

**Federal Communications Commission**  
*Office of the Managing Director*



**Privacy Impact Assessment<sup>1</sup> (PIA) for the  
Customer Comment Database (CCD)  
September 15, 2008**

**FCC Bureau/Office:** Public Safety Homeland Security Bureau -- Public Outreach

**Privacy Analyst:** Leslie F. Smith  
**Telephone Number:** (202) 418-0217  
**E-mail Address:** [Leslie.Smith@fcc.gov](mailto:Leslie.Smith@fcc.gov)

---

<sup>1</sup> This questionnaire is used to analyze the impacts on the privacy and security of the personally identifiable information (PII) that is being maintained in these records and files.

The *Privacy Act of 1974*, as amended, 5 U.S.C. 552a, requires Federal agencies to take special measures to protect personal information about individuals when the agencies collect, maintain, and use such personal information.

Having established through the **Privacy Threshold Assessment** that this information system contains information about individuals, *e.g.*, personally identifiable information (PII), it is important that when the FCC makes changes to such an information system, the FCC then analyzes:

- (a) What changes are being made to the information that the system presently collects and maintains; and/or
- (b) What new information will be collected and maintained to determine the continuing impact(s) on the privacy of the individuals.

The Privacy Impact Assessment template's purpose is to help the bureau/office to evaluate the changes in the information in the system and to make the appropriate determination(s) about how to treat this information, as required by the Privacy Act's regulations.

**Section 1.0 Information System's Contents:**

1.1 Status of the Information System:

- New information system—Implementation date: September 2008
- Revised or upgraded information system—Revision or upgrade date:

If this system is being revised—what will be done with the newly derived information:

- Placed in existing information system—Implementation Date:
- Placed in new auxiliary/ancillary information system—Date:
- Other use(s)—Implementation Date:

Please explain your response:

1.2 Has a Privacy Threshold Assessment been done?

- Yes  
Date: September 2008
- No

If a Privacy Threshold Assessment has not been done, please explain why not:

If the Privacy Threshold Assessment (PTA) has been completed, please skip to Question 1.15

1.3 Has this information system, which contains information about individuals, *e.g.*, personally identifiable information (PII), existed under another name, *e.g.*, has the name been changed or modified?

- Yes
- No

If yes, please explain your response:

1.4 Has this information system undergone a “substantive change” in the system’s format or operating system?

- Yes
- No

If yes, please explain your response:

If there have been no such changes, please skip to Question 1.7.

1.5 Has the medium in which the information system stores the records or data in the system changed from paper files to electronic medium (computer database); or from one electronic information system to another, *i.e.*, from one database, operating system, or software program, *etc.*?

- Yes
- No

If yes, please explain your response:

1.6 Has this information system operated as part of another information system or was it linked to another information system:

- Yes
- No

If yes, please explain your response:

If the information system is not part of, nor linked to another information system, please skip to Question 1.8

1.7 If so, was it operated by another bureau/office or transferred from another Federal agency to the FCC?

- Yes
- No

Please explain your response:

1.8 What information is the system collecting, analyzing, managing, storing, transferring, *etc.*:

**Information about FCC Employees:**

- No FCC employee information
- FCC employee’s name
- Other names used, *i.e.*, maiden name, *etc.*
- FCC badge number (employee ID)
- SSN
- Race/Ethnicity
- Gender
- U.S. Citizenship
- Non-U.S. Citizenship

- Biometric data
  - Finger prints
  - Voice prints
  - Retina scans/prints
  - Photographs
  - Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc.*
- Birth date/age
- Place of birth
- Medical data
- Marital status
- Spousal information
- Miscellaneous family information
- Home address
- Home address history
- Home telephone number(s)
- Personal cell phone number(s)
- Personal fax number(s)
- Personal e-mail address(es)
- Emergency contact data:
- Credit card number(s)
- Driver's license
- Bank account(s)
- FCC personal employment records
- Military records
- Financial history
- Foreign countries visited
- Law enforcement data
- Background investigation history
- National security data
- Communications protected by legal privileges
- Digital signature
- Other information:

**Information about FCC Contractors:**

- No FCC contractor information
- Contractor's name
- Other name(s) used, *i.e.*, maiden name, *etc.*
- FCC Contractor badge number (Contractor ID)
- SSN
- U.S. Citizenship
- Non-U.S. Citizenship
- Race/Ethnicity
- Gender
- Biometric data
  - Finger prints
  - Voice prints
  - Retina scans/prints
  - Photographs
  - Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc.*
- Birth date/Age

- Place of birth
- Medical data
- Marital status
- Spousal information
- Miscellaneous family information
- Home address
- Home address history
- Home telephone number(s)
- Personal cell phone number(s)
- Personal fax number(s)
- Personal e-mail address(es)
- Emergency contact data:
- Credit card number(s)
- Driver's license number(s)
- Bank account(s)
- Non-FCC personal employment records
- Military records
- Financial history
- Foreign countries visited
- Law enforcement data
- Background investigation history
- National security data
- Communications protected by legal privileges
- Digital signature
- Other information:

**Information about FCC Volunteers, Visitors, Customers, and other Individuals:**

- Not applicable
- Individual's name:
- Other name(s) used, *i.e.*, maiden name, *etc.*
- FCC badge number (employee ID)
- SSN
- Race/Ethnicity
- Gender
- Citizenship
- Non-U.S. Citizenship
- Biometric data
  - Fingerprints
  - Voiceprints
  - Retina scans/prints
  - Photographs
  - Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc.*
- Birth date/Age
- Place of birth
- Medical data
- Marital status
- Spousal information
- Miscellaneous family information
- Home address
- Home address history

- Home telephone number(s)
- Personal cell phone number(s)
- Personal fax number(s)
- Personal e-mail address(es)
- Emergency contact data:
- Credit card number(s)
- Driver's license number(s)
- Bank account(s)
- Personal e-mail address(es)
- Non-FCC personal employment records
- Military records
- Financial history
- Foreign countries visited
- Law enforcement data
- Background investigation history
- National security data
- Communications protected by legal privileges
- Digital signature
- Other information:

**Information about Business Customers and others (usually not considered “personal information”):**

- Not applicable
- Name of business contact/firm representative, customer, and/or others
- Race/Ethnicity
- Gender
- Full or partial SSN
- Business/corporate purpose(s)
- Other business/employment/job description(s)
- Professional affiliations
- Business/office address
- Intra-business office address (office or workstation)
- Business telephone number(s)
- Business cell phone number(s)
- Business fax number(s)
- Business pager number(s)
- Business e-mail address(es)
- Bill payee name
- Bank routing number(s)
- Income/Assets
- Web navigation habits
- Commercially obtained credit history data
- Commercially obtained buying habits
- Credit card number(s)
- Bank account(s)
- Other information:

1.9 What are the sources for the information that you are collecting:

- Personal information from FCC employees:
- Personal information from FCC contractors:

- Personal information from non-FCC individuals and/or households:
- Non-personal information from businesses and other for-profit entities:
- Non-personal information from institutions and other non-profit entities:
- Non-personal information from farms:
- Non-personal information from Federal Government agencies:
- Non-personal information from state, local, or tribal governments:
- Other sources:

1.10 Will the information system obtain, use, store, analyze, *etc.* information about individuals *e.g.*, personally identifiable information (PII), from other information systems, including both FCC and non-FCC information systems?

