Description of document:	Census Bureau investigation report concerning the March 2007 unauthorized release of data
Requested date:	2007
Released date:	11-January-2008
Posted date:	15-October-2012
Source of document: US Census Bureau	FOIA Request FOIA and Information Branch FOIA officer 4600 Silver Hill Road Suitland, MD 20746

UNITED STATES DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. Census Bureau
Washington, DC 20233-0001
OFFICE OF THE DIRECTOR

January 11, 2008

This is a follow-up response to your letter requesting under the Freedom of Information Act (FOIA) "... the investigation report concerning the March 2007 unauthorized release of data."

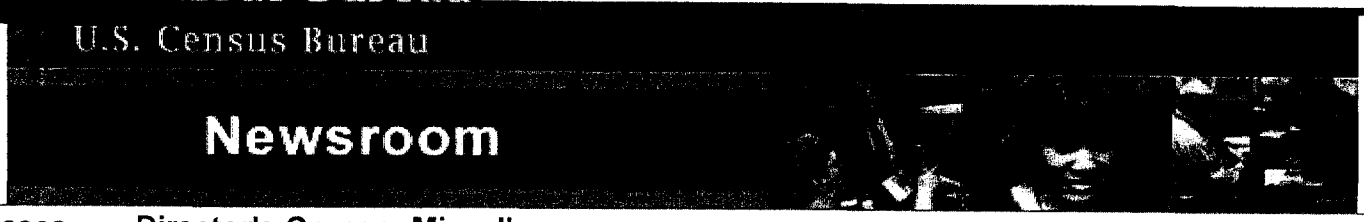
Enclosed are documents responsive to your request. This responds to your request in full. There is no charge for these records.

Sincerely,

Mary C. Potter

Mary C. Potter
FOIA Officer

Enclosures



U.S. Census Bureau News
U.S. Department of Commerce · Washington, D.C. 20233

FOR IMMEDIATE RELEASE
WEDNESDAY, MARCH 7, 2007

Ruth Cymber
Public Information Office
(301) 763-1225/763-3762 (fax)
(301) 457-1037 (TDD)
e-mail: <pio@census.gov>

CB07-38

Unauthorized Release Of Limited Household Data On Census Bureau Web Site

WASHINGTON — The Census Bureau today reported that a file containing limited respondent information on 302 households, commingled with fictitious test records, was improperly posted on one of the agency's externally accessible servers in violation of strict agency policies regarding the protection of respondent information. The file was immediately removed. No Social Security numbers were contained in the files and the Census Bureau has no evidence that any respondent data were misused.

"As soon as we learned of the improper posting, we moved quickly to fix the problem. We immediately shut down the site and began an investigation," said Census Director Charles Louis Kincannon. "We have an obligation to the public to be good stewards of personal data collected in our census and surveys. Protecting the confidentiality of personal information remains our highest priority. Thankfully we know of no instances of respondent data being improperly used; however, we regret that the information was improperly posted and that our safeguards did not prevent this violation of agency policies. A breach of this kind is unacceptable and we are committed to providing the highest level of public service. We are strengthening our internal procedures to further safeguard our data to prevent a recurrence."

On Feb. 15, 2007, the Census Bureau discovered that the file, containing records from 302 actual households commingled with 250 fictitious or test records, had been uploaded onto one of the agency's externally accessible servers. For the 302 households, the file contained names, addresses, phone numbers, birthdates, family income ranges, and other demographic data. There were no Social Security numbers contained in the file. The information was posted multiple times between October and February to test new software applications. This site is typically used to make large public use files available to census data users.

Once the improper posting was discovered, the file was immediately removed. The generally public nature of the information, and the commingling of data and test records indicated that it is unlikely the downloaded information would be useful to the casual user or someone with malicious intent. The Census Bureau is notifying the respondents and offering credit-monitoring assistance.

Census Law prohibits disclosure of sensitive data and the Census Bureau has strict policies protecting data including prohibiting the uploading of data to any nonsecured Web site. Information placed on the agency's Web site is required to undergo a disclosure avoidance review to ensure that no confidential information is released. This process was not followed.

