.2 Security Categorization of Systems [SPC 3-1.2.2]

The Census Bureau divides the system categorization of the NIST Risk Management Framework into three distinct steps: 1) the System Description, 2) System Categorization, and 3) System Registration.

#### *System Description*

The system description captures the system's purpose and its technical environment. The Office of Information Security (OIS) Risk Management Team (RMT) elicits information about the system from the System Owner (SO) and Information System Security Officer (ISSO) for documentation in the System Security Plan (SSP).

#### *System Categorization*

The security categorization of an information system identifies the potential impact to the security objectives of confidentiality, integrity, and availability. This process occurs at the Census Bureau in accordance with FIPS 199.

The SO and ISSO begin the system categorization process by identifying the information types that are processed, transmitted, and stored by the information system. Once the information types have been identified, the OIS RMT uses a Risk Profiling tool to automatically calculate the system categorization. The OIS RMT reviews the appropriateness of the overall system security category with the SO and ISSO and adjusts the overall system security category as necessary.

#### *System Registration*

The last step in the system categorization process is to register the information system. Based on the system description documented in the Risk Profiling tool, the OIS RMT registers the

information system in the FISMA system inventory tool to support system tracking, management, and reporting.

### **3.2.3 Security & Privacy Control Selection [SPC 3-1.2.3]**

The Census Bureau separates security control selection into two phases: 1) Risk Profiling and 2) Selection.

Control selection begins with a risk profiling questionnaire. OIS RMT works with the System Owner and ISSO to complete the questionnaire. The questionnaire facilitates definition of the system's risk profile based on business and technical factors. These factors identify the risks applicable to Census Bureau information systems that use a given business process or technology. The results of the questionnaire assist in the determination of security controls.

Next, the risk profiling questionnaire results, the FIPS 200 standard, and NIST SP 800-53 Rev 4 inform the selection of applicable security controls using the Risk Profiling tool. The tool automatically identifies applicable security controls. An initial security baseline is identified through the tool that allows custom tailoring and scoping to the operational environment. The OIS RMT works with the System Owner and ISSO to validate that the security control baseline has been tailored and scoped appropriately. Adjustments are made as necessary and documented in the Risk Profiling tool. The resulting selection of security controls constitutes the security controls of the Risk Profile SSP.

### **3.2.4 Security Test & Evaluation [SPC 3-1.2.4]**

The U.S. Census Bureau Risk Management Program (RMP) has developed an approach for transforming the three-year Certification & Accreditation (C&A) cycle into a risk-based process for monitoring information systems on a continuous basis. The Security Test & Evaluation (STE) activity at the Census Bureau consists of security control assessments (SCA). SCAs ensure that system security controls are implemented, operating as intended, and fulfill the system's security requirements.

An SCA begins with development and approval of a security control assessment plan. The SCA plan identifies the following information:

- SCA Objective.
- Scope.
- Approach.
- Timeline.
- Resources.

- Test Cases.

Once complete, The OIS RMT meets with the System Owner and ISSO to review the security assessment plan and set expectations for the assessment. The OIS RMT updates the security assessment plan as necessary based on feedback from the System Owner and ISSO.

A security control assessment can then proceed. There are two categories of assessments:

- **Developmental Testing:** This is an initial security control assessment conducted during the Development/Acquisition phase of the SDLC. Developmental testing identifies security issues early in the SDLC so they can be resolved in an efficient and cost-effective manner.
- **Formal Testing:** Once the information system is ready for production deployment in the Implementation phase of the SDLC, a security control assessment is performed to obtain system authorization. Formal testing needs to be performed by an independent assessment team for systems with security categorizations of “High” or “Moderate.” Independent assessors are not required for systems with a security categorization of “Low.”

There are two types of formal security control assessments at the Census Bureau. These include:

- **Automated Assessment:** Automation of the security control assessment process supports the continuous monitoring process by making it possible to conduct SCAs at a higher frequency than had been possible in the traditional Assessment & Authorization (A&A) process. Before an automated security assessment, secure configuration standards are developed for core infrastructure that serve as a baseline for automated checks. These secure configuration standards are based on best practices security benchmarks. These security benchmarks include guidance from:
  - United States Government Configuration Baseline (USGCB).
  - Defense Information Systems Agency (DISA).
  - National Institute of Standards and Technology (NIST).
  - Center for Internet Security (CIS).

The secure configuration standards are mapped to NIST 800-53A controls where applicable, and automated checks are developed to assess these technical controls. Automated checks are developed using the Security Content Automation Protocol (SCAP), which aligns to the security benchmarks used as the basis for the secure configuration standards. Each automated check is assigned a SCAP Open Vulnerability and Assessment Language (OVAL) ID.

- **Manual Assessment:** The Management and Operational NIST security control families need to be assessed manually, along with any technical controls for which an automated check has not been developed. The OIS RMT conducts manual assessments by

conducting interviews with the System Owner (SO) and ISSO, along with reviews of documentation provided by the SO and ISSO as evidence of control implementation.

Once a system is authorized for operation, a subset of security controls is assessed continuously according to the system's Continuous Monitoring Plan. The Risk Profile uses a quantitative model to calculate the system's Continuous Monitoring Plan based on the potential risk of security controls, the time required to conduct assessments, and the resource availability of assessors. The Continuous Monitoring Plan allows for security controls with higher risk to be assessed more frequently than controls associated with lower risk, so that resources are prioritized toward addressing the greatest risks. This continuous monitoring process allows a system to be authorized on a continuous basis based on the ongoing assessment and remediation of security controls.

The security control assessment process culminates in a security assessment report (SAR), where SCA results are documented. The SAR reports the most current security assessment results that were documented in the SSP during the "Assess Security Controls" step of the RMF Methodology. The SAR reports the following:

- Control Effectiveness.
- Vulnerabilities.
- Residual Risk.
- Recommendations.

Once the SAR is complete, the OIS RMT reviews the SAR with the SO and ISSO to discuss the findings and recommendations for remediation.

### **3.2.5 Vulnerability/Red Team Assessment [SPC 3-1.2.5]**

The OIS RMT, internal to the Census Bureau, is technically adept and experienced to evaluate the effectiveness of security controls in an independent manner. The OIS RMT performs assessments in an impartial manner without perceived or actual conflicts of interest in terms of the development, operation, or management of the information system that is assessed.

Formal security testing needs to be performed by an independent assessment team for systems with security categorizations of "High" or "Moderate." Independent assessors are not required for systems with a security categorization of "Low."

### **3.2.6 Risk/Issue Identification & Tracking [SPC 3-1.2.6]**

POA&Ms are the primary tool at the Census Bureau for identifying risks for tracking and closure (discussed in detail below). Additionally, a centralized identification and tracking tool is used to store system information, POA&Ms, and system security authorization packages.

### 3.2.7 System Security Plans (SSP) [SPC 3-1.2.7]

A centralized tool is used to create and update System Security Plans at the Census Bureau. Many pieces comprise the structure of an SSP and determine the final selection of controls. These include:

- System Description.
- Security Categorization.
- Risk Profiling Questionnaire.
- Business Risks.
- Technical Risks.
- Security Control Selection.
- Scoping.

Once the security control baseline is tailored and scoped by the Risk Profiling tool, the Office of Information Security Risk Management Team works with the System Owner and ISSO to validate that the security control baseline has been tailored and scoped appropriately for the operational environment. Adjustments are made as necessary and documented in the Risk Profiling tool. The resulting selection of security controls constitutes the security controls of a system's Risk Profile SSP. The Census Bureau Risk Management Framework and Risk Management Program User Guide describe SSP creation in detail.

