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

Geographic Support Systems

OMB 300 ID#:006-07-01-02-01-4009-00-315-181

March, 2008

USCENSUSBUREAU

Helping You Make Informed Decisions

DATA STEWARDSHIP/PRIVACY IMPACT ASSESSMENT INTRODUCTION

The Objective of Data Stewardship/Privacy Impact Assessments

Privacy Impact Assessments (PIAs) are required by the E-Government Act of 2002 whenever “developing or procuring information technology . . . or initiating a new collection of information . . . in an identifiable form . . . ” They also are required by Office of Management and Budget (OMB) Circular No. A-11 and OMB Exhibit 300, “Capital Asset Plan and Business Case,” which tie together privacy considerations, executive agency funding requests, and Enterprise Architecture (EA) requirements. Finally, PIAs link project and system risk assessments to ensure the provision of adequate security, as defined by OMB Circular A-130. Consistent with the objectives of the E-Government Act and to ensure the continued trust of our constituency, on February 3, 2004, the Census Bureau is releasing this PIA to the public.

The purpose of PIAs is to ensure no collection, storage, access, use, or dissemination of identifiable respondent information (businesses and individuals) that is not needed or permitted. According to OMB, "PIAs are structured reviews of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to identify and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." The review makes use of a structured tool--a series of questions that determine whether the planned system or activity is consistent with our organization’s privacy principles, procedures, and controls.

Despite the use of the term “privacy,” PIAs typically cover privacy, confidentiality, integrity, and availability issues, which the Census Bureau would equate with “data stewardship.” Therefore, the U.S. Census Bureau refers to these evaluations as Data Stewardship/Privacy Impact Assessments (DS/PIAs). DS/PIAs can facilitate data stewardship, management, awareness, and compliance efforts.

At the Census Bureau, DS/PIAs also provide a project management tool, allowing program and project managers to integrate data stewardship considerations into the planning and design phases of work. This approach has the advantage of early detection and avoidance of certain sensitivities altogether or of identifying risk mitigation activities that may need to be incorporated into a funding request.

Data Stewardship at the Census Bureau

Fully consistent with the E-Government Act of 2002, the Census Bureau has adopted a Data Stewardship program. Data Stewardship is the process of meeting the public need for statistical information and the legal and ethical obligation to respect individual privacy and protect confidentiality. It is a management approach to decision-making that facilitates meeting our mission requirements to collect and publish high quality data about our Nation’s people and economy and satisfies our ethical and legal requirements to respect the privacy and protect the confidentiality of all Census Bureau respondents, customers, contractors or bidders, and employees.

The Census Bureau has embarked upon a data stewardship program that addresses privacy and confidentiality as well as data access and use issues. At its core is the Data Stewardship Executive Policy Committee (DSEP), the Census Bureau executive staff focal point for decision making and communication on privacy, security, confidentiality and administrative records policy issues. The DSEP has adopted a set of Privacy Principles that aligns our mission with these principles and assists us in achieving our goals and objectives. The DSEP has developed new policies (available upon request) that strengthen our cultural commitment to data stewardship. The PIA is one tool for implementing and creating awareness of data stewardship policies.

The Census Bureau's DS/PIA Scope and Methodology

For the first application of DS/PIAs, the Census Bureau included in scope the full program covered by each OMB Exhibit 300, each with its own DS/PIA, whether or not the full amount of the program's funding was included in the OMB Exhibit 300. In one case, the Economic Census and Surveys OMB Exhibit 300, the wide variety of functions covered by multiple legal authorities required it to be parsed into multiple DS/PIAs. This DS/PIA tool, with slight modifications, is also intended for use with new data collections submitted under the Paperwork Reduction Act (PRA) to OMB.

A full DS/PIA is conducted on programs whether they contained Personally Identifiable Information (PII), Identifiable Business Information (IBI), or both. Identifiable information is defined as information that actually identifies people or businesses. Examples include direct references such as name, address, social security number, employer identification number, financial information, or other identifying number or code such as telephone number, email address, etc. It also includes any information used separately or in combination to reference other data elements that are used for identification such as gender, race, birth data, or geographic indicator. These two types of identifiers (PII and IBI) allow identification of specific individuals or businesses, as defined in the glossary. A partial DS/PIA (i.e., just the identification and systems components) is conducted on OMB Exhibit 300s that represent infrastructure system programs involving no "ownership" of data under the premise that the data and activity, or "program" components of the DS/PIA, are covered by program area DS/PIAs.