Appropriate administrative action regarding those employees involved has been taken pending the investigation. Once the investigation is concluded, a determination will be made as to appropriate personnel action. The Census Bureau has also referred the matter to the Department of Commerce's Inspector General. Additional training on the proper handling of Title 13 survey responses and the Census Bureau's telework policies will be conducted.

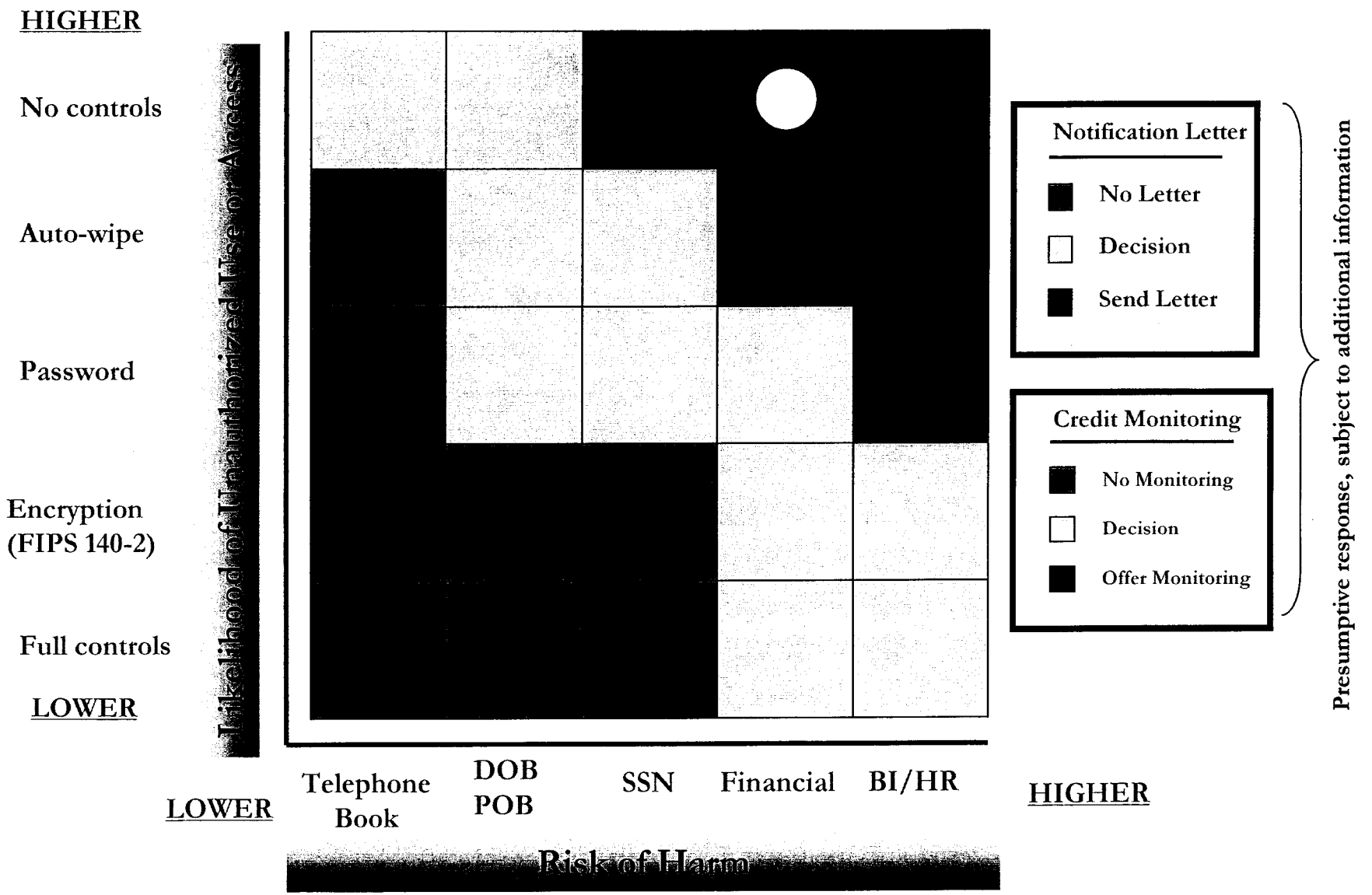
-X-

Census PII Loss

Incident # 146

ID Theft Task Force Meeting March 2, 2007

- **Incident Summary**
  - A computer file containing PII [Title 13] data affecting 302 households was made available on the Census ftp (file transfer protocol) publicly accessible website
- **Census Response to Incident**
  - Census CIO issued instruction to terminate capability to write to the anonymous FTP sites from internal Census machines. Directed Division Chiefs review of all IT operations to identify any potential vulnerability that exist due to improperly implemented policy or procedures
  - Census IT Security Officer investigated and updated policies and directory structure relating to system controls and permissions to prevent a reoccurrence



- SSN: Social Security Number
- BI: Background Investigation
- HR: Human Resources

ID Theft Task Force Decision

After hearing arguments within the ID Theft Task Force, including data loss variables and compensating controls, task force *voted not to send* notification letters or offer credit monitoring.

Report to the Department of Commerce Identify Theft Task Force, re: Title 13 Data Posted To Census FTP Site

Summary of Events

FP#146

Report Prepared March 2, 2007

Notification by Public

At 3:20 p.m., Wed., Feb. 14, 2007 the MSO staff received a question/comment from a person at doesnotmatter@aol.com stating the following:

"Was looking for county information and download files off your ftp site (ftp://ftp2.census.gov/pub/outgoing/) downloaded file (CPS_Basic_1.25_ASEC_1.69.exe). This file has personal information about actual households including names, children's names, address, ages, birthdates, phone #'s, employer, job title, it may contain SSN which I didn't see but saw referenced….this should not be made available to the general public"

Summary

- The Annual Social and Economic Supplement (ASEC) instrument has undergone testing since Oct. 12, 2007 and was posted to a Census public-facing FTP (File Transfer Protocol) site for ease of access by Census employees tasked to develop and test the instrument. The intent of posting to the FTP server was to allow continued access by these employees from home while teleworking to ensure the team continued on schedule with the application's conversion.