### 3.2.8 Plans of Action & Milestones (POA&Ms) [SPC 3-1.2.8]

System issues that have been discovered during the security control assessment process and need to be remediated are documented and tracked in a POA&M. A POA&M is created for each SAR finding that has a residual risk considered too high to accept that cannot be remediated within 30 days of the SAR review. The POA&M risk mitigation approach is designed to prioritize risk mitigation activities and resources toward correcting the vulnerabilities that represent the greatest risk exposure. Each POA&M includes the following information:

- **Vulnerability:** The POA&M provides a description of the vulnerability identified in the SAR as a result of a control weakness or deficiency. The POA&M also provides the residual risk of the vulnerability.
- **Remediation Activities:** The POA&M describes the remediation activities planned to address the vulnerability. Remediation activities may be based on the recommendations for remediation provided in the SAR.
- **Resources:** The POA&M specifies the resources required to perform the remediation activities.

- **Milestones:** The POA&M identifies milestones to track the progress of remediation activities.
- **Schedule:** The POA&M provides estimated completion dates for the milestones. “High” severity vulnerabilities must be resolved in 30 days. “Moderate” severity vulnerabilities must be closed within 90 days and “Low” impact vulnerabilities require closure within 180 days.

The POA&M is one of the security artifacts required for the security authorization package delivered to the AO. The AO relies on POA&Ms to monitor the progress of remediation activities for information systems. POA&Ms are incorporated into a centralized capability to track their status. Please see the Commerce Information Technology Requirement (CITR)-018 for additional information on POA&Ms.

### **3.3 Engineering & Information Security [SPC 3-1.3]**

The Engineering & Information Security activity area is subdivided into the following operational subactivities.

- Integration of InfoSec into SDLC [SPC 3-1.3.1].
- Management Controls Implementation [SPC 3-1.3.2].
- Operations Controls Implementation [SPC 3-1.3.3].
- Technical Controls Implementation [SPC 3-1.3.4].
- Privacy Controls Implementation [SPC 3-1.3.5].
- IT Security Procedures [SPC 3-1.3.6].
- Best Practices Guidance Implementation [SPC 3-1.3.7].
- Authorization to Operate (ATO) [SPC 3-1.3.8].
- Continuous Monitoring & Remediation [SPC 3-1.3.9].

Subsequent sections describe the Engineering & Information Security operational subactivities.

#### **3.3.1 Integration of InfoSec into SDLC [SPC 3-1.3.1]**

The Census Bureau is dependent on its information systems to fulfill its organizational mission in the face of a sophisticated and varied threat landscape. To better ensure the confidentiality, integrity, and availability of information and systems, the Census Bureau has established and implemented technologies, procedures and best practices to mitigate system risk and combat the dynamic threats it faces from the earliest stages of system design through monitoring and disposal. The U.S. *Census Bureau Risk Management Framework* describes engineering and information security activities performed at the Census Bureau. Additionally, the *IT Security in*

*Acquisition Checklist* is a core procedures document used to incorporate IT security into the SDLC.

### **3.3.2 Management Controls Implementation [SPC 3-1.3.2]**

Once security controls have been selected and documented in the Risk Profile SSP for a particular system at the Census Bureau, security control implementation can proceed. Security controls are integrated into the information system, in accordance with secure information system development processes, best practices guidance, and secure coding practices.

Management controls are those security controls for an information system that focus on the management of risk and the management of information system security. The Management control families of the NIST SP 800-53 Revision 4 include:

- Security Assessment and Authorization.
- Contingency Planning.
- Planning.
- Risk Assessment.
- System and Services Acquisition.
- Program Management.

The System Owner, with support from developers and the ISSO, is responsible for overseeing the selection and implementation of controls to ensure the system meets minimum assurance requirements. Management, operational, and technical control implementation is consistently reviewed to confirm that: 1) Controls are implemented correctly, 2) Controls operate as intended, and 3) Controls address the security requirements for the information system. Section 3.4.1 of the U.S. *Census Bureau Risk Management Framework* describes security control implementation.

### **3.3.3 Operational Controls Implementation [SPC 3-1.3.3]**

Operational controls are those security controls for an information system that are primarily implemented and executed by people, rather than systems. The Operational control families of the NIST SP 800-53 Revision 4 include:

- Awareness and Training.
- Configuration Management.
- Incident Response.
- Maintenance.

- Media Protection.
- Physical and Environmental Protection.
- Personnel Security.
- System and Information Integrity.

Section 3.4.1 of the U.S. *Census Bureau Risk Management Framework* describes security control implementation.

### **3.3.4 Technical Controls Implementation [SPC 3-1.3.4]**

The technical controls are those security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. The control families of the NIST SP 800-53 Revision 4 include:

- Access Control.
- Audit and Accountability.
- Identification and Authentication.
- System and Communications Protection.

Section 3.4.1 of the U.S. *Census Bureau Risk Management Framework* describes security control implementation.

### **3.3.5 Privacy Controls Implementation [SPC 3-1.3.5]**

The NIST SP 800-53 Revision 4, Appendix J, introduced federal organizations to eight new privacy control families. Privacy controls are interrelated with the information security control families within the NIST SP 800-53 but are distinct from them. Privacy controls address the administrative, technical, and physical safeguards that are required to be employed within organizations to protect and ensure the proper handling of Personally Identifiable Information (PII) throughout its full life cycle.

Federal entities that collect, use, maintain, share, and dispose of the PII of individuals within programs and information systems have a responsibility to protect that information in accordance with best practices, federal legislation, policies, and procedures. The privacy controls in NIST SP 800-53 Revision 4, Appendix J, are based on the Fair Information Practice Principles embodied in the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, and OMB policies.

The eight new privacy control families are as follows:

- Authority and Purpose (AP).
- Accountability, Audit, and Risk Management (AR).
- Data Quality and Integrity (DI).
- Data Minimization and Retention (DM).
- Individual Participation and Redress (IP).
- Security (SE).
- Transparency (TR).
- Use Limitation (UL).

Please refer to section 4 of this document for a comprehensive overview of Privacy at the Census Bureau.

### **3.3.6 IT Security Procedures [SPC 3-1.3.6]**

While IT security policy at the Census Bureau informs and guides decision-making at all levels of the organization, IT security procedures are the application of written security policy. These procedures are critical to the engineering, operation, and IT security of both the Census Bureau and 2020 Census systems.

The Census Bureau has composed a number of planning and procedures documents that provide guidance in the secure operation of IT systems. These include:

- Secure System Development Life Cycle Methodology.
- New System Security Control Assessment Standard Operating Procedure.
- Census Bureau Risk Management Framework Methodology.
- Risk Management Program System User Guide.
- IT Security in Acquisition Checklist.
- Required Security Controls for Census Bureau.
- Census Continuous Monitoring FAQ.

### **3.3.7 Best Practices Guidance Implementation [SPC 3-1.3.7]**

The Census Bureau has implemented best security practices guidance to better secure underlying operating systems, databases, and infrastructure for both organization-wide systems as well as 2020 Census systems. Best practices guidance implementation at the Census Bureau is a core part of the Continuous Monitoring Process through the creation of secure configuration

standards. These secure configuration standards are based on best practices security benchmarks, which include:

- United States Government Configuration Baseline (USGCB).
- Defense Information Systems Agency (DISA).
- National Institute of Standards and Technology (NIST).
- Center for Internet Security (CIS).

The secure configuration standards are mapped to NIST SP 800-53A controls, where applicable, and automated checks are developed to assess these technical controls within the security control assessment process.

### **3.3.8 Authorization To Operate (ATO) [SPC 3-1.3.8]**

The System Authorization process at the Census Bureau determines whether the overall risk level for an information system is acceptable. The Authorizing Official (AO) evaluates the security authorization package, consisting of the System Security Plan (SSP), Security Assessment Report (SAR), Plan of Actions and Milestones (POA&M), Continuous Monitoring Plan, and security assessment memo to issue a security authorization decision for the information system.