- Yes
- No

Please explain your response:

If the information system does not use any PII from other information systems, including both FCC and non-FCC information systems, please skip to Question 1.15

1.11 If the information system uses information about individuals from other information systems, what information will be used?

- FCC information system and information system name(s):
- non-FCC information system and information system name(s):
- FCC employee's name
- (non-FCC employee) individual's name
- Other names used, *i.e.*, maiden name, *etc.*
- FCC badge number (employee ID)
- Other Federal Government employee ID information, *i.e.*, badge number, *etc.*
- SSN
- Race/Ethnicity
- Gender
- U.S. Citizenship
- Non-U.S. Citizenship
- Biometric data
  - Finger prints
  - Voice prints
  - Retina scan/prints
  - Photographs
  - Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc.*
- Birth date/Age
- Place of birth
- Medical data
- Marital status
- Spousal information
- Miscellaneous family information:
  - Home address
  - Home address history
  - Home telephone number(s)
  - Personal cell phone number(s)

- Personal fax number(s)
- Personal e-mail address(es)
- Emergency contact data
- Credit card number(s)
- Driver's license
- Bank account(s)
- Personal e-mail address(es)
- Non-FCC personal employment records
- Non-FCC government badge number (employee ID)
- Law enforcement data
- Military records
- National security data
- Communications protected by legal privileges
- Financial history
- Foreign countries visited
- Background investigation history
- Digital signature
- Other information:

**Information about Business Customers and others (usually not considered “personal information”):**

- Not applicable
- Name of business contact/firm representative, customer, and/or others
- Race/Ethnicity
- Gender
- Full or partial SSN
- Business/corporate purpose(s)
- Other business/employment/job description(s)
- Professional affiliations
- Intra-business office address (office or workstation)
- Business telephone number(s)
- Business cell phone number(s)
- Business fax number(s)
- Business e-mail address(es)
- Bill payee name
- Bank routing number(s)
- Income/Assets
- Web navigation habits
- Commercially obtained credit history data
- Commercially obtained buying habits
- Personal clubs and affiliations
- Credit card number(s)
- Bank account(s)
- Other information:



1.12 Will this information system derive new information, records, or data, or create previously unavailable information, records, or data, through aggregation or consolidation from the information that will now be collected via this link to the other system, including information, records, or data, that is being shared or transferred from the other information system(s)?

- Yes
- No

Please explain your response:

1.13 Can the information, whether it is: (a) in the information system, (b) in a linked information system, and/or (c) transferred from another system, be retrieved by a name or a “unique identifier” linked to an individual, *e.g.*, SSN, name, home telephone number, fingerprint, voice print, *etc.*?

- Yes
- No

Please explain your response:

1.14 Will the new information include personal information about individuals, *e.g.*, personally identifiable information (PII), be included in the individual’s records, or be used to make a determination about an individual?

- Yes
- No

Please explain your response:

1.15 Under the *Privacy Act of 1974*, as amended, 5 U.S.C. 552a, Federal agencies are required to have a System of Records Notice (SORN) for an information system like this one, which contains information about individuals, *e.g.*, “personally identifiable information” (PII).

A System of Records Notice (SORN) is a description of how the information system will collect, maintain, store, and use the personally identifiable information (PII).

Is there a SORN that already covers this PII in this information system?

- Yes
- No

If yes, what is this System of Records Notice (SORN):

Please provide the citation that was published in the *Federal Register* for the SORN:

If a SORN already covers this PII, please skip to **Section 2.0 System of Records Notice (SORN) Update** to address any changes to this SORN.

If a system of records notice (SORN) does not presently cover the information about individuals in this system, then it is necessary to determine whether a new FCC system of records notice must be created for the information.

- 1.16 If this information system is not covered by a system of records notice (SORN), does the information system exist by itself, or does it now, or did it previously exist as a component or subset of another SORN?

Yes  
 No

If yes, please explain what has occurred:

The personally identifiable information that will be collected, maintained, and used by PSHSB is derived from the information that individuals provide when they voluntarily submit their comments via the two website Comment Cards and/or the comment paper sheet will be covered by a new system of records notice, FCC/PSHSB-1, "Comment Card Database."

What is the System of Records Notice (SORN) of which it is currently or previously a component or subset:

This is a new SORN.

Please also provide the citation that was published in the *Federal Register* for the SORN:

- 1.17 What are the purposes or functions that make it necessary to create a new a system of records notice (SORN) for this information system, *e.g.*, why is the information being collected?

A new SORN needs to be created to cover the personally identifiable information that individuals may submit voluntarily via the PSHSB Comment Card Database information system. PSHSB may use either and/or both the electronic and paper (hardcopy) comment cards in other PSHSB public events, such as summits, conferences, forums, expos, lectures, *etc.*

- 1.18 Where is this information for the system of records notice (SORN) located?

This information system will be located in the FCC's Public Safety and Homeland Security Bureau (PSHSB).

- 1.19 Is the use of the information both relevant and necessary to the purposes for which the information system is designed, *e.g.*, is the SORN only collecting and using information for the specific purposes for which the SORN was designed so that there is no "extraneous" information included in the database(s) or paper files?

Yes  
 No

Please explain your response:

The new SORN will cover personally identifiable information that individuals provide voluntarily when they submit their comments via the PSHSB Comment Card websites:

(a) The Summit Comment Card: <http://www.fcc.gov/pshs/pshsdev/summits/comment-card.html>;  
and

(b) The PSHSB Comment Card: <http://www.fcc.gov/pshs/pshsdev/comment-card.html>.

PSHSB will also have a paper copy of each comment card available for summit conference and public forum participants to write their comments. PSHSB may use either and/or both the electronic and paper (hardcopy) comment cards in other PSHSB public forums, such as summits, conferences, expos, lectures, *etc.*

If the use of this information is both relevant and necessary to the processes for this information system is designed, please skip to Question 1.21.

1.20 If not, why or for what reasons is the information being collected?

1.21 Is the information covered under a Security Classification as determined by the FCC Security Officer?

- Yes
- No

Please explain your response:

There is no government classified information included in the information that is collected by the two PSHSB Customer Comment Cards.

1.22 What is the legal authority that authorizes the development of the information system and the information/data collection?

Sections 151, 152, 155, 257, 303 of the Communications Act of 1934, as amended, 47 U.S.C. 151.152, 155, 257; and 5 U.S.C. 602(c) and 609(a)(3).

