U.S. Census Bureau
Data Stewardship /
Privacy Impact Assessment

CEN 27 Print 2010

OMB 300 ID#:006-07-01-02-01-4004-00

February, 2009

USCENSUSBUREAU

Helping You Make Informed Decisions

	B	C	D	E	F	G
1			**Privacy Impact Assessment Questions**			
2						
3					**Enter an 'x'**	
4	**PP**		**Identification Section**			
5	0	ID	1a) Is the project identifiable by an OMB 300 or IT Business Plan?		X	Yes
6	0	ID				No
7	0	ID	1b) If yes, what is its name?			Census - Decennial 2010 Systems Design and Integration, and Decennial 2010 Testing and Evaluation
8	0	ID	1c) What is the unique project identifier number/ITBP Number?			006-07-01-02-01-4004-00
9	0	ID	2a) Is the project identifiable by a PRA (ICS) identifier?			Yes
10	0	ID			X	No
11	0	ID	2b) If yes, what is the name?			
12	0	ID	2c) What is the control number (in Part II, C, 3 of the OMB 300)?			
13	0	ID	3) Who is the project owner (Associate Director)?			Jackson, Arnold
14	0	ID	4) Who is the staff contact person?			Marsden, James
15	0	ID	5) What is the phone number of the staff contact person?			301-763-8857
16	0	ID	6) What is the e-mail address of the staff contact person?			james.j.marsden@census.gov
17	0	ID	7) For which area(s) is the project relevant and necessary?			Economic
18	0	ID				Demographic
19	0	ID			X	Decennial
20	0	ID				Administrative (e.g., H.R.)
21	0	ID	8) Which of the following computer systems support this project?			CEN01 IT Infrastructure
22	0	ID				CEN02 Administrative Systems
23	0	ID				CEN03 Economic Census and Surveys and Special Processing
24	0	ID				CEN04 Commerce Business Systems (CBS)
25	0	ID				CEN05 Field
26	0	ID				CEN06 NPC
27	0	ID				CEN07 Geography
28	0	ID				CEN08 Decennial
29	0	ID				CEN11 Demographic Census, Surveys, and Special Processing
30	0	ID				CEN12 Automated Export System AESDirect
31	0	ID				CEN13 Census Research Data Centers (RDCs)
32	0	ID				CEN14 Longitudinal Employer-Household Dynamics (LEHD)
33	0	ID				CEN16 Network Services
34	0	ID				CEN17 Client Services
35	0	ID				CEN18 Enterprise Applications
36					X	CEN23 Decennial Response Integration System (DRIS)
37	0	ID				CEN25 CBS Consolidated Infrastructure
38	0	ID			X	CEN27 Decennial 2010 Print
39	0	ID				CEN28 Wireless Data Communications
40	0	AR	9) What type of direct data collection does the project involve?			New
41	0	AR				Ongoing
42	0	AR			X	None
43	0	ID	10) Please provide a brief description of the project and its purpose (suggested source is the OMB 300, Exhibit 13. or PRA submission)			The Census Bureau 2010 Print Contract is a Government Printing Office administrated contract that involves the printing, finishing, and distribution of 2010 Census questionnaire packages, to include the initial mailout/mailback, bilingual, and replacement mailing questionnaire packages. The project scope includes participation in all tests leading up to the 2010 Census, i.e., the 2008 Dress Rehearsal (DR) and any mini-tests or prototypes required. It also includes interfacing with the United States Postal Service (USPS) and the Decennial Response Integration System (DRIS) contractor responsible for the data capture. This effort continues through the closeout of Print 2010 operations.

	B	C	D	E	F	G
44	0	ID	11) Is the data collection mandatory, voluntary, or not a direct data collection?			Mandatory
45	0	ID				Voluntary
46	0	ID			X	Not a direct data collection
47	0	ID				Direct data collection, not involving a respondent
48	0	ID	12) Under what legal authority does the Census Bureau conduct this project (for Title 13, please enter section)?		X	Title 13, U.S.C., Section 141
49	0	ID				Title 15, U.S.C., Section 1525
50	0	ID				Title 5, U.S.C.