Based on the information provided, the AO determines whether the system's level of residual risk is acceptable given the mission and operational needs of the Census Bureau. The final decision by the AO is captured in the authorization memo, which includes the following:

- **Authorization Decision:** The authorization decision can take the form of an Authorization to Operate (ATO), Interim Authorization to Operate (IATO), or Denial of Authorization to Operate (DATO). The authorization decision indicates to the System Owner (SO) whether the information system is approved for operation.
- **Terms and Conditions for Authorization:** The terms and conditions constitute any limitations or restrictions that the SO needs to comply with when operating the information system. In some cases, the SO may be required to perform immediate remediation activities prior to being granted system authorization.
- **Authorization Termination Date:** The authorization termination date indicates when the security authorization expires. The authorization termination date may be phased out by continuous monitoring activities that provide the AO with ongoing risk acceptance opportunities.

Once the SO accepts and implements the terms and conditions of the authorization, the information system can now be transitioned to the continuous monitoring process. Further information on the Authorization process can be found in the U.S. *Census Bureau IT Security Program Policies (ITSP)* and *Census Bureau Risk Management Framework Methodology*.

### **3.3.9 Continuous Monitoring & Remediation [SPC 3-1.3.9]**

The continuous monitoring process at the Census Bureau facilitates the continuous authorization of systems based on the ongoing assessment and remediation of security controls. Once a system is authorized for operation, a subset of security controls is assessed continuously according to the system's Continuous Monitoring Plan. The system's Risk Profile uses a quantitative model to calculate the system's continuous monitoring plan based on the potential risk of security controls, the time required to conduct assessments, and the resource availability of assessors. The Continuous Monitoring Plan allows for security controls with a higher risk to be assessed more frequently than controls associated with lower risk, so that resources can be prioritized toward addressing the greatest risks. Monthly risk reports are generated and sent to system ISSOs and other system stakeholders to apprise them of the current security posture. The U.S. *Census Bureau RMF Methodology* illustrates the continuous monitoring and remediation process in detail.

### **3.4 Incident Response (IR) [SPC 3-1.4]**

The Incident Response (IR) activity area is subdivided into the following operational subactivities.

- Computer Security Operations Center (CSOC) [SPC 3-1.4.1].
- IR Procedures [SPC 3-1.4.2].
- External Agency Partnership [SPC 3-1.4.3].
- IR Capability Testing/Training [SPC 3-1.4.4].

Subsequent sections describe the IR operational subactivities.

#### **3.4.1 Computer Security Operations Center (CSOC) Functions [SPC 3-1.4.1]**

The Bureau of Census (BOC) Computer Incident Response Team (CIRT) is primarily tasked with performing the Computer Security Incident Response Capability (CSIRC) on behalf of the Census Bureau. The BOC CIRT coordinates incident response activities with the Department of Commerce CIRT to identify, contain, and eradicate malicious activity and restore operations.

#### **3.4.2 Incident Response Procedures [SPC 3-1.4.2]**

The Census Bureau has implemented best practices guidance in its IR methodology. IR procedures consist of six core stages:

- **Preparation Stage:** Preparation is the foundation for an effective incident response capability. Incident response policies and procedures have been established, an incident

response team has been created, tools have been selected, and leadership approvals have been granted.

- **Identification Stage:** Information is gathered in this stage for analysis to positively identify whether an incident has occurred. Hosts are removed from production when positive identification of an incident occurs.
- **Containment Stage:** This stage prevents the further propagation of malicious activity/software in the production environment.
- **Eradication Stage:** Eradication prohibits further malicious activity by removing malicious software from the infected hosts.
- **Recovery Stage:** This stage returns hosts to the production environment. Hosts are monitored to ensure that the malicious software/activity was successfully eradicated.
- **Lessons Learned Stage:** Lessons learned from the incident are incorporated into incident response policy and procedures to enhance the overall IR capability.

Further information can be found in the *Information Security Incident Response Plan* [2015] and the *Incident Handling Handbook*.

### **3.4.3 External Agency Partnership [SPC 3-1.4.3]**

The Census Bureau incident response capability collaborates with external agencies. Census may work with Federal law enforcement organizations for investigative support, the Intelligence Community to receive threat information, and various other entities to enhance the IR capability.

### **3.4.4 IR Capability Testing/Training [SPC 3-1.4.4]**

BOC CIRT incident responders continuously train to enhance IR skills. A minimum of one exercise is scheduled annually to test the IR Plan and capability. Exercises involve participants from several areas throughout the Census Bureau. During an exercise, participants are required to identify, process, and respond to an incident scenario.

## **3.5 Security Training & Awareness [SPC 3-1.5]**

The Census Bureau has established an IT Security Awareness, Training, and Education component to ensure compliance with the Federal Information Security Management Act (FISMA), Department of Commerce (DOC) mandates, and NIST SP 800-50 guidance. To meet these requirements and mandates, the IT Security Office has implemented a strong IT Security Training Program. The Security Training & Awareness activity area is subdivided into the following operational subactivities.

- General User Annual Training & Awareness [SPC 3-1.5.1].
- Technical Staff Development [SPC 3-1.5.2].

- Training & Awareness Communications [SPC 3-1.5.3].

Subsequent sections describe the Security Training & Awareness operational subactivities.

### **3.5.1 General User Annual Training & Awareness [SPC 3-1.5.1]**

Census Bureau staff are required to complete annual security training & awareness. Training must be completed by June 30 of each year. Employees must score a 70 percent or higher to receive credit for completing this training. Training for all employees is tracked and displayed within each employee's training history as well as within the training management system.

Annual security & awareness training includes a selection of topics such as:

- Data Stewardship.
- Laws & Regulations.
- IT Security Threats: Malware.
- IT Security Threats: Social Engineering.
- IT Security Vulnerabilities.
- Safeguarding Data.
- Physical Security.
- Unauthorized Browsing.
- Laptop/Mobile Device Security.
- IT Acceptable Use.
- Password Best Practices.
- Email Security.
- Security Incident Reporting.

### **3.5.2 Technical Staff Development [SPC 3-1.5.2]**

Technical staff supporting IT security are critical to ensuring the Census Bureau maintains a secure posture. Individuals with significant IT security responsibilities must 1) complete role-based training upon appointment to the role, or within 30 days of appointment, so that they understand the scope of their responsibilities, and 2) complete role-based training within that fiscal year and annually thereafter.

The Commerce Information Technology Requirement (CITR)-006 specifies requirements for information system security training or IT security professional certification for those personnel with significant information system security responsibilities.

### **3.5.3 Training & Awareness Communications [SPC 3-1.5.3]**

The Census Bureau conveys security-related topics throughout the organization using several mediums. The organization uses Bureau of Census Broadcast email messages to communicate alerts, such as malware infections. Also, the Office of Information Security uses a listserv to promulgate security information, such as periodic vulnerability summaries, to communities of interest. Additionally, training & awareness content is delivered via a web-based application.

## **4. SPC Operation Detailed Process Description – Privacy and Confidentiality [SPC 3-2]**

The Census Bureau is committed to protecting the privacy and confidentiality of the information about individuals that it collects and uses. Census Bureau Privacy Principles focus on:

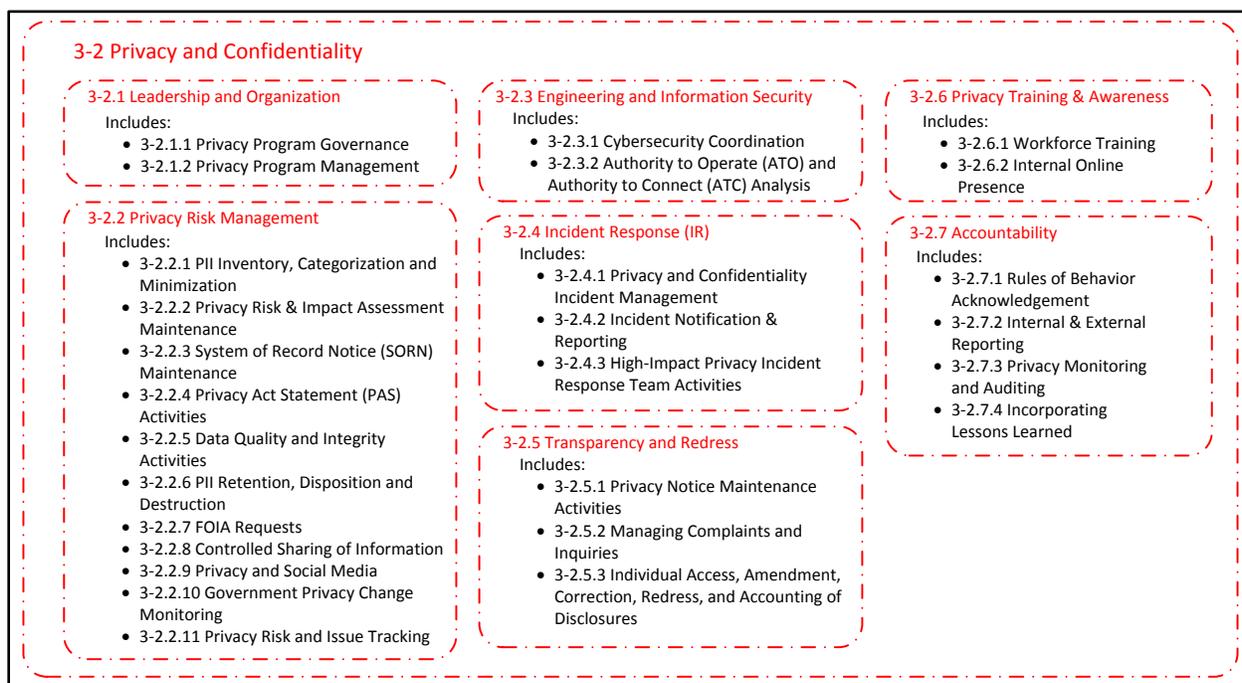
- Collecting only the PII that is necessary.
- Using PII only for the authorized purposes for which it was collected in the first place.
- Providing notice to individuals about the purposes and uses for which PII is collected and used.
- Treating respondents respectfully
- Protecting the confidentiality of information.

In particular, PII is collected for statistical purposes only, and it is never used to identify individuals. Privacy threats change continuously, and the Census Bureau maintains a comprehensive privacy program that addresses all privacy requirements and implements effective practices in order to minimize privacy risk for the 2020 Census.

The privacy and confidentiality discussion in this section focuses on the Operation and Maintenance (O&M) of the Privacy and Confidentiality components of the 2020 Census. The Privacy and Confidentiality planning activities are described elsewhere.

The Privacy and Confidentiality Activity Area of the SPC operation [SPC 3-2] is subdivided into the following constituent activities (See Figure 4).

- Leadership & Organization [SPC 3-2.1]
- Privacy Risk Management [SPC 3-2.2]
- Engineering & Information Security [SPC 3-2.3]
- Incident Response (IR) [SPC 3-2.4]
- Transparency and Redress [SPC 3-2.5]
- Privacy Training & Awareness [SPC 3-2.6]
- Accountability [SPC 3-2.7]



**Figure 4: Privacy and Confidentiality [SPC 3-2] Constituent Activities**

The business processes for each of these Privacy and Confidentiality activity areas are discussed along with their inputs and outputs in the following subsections.

#### **4.1 Leadership & Organization [SPC 3-2.1]**

The Leadership & Organization activity area is subdivided into the following operational subactivities.

- Privacy Program Governance [SPC 3-2.1.1]
- Privacy Program Management [SPC 3-2.1.2]

This area consists of activities that provide organizational support for Census Bureau privacy program priorities and initiatives through governance and management activities.

Subsequent sections describe the Leadership & Organization operational subactivities.

##### **4.1.1 Privacy Program Governance [SPC 3-2.1.1]**

The Senior Agency Official for Privacy (SAOP) responsible for the Census Bureau is located within the Department of Commerce. The Census Bureau Chief Privacy Officer (CPO) reports directly to the Deputy Director. In addition, there is a Census Bureau Privacy Officer who reports to the CPO and performs day-to-day operational privacy activities. The Privacy Compliance Branch reports to the CPO and oversees all matters pertaining to privacy

compliance, including Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs). The Chief of the Privacy Compliance Branch is a member of the Data Stewardship Executive Committee. The privacy program has executive-level leadership support at the highest level of the Census Bureau.

Operational privacy policies and procedures that implement the Census Bureau's privacy principles and govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII are developed, disseminated, and implemented via a series of processes that are built into the Census Bureau infrastructure.

Enterprise-wide changes to privacy policy and procedures are communicated to personnel in advance of compliance dates through the Data Stewardship Executive Committee using announcements and broadcast messages in both paper and electronic form.

Privacy policies and procedures as well as all documented aspects of the privacy program, including PIAs, SORNs, and privacy policies, are reviewed annually and updated if needed. They may be updated more frequently if changes are needed sooner than the annual review. If a new area is introduced, the program manager is required to contact the Privacy Compliance Branch. The Chief of the Privacy Compliance Branch is a standing member of the IT Governance Board, so the Privacy Compliance Branch becomes involved in programs via an early view of upcoming systems provided by the IT Governance Board. A privacy acquisition review checklist is completed for every program that is being procured to identify privacy considerations, including completion of a Privacy Threshold Analysis (PTA), PIA, and SORN.

#### **4.1.2 Privacy Program Management [SPC 3-2.1.2]**

The Census Bureau has multiple documents that outline their privacy controls, policies, and procedures. It is in the process of developing a strategic organizational privacy plan that will put everything into one document.

The Census Bureau has adopted the concept of Privacy by Design so that they have privacy considerations built into the design of systems. They use an IT Governance Office to manage this, and the Privacy Compliance Branch is part of the overall process.

## **4.2 Privacy Risk Management [SPC 3-2.2]**

The Privacy Risk Management activity area is subdivided into the following operational subactivities.

- PII Inventory, Categorization and Minimization [SPC 3-2.2.1]
- Privacy Risk & Impact Assessment Maintenance [SPC 3-2.2.2]
- System of Record Notice (SORN) Maintenance [SPC 3-2.2.3]

- Privacy Act Statement (PAS) Activities [SPC 3-2.2.4]
- Data Quality and Integrity Activities [SPC 3-2.2.5]
- PII Retention, Disposition and Destruction [SPC 3-2.2.6]
- FOIA Requests [SPC 3-2.2.7]
- Controlled Sharing of Information [SPC 3-2.2.8]
- Privacy and Social Media [SPC 3-2.2.9]
- Government Privacy Change Monitoring [SPC 3-2.2.10]
- Privacy Risk and Issue Tracking [SPC 3-2.2.11]

This area consists of methods and processes that the Census Bureau uses to identify, assess, prioritize, and manage privacy risk.

Subsequent sections describe the Privacy Risk Management operational subactivities.

#### **4.2.1 PII Inventory, Categorization and Minimization [SPC 3-2.2.1]**

An inventory is established, maintained, and periodically updated that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII. Identification of systems with PII is done via the PIA process, and a PIA is completed for every system. The level of privacy risk is assigned based on the type of PII that is identified while performing the PIA.

The Census Bureau ensures that the collection, use, and retention of PII is limited to the minimum elements identified for the purposes for which it was collected and as described in the SORN.

#### **4.2.2 Privacy Risk & Impact Assessment Maintenance [SPC 3-2.2.2]**

Privacy risk is assessed and managed at the Census Bureau at the IT security level by identifying whether PII is in a system and what privacy risks there are during the ATO process. This process is reinforced through the data stewardship training provided at the Census Bureau. In addition, PIAs are conducted for information systems, programs, or other activities that pose a privacy risk. The Census Bureau follows Data Stewardship policy DS 019, *Policy on Conducting Privacy Impact Assessments*. The PIA process begins whenever a new system is proposed via the completion of an IT security checklist and a privacy acquisition review checklist. The privacy acquisition review checklist highlights whether a PTA is necessary. Completion of the PTA determines whether a PIA is required or not. A PIA may also be initiated when ISSOs and data owners reach out to the Privacy Compliance Branch when they have systems that need privacy review. There is also an annual review process where the Privacy Compliance Branch reviews existing PIAs and compares them against systems to ensure that every system has a

corresponding PIA. The *Privacy Impact Assessment for CEN08 Decennial* is published on the Census Bureau public website.