1.23 In what instances would the information system's administrator/manager/developer permit disclosure to those groups outside the FCC for whom the information was not initially intended.

Such disclosures, which are referred to as "Routine Uses," are those instances that permit the FCC to disclose information from a SORN to specific "third parties." These disclosures may be for the following reasons:

(check all that are applicable)

- Adjudication and litigation:
- Committee communications:
- Compliance with welfare reform requirements:
- Congressional inquiries:
- Emergency response by medical personnel and law enforcement officials:
- Employment, security clearances, licensing, contracts, grants, and other benefits by the FCC:
  
- Employment, security clearances, licensing, contracts, grants, and other benefits upon a request from another Federal, state, local, tribal, or other public authority, *etc.*:
- FCC enforcement actions:
- Financial obligations under the Debt Collection Information Act:
- Financial obligations required by the National Finance Center:
- First responders, *e.g.*, law enforcement, DHS, FEMA, DOD, NTIA, *etc.*:
- Government-wide oversight by NARA, DOJ, and/or OMB:
- Labor relations (NTEU):
- Law enforcement and investigations:
- Program partners, *e.g.*, WMATA, *etc.*: PSHSB may provide statistics and/or summaries of the comments it receives to first responders such as the Red Cross, Homeland Security, *etc.*, law enforcement organizations, and medical organizations, as summit conference participants who may be interested in such comments. Such third party disclosures will be made as PSHSB deems appropriate, but such disclosures will provide a summary or analysis of

comments, so that it can not identify an individual's comments and other relevant information.

- Breach of Federal data:
- Other Routine Use disclosures not listed above:

1.24 Will the information be disclosed to consumer reporting agencies?

- Yes
- No

Please explain your response:

1.25 What are the policies for the maintenance and secure storage of the information?

This information will be stored in a locked file cabinet, and the computer files that contain a compilation of the information that is submitted via the two Comment Card websites will be stored in the PSHSB Comment Card Database information system, access to which is available only to PSHSB employees.

1.26 How is information in this system retrieved?

PSHSB staff can retrieve the personally identifiable information (PII) in the Comment Card Database information system by such personal identifiers as the individual submitter's name, personal e-mail address, and/or personal cell phone and telephone numbers. Except for an individual's name, PSHSB is not requesting other PII. Personal cell phone numbers, home telephone numbers, and personal e-mail addresses may be provided by submitters who operate businesses from their homes, i.e., consultants, contractors, etc., and/or others who note that the information they provide is "personal."

1.27 What policies and/or guidelines are in place on how long the bureau/office will retain the information?

The Records Management Officer in the Performance Evaluation and Records Management Division of the Office of the Managing Director (OMD-PERM) has determined that the National Archives and Records Administration (NARA) has not developed a records retention and disposal schedule for PSHSB's new CCD information system that is covered by FCC/PSHSB-2, "Customer Comment Database (CCD)" SORN. OMD-PERM will assign the appropriate records retention schedule for this SORN that covers the personally identifiable information (PII) when NARA has made such determination. No records or other information will be destroyed until a records retention schedule has been approved by NARA.

1.28 Once the information is obsolete or out-of-date, what policies and procedures have the system's managers/owners established for the destruction/purging of the data?

The Records Management Officer in the Performance Evaluation and Records Management Division of the Office of the Managing Director (OMD-PERM) has determined that the National Archives and Records Administration (NARA) has not developed a records retention and disposal schedule for PSHSB's new CCD information system that is covered by FCC/PSHSB-2, "Customer Comment Database (CCD)" SORN. OMD-PERM will assign the appropriate records retention schedule for this SORN that covers the PII when NARA has made such determination for the appropriate destruction/purging of the information collected for the CCD according to the NARA guidelines. No records or other information will be destroyed until a disposal schedule has been approved by NARA.

1.29 Have the records retention and disposition schedule(s) been issued or approved by the National Archives and Records Administration (NARA)?

- Yes
- No

Please explain your response:

The Records Management Officer of OMD-PERM has reviewed the Customer Comment Database information system and has determined that NARA has not developed a records retention and disposal schedule for PSHSB's new CCD information system that is covered by FCC/PSHSB-2, "Customer Comment Database (CCD)" SORN. OMD-PERM will assign the appropriate records retention schedule for this SORN that covers the PII when NARA has made such determination for the appropriate destruction/purging of the information collected for the CCD according to the NARA guidelines. No records will be destroyed until a disposal schedule is approved by NARA. .

If a NARA records retention and disposition schedule has been approved for this System of Records Notice (SORN), please skip to **Section 2.0 System of Records Notice (SORN) Update:**

1.30 If there is no NARA approved records retention and disposal schedule, has there been any coordination with the Performance Evaluation and Records Management Branch (PERM) or the Records Officer?

- Yes
- No

Please explain your response:

The PSHSB staff have contacted the Records Officer in OMB-PERM. As noted above, the Records Officer will work with the PSHSB staff to determine the appropriate records schedule consistent with NARA guidelines.

If this is a new System of Records Notice (SORN), please skip to **Section 3.0 Development, Management, and Deployment and/or Sharing of the Information:**

### **Section 2.0 System of Records Notice (SORN) Update:**

If a System of Records Notice (SORN) currently covers the information, please provide information to update and/or revise the SORN:

2.1 Have there been any changes to the Security Classification for the information covered by the system of records notice (SORN) from what was originally determined by the FCC Security Officer?

- Yes
- No

Please explain your response:

2.2 Have there been any changes to the location of the information covered by the system of records notice (SORN)?

- Yes
- No

Please explain your response:

2.3 Have there been any changes to the categories of individuals covered by the system of records notice (SORN)?

- Yes
- No

Please explain your response:

2.4 Have there been any changes to the categories of records, *e.g.*, types of information (or records) that the system of records notice (SORN) collects, maintains, and uses?

- Yes
- No

Please explain your response:

2.5 Have there been any changes to the legal authority under which the FCC collects and maintains the information covered by the system of records notice (SORN)?

- Yes
- No

Please explain your response:

2.6 Have there been any changes to the purposes for collecting, maintaining, and using the information covered by the system of records notice (SORN)?

- Yes
- No

Please explain your response:

2.7 Have there been any changes to the Routine Uses under which disclosures are permitted to “third parties” as noted in the system of records notice (SORN)?