The DS/PIA is organized by the Census Bureau's four Privacy Principles, addressing:

- Mission Necessity
- Informed Consent
- Respectful Treatment of Respondents
- Confidentiality

A complete assessment ensures alignment with Census Bureau data stewardship strategies, goals, principles and policies. The guidance from OMB directs that PIAs cover the following items:

1. What information is to be collected.
2. Why the information is being collected.
3. The intended use of information by the agency.
4. With whom the information will be shared.
5. What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared.
6. How the information will be secured.
7. Whether a system of records is being created under Section 552a of Title 5, United State Code, (commonly referred to as the "Privacy Act").

We address these items in three groupings, consistent with our privacy principles:

· The nature and type of **data** being collected (Items 1, 2, and 5 in part, above)
· The **activities** surrounding the handling of, use of, and access to the data (Items 3, 4, 5 in part, and 7 above)
· The computer **systems** through which the data will pass and/or in which they will reside (Item 6, above)

The first two components comprise the "project" aspects of the program, while the third focuses on supporting systems. The DS/PIA assessment uses responses to a series of questions measuring sensitivity and mitigation to achieve a net rating of low, medium, or high for the "data" and "activity" aspects of a project. Project data sensitivity may vary substantially, however stringent mitigation activities keep all project data protected. The goal is to mitigate projects from high or medium to the medium or low levels. For the third component, the net assessment score comes from the security review and certification process, with the documentation based on agency security plans.

Most of the mitigation questions ask about the applicability of and conformance to statute, regulation, or policy. The Census Bureau's suite of data stewardship policies covers most of the data, activity, and systems sensitivity areas. In a few cases, policies are under development. Therefore, the tool asks about additional activities that a program area may voluntarily undertake to reduce or mitigate sensitivity or risk.

Staff familiar with the privacy principles, policies and the DS/PIA tool assist program managers in completing the DS/PIA through face-to-face meetings, thereby ensuring consistency and understanding.

Limitations

The Census Bureau's plan for this tool is for it to be used by program and project managers throughout the lifecycle of the project; beginning as part of the initial decision making process when initiating and designing projects involving the collection or use of identifiable data and the dissemination of protected products by disclosure avoidance techniques. However, during the first implementation, the tool was used primarily to reflect the current state of program plans, which serves as a benchmark for future PIA assessments. This limitation of our tool is offset by the fact that the current state of programs is currently influenced by data stewardship policies and controls that are at the foundation of this assessment tool. In the future, the Census Bureau intends to utilize the original strategy of asking subsets of questions from the PIA assessment throughout the project development life cycle. This approach will allow for the PIA tool to be an intrinsic part of the project management process at the Census Bureau and assure that data stewardship becomes an integral part of program decision-making.

In addition, because the scoring system used to identify the adequacy of mitigation activities to sensitivities focus on net, or mitigated results, it is possible that some variation across programs may be masked. To address that concern, the unmitigated risk score is provided on the scoring sheets. Finally, there are a few content areas where additional analysis would be beneficial. We envision progressing on each of these issues as our tool develops.

DATA STEWARDSHIP/PRIVACY IMPACT ASSESSMENT USER GUIDE AND GLOSSARY

The Census Bureau's DS/PIA exists in Microsoft Excel, and each of the following sections is provided on a separate "sheet."

Sheet 1: Cover Page
Sheet 2: Introduction
Sheet 3: User Guide/Glossary
Sheet 4: The DS/PIA Instrument
Sheet 5: The DS/PIA System Write-up
Sheet 6: The DS/PIA Data Sensitivity Worksheet
Sheet 7: The DS/PIA Activity Sensitivity Worksheet

This sheet is the User Guide/Glossary, with an explanation of the items on sheets four through seven.

The DS/PIA Instrument

The instrument poses a set of questions to program managers. Program identification questions are asked to ensure a clear link to OMB Exhibit 300 or Paperwork Reduction Act (PRA) Information Collection Request (ICR), among other items.

The next set of questions under the first Privacy Principle on Mission Necessity covers the breadth and depth of a data collection, and whether sensitive topics are addressed. Sensitive topics are defined as: abortion; alcohol, drug, or other addictive products; illegal conduct; illegal immigration status; information damaging to financial standing, employability, or reputation; information leading to social stigmatization or discrimination; politics; psychological well-being or mental health; religion; same-sex partners; sexual behavior; sexual orientation; taxes; and other information due to specific cultural or other factors. The Census Bureau considers religion a uniquely sensitive topic and has a specific policy on the collection of information about religion.

The second Privacy Principle on Openness asks about tracking of notification for mandatory data collections, and about tracking of consent for voluntary data collections. It also asks about consent related to the use of proxies or data from third parties, which are often, but not always administrative records from other federal agencies.