Privacy risk management is integrated into the enterprise risk management function through the IT Governance Board as described in Section 4.1.1 above.

#### **4.2.3 System of Record Notice (SORN) Maintenance [SPC 3-2.2.3]**

System of Records Notices (SORNs) are published in the Federal Register for systems that collect or use PII. SORNs are kept current via annual reviews that are conducted by the Privacy Compliance Branch. SORN deletion notices are published when systems are retired. Census Bureau SORNS are published by the Department of Commerce. The *Decennial Census Program SORN (COMMERCE/CENSUS-5)* is published in the Federal Register.

#### **4.2.4 Privacy Act Statement (PAS) Activities [SPC 3-2.2.4]**

The Privacy Act requires that agencies inform individuals about the following privacy-related information when the agencies are collecting PII from the individuals: The authority for collecting the information, the purposes for which the information will be used, the routine uses of the information, and the effects on the individual if he or she does not provide the requested information. The Census Bureau will include a statement that contains this privacy-related information on printed and electronic forms for the 2020 Census.

#### **4.2.5 Data Quality and Integrity Activities [SPC 3-2.2.5]**

For the 2020 Census, PII is collected directly from individuals to the greatest extent practicable. This helps to ensure the quality of the data. There is a quality program within the Census Bureau, and that quality organization coordinates with the Privacy Compliance Branch on an as needed basis regarding the use and treatment of PII.

#### **4.2.6 PII Retention, Disposition, and Destruction [SPC 3-2.2.6]**

The collection of PII is retained to fulfill the purposes identified in the notice, in accordance with the applicable retention schedule, and as required by law. The retention schedule that applies to the 2020 Census is National Archives and Records Administration schedule N1-29-05-01. The retention schedule is a line item in the 2020 Census PIA, which is published online, so the public knows how long the data is being held.

#### **4.2.7 FOIA Requests [SPC 3-2.2.7]**

The Census Bureau has a FOIA process whereby an individual can submit a request for access to an agency record that is not publicly available. FOIA requests can be submitted to the Census Bureau in writing or electronically via the FOIAonline system. FOIAonline is also used to track the progress of each request and for the requestor to communicate directly with the Census

Bureau staff who are handling requests at all points in the process. The Census Bureau follows government requirements and standards for FOIA request processing. Information about the Census Bureau FOIA process is provided to the public on the Census Bureau website.

#### **4.2.8 Controlled Sharing of Information [SPC 3-2.2.8]**

The Privacy Compliance Branch evaluates proposed new instances of sharing PII, including ad hoc requests, with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. The Privacy Compliance Branch determines whether sharing the data meets the SORN for the system. The Office also looks at the type of data to determine whether it is appropriate to share the data, e.g., Title 13 and Title 26 data can only be shared with those who are Title-certified and who have a business need to know.

PII is shared externally only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes. Data that is approved to be shared must be legally allowed, and Census Bureau legal staff determine whether or not data can be shared with another external entity. The Data Disclosure Board and Data Stewardship Executive Committee are involved, and the sharing must be consistent with the SORN, legally permissible and approved by the Executive staff at Census Bureau.

Census Bureau staff receive mandatory data stewardship training that covers authorized sharing of PII with third parties and the consequences of unauthorized use or sharing of PII. In addition, other training is done throughout the year that covers unauthorized sharing and its penalties.

The 2020 Census PIA states that PII collected via the 2020 Census may be shared on a case-by-case basis within the Census Bureau, with other Department of Commerce Bureaus, and with other federal agencies.

Once the 2020 Census data is published, the Census Bureau will enter into agreements to allow access to statistical data. The process of creating these agreements is handled by the Administrative Records office. There are two main types of agreements. The first type is for joint statistical projects with other federal agencies that benefit both parties. The agreements between the Census Bureau and other federal agencies will contain compliance and safeguards information to protect the microdata that is shared. Federal agency agreements are approved by the Director of the Census Bureau or his designee. Federal agencies have a limited time that they can use the data; they must not exceed the retention schedule of the data they are accessing.

The second type of agreements allow qualified researchers to access restricted-used microdata at Federal Statistical Research Data Centers (RDCs) to address important research questions. The agreements contain terms and conditions to which the researchers have to agree, particularly to use the data only for statistical purposes. If a research proposal is approved by the Center for Economic Studies, the researcher can access 2020 Census data for a specific period of time for research only.

#### **4.2.9 Privacy and Social Media [SPC 3-2.2.9]**

Website privacy notices are published online for Census Bureau websites. The Privacy Compliance Branch oversees the process to ensure that all outlets have a privacy notice or at least a link to the Census Bureau privacy policy page when they do not own the page.

Third party website and application (TPWA) PIAs are completed for websites and applications used by the Census Bureau. The process for completing these is the same process as for regular PIAs, and the TPWA PIAs are reviewed each year. The Census Bureau Center for New Media are the managers of web-related activities. They coordinate with the Privacy Compliance Branch on privacy issues. There is also a Department of Commerce-wide SORN related to TPWAs.

#### **4.2.10 Government Privacy Change Monitoring [SPC 3-2.2.10]**

Federal privacy laws and policy are monitored for changes that affect the Census Bureau privacy program. The Chief of the Privacy Compliance Branch plays an active role in the Department of Commerce Privacy Council, which meets monthly to discuss current events and how they impact different programs. The Chief of the Privacy Compliance Branch is on the OMB mailing list, and receive notices regarding new OMB guidance. He is also part of the OMB Privacy Council. Whenever new legislation is proposed, the Chief of the Privacy Compliance Branch reviews and provides comments back to OMB.

Identification of privacy trends and best practices that may benefit the Census Bureau is done by monitoring activities of the Federal Privacy Council. The Chief of the Privacy Compliance Branch is on the Council's mailing list as well as the mailing lists for the privacy offices within DHS, Treasury, and several private entities. The Chief of the Privacy Compliance Branch is an active member of the International Association of Privacy Professionals (IAPP) and is a Certified Information Privacy Professional/U.S. Government specialization (CIPP/G).

#### **4.2.11 Privacy Risk and Issue Tracking [SPC 3-2.2.11]**

Entries in the Plan of Actions and Milestones (POA&M) within the system authorization process are used by the Census Bureau to manage privacy risks and issues, prioritize resolution, and track items through to closure. Please see Section 3.3.8 above for a description of the different parts of the system authorization process.

### **4.3 Engineering and Information Security [SPC 3-2.3]**

The Engineering and Information Security activity area is subdivided into the following operational subactivities.

- Cybersecurity Coordination [SPC 3-2.3.1]
- Authority to Operate (ATO) and Authority to Connect (ATC) Analysis [SPC 3-2.3.2]

This area consists of activities that are used to incorporate privacy into the Census Bureau's enterprise systems engineering approach and to integrate privacy with security.

Subsequent sections describe the Engineering and Information Security operational subactivities.

#### **4.3.1 Cybersecurity Coordination [SPC 3-2.3.1]**

In general, the privacy program leverages the Data Stewardship program in order to engage with cybersecurity. Cybersecurity participates in almost all of the same groups in which privacy participates. In addition, Census Bureau privacy principles and activities are aligned with cybersecurity processes and activities by having a cybersecurity representative participate as an active member of the PIA team.