- Yes
- No

If the Routine Uses have changed, what changes were made:  
(check all that apply and explain the changes)

- Not applicable—there have been no changes to the Routine Uses
- Adjudication and litigation:
- Committee communications:
- Compliance with welfare reform requirements:

- Congressional inquiries:
- Emergency response by medical personnel and law enforcement officials:
- Employment, security clearances, licensing, contracts, grants, and other benefits by the FCC:
- Employment, security clearances, licensing, contracts, grants, and other benefits upon a request from another Federal, state, local, tribal, or other public authority, *etc.*:
- FCC enforcement actions:
- Financial obligations under the Debt Collection Act:
- Financial obligations required by the National Finance Center:
- First responders, *e.g.*, law enforcement, DHS, FEMA, DOD, NTIA, *etc.*:
- Government-wide oversight by NARA, DOJ, and/or OMB:
- Labor relations:
- Law enforcement and investigations:
- Program partners, *e.g.*, WMATA:
- Breach of Federal data:
- Others Routine Use disclosures not listed above:

2.8 Have there been any changes as to whether the FCC will permit the information covered by the system of records notice (SORN) can be disclosed to consumer reporting agencies?

- Yes
- No

Please explain your response:

2.9 Have there been any changes to the policies and/or guidelines for the storage and maintenance of the information covered by this system of records notice (SORN)?

- Yes
- No

Please explain your response:

2.10 Have there been any changes to how the information covered by the system of records notice (SORN) is retrieved or otherwise accessed?

- Yes
- No

Please explain your response:

2.11 Have there been any changes to the safeguards that the system manager has in place to protect unauthorized access to the information covered by the system of records notice (SORN)?

- Yes
- No

Please explain your response:

Please note that you must also provide an update of the current protections, safeguard, and other security measures that are in place in this SORN in **Section 5.0 Safety and Security Requirements:**

2.12 Have there been any changes to the records retention and disposition schedule for the information covered by the system of records notice (SORN)? If so, has the system manager worked with the Performance Evaluation and Records Management (PERM) staff to insure that this revised schedule been approved by the National Archives and Records Administration (NARA)?

- Yes
- No

Please explain your response:

### **Section 3.0 Development, Management, and Deployment and/or Sharing of the Information:**

3.1 Who will develop the information system(s) covered by this system of records notice (SORN)?

- Developed wholly by FCC staff employees:
- Developed wholly by FCC contractors:
- Developed jointly by FCC employees and contractors:
- Developed offsite primarily by non-FCC staff:
- COTS (commercial-off-the-shelf-software) package:
- Other development, management, and deployment/sharing information arrangements:

3.2 Where will the information system be hosted?

- FCC Headquarters
- Gettysburg
- San Diego
- Colorado
- New York
- Columbia Lab
- Chicago
- Other information:

3.3 Who will be the primary manager(s) of the information system who will be responsible for assuring access to, proper use of, and protecting the security and integrity of the information? (Check all that apply and provide a brief explanation)

- FCC staff in this bureau/office exclusively: The PSHSB staff will have responsibility for access and proper use of the information in the CCD information system.
- FCC staff in other bureaus/offices:
- Information system administrator/Information system developers:
- Contractors:
- Other information system developers, *etc*:

3.4 What are the FCC's policies and procedures that the information system administrators and managers use to determine who gets access to the information in the system's files and/or database(s)?

The PSHSB staff has determined that as a general policy only staff who have a "need to know" as part of their job duties and responsibilities may have access.



- 3.5 How much access will users have to data in the information system(s)?
- Access to all data: PSHSB's outreach staff who administer the summit conferences and the outreach programs and designated others.
  - Restricted access to data, as determined by the information system manager, administrator, and/or developer: FCC employees and contractors in PSHSB or (OMD-FO) may be granted access on a "need-to-know" basis as part of their job duties and responsibilities.
  - Other access policy:

3.6 Based on the Commission policies and procedures, which user group(s) may have access to the information at the FCC:

(Check all that apply and provide a brief explanation)

- Information system managers: FCC employees in the FCC's Information Technology Divisions of the Office of the Managing Director (OMD-IT) and IT staff in PSHSB.
- Information system administrators: Staff in the PSHSB, including both FCC employees and contractors, who manage the CCD information system functions.
- Information system developers:
- FCC staff in this bureau/office: FCC employees in the PSHSB granted access based on a "need to know" basis as part of their job duties and responsibilities.
- FCC staff in other bureaus/offices:
- FCC staff in other bureaus/offices in FCC field offices:
- Contractors: Contractors working at the FCC are granted access based on a "need to know" basis.
- Other Federal agencies:
- State and/or local agencies:
- Businesses, institutions, and other groups:
- International agencies:
- Individuals/general public:
- Other groups:

3.7 If contractors are part of the staff in the FCC who collect, maintain, and access the information, does the IT supervisory staff ensure that contractors adhere fully to the Privacy Act provisions, as required under subsection (m) of the Privacy Act, as amended, 5 U.S.C. 552a(m)?

- Yes
- No

Please explain your response:

The FCC's Information Technology (IT) supervisory staff provide periodic privacy training to the IT contractors.

3.8 Has the Office of the General Counsel (OGC) signed off on any Section M contract(s) for any contractors who work with the information system covered by this system of records notice (SORN)?

- Yes
- No

Please explain your response:

The Office of the General Counsel has approved the Section M contracts for all IT contractors who provide support for the CCD information system.

3.9 Does the information system covered by this system of records noticed (SORN) transmit/share personal information, *e.g.*, personally identifiable information (PII), between the FCC information technology (IT) network(s) and a public or other non-FCC IT network(s), which are not covered by this Privacy Impact Assessment?

- Yes
- No

Please explain your response:

The Comment Card Database (CCD) information system is a "stand alone" information system. It has no links to any other information systems.

If there is no information sharing or transmission, please skip to **Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:**

3.10 If the information system covered by this system of records noticed (SORN) transmits/shares personal information between the FCC network and a public or other non-FCC network, which is not covered by this Privacy Impact Assessment, what information is shared/transmitted/disclosed and for what purposes?

3.11 If there is such transmission/sharing of personal information, how is the information secured for transmission—what security measures are used to prevent unauthorized access during transmission, *i.e.*, encryption, *etc.*?

3.12 If there is sharing or transmission to other information systems, with what other non-FCC organizations, groups, and individuals will the information be shared?  
(Check all that apply and provide a brief explanation)

- Other Federal agencies:
- State, local, or other government agencies:
- Businesses:
- Institutions:
- Individuals:
- Other groups:

If there is no “matching agreement,” *e.g.*, *Memorandum of Understand (MOU), etc.*, please skip to **Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:**

3.13 What kind of “matching agreement,” *e.g.*, *Memorandum of Understanding (MOU), etc.*, as defined by 5 U.S.C. 552a(u) of the Privacy Act, as amended, is there to cover the information sharing and/or transferal with the external organizations?

3.14 Is this a new or a renewed matching agreement?

- New matching agreement
- Renewed matching agreement

Please explain your response:

3.15 Has the matching agreement been reviewed and approved (or renewed) by the FCC’s Data Integrity Board, which has administrative oversight for all FCC matching agreements?

Yes

If yes, on what date was the agreement approved:

No

Please explain your response:

3.17 How is the information that is covered by this system of records notice (SORN) transmitted or disclosed with the external organization(s) under the *MOU* or other “matching agreement?”