The third Privacy Principle on Respectful Treatment of Respondents is relevant to the actual data collection activities. It asks about targeting population groups, and about burden and frequency of the collection.

The fourth Privacy Principle on Confidentiality covers internal controls related to need-to-know access, use of off-site facilities, data transfers among systems, dissemination of products that have been protected by disclosure avoidance techniques, and archiving plans. It asks about control of any sensitive data (including sensitive topics, but broader) or information.

The DS/PIA Data Sensitivity Worksheet

This sheet categorizes all of "data" related questions asked on the instrument into either "sensitivities" or "mitigations." For example, asking about a sensitive topic introduces "sensitivities" to the project. Ensuring adherences to the Respondent Identification Policy, which addresses within household confidentiality, is a mitigation activity. A score is associated with each question to “net” a ranking by topic of low, medium, or high for each topical area. The objective is both to assess strengths for each topical area and for the overall project's "data" components.

The DS/PIA Activity Sensitivity Worksheet

This sheet is organized in the same manner as the Data Sensitivity Sheet. It covers all of the activity-related question topics, such as those related to use of Special Sworn Status or use of off-site facilities.

The DS/PIA IT Systems Risk Worksheet

This narrative describes the specific mitigations in place for the particular IT systems supporting a program. It also describes the Census Bureau's IT security review and certification process, which is undertaken for a computer system. The DS/PIA uses results from this process to inform its systems component.

Glossary

Administrative Records - Administrative records and administrative records data refer to microdata records contained in files collected and maintained by administrative (i.e., program) agencies and commercial entities. Government and commercial entities maintain these files for the purpose of administering programs and providing services. Administrative records are distinct from systems of information collected exclusively for statistical purposes, such as those the U.S. Census Bureau produces under the authority of Titles 13 or 15 of the United States Code (U.S.C.). For the most part, the Census Bureau uses, and seeks to use, administrative records developed by federal agencies, as directed by Title 13, Section 6. To a lesser degree, it may use information from state, local, and tribal governments, as well as from commercial entities.

Administrative Records Handbook - The Administrative Records Handbook, re-issued on May 16, 2001, states the restricted access policy for administrative records and describes the processes and procedures that implement the policy. It is available on-line at the Policy Office Intranet site.

Articulating the Title 13 Benefits of Census Bureau Projects Policy - This policy provides guidance and criteria for determining whether a project delivers a benefit to the Census Bureau. The policy is available from the Census Bureau's Policy Office.

Commingled Data Sets - These are files that contain Administrative Records data, such as tax data, along with Title 13-protected data. Such files remain commingled even if the Administrative Records data use was limited to the sample selection phase. They are typically subject to both Title 13 and any additional data-supplier imposed restrictions.

Confidentiality Protection in Statute - United States Code, Title 13, Sections 9 and 214 protects the confidentiality of personal information, including about businesses, collected during the decennial census and other censuses.

Controlling Non-Employee Access to Title 13 Data Policy - Issued on July 15, 2002, this policy provides guidance on (1) when it is appropriate to confer special sworn status (SSS) on an individual for purposes of working with Census Bureau confidential data; and (2) when it is appropriate for access to those data to take place at a non-U.S. Census Bureau site or facility, including security requirements. The policy is available through the Census Bureau's Policy Office.

Data Stewardship Assurance Mechanisms - Data Stewardship is a management approach to decision-making that facilitates meeting our mission requirements to collect and publish high quality data about our Nation's people and economy and satisfies our ethical and legal requirements to respect the privacy and protect the confidentiality of all U.S. Census Bureau respondents, customers, contractors or bidders, and employees.

Data Stewardship assures that the Census Bureau can effectively collect and its customers can use high quality data about the Nation's people and economy while fully meeting the Census Bureau's ethical and legal obligations to respondents to respect privacy and protect confidentiality. This includes fully meeting the legal and reporting obligations levied by the Census Act, the Privacy Act, and other applicable statutes, including the requirements of governmental and other suppliers of data to the Census Bureau. It also includes meeting the ethical standards identified by our Privacy Principles and other data stewardship best practices. It assures that high quality data are available for use through effective application of security and technology. It includes the use of alternative data sources as appropriate to reduce burden, minimize cost, and improve data quality and timeliness. Our Data Stewardship approach is supported by our culture, education, awareness, methodologies, and organizational structure.

Disclosure Review Board (DRB) Checklist on Disclosure Potential of Data - Is a tool that assists the DRB in reviewing disclosure-limited data products. The checklist are completed and submitted to the DRB.