- The ASEC instrument, or interview tool, was changed due to program updates while the test input file containing live cases, and Title 13 data, remained constant. 522 cases were used as part of the testing, which included 302 cases determined to have live Title 13 data. It was later determined that no Social Security Numbers (SSN) were included in the files.
- The zipped file containing the instrument, files needed to run the instrument, and the test input file (CPS_Basic_1.25.ASEC_1.69.exe) was placed on the public FTP server a total of 23 separate times from Oct. 12, 2006 until the version on Feb. 12, 2007 that precipitated the incident. The file was not encrypted or password protected.
- The individuals who created the test input file knowingly used live case data due to the complexity of the conversion of the CPS/ASEC from authoring tools used by Census staff. The program developers did not have a test file that contained all the flags and special variables that needed to accurately test the application's functionality. The use of live data for testing has been going on since late 2001/early 2002 according to a supervisor in Demographic Surveys Division (DSD), but was only used to test instruments *within* the Census Bureau and never placed on the FTP site.
- The individuals never informed the authoring staff in the Technologies Management Office (TMO) that the program's test input file contained live data when they requested it be placed on the FTP server. TMO authoring staff also did not ask if the file contained sensitive information, as required by TMO policy.
- The file was downloaded 279 via FTP between Oct. 12, 2006 and Feb. 15, 2007. In addition the page was viewed using HTTP (Hyper Text Transfer Protocol) a total 629 times during the same period.

Census Findings

- While not malicious, the activity of the 2 DSD employees was deliberate and violated two essential Census policies:
- Telework policy - which states "you are not allowed to use sensitive Title 13 data while teleworking." Both employees were authorized to telework and acknowledged understanding Census policy during training,
- Remote Access policy (4.2.17) and Appendix B of the Census Bureau IT Security Program Policy.
- TMO personnel did not follow TMO procedures ("Rules of Behavior for US Census Bureau Information Technology Systems for TMO Authoring Staff"),
- TMO staff did not request written notification from the DSD personnel that data being posted to the FTP site did not contain Title 13/sensitive data.