3.18 How is the shared information secured by the recipient under the *MOU*, or other “matching agreement?”

#### **Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:**

OMB regulations require Federal agencies to insure that the information/data that they collect and use meets the highest possible level of quality and integrity. It is important, therefore, that the information the Commission’s information systems use meets the “benchmark standards” established for the information.

4.1 How will the information that is collected from FCC sources, including FCC employees and contractors, be checked for accuracy and adherence to the Data Quality guidelines?  
(Please check all that apply)

Information is processed and maintained only for the purposes for which it is collected.

Information is reliable for its intended use(s).

Information is accurate.

Information is complete.

Information is current.

Not applicable: The information that submitters provide is from non-FCC sources, *i.e.*, participants in the PSHSB summits, forums, and conferences, *etc.*, and the public-at-large, who submit comments voluntarily.

Please explain any exceptions or clarifications:

If the Data Quality Guidelines do not apply to the information in this information system, please skip to **Section 5.0 Safety and Security Requirements:**

4.2 Is any information collected from non-FCC sources; if so, how will the information sources be checked for accuracy and adherence to the Data Quality guidelines?  
(Please check all that apply and provide an explanation)

- Yes, information is collected from non-FCC sources: The information that submitters provide is entirely from non-FCC sources, *i.e.*, participants in the PSHSB's public forums, summit conferences, *etc.*, and the public-at-large, who submit comments voluntarily. In addition, the PSHSB staff does not evaluate the data quality of the comments that summit and conference attendees and the public-at-large provide voluntarily.
- Information is processed and maintained only for the purposes for which it is collected: The PSHSB staff only collects this information as part of the bureau's efforts to get "feed back" from summit and conference participants and the public-at-large in order to improve the PSHSB's outreach activities.
- Information is reliable for its intended use(s): The PSHSB staff believes that the information that summit and conference participants and the public-at-large submit is a reliable indicator of how these two groups view the PSHSB's outreach efforts.
- Information is accurate: It is to the advantage of comment submitters to provide accurate information.
- Information is complete: It is to the advantage of comment submitters to provide complete information.
- Information is current: It is to the advantage of comment submitters to provide current information.
- No information comes from non-FCC sources:

Please explain any exceptions or clarifications:

While the PSHSB staff will not analyze or evaluate the data quality of the comments the bureau receives from summit conference and public forum attendees and the public-at-large, the staff does assume that the commenters are providing information that the commenters believe will be useful in improving the quality of future summit conferences and public forums, *etc.*, and the PSHSB's outreach efforts.

If the information that is covered by this system of records notice (SORN) is not being aggregated or consolidated, please skip to Question 4.5.

- 4.3 If the information that is covered by this system of records notice (SORN) is being aggregated or consolidated, what controls are in place to insure that the information is relevant, accurate, and complete?
- 4.4. What policies and procedures do the information system's administrators and managers use to insure that the information adheres to the Data Quality guidelines both when the information is obtained from its sources and when the information is aggregated or consolidated for the use by the bureaus and offices?
- 4.5 How often are the policies and procedures checked routinely—what type of annual verification schedule has been established to insure that the information that is covered by this system of records notice adheres to the Data Quality guidelines?

## **Section 5.0 Safety and Security Requirements:**

5.1 How are the records/information/data in the information system covered by this system of records notice (SORN) stored and maintained?

- IT database management system (DBMS)
- Storage media including diskettes, CDs, CD-ROMs, *etc.*
- Electronic tape
- Paper files
- Other:

5.2 Is the information collected, stored, analyzed, or maintained by this information system available in another form or from another source (other than a "matching agreement" or *MOU*, as noted above)?

- Yes
- No

Please explain your response:

The PSHSB Comment Card Database is a "stand alone" information system that collects the comments that are filed via the two website comment card and paper comment cards--it has no links to any other sources.

5.3 Is the information system covered by this system of records notice (SORN) part of another FCC information system that collects personally identifiable information (PII)?

- Yes
- No

Please explain your response:

The PSHSB Comment Card Database is a "stand alone" electronic information system--it has no links to any other electronic databases nor are its paper files shared with any other filing systems, *etc.*

If this information system is not part of another FCC information system, please skip to Question 5.7.

5.4 If the information system (under review here) has personally identifiable information (PII) and is part of another FCC information system, is there a transfer of records/data/information between these two FCC information system(s)?

- Yes
- No

Please explain your response:

5.5 If the information system's personally identifiable information (PII) is part of another FCC information system, does the information system have processes and/or applications that are part of those from the other FCC information systems?

- Yes
- No

Please explain your response:

5.6 If either or both such situations, as noted in Questions 5.4 and 5.5 exist, what security controls are there to protect the PII information and to prevent unauthorized access?

Not applicable.

Please explain your response:

5.7 Would the unavailability of this information system prevent the timely performance of FCC operations?

Yes

No

Please explain your response:

The PSHSB staff has developed these two comment cards to help the PSHSB be more efficient and effective in its outreach efforts, *i.e.*, it helps the PSHSB to develop an accurate database to alert participants to future meetings, and it gives the public the opportunity to make the PSHSB aware of their concerns.

5.8 Will the information system include an externally facing information system or portal such as an Internet accessible web application at [www.fcc.gov](http://www.fcc.gov) or other URL that allows customers/users to access development, production, or internal FCC networks, and which may pose potential risks to the information's security?

Yes

No

Please explain your response:

PSHSB's Customer Comment Database or CCD has two webpage electronic public comment cards that are located on the FCC's webpages. These are:

(a) The PSHSB Comment Card: <http://www.fcc.gov/pshs/pshsdev/comment-card.html>; and

(b) The Summit Comment Card: <http://www.fcc.gov/pshs/pshsdev/summits/comment-card.html>.

However, the PSHSB staff has taken precautions to insure that the CCD information system functions can avoid any potential security risks.

If there is no externally facing information system portal at [www.fcc.gov](http://www.fcc.gov) or other URL, please skip to Question 5.11.

5.9 If the information is collected via [www.fcc.gov](http://www.fcc.gov) from the individuals, how does the information system notify users about the Privacy Notice:

Link to the FCC's privacy policies for all users: <http://www.fcc.gov/fccprivacypolicy.html>.

Privacy notice displayed on the webpage:

Privacy notice printed at the form or document:

Website uses another method to alert users to the Privacy Act Notice, as follows:

If there is no link or notice, why not:

5.10 If a privacy notice is displayed, which of the following are included?

Proximity and timing—the privacy notice is provided at the time and point of data collection.

Purpose—describes the principal purpose(s) for which the information will be used.

- Authority—specifies the legal authority that allows the information to be collected.
- Conditions—specifies whether providing the information is voluntary, and the effects, if any, of not providing it.
- Disclosures—specify the routine use(s) that may be made of the information.
- Not applicable, as information will not be collected in any other way.