Geospatial Information - This term covers the collection, information extraction, storage, dissemination, and exploitation of geodetic and geomagnetic imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the earth's surface. It is information produced by multiple sources to common interoperable data standards. It may be presented in the form of printed maps, charts, and publications; in digital simulation and modeling databases; in photographic form; or in the form of digitized maps and charts or attributed centerline data.

High Sensitivity - High sensitivity projects involve data or activities that, if not mitigated, can significantly harm public confidence in the Census Bureau's ability to protect privacy and confidentially, thereby significantly inhibiting its ability to carry out its mission.

Identifiable form - As defined by the OMB Order Providing for the Confidentiality of Statistical Information, identifiable form "means any representation of information that permits information concerning a specific respondent to be reasonably inferred by either direct or indirect means."

Identifiable Information (II) - This is information that actually identifies persons (see persons). Examples include direct reference such as name, address, social security number, employer identification number, financial information, or other identifying number or code such as telephone number, email address, etc. It also includes any information used to reference other data elements that are used for identification such as gender, race, birth date, geographic indicator, etc.

Personally Identifiable Information (PII) - Identifiable Information (II) that refers to individuals.

Identifiable Business Information (IBI) - Identifiable Information (II) that refers to organizations or businesses.

Information - As defined by the OMB Order Providing for the Confidentiality of Statistical Information, information "means information of any kind that is not generally available to the public, and includes data."

Informed Consent - This is the agreement of the respondent to provide personal data for research and/or statistical purposes based on the full exposure to the facts, including any risks involved and available alternatives to providing the data needed to make an intelligent decision to participate. It applies when respondents have a clear choice to participate or not and are not subject to any penalties for failing to provide data.

Low Sensitivity - Low sensitivity projects involve data or activities that, if not mitigated, have limited potential to harm public confidence in the Census Bureau's ability to protect privacy and confidentially, thereby having limited potential to inhibit its ability to carry out its mission.

Medium Sensitivity - Medium sensitivity projects involve data or activities that, if not mitigated, can harm public confidence in the Census Bureau's ability to protect privacy and confidentially, thereby somewhat inhibiting its ability to carry out its mission.

Microdata File - These are electronic files consisting of individual records each containing values of variables for a single person, business establishment or other unit.

Moderate Risk Level - NIST FIPS 199 defines a "Moderate risk level" as: "The event could be expected to have a serious adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals. The event causes significant degradation in mission capability, places the agency at a significant disadvantage, or results in major damage to assets, requiring extensive corrective actions or repairs."

Notification - Denoted for a condition in which the respondent provides personal data for a mandatory data collection. As with informed consent, the respondent provides data under a full exposure to the facts associated with the collection, but the choice or agreement to participate is not present.

OMB Exhibit 300 - The Exhibit 300 is designed to coordinate OMB's collection of agency information for its reports to Congress required by the Federal Acquisition Streamlining Act of 1994 (FASA) (Title V) and the Clinger-Cohen Act of 1996; to ensure that the business case for investments is made and tied to the mission statements, long-term goals and objectives, and annual performance plans developed pursuant to the Government Performance and Results Act of 1993 (GPRA); and for Information Technology, to ensure that security, privacy, records management, and electronic transactions policies are fully implemented.

Persons - As defined by the OMB Order Providing for the Confidentiality of Statistical Information, persons "mean individuals, organized groups of individuals, societies, associations, firms, partnerships, business trusts, legal representatives, companies, joint stock companies, and corporations, and refers to both the singular and the plural."

Privacy - This concerns how the Census Bureau respects and minimizes intrusion on the personal life or business operations of the respondent by the manner of collecting information and the nature of the information sought.

Privacy Impact Assessments (PIA) - PIAs are required by the E-Government Act of 2002 and by the Office of Management and Budget (OMB) Circular Number A-11, OMB Exhibit 300, "Capital Asset Plan and Business Case." According to OMB, "PIAs are structured reviews of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to identify and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." PIAs also ensure consistency with an organization's privacy principles, procedures, and controls. Despite the use of the term "privacy," PIAs typically cover privacy, confidentiality, security, and data use issues.

Public-Use Microdata Files - These are statistical products released without restriction on use or other conditions except for payment of purchase fees. These are files with records that contain information about individuals or households, or about businesses, with all personal identifiers removed. They are released only after disclosure avoidance techniques have been applied to protect the data.

Reimbursable Project Acceptance Criteria Policy - This policy establishes criteria for accepting reimbursable projects at the U.S. Census Bureau. This covers all projects for which the Census Bureau would receive funds and for which a BC-505-A form is required by the Budget Office, excluding product sales. The policy is available at the Policy Office Intranet site.