Census Response/Actions

- The file was first protected by System Support Division (so as not to allow anyone to access it) at 8:40 a.m. on Feb. 15th and was removed from the server at 9:00 a.m. the same day. In order to ensure no other files would be uploaded to the server, the ability of users to upload files to the server was disabled at noon on February 15th. It was verified that no other files containing sensitive information were found on the server.
- **Census CIRT Incident # 146 was opened** because "a CPS File Containing PII [Title 13] Data (CPS_Basic_1.25.ASEC_1.69.exe) was made available on the Census ftp (file transfer protocol) publicly accessible website.
- The two individuals from DSD who are currently on administrative leave pending the outcome of the Census investigation.
- Due to the system logs showing activity from China, BOC CIRT is performing a check of all firewall and IDS (Intrusion Detection System) logs for the time period to see if any other unusual activity was initiated from these IP ranges.
- Census staff is gathering the policies and procedures from the six Divisions responsible for both secure and public directories data posted to the FTP server to ensure the sites provide sufficient controls (password protected and encrypted files) and that policies are implemented properly.

Census Response/Actions (con't)

- The Census CIO:
  - Has directed that the capability to write to the anonymous FTP sites from internal Census machines be terminated. The Census ITSO (IT Security Officer) is reviewing the complete directory structure of the server in question to ensure required security controls, and
  - Has also directed his division chiefs to begin a review of all IT operations to identify any potential vulnerability that may exist due to improperly implemented policy or procedures.
- The Census ITSO is continuing to review the DSD and TMO policies as well relating to this activity as well as System Support Division (SSD) policies on the FTP server, and
- The incident has been reported to US CERT (DHS) and DOC CIRT (OCIO) per OMB M-06-19. The case remains open as ITSO continues its work.

Log Analysis and Statistics

- The Census IT Security Officer, and his team, acquired a demonstration version of a log file analysis and reporting tool, Sawmill, to quickly perform analysis of the high volume of logs generated and retained for the Census FTP site. A summary of log analysis and statistics are provided below, with a full report attached in two formats (FTP log review, and HTTP log review) for review and consideration.
- 195 total connections were created to the Census site from Oct. 12, 2006 – Feb. 15, 2007 and include:
  - 16 FTP-only connections,
  - 115 were HTTP-only connections,
  - 64 of the total 195 connections created both FTP & HTTP sessions.
- 80 connections were made to the Census FTP site, with 279 downloads made of the Census file, of which:
  - 273 downloads occurred from 177 United States issued IP addresses, and
  - 6 downloads occurred from 3 China issued IP addresses
-
- Other IP addresses used to view the Census file originated from:
  - Germany (2)
  - Italy (2)
  - Australia (2)
  - France (1)
  - Japan (1)
  - Mexico (1)
  - Philippines (1)
  - Ukraine (1)
  - Uruguay (1)
- Based on log reviews, the high period of connections to the Census file occurred between 2:00 a.m. and 3:00 a.m. for the period of Oct. 12, 2006 through February 15, 2007.

CPS

- Current Population Survey (CPS) is a monthly survey of about 50,000 households conducted by the Bureau of the Census for the Bureau of Labor Statistics. The survey has been conducted for more than 50 years and is the primary source of information on the labor force characteristics of the U.S. population. The sample is scientifically selected to represent the civilian non-institutional population. Respondents are interviewed to obtain information about the employment status of each member of the household 15 years of age and older. However, published data focus on those ages 16 and over. The sample provides estimates for the nation as a whole and serves as part of model-based estimates for individual states and other geographic areas.

ASEC

- Annual Social and Economic Supplement (ASEC) of the Current Population Survey (CPS) is the official source of income and poverty estimates for the nation. It provides annual estimates based on a survey of more than 75,000 households. The survey contains detailed questions covering social and economic characteristics of each person who is a household member as of the interview date. Income questions refer to income received during the previous calendar year. These questions measure the level of family income and household composition from which we determine poverty status. For example, the survey conducted in March 2002 was combined with information on household characteristics as of that date with reports of income in the preceding year to produce estimates of 2001 income and poverty.