#### **4.3.2 Authority to Operate (ATO) and Authority to Connect (ATU) Analysis [SPC 3-2.3.2]**

The Census Bureau uses ATOs and ATUs (Authorizations to Use, which are typically completed for third party websites and applications) to prevent the operation of information systems that have not met applicable privacy requirements. The ATOs and ATUs are approved by the Privacy Compliance Branch, and operation or use of the systems, third party websites, or applications cannot go forward without approval.

### **4.4 Incident Response (IR) [SPC 3-2.4]**

The Incident Response (IR) activity area is subdivided into the following operational subactivities.

- Privacy and Confidentiality Incident Management [SPC 3-2.4.1]
- Incident Notification & Reporting [SPC 3-2.4.2]
- High-Impact Privacy Incident Response Team Activities [SPC 3-2.4.3]

This area consists of activities that support the Census Bureau's management of and response to privacy incidents, including breaches.

Subsequent sections describe the Incident Response (IR) operational subactivities.

#### **4.4.1 Privacy and Confidentiality Incident Management [SPC 3-2.4.1]**

The Census Bureau follows a Department of Commerce privacy incident response plan that enables the organization to respond promptly to privacy incidents, including breaches. The Plan is titled *United States Department of Commerce Personally Identifiable Information (PII), Business Identifiable Information (BII), and Privacy Act (PA) Breach Response and Notification Plan*, Version 2.0, July 2013. There is also an *Addendum to the DS-22 Data Breach Policy* that enhances the procedures for handling high-level PII breaches by establishing the role and function of the Census Bureau's Data Breach Response Committee (DBRC) and identifying the responsibilities of Division Chiefs and department heads, and organizing communications between the DBRC, senior managers, Associate Directors, the Deputy Director, and the Department of Commerce's Chief Privacy Officer. The Census also follows the *Data Stewardship Policy for Notifying Management Officials of Employees Who Committed an Unauthorized Disclosure of Sensitive Personally Identifiable Information (PII)*, dated September 10, 2015.

#### **4.4.2 Incident Notification & Reporting [SPC 3-2.4.2]**

The Census Bureau workforce receives annual training from the Department of Commerce regarding incident response reporting procedures. Multiple channels are provided for reporting privacy incidents, including via telephone or Internet. Incidents can also be reported directly to a supervisor. All reported incidents go to the help desk, which is where the tickets are created for tracking the resolution of incidents.

#### **4.4.3 High-Impact Privacy Incident Response Team Activities [SPC 3-2.4.3]**

The Census Bureau has a Breach Response Committee, which is an incident response team comprised of senior leadership with decision-making authority from relevant offices within the organization to respond to high-impact privacy incidents. Members of the Committee include the CPO, who chairs the Committee; the Associate Director for Communications; the CIO; the Associate Director for Administration; the Deputy Director; and the Privacy Compliance Officer. Other Associate Directors may be invited to participate with the Committee at times depending upon where a breach occurred.

## **4.5 Transparency and Redress [SPC 3-2.5]**

The Individual Participation, Transparency and Redress activity area is subdivided into the following operational subactivities.

- Privacy Notice Maintenance Activities [SPC 3-2.5.1]
- Managing Complaints and Inquiries [SPC 3-2.5.2]
- Individual Access, Amendment, Correction, Redress, and Accounting of Disclosures [SPC 3-2.2.3]

This area consists of activities that provide visibility into the information about the public that the Census Bureau collects and uses as well as its ability to address inquiries and complaints.

Subsequent sections describe the Transparency, and Redress operational subactivities.

### **4.5.1 Privacy Notice Maintenance Activities [SPC 3-2.5.1]**

Required privacy documentation, such as PIAs, SORNs, and computer matching agreements (CMAs) as well as online Privacy Policies are published by the Census Bureau on their website and in the Federal Register as required. Privacy documentation is reviewed annually to ensure that it remains current, and the documentation is revised as needed.

The Census Bureau provides effective notice to the public and to individuals in plain language before or at the time of collection through the use of Privacy Act Statements, online Privacy Policy, Privacy Notices, and published PIAs and SORNs. Changes to identified purposes are communicated to the public via publication of a Federal Register announcement before the SORN change is published.

### **4.5.2 Managing Complaints and Inquiries [SPC 3-2.5.2]**

The Census Bureau provides the name and phone number of the person to contact regarding questions or complaints about organizational privacy practices in the Census Bureau online privacy policy and also in published PIAs and SORNs. A log is used at the Census Bureau to handle inquiries and track them through to resolution and closure.

### **4.5.3 Individual Access, Amendment, Correction, Redress, and Accounting of Disclosures [SPC 3-2.2.3]**

According to the Decennial Census Program SORN, the Decennial Census, including the 2020 Census, is exempt from the otherwise applicable notification, access, and contest requirements of the agency procedures in the Privacy Act. This exemption is applicable because the data are maintained by the Census Bureau, as required under Title 13 U.S.C., to be used solely as statistical records, and are not used to make any determination about an identifiable individual.

Thus, for 2020 Census records, the Census Bureau is not required to notify individuals if the system contains records about them, provide individuals with access to the records about them, amend those records, and maintain an accounting of disclosures regarding the records that are provided to individuals at their request.

#### **4.6 Privacy Training & Awareness [SPC 3-2.6]**

The Privacy Training & Awareness activity area is subdivided into the following operational subactivities.

- Workforce Training [SPC 3-2.6.1]
- Internal Online Presence [SPC 3-2.6.2]

This area consists of activities that support the establishment and maintenance of Census Bureau workforce privacy training and a culture of privacy awareness.

Subsequent sections describe the Privacy Training & Awareness operational subactivities.

##### **4.6.1 Workforce Training [SPC 3-2.6.1]**

The Census Bureau has a comprehensive privacy training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. Basic privacy training is administered annually via both data stewardship training, which is computer-based, and privacy training, which is in person. Completion of data stewardship training is required before authorizing access to PII.

Targeted, role-based privacy training for individuals having responsibility for PII or for activities that involve PII is administered annually. The training is currently provided in person, and the Census Bureau is working to make the training computer-based. Role-based privacy training is provided in four different modules, each of which is targeted to specific roles. The roles are:

- **Module 1:** General privacy; targeted at everyone at the Census Bureau.
- **Module 2:** Privacy Act of 1974; targeted at individuals who handle a large amount of PII.
- **Module 3:** E-Government Act and privacy requirements, including PIAs, PTAs, and posting website privacy policies; targeted at the IT Directorate.
- **Module 4:** Privacy and new Technology: Covers topics such as Third-Party Websites and Applications (TPWAs), Bring Your Own Device (BYOD); covers those who work with public relations and IT.

Completion of mandatory annual privacy training commensurate with professional responsibilities is tracked by the Data Stewardship Office. If the training is not completed, staff lose access to Census Bureau systems.

It is a requirement for privacy staff to attend International Association of Privacy Professionals (IAPP) privacy conferences twice a year to obtain information on the latest developments in the privacy field. Privacy managers also attend a third IAPP privacy conference annually.

Training and awareness materials are evaluated annually to determine effectiveness and whether they are current and are revised to reflect feedback.

#### **4.6.2 Internal Online Presence [SPC 3-2.6.2]**

The Census Bureau workforce is provided with access to current privacy resources at several internal sites. All of the Census Bureau's privacy documentation and resources are published online on the intranet. There is also a location on the intranet to which only individuals in the privacy community have access. Privacy information specific to the 2020 Census will be added to the internal privacy sites.

### **4.7 Accountability [SPC 3-2.7]**

The Accountability activity area is subdivided into the following operational subactivities.

- Rules of Behavior Acknowledgement [SPC 3-2.7.1]
- Internal & External Reporting [SPC 3-2.7.2]
- Privacy Monitoring and Auditing [SPC 3-2.7.3]
- Incorporating Lessons Learned [SPC 3-2.7.4]

This area consists of activities that support the responsibility of the Census Bureau workforce to implement privacy principles and requirements and the answerability of the Census Bureau to the public regarding its privacy program.