Respondent - As defined by the OMB Order Providing for the Confidentiality of Statistical Information, respondent "means a person (other than a Federal employee responding to inquiries within the scope of his employment, see CFR 1320.3(c)(4)) who is requested to provide information, or is the subject of that information, or who provides that information." (See "persons.")

Respondent Identification Policy - Issued on August 6, 1998, the policy provides guidance for the decennial census and household surveys employing dependent interviewing techniques. The policy applies when field representatives revisit a household for a follow-up interview or quality control operation, and the field representative is instructed to update/review information previously provided. The policy is available at the Policy Office Intranet site.

Sensitive Information - This is defined in the Computer Security Act of 1987 as, " . . . any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." This includes information about Census Bureau investigations, enforcement actions, personnel contracts, financial matters, EEO cases, and reorganizations.

Sensitive Topics - They include: abortion; alcohol, drug or other addictive products; illegal conduct; illegal immigration status; income, information damaging to financial standing, employability, or reputation; information leading to social stigmatization or discrimination; politics; psychological well-being or mental health; religion; same-sex partners; sexual behavior; sexual orientation; taxes; and other information due to specific cultural or other factors. The Census Bureau considers religion a uniquely sensitive topic and has a specific policy on the collection of information about religion.

Special Sworn Status (SSS) - Special Sworn Status is the designation given to non-employees who are given the Oath of Nondisclosure in order to access confidential, and other statutory protected data, in support of Title 13 programs. SSS is authorized by Title 13, U.S.C., Section 23(c), which permits the temporary staff to be sworn to assist the work of the Census Bureau provided they observe the limitations imposed by Title 13, U.S.C., Section 9.

System of Records - Under the Privacy Act, it is defined as “a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

Tabular Data - Tabular data is a means of bringing together and presenting related material or other information in columns or rows.

Title 13 Training - This refers to the Title 13 Computer-Based Training (CBT) used to teach those new to the Census Bureau and to annually remind current workers of the Census Bureau’s strict confidentiality standards and how the standards apply to everyday worklife at the Census Bureau. The training provides awareness and a basic understanding of the oath of nondisclosure, the confidentiality aspects of Title 13, the basic differences between Title 13 and Title 15, and the Privacy Principles and Unauthorized Browsing policy.

Unauthorized Browsing - It is the act of searching or looking through, for other than work-related purposes, protected personal or business-related information that directly or indirectly identifies individual persons or businesses. Unauthorized browsing is prohibited.

Privacy Impact Assessment Questions

	PP		Identification Section	Enter an 'x'	
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?		Geographic Support Systems
8	0	ID	1c) What is the unique project identifier number/ITBP Number?		006-07-01-02-01-4009-00-315-181
9	0	ID	2a) Is the project identifiable by a PRA (ICS) identifier?	x	Yes
10	0	ID			No
11	0	ID	2b) If yes, what is the name?		Boundary and Annexation Survey
12	0	ID	2c) What is the control number (in Part II, C, 3 of the OMB 300)?		0607-0151 BAS
13	0	ID	3) Who is the project owner (Associate Director)?		Arnold A. Jackson
14	0	ID	4) Who is the staff contact person?		Michael T. Thieme
15	0	ID	5) What is the phone number of the staff contact person?		301-763-9062
16	0	ID	6) What is the e-mail address of the staff contact person?		michael.t.thieme@census.gov
17	0	ID	7) For which area(s) is the project relevant and necessary?	x	Economic
18	0	ID		x	Demographic
19	0	ID		x	Decennial
20	0	ID		x	Administrative (e.g., H.R.) (for dapps)
21	0	ID	8) Which of the following computer systems support this project?	x	CEN01 IT Infrastructure
22	0	ID		x	CEN02 Administrative Systems
23	0	ID		x	CEN03 Economic Census and Surveys and Special Processing
24	0	ID		x	CEN04 Commercie Business Systems (CBS)
25	0	ID		x	CEN05 Field
26	0	ID		x	CEN06 NPC
27	0	ID		x	CEN07 Geography
28	0	ID		x	CEN08 Decennial
29	0	ID		x	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		x	CEN16 Network Services
34	0	ID		x	CEN17 Client Services
35	0	ID		x	CEN18 Enterprise Applications
36	0	ID		x	CEN25 CBS Consolidated Infrastructure
37	0	ID			CEN28 Wireless Data Communications
38	0	AR	9) What type of direct data collection does the project involve?		New
39	0	AR		x	Ongoing
40	0	AR			None
41	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)	x	The Geographic Support System is one of the cornerstones of Census Bureau data collection, processing, and dissemination operations. It provides the basic maps, address lists, address and geographic reference files, and associated processing systems needed to meet the geographic requirements of all Census Bureau programs. The GSS manages large volumes of information from both internal and external sources to establish and maintain a current and complete inventory of streets, addresses, accurate boundaries, and other attribute information.
42	0	ID	11) Is the data collection mandatory, voluntary, or not a direct data collection?		Mandatory
43	0	ID		x	Voluntary
44	0	ID			Not a direct data collection
45	0	ID		x	Direct data collection, not involving a respondent

