

Federal Communications Commission
Office of the Managing Director



Privacy Threshold Analysis (PTA)¹
Signal Booster Registration System
August 5, 2013

FCC Bureau/Office: Wireless Telecommunications Bureau (WTB)
Division(s): Technologies, Systems and Innovation Division

Privacy Analyst: Les Smith
Telephone Number: 202-418-0217
E-mail Address: Leslie.Smith@fcc.gov

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.

¹ This form is used to determine whether this information system requires a Privacy Impact Assessment.

The E-Government Act of 2002 defines an information technology and/or system by reference to the definition sections of Titles 40 and 44 of the United States Code (U.S.C.). The following summarize these definitions:

- “Information Technology” means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. *See* 40 U.S.C. 11101(6).
- “Information System” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. *See* 44 U.S.C. 3502(8).

It is important, therefore, that when the FCC develops or makes changes to its information systems, the FCC should analyze what information the system will collect and maintain to determine whether there are any privacy issues.

The purpose of the **Privacy Threshold Analysis (PTA)** is to help the FCC’s bureaus/offices evaluate the information/data in the system and make the appropriate determination about how to treat the information/data, as required by the Privacy Act’s regulations.

Thus, the Privacy Threshold Analysis helps the bureaus and offices to determine if the data in the information system include information about individuals, *e.g.*, personally identifiable information (PII), which will require a **Privacy Impact Analysis** to be conducted.

Section 1.0 Information System’s Status:

1.1 Status of the Information System/Database:

- New information system—Implementation date: November 2013
- Revised or upgraded information system—Revision or upgrade date:
- Other changes, revisions, etc. and 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:

In February 2013, the FCC adopted a *Report and Order*, Improve Wireless Coverage Through the Use of Signal Boosters, WT Docket No. 10-4, FCC 13-21, which requires certain types of signal boosters to be registered with the FCC (*i.e.*, Signal Booster Registration System). The Wireless Telecommunications Bureau (WTB) is implementing the Signal Booster requirements under Part 90 of the Commission’s rules (47 CFR Part 90). Under Part 90, (business) applicants must register with the FCC so that the Commission will have a database of Part 90 signal booster owners who may

be contacted should a business experiences any interference issues to remedy such interference.

If this is a new information system or database, please skip to Question 1.6.

- 1.2 Has this information system existed under another name, or has the name been changed or modified?

Yes
 No

Please explain your response:

- 1.3 Has this information system or database existed previously or been operated under any other software program, information system medium, *i.e.*, electronic database or paper files, and/or other format?

Yes
 No

Please explain your response:

- 1.4 Has this information system existed under a system of records notice (SORN) by itself, or was it ever part or component of another SORN?

Yes
 No

Please explain your response:

- 1.5 Is this information system/database being changed or upgraded, and if so, what are the purposes for system's changes, and/or will any changes now include information about individuals, *i.e.*, personally identifiable information (PII):

Yes
 No

Please explain your response:

- 1.6 Why is the information being collected, *i.e.*, what are the information system's purposes, intended uses, and/or functions:

As noted in Question 1.1, the information in the Signal Booster Registration System's database is being collected in order to register businesses which use signal boosters, as required under Part 90 of FCC rules. The information in this database will help businesses that receive interference from Part 90 signal boosters to contact the owners of the Part 90 signal boosters to remedy this interference.

1.7 What information is the system/database collecting, analyzing, managing, storing, transferring, *etc*:

Information about FCC Employees:

- No FCC employee(s) data
- FCC employee's name
- Other names used, *i.e.*, maiden name, *etc*.
- FCC badge number (employee ID)
- SSN
- Race/ethnicity
- Gender
- US Citizenship
- Non-US Citizenship
- Biometric data
 - Fingerprints
 - 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)
- 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 personal/background information:

Information about FCC Contractors:

- No FCC contractor information
- Contractor's name

- Other names used, *i.e.*, maiden name, *etc.*
- FCC Contractor badge number (Contractor ID)
- SSN
- Race/ethnicity
- Gender
- US Citizenship
- Non-US Citizenship
- Biometric data
 - Fingerprints
 - Voice prints
 - Retina scan/prints
 - Photographs
 - Other physical information, *e.g.* 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 personal/background information:

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

- Not applicable
- Individual's name:
- Other name(s) used, *e.g.*, maiden name, *etc.*
- FCC badge number (employee ID)
- SSN:
- Citizenship
- Non-U.S. Citizenship:

- Race/Ethnicity
- Gender
- Biometric data
 - Fingerprints
 - Voiceprints
 - Retina scans/prints
 - Photographs
 - Other physical information, *e.g.*, 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 Business Customers (usually not considered “personal information”):

- Not applicable
- Name(s) of business contact(s)/firm representative(s), customer and/or others: Businesses that operate signal boosters are required to register their name, location, and contact information under Part 90 of FCC rules in the Signal Booster Registration System's database.
- Race/Ethnicity
- Gender
- Citizenship
- Non-U.S. Citizenship:
- 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 cubical number)
- 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
- Personal clubs and affiliations
- Credit card number(s)
- Bank account(s)
- Other information:

“Non-personal” information obtained from FCC sources:

- Not applicable
- Economic data
- Engineering/scientific data
- Accounting/financial data
- Legal/regulatory/policy data
- Other information, please specify:

Miscellaneous Business, Technology, or Other Information:

- Not applicable
- Not publicly available business or technology data, *e.g.*, trade or propriety information:
- Other information, please specify:

1.8 What are the sources for the information, including PII, 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:
Businesses that operate signal boosters under the FCC's Part 90 rules.
- 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, please specify:

1.9 Does this information system have any links to other information systems or databases?

An information system (or database) may be considered as linked to other information systems (or databases) if it has one or more of the following characteristics:

- The information system is a subsystem or other component of another information system or database that is operated by another FCC bureau/office or non-FCC entity (like the FBI, DOJ, National Finance Center, etc.);
- The information system transfers or receives information, including PII, between itself and another FCC or non-FCC information system or database;
- The information system has other types of links or ties to other FCC or non-FCC information systems or databases;
- The information system has other characteristics that make it linked or connected to another FCC or non-FCC information system or database;
- The information system has no links to another information system (or database), *i.e.*, it does not share, transfer, and/or obtain data from another system.

If this system has any of these criteria or characteristics, please explain; otherwise please skip to Question 1.11:

The information in the Signal Booster Registration System's database, which includes the locational data on those businesses that operate signal boosters, has links to the FCC's CORES Registration System. Applicants (businesses) must register with the FCC as required by the Part 90 rules to receive their FCC Registration Number (FRN) before they can submit their location data in the Signal Booster Database. The FRN authorizes these businesses to use WTB's Universal Service Licensing System (ULS) and validates their Call Signs. The Google Geocoding Application (API) is used to provide the longitude and latitude for these call signs that these businesses use.

1.10 What information system(s)/database(s) have links to this system/database that allow information to be shared or transferred between these systems/databases?

- FCC information system and information system name(s): CORES and ULS
- Non-FCC information system and information system name(s): Google Geocoding Application (API)

If this information system is a "stand alone" information system, and it does not use or share information with another system/database (other than CORES registration), please skip to Question 1.13.

1.11 If the system uses information, including PII, from other information systems/databases, what information is used or shared?

Information system name(s):

- Individual's name

- Other names, *i.e.*, maiden name, *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 number(s)
- Bank account(s)
- Non-FCC personal employment records
- Non-FCC government badge or employee ID number(s), *e.g.*, contractor's badge number.
- Law enforcement data
- Background investigation history
- Military history
- National security data
- Foreign countries visited
- Other information, please specify:

Information about Business Customers and others (usually not considered "personal information"):

- Not applicable
- Name of business contact/firm representative, customer, or others:
Google Geocoding Application (API)
- Business/corporate purpose(s)
- Other business/employment/job description(s)
- Professional/Personal clubs and/or affiliations
- Full or partial SSN:
- Intra-business office address (office or workstation)
- Business/office address

- Business telephone number(s)
- Business cell phone number(s)
- Business fax number(s)
- Business pager number(s)
- Business e-mail address(es)
- Race/Ethnicity
- Customers' gender(s)
- 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)
- Credit report(s)
- Other information, please specify:
 1. CORES registration system validates the FRN assigned to each business registrant;
 2. The ULS system validates the (signal booster) call sign(s); and
 3. Google Geocoding Application (API) system validates the coordinates (*i.e.*, longitude and latitude)/address of the signal booster.
 4. The Signal Booster Registration System's database will include:
 - (a) Location of the signal booster: latitude and longitude and physical address;
 - (b) Company that owns the booster--company name, address, phone number, and e-mail address(es);
 - (c) Call sign(s) that the booster operates under--up to six call signs can be provided;
 - (d) Contact information--name, address, phone number, and e-mail address (this can be the same or different than the company that owns the booster); and
 - (e) Electronic signature of the person authorized by the company to register the signal booster.