Please explain your response:

5.11 Will the information system include another customer-facing web site not on [www.fcc.gov](http://www.fcc.gov) or other URL?

- Yes
- No

Please explain your response:

If the information is collected by some method or process other than via the FCC Intranet for FCC employees and contractors working at the FCC, please skip to Question 5.14.

5.12 If the information system has a customer-facing web site via the FCC Intranet for FCC employees and contractors working at the FCC, does this web site(s) have a Privacy Act Notice and how is it displayed?

- Yes
  - Notice is displayed prominently on this FCC Intranet website:
  - Link is provided to a general FCC Privacy Notice for all users:
  - Privacy Notice is printed at the end of the form or document:
  - Website uses another method to alert users to the Privacy Act Notice:
- No

If there is no Privacy Act Notice, please explain why not:

5.13 If a privacy notice is displayed, which of the following information is included?

- Proximity and timing—the privacy notice is provided at the time and point of data collection.
- Purpose—describes the principal purpose(s) for which the information will be used.
- Authority—specifies the legal authority that allows the information to be collected.
- Conditions—specifies if providing the information is voluntary, and the effects, if any, of not providing it.
- Disclosures—specify the routine use(s) that may be made of the information.
- Not applicable, as information will not be collected in any other way.

Please explain your response:

If information is only collected via a customer-facing portal on the FCC Internet at [www.fcc.gov](http://www.fcc.gov) or the FCC Intranet for FCC employees and contractors, please skip to Question 5.16.

5.14 If information is collected from the individual by fax, e-mail, FCC form(s), or regular mail, how is the privacy notice provided?

- Privacy notice is on the document, *e.g.*, FCC form, *etc.* The PSHSB Comment Card Database information system also includes a paper comment sheet, which has a "Privacy Advisory" notice explaining the privacy protections afforded to comment submitters.
- Privacy notice displayed on the webpage where the document is located:
- Statement on the document notifies the recipient that they may read the FCC Privacy Notice at <http://www.fcc.gov/fccprivacypolicy.html>.
- Website or FCC document uses other method(s) to alert users to the Privacy Act Notice:
- Privacy notice is provided via a recorded message or given verbally by the FCC staff handling telephone calls:
- No link or notice, please explain why not:
- Not applicable, as personally identifiable information (PII) will not be collected.

5.15 If a privacy notice is displayed, which of the following information is included?

- Proximity and timing—the privacy notice is provided at the time and point of data collection.
- Purpose—describes the principal purpose(s) for which the information will be used.
- Authority—specifies the legal authority that allows the information to be collected.
- Conditions—specifies if providing the information is voluntary, and the effects, if any, of not providing it.
- Disclosures—specify the routine use(s) that may be made of the information.
- Not applicable, as information will not be collected in any other way.

Please explain your response:

The "Privacy Advisory" on the paper comment card does not include all the privacy requirements listed above since the web address for the FCC's privacy policy is provided. The Commission believes that giving a brief summary of the privacy protections and providing this link offer sufficient notice to commenters.

If there is no access to the information system from outside the FCC via [www.FCC.gov](http://www.FCC.gov) or other URL, please skip to Question 5.17.

5.16 If consumers may access the information and/or the information system on-line via [www.FCC.gov](http://www.FCC.gov) or other URL, does it identify ages or is it directed to people under 13 years old?

- Yes
- No

Please explain your response:

The PSHSB Comment Card Database's purposes are to provide summit conference and public forum attendees and the public-at-large with the opportunity to submit their comments on a voluntary basis to the PSHSB, which will help the PSHSB improve its summits, conferences, public forums, and other outreach efforts and activities.

Furthermore, the FCC Website policy states that although the Commission's Website contains some pages that offer educational content to children, it is FCC policy, in compliance with the requirements of the Children's Online Privacy Protection Act (COPPA), not to collect information online about or from children age 13 and under, except when it is needed to identify a submission or to answer a question. Under no circumstances will any of this information be used for another purpose or shared with third parties, nor will personally identifying information be published on the FCC website.



5.17 Will the FCC use the newly obtained information or revised information in this information covered by the existing system of records notice (SORN) to make a determination about the individual?

- Yes
- No

Please explain your response:

The PSHSB Comment Card Database's purposes are solely to provide attendees at PSHSB summit conferences, public forums, *etc.*, and the public-at-large with the opportunity to submit their comments on a voluntary basis to the PSHSB, which will help the PSHSB improve its summits, public forums, *etc.*, and its outreach efforts and activities.

5.18 Do individuals have the right to decline to provide personally identifiable information (PII)?

- Yes
- No

Please explain your response:

Summit conference and public forum attendees and the public-at-large may submit comments; however, the request for comments is purely voluntary. The PSHSB's electronic comment cards and the paper comment sheet do ask commenter to provide their first and last names, a telephone number, and an e-mail address, which depending upon the commenters business situation may include a personal cell phone number, personal home telephone number and/or a personal e-mail address, although none of this information is required.

5.19 Do individuals have the right to consent to particular uses of their personal information?

- Yes
- No

Please explain your response:

Commenters who submit comments do so voluntarily. They may provide as much or as little information in their comments as they choose, although, as noted above, PSHSB does request that commenters provide their first and last names. In addition, in the case of the summit conference/public forum comment card, failing to provide contact information may prevent the FCC from contacting the submitter to provide them with information about future summits and conferences.

If individuals do not have the right to consent to the use of their information, please skip to Question 5.23.

5.20 If individuals have the right to consent to the use of their personal information, how does the individual exercise this right?

5.21 What processes are used to notify and to obtain consent from the individuals whose personal information is being collected?

5.22 What kinds of report(s) can the information system and/or the information be used to produce on the individuals whose PII data are in the information system covered by the system of records notice (SORN)?

5.23 What safeguards and security measures, including physical and technical access controls, are in place to secure the information and to minimize unauthorized access, use, or dissemination of the information that is stored and maintained in the information system?

(Check all that apply)

- Account name
- Passwords
  - Accounts are locked after a set period of inactivity
  - Passwords have security features to prevent unauthorized disclosure, *e.g.*, “hacking”
  - Accounts are locked after a set number of incorrect attempts
  - One time password token
  - Other security features:
- Firewall
- Virtual private network (VPN)
- Data encryption:
- Intrusion detection application (IDS)
- Common access cards (CAC)
- Smart cards
- Biometrics
- Public key infrastructure (PKI)
- Locked file cabinets or fireproof safes
- Locked rooms, with restricted access when not in use
- Locked rooms, without restricted access
- Documents physically marked as “sensitive”
- Guards
  - Identification badges
  - Key cards
  - Cipher locks
  - Closed circuit TV (CCTV)
  - Other:

5.24 Please explain what staff security training and other measures are in place to assure that the security and privacy safeguards are maintained adequately?