	A	B	C	D	E	F	G	H
46		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	
47		0	ID				Title 15, U.S.C., Section 1525	
48		0	ID	13) Will the project require new IT resources outside those specified in the OMB 300?			Yes	
49		0	ID			x	No	
50		1		**Privacy Principle I: Mission Necessity**				
51		1	DR	1a) Which type(s) of data does the project involve?		x	Personally Identifiable Information (PII) only	
52		1	DR			x	Identifiable Business Information (IBI) only	
53		1	DR				Linked/Commingled PII to IBI	
54		1	DR				No protected identifiable information--go to end	
55		1	DR				Linked Geospatial data to PII and/or IBI	
56		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	
57		1	DR			x	No	
58		1	DR	1c) Is the linking/commingling happening under the scope of your project?			Yes	
59		1	DR				No	
60		1	DRM	2a) Will the system track the method of commingling and/or linking?			Yes	
61		1	DRM				No	
62		1	DRM				N/A	
63		1	DRM	2b) If yes, describe specifications				
64		1	DR	3) What is the project's intended scope/breadth?			Sample of size to produce national, general purpose estimates (e.g., CPS)	
65		1	DR				Sample of size to produce detailed, geographic- or industry-level estimates (e.g., ACS)	
66		1	DR			x	Universe (e.g., special censuses, industry sector census)	
67		1	DR	4) What is the project's depth?		x	PII or IBI with characteristics	
68		1	DR				PII or IBI plus general characteristic data (e.g., age, address [decennial short form])	
69		1	DR				PII or IBI plus detailed characteristic data/cross sectional (e.g., income, race [ACS, decennial long form])	
70		1	DR				PII or IBI plus detailed characteristic data/longitudinal (e.g., SIPP)	
71		1	DR				PII and IBI plus general characteristic data	
72		1	DR				PII and IBI plus detailed characteristic data (e.g., LEHD)	
73		1	DR			x	Geospatial	
74		1	DR	5) How many, if any, sensitive topics will the project cover?		x	None	
75		1	DR				One	
76		1	DR				Two or more	
77		1 and 3	DR	6) If more than one sensitive topic, are the topics related to each other?			Yes	
78		1 and 3	DR				No	
79		1 and 3	DR			x	N/A	

	A	B	C	D	E	F	G	H
80		2		**Privacy Principle II: Openness**				
81		2	ID	1a) Does the project make use of administrative records?		x	Yes	
82		2	ID				No	
83		2	ID	1b) If yes, state the data sources and types		x	U.S. Postal Service file - Note that a determination has been made that these data are not subject to ADREC review and Handbook procedures. Therefore, the following questions are not applicable: 2, 3a, and 3b.	
84		2	ARM	2) If the project uses administrative records, has it received all required approvals, including those by the Administrative Records Coordinator?			Yes	
85		2	ARM				No	
86		2	ARM			x	N/A	
87		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	
88		2	AR				No	
89		2	AR			x	N/A	
90		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	
91		2	ARM				No	
92		2	AR	4a) Are there known external constraints on use of data?			Yes	
93		2	AR			x	No	
94		2	AR	4b) If yes, state constraints				
95		2	AR	5a) Are there known internal (policy) constraints on use of data?		x	Yes	
96		2	AR				No	
97		2	AR	5b) If yes, state policy constraints		x	Several constraints found in our Data Stewardship polices are: non-employee access to data, off-site access to data, reuse of data, browsing of data, data transmission.	
98		2	DRM	6) What are the planned mechanisms for tracking and/or ensuring notice or consent?		x	Advanced letter (informs officials on use of data)	
99		2	DRM				Signed consent form	
100		2	DRM				None or N/A	
101		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?		x	Yes	
102		2	DRM				No	
103		2	DRM				N/A	
104		2	AR	8) If a direct data collection, does it involve the use of proxies (i.e., someone other than the intended respondent)?			Yes	
105		2	AR			x	No	
106		2	AR				N/A	
107		2	ARM	9) Are mechanisms in place or planned to capture notice/consent by proxies or third parties?			Yes	
108		2	ARM				No	
109		2	ARM			x	N/A	