	B	C	D	E	F	G
51	0	ID	13) Will the project require new IT resources outside those specified in the OMB 300?			Yes
52	0	ID			X	No
53	1		**Privacy Principle I: Mission Necessity**			
54	1	DR	1a) Which type(s) of data does the project involve?		X	Personally Identifiable Information (PII) only - Address Data Only
55	1	DR				Identifiable Business Information (IBI) only
56	1	DR				Linked/Commingled PII to IBI
57	1	DR				No protected identifiable information--go to end
58	1	DR				Linked Geospatial data to PII and/or IBI
59	1	DR	1b) If PII or IBI only, is there PII to PII linkages/commingling or IBI to IBI linkages/commingling (e.g., SIPP to ACS)?			Yes
60	1	DR			X	No
61	1	DR	1c) Is the linking/commingling happening under the scope of your project?			Yes
62	1	DR			X	No
63	1	DRM	2a) Will the system track the method of commingling and/or linking?			Yes
64	1	DRM				No
65	1	DRM			X	N/A
66	1	DRM	2b) If yes, describe specifications			
67	1	DR	3) What is the project's intended scope/breadth?			Sample of size to produce national, general purpose estimates (e.g., CPS)
68	1	DR				Sample of size to produce detailed, geographic- or industry-level estimates (e.g., ACS)
69	1	DR			X	Universe (e.g., special censuses, industry sector census)
70	1	DR	4) What is the project's depth?			PII or IBI with characteristics
71	1	DR				PII or IBI plus general characteristic data (e.g., age, address [decennial short form])
72	1	DR				PII or IBI plus detailed characteristic data/cross sectional (e.g., income, race [ACS, decennial long form])
73	1	DR				PII or IBI plus detailed characteristic data/longitudinal (e.g., SIPP)
74	1	DR				PII and IBI plus general characteristic data
75	1	DR				PII and IBI plus detailed characteristic data (e.g., LEHD)
76	1	DR			X	Geospatial
77	1	DR	5) How many, if any, sensitive topics will the project cover?		X	None
78	1	DR				One
79	1	DR				Two or more
80	1 and 3	DR	6) If more than one sensitive topic, are the topics related to each other?			Yes
81	1 and 3	DR				No
82	1 and 3	DR			X	N/A
83	2		**Privacy Principle II: Openness**			
84	2	ID	1a) Does the project make use of administrative records?			Yes
85	2	ID			X	No
86	2	ID	1b) If yes, state the data sources and types			
87	2	ARM	2) If the project uses administrative records, has it received all required approvals, including those by the Administrative Records Coordinator?			Yes
88	2	ARM				No
89	2	ARM			X	N/A

	B	C	D	E	F	G
90	2	AR	3a) If the project uses or will use administrative records, does this project return (or plan to return) non-census confidential value-added identifiable microdata to its source agency?			Yes
91	2	AR				No
92	2	AR			X	N/A
93	2	ARM	3b) If so, are Title 15 agreements and security procedures in place to assure conformance to Title 13 legal mandates, the Privacy Act, and ethical commitments spelled out in the policy?			Yes
94	2	ARM				No
95	2	AR	4a) Are there known external constraints on use of data?		X	Yes
96	2	AR				No
97	2	AR	4b) If yes, state constraints			Title 13
98	2	AR	5a) Are there known internal (policy) constraints on use of data?		X	Yes - Contractor Internal Policy
99	2	AR				No
100	2	AR	5b) If yes, state policy constraints			
101	2	DRM	6) What are the planned mechanisms for tracking and/or ensuring notice or consent?			Advanced letter
102	2	DRM				Signed consent form
103	2	DRM			X	None or N/A
104	2	DRM	7) If this is a voluntary survey, is there a mechanism for notating refusal or limitation of consent and number of previous refusals to participate in the survey?			Yes
105	2	DRM				No
106	2	DRM			X	N/A
107	2	AR	8) If a direct data collection, does it involve the use of proxies (i.e., someone other than the intended respondent)?			Yes
108	2	AR				No
109	2	AR			X	N/A
110	2	ARM	9) Are mechanisms in place or planned to capture notice/consent by proxies or third parties?			Yes
111	2	ARM				No
112	2	ARM			X	N/A