Miscellaneous Business Information:

- Not applicable
- Not publicly available business data, *i.e.*, trade or propriety information
- Other information, please specify:

“Non-personal” information:

- Not applicable
- Economic data
- Engineering/scientific data
- Accounting/financial data
- Legal/regulatory/policy data
- Other information, please specify:

1.12 What are the sources for the information from the other system(s)/database(s) 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:
Information that businesses and non-profits provide when registering in CORES that are entered into the Signal Booster Registration System's database.
- 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:

1.13 Does this system/database have the capability to manipulate, transform, or create new information from the information it collects through data analysis, aggregation, or consolidation from the information that is being collected, including (where applicable) information that is being shared or transferred from another information system?

- Yes
- No

Please explain your response:

As explained in Questions 1.1 and 1.6, the Signal Booster Registration System's database is used to store information (i.e., longitude and latitude and physical address) of signal booster owners, who can then be contacted to remedy any signal interference issues that they may be causing to other a business experiences.

If the information system does not contain information about individuals (PII), please skip to Question 1.17.

1.14 Can the PII in this information system or linked to other information systems/databases 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:

1.15 Will the new information include PII that is to be included in an individual's records or to be used to make a determination about an individual?

- Yes
- No

Please explain your response:

- 1.16 What is the potential impact or “security risk” 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:

- 1.17 What is the potential impact or “security risk” for the information that is maintained in the information system if an unauthorized disclosure or misuse of information occurs?
(check one) [maybe I confused you, but 1.15 and 1.16 were supposed to be an “either/or” response—if the information system has PII, complete 1.15, if non, complete 1.16]

- Results in little or no harm, embarrassment, inconvenience, or unfairness.
- Results in moderate harm, embarrassment, inconvenience, or unfairness.
- Results in significant harm, embarrassment, inconvenient, or unfairness.

Please explain your response:

The information in the Signal Booster Registration System's database is publicly available and can be accessed through an interface on the FCC's website, *i.e.*, no proprietary data or other sensitive non-PII information (audit tables with time stamps and FRN) are not exposed.

- 1.18 Is this impact level consistent with the guidelines as determined by the FIPS 199 assessment?

- Yes
- No

Please explain your response:

The Signal Booster Registration System's database meets the FIPS 199 assessment guidelines, *i.e.*, "low impact" designation, since only the CORES registration is required to authorize each business to submit their data in this database.

- 1.19 When was “Assessment and Accreditation” (A&A) last completed?

The A&A is on-going.

- 1.20 Has the Chief Information Officer (CIO) and/or the Chief Information Security Officer (CISO) designated this information system as requiring an

- Independent risk assessment
- Independent security test and evaluation

- Other risk assessment and/or security testing procedure, *etc.*
- Not applicable.

Please explain your response:

The Signal Booster Registration System's database will have an on-going risk assessment.

1.21 Based on the information that you have provided thus far, if:

- The information you are collecting does not include PII if you answered **NO** to questions 1.4, 1.5, 1.7, 1.8, 1.11, 1.12, and/or 1.17, then:

The information system (IT application or paper files) does not contain PII nor does it have shared links with other information systems that may also contain PII that could constitute a privacy issue.

A Privacy Impact Assessment is **not required**.

- The information you are collecting does include PII, and you answered **YES** to questions 1.4, 1.5, 1.7, 1.8, 1.11, 1.12, 1.14, and/or 1.15, then:

The information system (IT application or paper files) does contain PII, or it does have shared links with other information systems that may also contain PII that could constitute a privacy issue.

This information system/database **requires** a Privacy Impact Assessment (PIA).