All FCC employees and contractors who will work with PSHSB's Comment Card Database Information System are required to complete privacy training. In addition the PSHSB staff issues periodic reminders to the FCC employees and contractors who have access that the PII in the CCD information system is not to be shared or disclosed without authorization.

5.25 How often are security controls reviewed?

- Six months or less:
- One year
- Two years
- Three years
- Four years
- Five years
- Other:

5.26 How often are personnel (information system administrators, users, information system/information system developers, contractors, *etc.*) who use the information system trained and made aware of their responsibilities for protecting the information?

- There is no training
- One year: The PSHSB staff will require that the FCC employees and contractors who administer, manage, and/or use the CCD information system must attend training at least once a year to be review their responsibilities to protect the PII contained in the CCD information system.
- Two years
- Three years
- Four years
- Five years
- Other: The FCC has also inaugerated a Commission-wide privacy training program, and all employees and contractors were required to complete the privacy training course in September 2006.

If privacy training is provided, please skip to Question 5.28.

5.27 What are the safeguards to insure that there are few opportunities for disclosure, unavailability, modification, and/or damage to the information system covered by this system of records notice (SORN), and/or prevention of timely performance of FCC operations if operational training is not provided?

5.28 How often must staff be “re-certified” that they understand the risks when working with personally identifiable information (PII)?

- Less than one year:
- One year: The PSHSB staff requires that the FCC employees and contractors who administer, manage, and/or use the information system in the CCD information system attend training at least once annually to review their responsibilities for protecting the PII contained in CCD information system.
- Two years
- Three or more years
- Other re-certification procedures:

5.29 Do the Commission’s training and security requirements for this information system that is covered by this system of records notice (SORN) conform to the requirements of the Federal Information Security Management Act (FISMA)?

- Yes
- No

Please explain your response:

The PSHSB staff plans to require that the CCD information system conform to the FISMA requirements that govern the FCC's training and security requirements.

If the Privacy Threshold Assessment was completed recently as part of the information system’s evaluation, please skip to Question 5.34.

- 5.30 What is the potential impact on individuals on whom the information is maintained in the information system(s) if unauthorized disclosure or misuse of information occurs?  
(check one)
- Results in little or no harm, embarrassment, inconvenience, or unfairness to the individual.
  - Results in moderate harm, embarrassment, inconvenience, or unfairness to the individual.
  - Results in significant harm, embarrassment, inconvenient, or unfairness to the individual.

Please explain your response:

- 5.31 Is the impact level for the information system(s) covered by this system of records notice (SORN) consistent with the guidelines as determined by the FIPS 199 assessment?
- Yes
  - No

Please explain your response:

- 5.32 Has a "Certification and Accreditation" (C&A) been completed for the information system(s) covered this system of records notice (SORN)?
- Yes
  - No

If yes, please explain your response and give the C&A completion date:

- 5.33 Has the Chief Information Officer (CIO) and/or the Chief Security Officer (CSO) designated this information system as requiring one or more of the following:
- Independent risk assessment:
  - Independent security test and evaluation:
  - Other risk assessment and/or security testing procedures, *etc.*:
  - Not applicable:

- 5.34 Is the system using technology in ways that the Commission has not done so previously, *i.e.*, Smart Cards, Caller-ID, *etc.*?
- Yes
  - No

Please explain your response:

- 5.35 How does the use of the technology affect the privacy of the general public and FCC employees and contractors?

The individuals from the general public who submit comments voluntarily via either or both of the PSHSB CCD information system's websites are only asked to provide a minimal amount of personally identifiable information (PII). This PII is contained in the information system's electronic database records. The FCC believes that the technology it is using to obtain the

comments will have a minimal effect on the privacy of the general public. The CCD information system does not collection any information, including PII from FCC employees and contractors.

- 5.36 Will the information system that is covered by this system of records notice (SORN) include a capability to identify, locate, and/or monitor individuals?

- Yes  
 No

Please explain your response:

The personally identifiable information that individuals are asked to submit voluntarily with their comments is done so that the PSHSB staff can provide information that the submitters have requested or to respond to their comments. Failing to provide this PII means that the PSHSB staff can not reply directly to these requests and/or comments, which would be an impediment to the PSHSB's public outreach efforts to improve the PSHSB's summits, forums, conferences, and other outreach activities.

If the information system does not include any monitoring capabilities, please skip to **Section 6.0 Information Collection Requirements under the Paperwork Reduction Act (PRA):**

- 5.37 If the information system includes these technical capabilities identified in Questions 5.34 through 5.36 above, what kinds of information will be collected as a function of the monitoring of individuals?

- 5.38 Does the information system covered by this system of records notice (SORN) contain any controls, policies, and procedures to prevent unauthorized monitoring?

- Yes  
 No

Please explain your response:

**Section 6.0 Information Collection Requirements under the Paperwork Reduction Act (PRA):**

- 6.1 Does this system of records notice (SORN) require non-FCC employees and contractors to perform any paperwork or recordkeeping activities?

- Yes, individuals, who are not FCC employees or contractions, are required to complete paperwork or recordkeeping functions or activities, *i.e.*, fill out forms and/or licenses, participate in surveys, and or maintain records *etc.*

Please explain your response:

- No, individuals, who are not FCC employees or contractors, are not required to perform any paperwork or recordkeeping functions or activities

Please explain your response:

The PSHSB Comment Card Database information system is a purely voluntary comment submission program. Summit, conference, and forum attendees and members of the public-at-large are not required to submit comments.

No, this system of records notice includes only FCC employees and/or contractors, which exempts it from the PRA. Please skip to **Section 7.0 Correction and Redress**:

6.2 If the website requests information, such as the information necessary to complete an FCC form, license, authorization, *etc.*, has the information collection covered by this system of records notice (SORN) been identified for possible inclusion under the FCC's Paperwork Reduction Act (PRA) requirements?

Yes  
 No

Please explain your response:

If there are no PRA information collections associated with the information system or its applications, please skip to **Section 7.0 Correction and Redress**:

6.3 If yes, what PRA information collections covered by this system of records notice (SORN) are associated with this database please list the OMB Control Number, Title of the collection, Form number(s) as applicable, and Expiration date:

6.4 If there are any FCC forms associated with the information system(s) covered by this system of records notice (SORN), do the forms carry the Privacy Act notice?

Yes

FCC Form Number(s) and Title(s):

No

Not applicable—the information collection does not include any forms.

6.5 Have the system managers contacted the Performance Evaluation and Records Management (PERM) staff to coordinate PRA requirements and submission of the information collection to the Office of Management and Budget?

Yes  
 No

Please explain your response:

### **Section 7.0 Correction and Redress:**

7.1 Are the procedures for individuals wishing to inquire whether this system of records notice (SORN) contains information about them consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act and Freedom of Information Act (FOIA) requirements?