	A	B	C	D	E	F	G	H
110		2	ARM	10a) Will the project/system create a new "System of Records (SOR)"?			Yes	
111		2	ARM				No	
112		2	ARM			x	N/A	
113		2	ARM	10b) If no, under which existing SOR does the project fit?			Census-2 Employee Productivity Measurement Records	
114		2	ARM				Census-3 Individual & Household Statistical Surveys Records and Special Studies Records	
115		2	ARM				Census-4 Women- and Minority-Owned Business Enterprise Survey	
116		2	ARM				Census-5 Population and Housing Census Records of the 2000 Census Including Preliminary Statistics for the 2010 Decennial Census	
117		2	ARM				Census-6 Population Census Personal Service Records for 1900 and All Subsequent Decennial Censuses	
118		2	ARM				Census-7 Special Censuses of Population Conducted for State and Local Government	
119		2	ARM				Census-8 Statistical Administrative Records System (STARS)	
120		2	ARM				Census-9 Longitudinal Studies	
121		2	ARM				Census-10 American Community Survey	
122		3		**Privacy Principle III: Respectful Treatment of Respondents**				
123		3	DR	1) What universe is the project targeting?		x	No targeting	
124		3	DR				Targeting sensitive population	
125		3	DR				Population other than sensitive population	
126		3	DR	2) How much respondent time is needed?		x	0 - 30 minutes (note: the Boundary and Annexation Survey does not fall within the scope of this DS/PIA because it uses public records collected from governmental entities.)	
127		3	DR				31 - 60 minutes	
128		3	DR				61 - 90 minutes	
129		3	DR				91+ minutes	
130		3	DR	3) What is the frequency of contact with respondent over a 5-year period?			Once	
131		3	DR				2 to 5 times	
132		3	DR				6 or more times	
133		3	DR			x	N/A	

	A	B	C	D	E	F	G	H
134		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	
135		3	DRM				No	
136		3	DRM				N/A	
137		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	
138		3	DRM				No	
139		3	DRM			x	N/A	
140		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	
141		3	DRM				No	
142		3	DRM			x	N/A	
143		4		**Privacy Principle IV: Confidentiality**				
144		4	AR	1) Does the data collection include the use of any new technology for which privacy concerns could arise?			Yes	
145		4	AR			x	No	
146		4	ARM	1b) If so, what mitigation strategies are being adopted?				
147		4	AR	2a) Does the data collection raise any specific concerns about field representative safety or access?			Yes	
148		4	AR			x	No	
149		4	ARM	2b) If so, what mitigation strategies are being adopted?				
150		4	ARM	3a) Is there any actual or planned access of data by Special Sworn Status (SSS) at a secure non-Census Bureau facility?			Yes	
151		4	ARM			x	No	
152		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?			Yes	
153		4	ARM				No	
154		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	
155		4	AR			x	No	
156		4	AR	5) From what frame did you develop the project's sample?			Random	
157		4	AR				Census Bureau - census or survey file	
158		4	AR				MAF	
159		4	AR				Business Register	
160		4	AR				3rd party / administrative record data	
161		4	AR			x	N/A	
162		4	ARM	6a) Will the data collected/used as part of this project be afforded confidentiality protections by statute?		x	Yes	
163		4	ARM				No	
164		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 - All data are subject to IT Security Standards, including, defined restricted access, strong pass-word protection, and regular intrusion testing and detection.	
165		4	ARM				No	

	A	B	C	D	E	F	G	H
166		4	AR	7) After collection, will you turn over responsibilities to an outside agency/organization for the identifiable microdata?			Yes	
167		4	AR			x	No	
168		4	AR	8) What are the planned types of publicly available products?			Detailed tabular data files	
169		4	AR				Public use microdata file	
170		4	AR				Analytical reports	
171		4	AR			x	Geospatial products	
172		4	AR				None	
173		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	
174		4	AR			x	No	
175		4	ARM	9b) Will the products be subject to the Checklist On Disclosure Potential of Data?		x	Yes	
176		4	ARM				No	
177		4	ARM	10a) Are there data transfers (e.g., hand-offs between systems)?		x	Yes	
178		4	ARM				No	
179		4	ARM	10b) State mechanism for project tracking of data transfers (e.g., agreements, automated tracking).		x	Automated tracking and internal and external agreements	
180		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	
181		4	DRM				No	
182		4	AR	12) Will the project produce multiple extracts/versions of the sensitive data?			Yes	
183		4	AR			x	No	
184		4	ARM	13) Is there something in place already to enforce sensitive information document access and control?		x	Yes - Any memoranda that explain algorithms for creating test data are treated as sensitive documents, and protected under lock and key.	
185		4	ARM				No	
186		4	ARM				N/A	
187		4	AR	14a) Is the anticipated life expectancy of the identifiable microdata indefinite?		x	Yes	
188		4	ARM				No	
189		4	ARM	14b) If not, what is the anticipated life expectancy?				
190		4	AR	15) After the project is over, the identifiable microdata will:			Be destroyed	
191		4	AR				Continue to exist within the Census Bureau, archived	
192		4	AR			x	Continue to exist within the Census Bureau, not archived	
193		4	AR				Continue to exist at the National Archives and Records Administration	
194		4	AR				Become public by law	
195		4	AR				Other	
196							N/A	
197		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.			Yes-Records Schedule(s)=	
198		4	ARM			x	No	