Subsequent sections describe the Accountability operational subactivities.

#### **4.7.1 Rules of Behavior Acknowledgement [SPC 3-2.7.1]**

Census Bureau personnel certify acceptance of responsibilities for privacy requirements annually by signing the Data Stewardship acknowledgement. The Census Bureau has formally documented enforcement mechanisms that support the privacy rules of behavior. These enforcement mechanisms include monitoring completion of training, and removing access to the network if training is not completed. The Policy Coordination Office's Privacy Compliance Branch monitors all reported PII breaches and reports to office/division managers biweekly the names of employees who have committed an unauthorized disclosure of sensitive PII. If there are

egregious violations, the Privacy Compliance Branch is empowered to block an individual's access to the network. This process is formally documented in the *Data Stewardship Policy for Notifying Management Officials of Employees Who Committed an Unauthorized Disclosure of Sensitive Personally Identifiable Information (PII)*, dated September 10, 2015.

#### **4.7.2 Internal & External Reporting [SPC 3-2.7.2]**

Reports that demonstrate accountability with specific statutory and regulatory privacy program mandates are created by the Department of Commerce with input from different Census Bureau offices. The Privacy Compliance Branch reports on the number of PIAs, SORNs, and other privacy compliance metrics.

#### **4.7.3 Privacy Monitoring and Auditing [SPC 3-2.7.3]**

The effectiveness of the Census Bureau privacy program is assessed based on the number of PII incidents and confirmed breaches. Privacy controls and internal privacy policy are monitored and audited periodically by Census Bureau staff to ensure effective implementation. The Census Bureau has not yet formally documented their privacy continuous monitoring program. However, their infrastructure is structured so that privacy is considered at every level of their programs and they address all elements of a comprehensive privacy program. The CPO is briefed every two weeks regarding the results of privacy program monitoring and evaluation activities.

#### **4.7.4 Incorporating Lessons Learned [SPC 3-2.7.4]**

The purpose of the Privacy Policy and Research Committee (PPRC) is to support the Data Stewardship Executive Policy Committee by identifying, researching, analyzing, and reporting on privacy-related policy issues to inform executive decision-making. The PPRC's responsibilities are described in the *Privacy Policy and Research Committee Charter*. In addition, privacy incidents are monitored and evaluated by the Census Bureau Breach Response Committee. If the Breach Response Committee identifies gaps, the gaps are given to the Privacy Policy and Research Committee, which then creates an approach for addressing the gaps.

## 5. Cost Factors

Investment in SPC is expected to have minimal influence on the overall cost of the 2020 Census. While the SPC operation is not a major cost driver for the 2020 Census, the following mechanisms from the IDEF0 Context Diagram represent the resources used to support this operation and comprise part of the 2020 Census cost elements:

### Staff

- HQ Staff
- FLD Staff

### Sites

- HQ
- NPC
- FLD Sites (RO, RCC, ACO)
- Data Centers (BCC, TI, Cloud)

### Systems

- CSAM
- RMPS
- Remedy

### Other

- Networks
- Mobile Devices/DaaS

## 6. Measures of Success

For the 2020 Census operations, the corresponding Measures of Success will be documented in the operational assessment study plans and final reports. The operational assessment study plan documents the criteria that will be used to define successful completion of the operation. The operational assessment report will provide results on whether the criteria were met.

In general, operational assessments report on planned to actual variances in budget, schedules, and production and training workloads. The corresponding Measures of Success (as documented in the operational assessment study plan) include variances that exceed established thresholds. See *Content Guidelines for the 2020 Census Operational Assessments* for the potential scope of assessment.

Types of success measures include:

- **Process Measures** that indicate how well the process works, typically including measures related to completion dates, rates, and productivity rates.
- **Cost Measures** that drive the cost of the operation and comparisons of actual costs to planned budgets. Costs can include workload as well as different types of resource costs.
- **Measures of the Quality** of the results of the operation, typically including things such as rework rates, error rates, and coverage rates.

See the corresponding operational assessment study plan and report for the Security, Privacy, and Confidentiality (SPC) operation for details on the measures of success.

## Appendix A – Acronyms and Terminology

Table 7 lists the acronyms and abbreviations used within this Detailed Operational Plan document.

Table 8 lists a Glossary of Terms used within this Detailed Operational Plan document.

**Table 7: Acronyms and Abbreviations List**

<b>Acronym</b>	<b>Meaning</b>
ACO	Area Census Office
AO	Authorizing Official
AP	Authority and Purpose
AR	Accountability, Audit, and Risk Management
ATC	Authority to Connect
ATO	Authority to Operate
ATU	Authorizations to Use
BCC	Bowie Computer Center
BII	Business Identifiable Information
BOC	Bureau of Census
BYOD	Bring Your Own Device
CIO	Chief Information Officer
CIPP/G	Certified Information Privacy Professional/U.S. Government specialization
CIRT	Computer Incident Response Team
CIS	Center for Internet Security
CISO	Chief Information Security Officer

Acronym	Meaning
CITR	Commerce Information Technology Requirement
COOP	Continuity of Operations
CPO	Chief Privacy Officer
CQA	Census Questionnaire Assistance
CSAM	Cyber Security Asset Management
CSIRC	Computer Security Incident Response Capability
CSOC	Computer Security Operations Center
DATO	Denial of Authorization to Operate
DBRC	Data Breach Response Committee
DHS	Department of Homeland Security
DI	Data Quality and Integrity
DISA	Defense Information Systems Agency
DITD	Decennial IT Division
DM	Data Minimization and Retention
DOC	Department of Commerce
DOP	Detailed Operational Plan
DSC	Decennial Service Center
ESP	Enterprise Standards Profile
FAQ	Frequently Asked Questions
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FLD	Field

Acronym	Meaning
FLDI	Field Infrastructure
FOIA	Freedom of Information Act
HQ	Headquarters
IA	Island Areas
IAPP	International Association of Privacy Professionals
IATO	Interim Authorization to Operate
IP	Individual Participation and Redress
IPT	Integrated Project Team
IS	Information System
ISA	Interconnection Security Agreements
ISSO	Information System Security Officer
IT	Information Technology
ITIN	IT Infrastructure
ITSPP	IT Security Program Policy
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NPC	National Processing Center
OIS	Office of Information Security
OMB	Office of Management and Budget
OVAL	Open Vulnerability and Assessment Language
PAS	Privacy Act Statement

Acronym	Meaning
PDC	Paper Data Capture
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
PM	Program Management
POA&Ms	Plans of Action & Milestones
PPRC	Privacy Policy and Research Committee
PTA	Privacy Threshold Analysis
RCC	Regional Census Center
RMF	Risk Management Framework
RMP	Risk Management Program
RMPS	Risk Management Program System
RMT	Risk Management Team
SAISO	Senior Agency Information Security Officer
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SCA	Security Control Assessments
SCAP	Security Content Automation Protocol
SDLC	Systems Development Life Cycle
SE	Security
SEI	Systems Engineering and Integration
SLA	Service Level Agreements
SO	System Owners

<b>Acronym</b>	<b>Meaning</b>
SORN	System of Records Notices
TI	Technical Integrator
TPWA	Third-Party Website and Application
TR	Transparency
UL	Use Limitation
USGCB	United States Government Configuration Baseline

**Table 8: Glossary of Terms**

<b>Term</b>	<b>Meaning</b>
Authorization To Operate (ATO)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls.
Automated Security Monitoring	Use of automated procedures to ensure security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the information system.
Continuous Monitoring	The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information sharing decisions involving the enterprise.

Term	Meaning
Enterprise Architecture	The description of an enterprise’s entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise’s boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise’s overall security posture.
Enterprise Risk Management	The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary.
Freedom of Information Act (FOIA)	Law that allows individuals to request access to government information. Access to information is provided subject to certain exceptions and exclusions.
Incident	An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Personally Identifiable Information (PII)	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 (Source: OMB Circular A-130).
Privacy Act	Foundational law that focuses and limits how U.S. government agencies collect, maintain, use, and disclose personal information.
Privacy by Design	The idea that privacy cannot be assured solely by compliance with regulatory frameworks but should also be built into system and program design and business practices.