	B	C	D	E	F	G
113	2	ARM	10a) Will the project/system create a new “System of Records (SOR)”?			Yes
114	2	ARM			X	No
115	2	ARM				N/A
116	2	ARM	10b) If no, under which existing SOR does the project fit?			Census-2 Employee Productivity Measurement Records
117	2	ARM				Census-3 Individual & Household Statistical Surveys Records and Special Studies Records
118	2	ARM				Census-4 Women- and Minority-Owned Business Enterprise Survey
119	2	ARM			X	Census-5 Population and Housing Census Records of the 2000 Census Including Preliminary Statistics for the 2010 Decennial Census
120	2	ARM				Census-6 Population Census Personal Service Records for 1900 and All Subsequent Decennial Censuses
121	2	ARM				Census-7 Special Censuses of Population Conducted for State and Local Government
122	2	ARM				Census-8 Statistical Administrative Records System (STARS)
123	2	ARM				Census-9 Longitudinal Studies
124	2	ARM				Census-10 American Community Survey
125	2	ARM				Other (list) - N/A - not a SOR
126	3		**Privacy Principle III: Respectful Treatment of Respondents**			
127	3	DR	1) What universe is the project targeting?		X	No targeting
128	3	DR				Targeting sensitive population
129	3	DR				Population other than sensitive population
130	3	DR	2) How much respondent time is needed?		X	0 - 30 minutes
131	3	DR				31 - 60 minutes
132	3	DR				61 - 90 minutes
133	3	DR				91+ minutes
134	3	DR	3) What is the frequency of contact with respondent over a 5-year period?			Once
135	3	DR			X	2 to 5 times
136	3	DR				6 or more times
137	3	DR				N/A
138	3	DRM	4) Does the project meet the criteria specified in the "Articulating the Title 13 Benefits of Census Bureau Projects" policy, ensuring both the mission necessity and the appropriate use of Special Sworn Status individuals?		X	Yes
139	3	DRM				No
140	3	DRM				N/A
141	3	DRM	5) If the project involves reimbursable activities, is it consistent with the "Reimbursable Project Acceptance Criteria" policy, in order to ensure conscious acceptance and mitigation of project risk?			Yes
142	3	DRM				No
143	3	DRM			X	N/A

	B	C	D	E	F	G
144	3	DRM	6) If the project involves household data collection, does its procedures ensure within household confidentiality, as specified in the "Respondent Identification" policy?			Yes
145	3	DRM				No
146	3	DRM			X	N/A

	B	C	D	E	F	G
147	4		**Privacy Principle IV: Confidentiality**			
148	4	AR	1) Does the data collection include the use of any new technology for which privacy concerns could arise?			Yes
149	4	AR			X	No
150	4	ARM	1b) If so, what mitigation strategies are being adopted?			
151	4	AR	2a) Does the data collection raise any specific concerns about field representative safety or access?			Yes
152	4	AR			X	No
153	4	ARM	2b) If so, what mitigation strategies are being adopted?			
154	4	ARM	3a) Is there any actual or planned access of data by Special Sworn Status (SSS) at a secure non-Census Bureau facility?		X	Yes - Printing completed by contractor/sss at contractors approved secure facility
155	4	ARM				No
156	4	AR	3b) If so, has the Data Stewardship Executive Policy Committee approved this plan and has the facility been approved by ITSO to house this data?		X	Yes
157	4	ARM				No
158	4	AR	4) Will the processing or analysis of identifiable data involve access or potential access by employees or special sworn status individuals without a need to know?			Yes
159	4	AR			X	No
160	4	AR	5) From what frame did you develop the project's sample?			Random
161	4	AR				Census Bureau - census or survey file
162	4	AR			X	MAF
163	4	AR				Business Register
164	4	AR				3rd party / administrative record data
165	4	AR				N/A
166	4	ARM	6a) Will the data collected/used as part of this project be afforded confidentiality protections by statute?		X	Yes
167	4	ARM				No
168	4	ARM	6b) Will the data collected/used as part of this project be afforded confidentiality protections via some mechanism other than statute?		X	Yes - BOC IT Security Policy & Procedures along with National Institue of Standards and Technology (NIST) Special Publications
169	4	ARM				No
170	4	AR	7) After collection, will you turn over responsibilities to an outside agency/organization for the identifiable microdata?			Yes
171	4	AR			X	No
172	4	AR	8) What are the planned types of publicly available products?			Detailed tabular data files
173	4	AR				Public use microdata file
174	4	AR				Analytical reports
175	4	AR				Geospatial products
176	4	AR			X	None
177	4	AR	9a) Does the project raise unmitigated concerns for data release based on responses to the Checklist On Disclosure Potential of Data or other source? Write in explanation.			Yes
178	4	AR			X	No
179	4	ARM	9b) Will the products be subject to the Checklist On Disclosure Potential of Data?			Yes
180	4	ARM			X	No
181	4	ARM	10a) Are there data transfers (e.g., hand-offs between systems)?		X	Yes
182	4	ARM				No
183	4	ARM	10b) State mechanism for project tracking of data transfers (e.g., agreements, automated tracking).		X	The Census Bureau address label file will be delivered via a Secure File Transfer Protoco (SFTP) to the vendor. For Replacement Mailings the Government has an Interconnection Security Agreement (ISA) in place between CEN 23 Decennial Response Integration System and CEN 27 Print 2010 for Print Vendor.
184	4	DRM	11) Will the project produce sensitive documentation requiring security related control (e.g., Title 13 sensitive reports, algorithms) for internal use only?		X	Yes
185	4	DRM				No
186	4	AR	12) Will the project produce multiple extracts/versions of the sensitive data?			Yes
187	4	AR			X	No