199		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	
200		4	ARM				No	
201		4	ARM	18) Will the project train employees on the prohibition against unauthorized browsing as specified in the "Unauthorized Browsing" policy?		x	Yes	
202		4	ARM				No	
203		4	ARM	19) Have people associated with this project taken IT security training?		x	Yes	
204		4	ARM				No	
205		4	ARM	20) List any additional Data Stewardship assurance/enforcement mechanisms.				
206		4	ARM	21a) Are there any additional privacy risks that have not been addressed elsewhere in this assessment?			Yes	
207		4	ARM			x	No	
208		4	ARM	21b) If so, are these risks you cannot mitigate, that would be detrimental to the Census Bureau mission?			Yes	
209		4	ARM				No	
210		4	ARM	21c) Please specify				
211		7	DR					
212		7	DR	NET DATA SENSITIVITY SCORE =	**Low**			
213		7	DR					
214		7	AR	NET ACTIVITY SENSITIVITY SCORE =	**Low**			
215		7	AR					
216		7	SYS	PROJECT SCORE (Activity + Data)	**Low**			
217		7	SYS					
218		7	ARM					
219		7	ARM	SYSTEM SCORE	**Moderate**			

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.

[23]

	A	B	C	D	E	F	G	H
255								

U.S. Census Bureau IT System Security Evaluation for Privacy Impact Assessments
Geographic Support Systems - CEN07
Risk Level – Moderate

The Census Bureau IT Security Office, based on the information contained in the IT security documentation provided for Geographic Support Systems 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 their systems. 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 the GSS 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 for authorization to process sensitive data on the Census network. The main computing system resides behind the Census Bureau firewall. Below are components of the GSS located in the following areas:

Bowie Computer Center (BCC) - The MAF/TIGER database resides on Egenera blade servers running the Redhat Linux Operating System. The Computer Services Division provides system administration and backup services. The BCC houses a tape library system used for systems backup--it serves as the off-site alternate for the headquarters area. There are other UNIX (Sun Enterprise 6500 and 4500 models running the Solaris operating system) and Windows servers at the BCC used for production control, COTS software development and production, and Oracle database service.

Regional Offices - Users are able to update MAF/TIGER and print maps and address lists through network connection to the BCC.

National Processing Center (NPC) - The NPC geographic update and production systems show emphasis on continuing Census Bureau operations. There are Sun Enterprise 6500 and 4500 servers running the Solaris operating system used for production control and Oracle database service. One Dell server running the Linux operating system functions as a ten-terabyte file server. There are multiple Windows-based servers and numerous large- and small-format printers for map production.

Headquarters – The Geography Division at headquarters performs all software development work. Headquarters also has users that update and access the MAF/TIGER databases and are able to print maps/address lists. The emphasis is on special purpose and management operations. The Geography Division is located in Census Bureau's headquarters.

The Census Bureau has organized its IT systems by business area into 17 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	1
	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	1
	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	1
	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	0				
	6 or more	3	0				
							0

							0
					Post-mitigation Sensitivity		Low
	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	1		Covered by System of Record	1	0
	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	0		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
							0
							1
					Post-mitigation Sensitivity		Low
	Processing/Analysis (5)						
	Requires use of a secure non-Census Bureau facility	1	0		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	0
	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
							2
							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	0				
	Sample frame derived from Business Register	1	0				
	Sample frame derived from 3rd party/administrative record data	1	0				

					Post-mitigation Sensitivity		Low
	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	1
	Analytic reports will be produced	1	0				
	Geospatial products	1	1				
	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	1		DS017 Title 13/26 training	1	1
	Will not be destroyed after useful life	2	2		DS018 Unauthorized Browsing policy	1	1
	Continue to exist	1	0		Archiving plan is being developed/in effect	1	0
	Will continue to exist outside a formal archiving plan	1	1		Any additional Data Stewardship assurance mechanisms	1	0
					Post-mitigation Sensitivity		Medium
	Total unmitigated risk level		Low				

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