Term	Meaning
Privacy Impact Assessment (PIA)	An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis. Completion of PIAs is required by the E-Government Act (Source: OMB Circular A-130).
Privacy Threshold Analysis (PTA)	A form that is completed by an agency to determine whether or not a new Privacy Impact Assessment (PIA) needs to be completed for a system or program or whether an existing PIA needs to be updated. Use of a PTA is an effective practice, but is not required.
Red Team	Interdisciplinary group of individuals authorized to conduct an independent and focused threat-based effort as a simulated adversary to expose and exploit system vulnerabilities for the purpose of improving the security posture of information systems.
Risk	Possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability.
Security Controls	Management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
System of Records Notice (SORN)	A public notice that describes the existence and characteristics of an agency's system of records. Completion of SORNs is required by the Privacy Act, and agencies must publish their SORNs at a minimum in the Federal Register (Source: Privacy Act of 1974).

<b>Term</b>	<b>Meaning</b>
Third-Party Website and Application (TPWA)	Web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a “.com” website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency’s official website (Source: OMB M-10-23).
Threat	Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
Vulnerability	Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited.
Vulnerability Assessment	Formal description and evaluation of vulnerabilities of an IS.

## Appendix B – References

Appendix B lists the documents or other resources used during the development of this Detailed Operational Plan document.

U.S. Census Bureau (2016), “2020 Census Operational Plan,” Version 2.0, October 28, 2016.

U.S. Census Bureau (2016), “Operational Assessment Content Guidelines for the 2018 End-to-End Census Test and the 2020 Census,” Draft, May 10, 2016.

U.S. Census Bureau, “Privacy Impact Assessment for CEN08 Decennial,” August 11, 2014, [http://www2.census.gov/about/policies/privacy/pias/CEN08\\_dec.pdf](http://www2.census.gov/about/policies/privacy/pias/CEN08_dec.pdf).

U.S. Census Bureau, COMMERCE/*CENSUS–5 Decennial Census Program System of Records Notice*, Federal Register, February 24, 2014 (79 FR 10090), <https://www.federalregister.gov/documents/2014/04/21/2014-08993/privacy-act-system-of-records>.

U.S. Census Bureau, DS-19, *Policy on Conducting Privacy Impact Assessments*, November 6, 2005.

U.S. Census Bureau, *DS-22 Data Breach Policy Addendum*, February 24, 2014.

U.S. Census Bureau, *Data Stewardship Policy for Notifying Management Officials of Employees Who Committed an Unauthorized Disclosure of Sensitive Personally Identifiable Information (PII)*, September 10, 2015.

U.S. Census Bureau, *Privacy Principles*, April 6, 2006.

U.S. Census Bureau, *Privacy Policy and Research Committee Charter*, October 5, 2011.

*United States Department of Commerce Personally Identifiable Information (PII), Business Identifiable Information (BII), and Privacy Act (PA) Breach Response and Notification Plan*, Version 2.0, July 2013.

*Census Bureau IT Security Program Policy (ITSP)* [November 2015]

*Census Bureau Risk Management Framework Methodology* [September 2016]

*IT Security in Acquisition Checklist*

*Information Security Incident Response Plan* [2015]

*Incident Handling Handbook*

## **Appendix C – Activity Tree for Security, Privacy, and Confidentiality Operation (SPC)**

This appendix presents the Activity Tree for the SPC operation. An Activity Tree uses an outline structure to reflect the decomposition of the major operational activities in the operation. Each activity is numbered according to its position in the outline. For example, for the current operation numbered “3,” the first activity would be numbered 3-1. Subactivities under this activity would be numbered sequentially, starting again with the number one. For example, the first subactivity under the first activity would be numbered 3-1.1 the second subactivity as 3-1.2. The second activity would be numbered 3-2, and so on.

- **3-1 Security**

- 3-1.1 Leadership & Organization

- 3-1.1.1 IT Security Responsibilities
    - 3-1.1.2 IT Security Road Map
    - 3-1.1.3 IT Security Governance
    - 3-1.1.4 IT Security Planning
    - 3-1.1.5 IT Security Law & Regulations
    - 3-1.1.6 IT Security Policy

- 3-1.2 Security Risk Management

- 3-1.2.1 Risk Management Framework (RMF)
    - 3-1.2.2 Security Categorization of Systems
    - 3-1.2.3 Security & Privacy Control Selection
    - 3-1.2.4 Security Test & Evaluation
    - 3-1.2.5 Vulnerability/Red Team Assessment
    - 3-1.2.6 Risk/Issue Identification & Tracking
    - 3-1.2.7 System Security Plans (SSP)
    - 3-1.2.8 Plans of Action & Milestones (POA&Ms)

- 3-1.3 Engineering & Information Security

- 3-1.3.1 Integration of InfoSec into SDLC
    - 3-1.3.2 Management Controls Implementation
    - 3-1.3.3 Operations Controls Implementation
    - 3-1.3.4 Technical Controls Implementation
    - 3-1.3.5 Privacy Controls Implementation
    - 3-1.3.6 IT Security Procedures
    - 3-1.3.7 Best Practices Guidance Implementation
    - 3-1.3.8 Authority to Operate (ATO)
    - 3-1.3.9 Continuous Monitoring & Remediation

3-1.4 Incident Response (IR)

- 3-1.4.1 Computer Security Operations Center (CSOC) Functions
- 3-1.4.2 Incident Response Procedures
- 3-1.4.3 External Agency Partnership
- 3-1.4.4 IR Capability Testing/Training

3-1.5 Security Training & Awareness

- 3-1.5.1 General User Annual Training & Awareness
- 3-1.5.2 Technical Staff Development
- 3-1.5.3 Training & Awareness Communications

• **3-2 Privacy and Confidentiality**

3-2.1 Leadership and Organization

- 3-2.1.1 Privacy Program Governance
- 3-2.1.2 Privacy Program Management

3-2.2 Privacy Risk Management

- 3-2.2.1 PII Inventory, Categorization and Minimization
- 3-2.2.2 Privacy Risk & Impact Assessment Maintenance
- 3-2.2.3 System of Record Notice (SORN) Maintenance
- 3-2.2.4 Privacy Act Statement (PAS) Activities
- 3-2.2.5 Data Quality and Integrity Activities
- 3-2.2.6 PII Retention, Disposition and Destruction
- 3-2.2.7 FOIA Requests
- 3-2.2.8 Controlled Sharing of Information
- 3-2.2.9 Privacy and Social Media
- 3-2.2.10 Government Privacy Change Monitoring
- 3-2.2.11 Privacy Risk and Issue Tracking

3-2.3 Engineering and Information Security

- 3-2.3.1 Cybersecurity Coordination
- 3-2.3.2 Authority to Operate (ATO) and Authority to Connect (ATC) Analysis

3-2.4 Incident Response (IR)

- 3-2.4.1 Privacy and Confidentiality Incident Management
- 3-2.4.2 Incident Notification & Reporting
- 3-2.4.3 High-Impact Privacy Incident Response Team Activities

3-2.5 Transparency and Redress

- 3-2.5.1 Privacy Notice Maintenance Activities
- 3-2.5.2 Managing Complaints and Inquiries
- 3-2.5.3 Individual Access, Amendment, Correction, Redress, and Accounting of Disclosures

3-2.6 Privacy Training & Awareness

3-2.6.1 Workforce Training

3-2.6.2 Internal Online Presence

3-2.7 Accountability

3-2.7.1 Rules of Behavior Acknowledgement

3-2.7.2 Internal & External Reporting

3-2.7.3 Privacy Monitoring and Auditing

3-2.7.4 Incorporating Lessons Learned