	B	C	D	E	F	G
188	4	ARM	13) Is there something in place already to enforce sensitive information document access and control?		X	Yes - Print vendor uses Encryption and physical and procedural security controls as described in the System Security Plan (SSP). Government documents controled by physical security controls.
189	4	ARM				No
190	4	ARM				N/A
191	4	AR	14a) Is the anticipated life expectancy of the identifiable microdata indefinite?			Yes
192	4	ARM			X	No
193	4	ARM	14b) If not, what is the anticipated life expectancy?			2 Years
194	4	AR	15) After the project is over, the identifiable microdata will:		X	Be destroyed
195	4	AR				Continue to exist within the Census Bureau, archived
196	4	AR				Continue to exist within the Census Bureau, not archived
197	4	AR				Continue to exist at the National Archives and Records Administration
198	4	AR				Become public by law
199	4	AR				Other
200						N/A
201	4	ARM	16) Has the disposal or archiving plan for data associated with this project been initiated for all types of media? Please identify any associated Records Schedules that may apply.		X	Yes-Records Schedule(s)= Sensitive electronic data shall be cleared/deleted from magnetic media no later than 90 work days after completion of each addressing process. (This includes returning magnetic media to a vendor for trade-in, servicing, or disposal.) In addition, the Contractor shall furnish a sworn affidavit to GPO, certifying that the defective address materials have been destroyed at the Contractor's plant or at a government-approved site by burning, pulverizing, or other method agreed to by the Contracting Officer.
202	4	ARM				No
203	4	ARM	17) Will the project include training employees on the confidentiality protections and proper handling procedures associated with Titles 13 and 26 (the latter only if applicable)?		X	Yes
204	4	ARM				No
205	4	ARM	18) Will the project train employees on the prohibition against unauthorized browsing as specified in the "Unauthorized Browsing" policy?		X	Yes
206	4	ARM				No
207	4	ARM	19) Have people associated with this project taken IT security training?		X	Yes - Contractor IT Staff
208	4	ARM				No
209	4	ARM	20) List any additional Data Stewardship assurance/enforcement mechanisms.			N/A
210	4	ARM	21a) Are there any additional privacy risks that have not been addressed elsewhere in this assessment?			Yes
211	4	ARM			X	No
212	4	ARM	21b) If so, are these risks you cannot mitigate, that would be detrimental to the Census Bureau mission?			Yes
213	4	ARM				No
214	4	ARM	21c) Please specify			

	B	C	D	E	F	G
215	7	DR				
216	7	DR	NET DATA SENSITIVITY SCORE =	Low		
217	7	DR				
218	7	AR	NET ACTIVITY SENSITIVITY SCORE =	Low		
219	7	AR				
220	7	SYS	PROJECT SCORE (Activity + Data)	Low		
221	7	SYS				
222	7	ARM				
223	7	ARM	SYSTEM SCORE	Moderate		Moderate only for system data availability

Key: PP=Privacy Principle, ID=Identification/contact; DR=Data Risk Assessment; AR=Activity Risk Assessment; DRM=Data Risk Mitigation; ARM=Activity Risk Mitigation.
Gray shaded questions represent a major question, **Yellow** shaded questions represent follow-up question to a major question, and **Orange** shaded cells denote a new section on the form.

I certify that this Data Stewardship/Privacy Impact Assessment appropriately identified data and activity sensitivity issues along with the planned and implemented mitigation measures, and that this program is in alignment with the Census Bureau's mission and data stewardship principles and policies.