Yes  
 No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

Individuals who submit their personally identifiable information (PII) to the FCC via the PSHSB CCD information system's electronic comment cards or the paper comment sheet, and who wish to inquire whether this SORN contains their PII may address their inquiries to the Outreach Media Director or Public Safety Outreach Coordinator of PSHSB for FCC/PSHSB-2, "Comment Card Database (CCD)," SORN. This is consistent with FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act, as noted in this SORN.

- 7.2 Are the procedures for individuals to gain access to their own records/information/data in this information system that is covered by this system of records notice (SORN) consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act and Freedom of Information Act (FOIA) requirements?

Yes  
 No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

Individuals who submit their personally identifiable information (PII) to the FCC via the PSHSB CCD information system's electronic comment cards or the paper comment sheet, and who wish to gain access to their own information in the FCC/PSHSB-2, "Comment Card Database (CCD)," SORN may seek access to this information by contacting the Outreach Media Director or Public Safety Outreach Coordinator of PSHSB. This is consistent with FCC policies and rules under 47 CFR §§ 0.554 – 0.555, as noted in the SORN.

- 7.3 Are the procedures for individuals seeking to correct or to amend records/information/data about them in the information system that is covered by this system of records notice (SORN) consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.556 – 0.558?

Yes  
 No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

Individuals who submit their personally identifiable information (PII) to the FCC via the PSHSB CCD information system's electronic comment cards or the paper comment sheet, and who seek to correct or to amend information about them in the FCC/PSHSB-2, "Comment Card Database (CCD)," SORN may contact the Outreach Media Director or Public Safety Outreach Coordinator of PSHSB. This is consistent with FCC policies and rules under 47 CFR §§ 0.554 – 0.555, as noted in the SORN.

- 7.4 Does the FCC provide any redress to amend or correct information about an individual covered by this system of records notice (SORN), and if so, what alternatives are available to the individual, and are these consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.556 – 0.558?

Yes  
 No

Please explain your response:

Individuals who submit their personally identifiable information (PII) to the FCC via the PSHSB CCD information system's electronic comment cards or the paper comment sheet, and who are

seeking redress to amend or to correct information about them in the FCC/PSHSB-2, "Comment Card Database (CCD)," SORN may contact the Outreach Media Director or Public Safety Outreach Coordinator of PSHSB. This is consistent with FCC policies and rules under 47 CFR §§ 0.554 – 0.555, as noted in the SORN.

If this is a new system of records notice (SORN), please skip to Question 7.6.

7.5 Have the sources for the categories of records in the information system(s) covered by this system of records notice (SORN) changed?

- Yes
- No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

7.6 Does this system of records notice (SORN) claim any exemptions to the notification, access, and correction, and/or amendment procedures as they apply to individuals seeking information about them in this SORN, and if so, are these exemptions consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.561?

- Yes
- No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

At this time, the PSHSB staff , which is responsible for the development and implementation of the new FCC/PSHSB-2, "Comment Card Database (CCD)," SORN that will cover the personally identifiable information that individuals provide when the submit comment voluntarily via the two electronic comment cards and/or the paper comment sheet, does not plan to seek any exemptions to the notification, access, and correction and/or amendment procedures as they apply to individuals seeking information about them in this SORN.

7.7 What processes are in place to monitor and to respond to privacy and/or security incidents? Please specify what is changing if this is an existing system of records notice (SORN) that is being updated or revised?

The PSHSB staff will post notices that the information systems's electronic data and records and paper files that are covered by FCC/PSHSB-2, "Comment Card Database (CCD)," SORN are "non public for internal use only." The PSHSB staff will also issue reminders periodically to those granted access to the information that they are to keep the PII confidential, to safeguard any printed materials, and to avoid any unauthorized disclosure of the PII that is covered by this SORN.

7.8 How often is the information system audited to ensure compliance with FCC and OMB regulations and to determine new needs?

- Six months or less
- One year
- Two years
- Three years
- Four years



- Five years
- Other audit scheduling procedure(s): The new CCD information system does not have an audit requirement at this time. Nonetheless, the PSHSB staff will determine what practices and procedures they should adopt to ensure compliance with FCC and OMB audit regulations and other new needs as necessary to safeguard the personally identifiable information (PII) contained in this information system covered by FCC/PSHSB-2, "Comment Card Database (CCD)," SORN.

**Section 8.0 Consumer Satisfaction:**

8.1 Is there a customer satisfaction survey included as part of the public access to the information covered by this system of records notice (SORN)?

- Yes
- No
- Not applicable

Please explain your response:

If there are no Consumer Satisfaction requirements, please skip to **Section 9.0 Risk Assessment and Mitigation:**

8.2 Have any potential Paperwork Reduction Act (PRA) issues been addressed prior to implementation of the customer satisfaction survey?

- Yes
- No

Please explain your response:

8.3 If there are PRA issues, were these issues addressed in the PRA component of this PIA template?

- Yes
- No

Please explain your response:

**Section 9.0 Risk Assessment and Mitigation:**

9.1 What are the potential privacy risks for the information covered by this system of records notice (SORN), and what practices and procedures have you adopted to minimize them?

**Risks:**

- a. Some of the information system's personally identifiable information (PII) includes paper documents that are stored in file cabinets.
- b. Some of the information system's personally identifiable information (PII) includes electronic records that are stored in the FCC's computer network databases.
- c. Since CCD is a new information system, there may be potential processes and procedures that could lead to PII security breaches that have not been discovered and remedied.

**Mitigating factors:**

- a. PII that is contained in paper documents is stored in locked file cabinets.
- b. PII that is contained in electronic records is protected in the FCC's computer network databases, which require users to provide login's and access rights to these records.
- c. PSHSB is working with the CCD information system developers to review all the CCD processes and procedures with reference to the issue of PII protection and security to avoid any such breaches once the CCD information system is fully operational.

9.2 What deficiencies did the bureau/office find in its procedures for evaluating the information system(s) covered by this system of records notice (SORN) and what remedies did the bureau/office enact following this Privacy Impact Assessment (PIA)?

**Deficiencies:**

- a. The room in which the file cabinets storing CCD paper comment sheet files is not locked.
- b.
- c.

**Remedies:**

- a. PSHSB should find a room with a locking system to store the file cabinets.
- b.
- c.

9.3 What is the projected production/implementation date for the database(s):

Initial implementation: September 2008  
Secondary implementation:  
Tertiary implementation:  
Other implementation:

9.4 Are there any ancillary and/or auxiliary information system(s) applications linked to this information system that is covered by this system of records notice (SORN), which may also require a Privacy Impact Assessment (PIA)?

- Yes
- No

If so, please state the application(s), if a Privacy Impact Assessment (PIA) has been done, and the completion date for PIA:

At this time in development, PSHSB staff does not anticipate that there will be any ancillary or auxillary information systems linked to implementation of the new CCD information system.