2/12/09

Associate Director (BOC) Date

I certify that this Data Stewardship/Privacy Impact Assessment appropriately identified system risk issues along with the planned and implemented mitigation measures, and that this program is in alignment with the Census Bureau's mission and data stewardship principles and policies.

Chief Information Officer (BOC) Date 2/17/09

I certify that this Data Stewardship/Privacy Impact Assessment appropriately identified data, activity and system sensitivity and risk issues along with the planned and implemented mitigation measures, and that this program is in alignment with the Census Bureau's mission and data stewardship principles and policies.

2/25/09

Chief Privacy Officer (BOC) Date

U.S. Census Bureau IT System Security Evaluation for Privacy Impact Assessments
Print 2010 Contract – CEN27
Risk Level – System impact levels are rated LOW for (1) confidentiality, LOW for (2) integrity, and MODERATE for (3) availability. Therefore, we establish the overall system categorization level for CEN 27 Print 2010 at MODERATE impact.

The Census Bureau IT Security Office, based on the information contained in the IT security documentation provided for the Print 2010 Contract, has determined the risk level of the system to be moderate. This risk level was determined by a careful review of information relating to IT configuration and security controls that make up the CEN 27 Print 2010 system. In addition to an independent review of security controls, the program area coordinated with the Technical Security Staff of the IT Security Office to perform a technical vulnerability assessment scan on thePrint 2010 Contract computing system. Security risks defined by this scan were corrected by the program area and were documented as part of the package provided to the Census Bureau Chief Information Officer (CIO) for authorization to process sensitive data on the Census Bureau network. The main computing system that stores and processes the Personally Identifiable Information (PII) resides behind the Census Bureau firewall. Access to the system and file structure is controlled by access control lists and specific user privileges. All activity on the system is recorded in security audit logs that are reviewed on a regular basis by designated personnel. Any anomalies noted are reported to the Census Bureau IT Security Office, which conducts an investigation and documents the findings for management review.

There are no data collection or input activities involved in CEN27 - Print 2010 Contract. The Census Bureau 2010 Print Contract is a Government Printing Office administrated contract that involves the printing, finishing, and distribution of 2010 Census questionnaire packages, to include the initial mailout/mailback, bilingual, and replacement mailing questionnaire packages. The project scope includes participation in all tests leading up to the 2010 Census, i.e., the 2008 Dress Rehearsal (DR) and any mini-tests or prototypes required. It also includes interfacing with the United States Postal Service (USPS) and the Decennial Response Integration System (DRIS) contractor responsible for the data capture. This effort continues through the closeout of Print 2010 operations.

The Census Bureau classifies its IT systems risk levels as high, moderate, or low as indicated by the individual risk levels to confidentiality, integrity, and availability. Confidentiality risk has the greatest bearing on privacy per the risk levels defined in the NIST Federal Information Processing Standards (FIPS) Publication 199. Confidentiality is defined as “Preserving authorized restrictions on information access and disclosure, including means for protecting privacy and proprietary information.” Systems judged to be moderate risk systems are further defined as systems processing information for which “The unauthorized disclosure of information could be expected to have a serious adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs." The Census Bureau standard for any system that processes sensitive information protected under United States Code is to have minimum-security controls in place for a system at the moderate risk level. The system may be elevated to a high-risk category if warranted: when combined with specific program information during the Privacy Impact Assessment process, or when the system functions change during the life cycle. Risk levels are reviewed regularly by the IT Security Office, program areas, and the Privacy Office to ensure that they reflect the level most appropriate for the system based on the PIA life-cycle and processing requirements.

The Census Bureau has organized its IT systems by business area into 09 major systems and all are categorized at the Sensitive, But Unclassified level. Each of these systems has a security plan completed in accordance with NIST Special Publication 800-18 and the requirements of the Federal Information Security Management Act, Title III of the E-Government Act of 2002. The security plans are prepared by the system owners and provide the basis for identification and implementation of required security controls. These controls ensure the appropriate level of security is applied, relative to the overall risk level of the system. Each system security plan provides the following information pertaining to the system:

Section:

3.2.1 - System Name/Title
3.2.2 - Responsible Organization
3.2.3 - Information Contact (System Owner)
3.4 - General Description/Purpose (Describes the type of data, as well as a general overview of functions)
3.5 - System Environment
3.6 - System Interconnection/Information Sharing
3.7 - Sensitivity of Information Handled
3.7.1 - Laws, Regulations, and Policies Affecting the System
3.7.2 - General Level of Sensitivity (Pertaining to confidentiality, integrity, and availability).
4.1 - Risk Assessment and Management
4.2 - Review of Security Controls (How does the system comply with existing security policies?).
4.3 - Rules of Behavior (Delineates the responsibilities and expected behavior of all individuals with access to the system.
5.1 - Personnel Security (Contains information about personnel security measures)
6.1 - Identification and Authentication
6.2 - Logical Access Controls (Authorization/Access Controls)
6.3 - Public Access Controls
6.4 - Audit Trails

The Census Bureau uses a multi-step IT security planning process that begins with the identification of a new system or modification to an existing system. Once identified, the system owner contacts the IT Security Office (ITSO) to determine what level of documentation is required for their system. The system owner develops and submits his/her documentation to the IT Security Office for review. The ITSO, working with the Information System Support and Review Office, coordinates with the system owner to ensure that all required information has been provided. Concurrently, a technical security review of the security controls and system security level is conducted by the ITSO to determine if the system's controls comply with the published security policies. This review also assures that all technical vulnerabilities are either corrected or mitigated to an acceptable level of risk prior to the CIO's authorization of the system to process sensitive data.

The Census Bureau has fully integrated the IT security process into its business planning. The IT security personnel are involved in the early stages of projects to ensure that appropriate security controls are addressed and that project personnel understand, and are responsive to, IT security requirements for protecting their systems and the data they process. This involvement extends throughout the life cycle of the project, and regular reviews are conducted to ensure continued compliance with security requirements.

All systems identified in the Census Bureau inventory have been Certified and Accredited using the "Guide for the Security Certification and Accreditation of Federal Information Systems", NIST Special Publication 800-37.

Security documentation, risk assessments, and corrective action plans for each system are kept on file in the ITSO and made available as requested to authorized individuals. These documents are classified as "For Official Use Only" and access is restricted to individuals with a demonstrated need to know.

The Census Bureau has ensured that the security controls required by NIST for systems with a moderate risk level are in place using the NIST guidance, "Guide for Mapping Types of Information and Information Systems to Categories, Special Pub 800-60, and "Standards for Security Categorization of Federal Information and Information Systems," FIPS Pub 199.

Data Sensitivity Matrix

		Required Sensitivity Score (if applicable)	Actual Sensitivity Score		Mitigation Item	Required Mitigation Score (if applicable)	Actual Mitigation Score
	Identifiable Data						
	PII	0	0				
	IBI	0	0				
	Linked PII and IBI	0	0				
	No Identifiable Data	0	0				
	Linked Geospatial data	0	0				
	Linkages/Commingling (2)						
	PII to PII Linkages	1	0		System tracks method of commingling/linking	1	0
	No PII to PII Linkages	0	0				
	IBI to IBI Linkages	1	0				
	No IBI to IBI Linkages	0	0				
	PII to IBI Linkages	2	0				
	No PII to IBI Linkages	0	0				
	Linked Geospatial data	1	0				
							0
							0
					Post-mitigation Sensitivity		Low
	Breadth/Scope (2)						
	Sample size=national estimates (e.g., CPS)	0	0		Confidentiality via statute	2	2
	Samples size=detailed geo/industry level estimates (e.g., ACS)	1	0		Subject to disclosure checklist	1	0
	Universe (e.g., decennial, special, or industry sector census)	2	2				
							2
							0
					Post-mitigation Sensitivity		Low

	Depth (3)						
	PII or IBI only	0	0		Notice & consent tracking	1	0
	PII or IBI plus general characteristic data (e.g., decennial short form)	0	0		Mechanisms for notating refusal or limitation of consent/previous refusals	1	0
	PII or IBI plus detailed characteristic data / cross sectional (e.g., ACS)	1	0		Confidentiality via statute	1	1
	PII or IBI plus detailed characteristic data / longitudinal (e.g., SIPP)	2	0				
	PII and IBI plus general characteristic data	2	0				
	PII and IBI plus detailed characteristic data (e.g., LEHD)	3	0				
	Geospatial only	0	0				
							0
							0
					Post-mitigation Sensitivity		Low
	Sensitive Topics (3)						
	None	0	0		DS015 Reimbursable policy	1	0
	One	1	0		DS002 Title 13 benefit	1	1
	Two or more	2	0		DS016 Respondent Identification policy	1	0
	Related	0	0				
	Unrelated	1	0				
							0
							0
					Post-mitigation Sensitivity		Low
	Targeting (1)						
	No targeting	0	0		DS015 Reimbursable policy	1	0
	Population other than sensitive population	0	0				
	Targeting sensitive population	1	0				
							0
							0
					Post-mitigation Sensitivity		Low
	Burden and Frequency (6)						
	Estimated at 0-30 minutes	0	0		DS015 Reimbursable policy - Basic (if applicable)	1	0
	Estimated at 31-60 minutes	1	0		DS015 Reimbursable policy- Supplementary (if applicable)	0	0
	Estimated at 61-90 minutes	2	0				
	Estimated at 91+ minutes	3	0				
	Once	1	0				
	2-5 times	2	2				
	6 or more	3	0				

							0
							2
					Post-mitigation Sensitivity		Medium

Mandatory/Voluntary (1)					
Voluntary	0	0			
Mandatory	1	0			
Mix	1	0			
Not a direct data collection	0	0			
Direct data collection, no respondent	0	0			
					0
					0
			Post-mitigation Sensitivity		Low
Purpose of Review (1)					
Ongoing surveys	0	0	Any additional Data Stewardship assurance mechanisms	1	0
New surveys	1	0			
					0
					0
			Post-mitigation Sensitivity		Low
Total unmitigated risk level		Low			

Net data sensitivity score (after mitigation):	**Low**

Activity Sensitivity Matrix	Required Sensitivity Score (if applicable)	Actual Sensitivity Score	Risk Mitigation Item	Required Mitigation Score (if applicable)	Mitigation Score
Data Collection (5)					
Is via administrative records	1	0	Covered by System of Record	1	1
Involves the use of proxies (e.g., someone other than the intended respondent)	1	0	New System of Record	1	0
Includes the use of any new technology for which privacy concerns could arise	1	0	Specific mitigation for field representative access/safety concerns	1	0
Raises specific concerns about field representative safety or access	1	0	Mechanisms to capture proxy/3rd party notice/consent	1	0
Are there external constraints on use of data	1	1	DS001 Administrative Record Handbook in effect	1	0
Return value-added information to source agency	1	0	DS016 Respondent Identification policy	1	0
			Title 15 agreements and security procedures in place to assure conformance	1	0
					1
					0
			Post-mitigation Sensitivity		Low
Processing/Analysis (5)					
Requires use of a secure non-Census Bureau facility	1	1	DS017 Title 13/26 training	1	1
Involves access or potential access by employees or special sworn status without a need to know	1	0	DS018 Unauthorized Browsing policy	1	1
Involves creation of multiple extracts/versions	1	0	DS006 Controlling Non-Employee Access policy	1	1
Involves creation of internal use only/Census confidential reports, algorithms or other information	1	1	Plan for controlling access to sensitive documents	1	1
Data Transfers	1	1	Data transfer plans	1	1
					3
					0
			Post-mitigation Sensitivity		Low
Methodology (1)					
Sample frame randomly derived	0	0			
Sample frame derived from census/survey file	1	0			
Sample frame derived from MAF	1	1			
Sample frame derived from Business Register	1	0			

	Sample frame derived from 3rd party/administrative record data	1	0				
					Post-mitigation Sensitivity		High

Dissemination (6)					
Detailed tabular data files will be produced	1	0	Disclosure research program	1	1
Public use microdata files will be produced	2	0	Subject to disclosure checklist	1	0
Analytic reports will be produced	1	0			
Geospatial products	1	0			
None	0	0			
Potential disclosure concerns identified via disclosure checklist (in addition to points above)	1	0			
			Post-mitigation Sensitivity		Low
Archiving (4)					
Useful life is indefinite	1	0	DS017 Title 13/26 training	1	1
Will not be destroyed after useful life	2	0	DS018 Unauthorized Browsing policy	1	1
Continue to exist	1	0	Archiving plan is being developed/in effect	1	1
Will continue to exist outside a formal archiving plan	1	0	Any additional Data Stewardship assurance mechanisms	1	0
			Post-mitigation Sensitivity		Low
Total unmitigated risk level		Medium			

Net activity sensitivity score (after mitigation):	**Low**
Revised score, based on additional risk (see PP4, question 21):	**No additional risk**