Federal Communications Commission

Office of the Managing Director

Privacy Impact Assessment[1] (PIA) for the Cadapult Space Management System

March 27, 2007

Information System: Cadapult Space Management System
FCC Bureau/Office: Office of the Managing Director
Division: Administrative Operations–Space Management Center

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

[1] 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 the 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—Development date [mm/dd/yyyy]:
☒ Revised or upgraded information system—Revision or upgrade date [mm/dd/yyyy]: Updated Fall 2005

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

☒ Placed in existing information system—Implementation Date [mm/dd/yyyy]: Fall 2005
☐ Placed in new auxiliary /ancillary information system—Date [mm/dd/yyyy]:
☐ Other use(s)—Implementation Date [mm/dd/yyyy]:

Please explain your response:

The Space Management Center updated the Cadapult Space Management System database in the Fall 2005.

1.2 Has a Privacy Threshold Assessment been done?

☒ Yes
Date: 03/12/2007
☐ 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); 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 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 employees names
☐ Other names used, *i.e.*, maiden names, *etc.*
☐ SSN
☐ 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)
- ☐ Emergency contact data
- ☐ Credit card number(s)
- ☐ Driver's license number(s)
- ☐ Bank account(s)
- ☐ Personal e-mail address(es)
- ☐ FCC personal employment records
- ☐ Military records
- ☐ Financial history
- ☐ Foreign countries visited
- ☐ FCC badge number (employee ID)
- ☐ Law enforcement data
- ☐ Background investigation history
- ☐ National security data
- ☐ Communications protected by legal privileges
- ☐ Digital signature
- ☐ Other information, please specify:

Information about FCC Contractors:

- ☐ No FCC contractor information
- ☐ Contractor's name
- ☐ Other names used, *i.e.*, maiden names, *etc.*
- ☐ SSN
- ☐ 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)
- ☐ 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
- [ ] FCC Contractor badge number (Contractor ID)
- [ ] Law enforcement data
- [ ] Background investigation history
- [ ] National security data
- [ ] Communications protected by legal privileges
- [ ] Digital signature
- [ ] Other information, please specify:

Information about FCC Customers or Visitors:

- [ ] Not applicable
- [ ] Consumer/customer name
- [ ] Citizenship
- [ ] Consumer/customer SSN
- [ ] Consumer/customer address
- [ ] Consumer/customer birthday/age
- [ ] Consumer/customer telephone number(s)
- [ ] Consumer/customer cell phone number(s)
- [ ] Consumer/customer telephone/cell phone account number(s)
- [ ] Digital signature
- [ ] Other information, please specify:

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

- [ ] Not applicable
- [ ] Name of business contact/firm representative
- [ ] Business/corporate purpose(s)
- [ ] Job description
- [ ] Professional affiliations
- [ ] Partial SSN
- [ ] Intra-business office address (office or cubical number)
- [ ] Business telephone number(s)
- [ ] Business cell phone number(s)
- [ ] Business fax number(s)
- [ ] Business e-mail address(es)
- [ ] Race/Ethnicity
- [ ] Gender
- [ ] 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, please specify:

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, please specify:

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, 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?

- ☐ SSN
- ☐ Other names used
- ☐ Citizenship
- ☐ Biometric data
  - ☐ Finger prints
  - ☐ Voice prints
  - ☐ Retina scan/prints
  - ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc.*
  - ☐ Photographs
- ☐ Birth date/Age
- ☐ Place of birth
- ☐ Medical data
- ☐ Marital status
- ☐ Spousal information
- ☐ Miscellaneous family information, please specify:
- ☐ Home address
- ☐ Home address history
- ☐ Home telephone number(s)
- ☐ Personal cell phone number(s)
- ☐ 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
- ☐ Non-FCC government badge number (employee ID)
- ☐ Law enforcement data
- ☐ Military history
- ☐ National security data
- ☐ Communications protected by legal privileges
- ☐ Consumer/customer name
- ☐ Consumer/customer SSN
- ☐ Consumer/customer address
- ☐ Consumer/customer birthday/age
- ☐ Consumer/customer telephone number(s)
- ☐ Consumer/customer cell phone number(s)
- ☐ Consumer/customer telephone/cell phone account number(s)
- ☐ Other information, please specify:

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

- ☐ Name of business contact/firm representative
- ☐ Business/corporate purpose(s)
- ☐ Job description
- ☐ Professional affiliations
- ☐ Partial SSN
- ☐ Intra-business office address (office or cubical number)
- ☐ Business telephone number(s)
- ☐ Business cell phone number(s)
- ☐ Business fax number(s)
- ☐ Business e-mail address(es)
- ☐ Race/Ethnicity
- ☐ Gender
- ☐ 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, please specify:

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 the information systems like this one, which contain 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 personal information.

Is there a SORN that already covers this personal information 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 there is a SORN, please skip to Question 1.17

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 covered by a SORN, does the SORN that cover the information system exist by itself, or did the information system exist previously as a component or subset of another system of records notice (SORN)?

☐ Yes
☐ No

If yes, please explain what has occurred:

What is this System of Records Notice (SORN):

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

Please skip to **Section 2.0 System of Records Notice (SORN) Update** to address any changes to this 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?

The information in the Cadapult Space Management System (CSMS) is used to allocate the offices, workstations, and facility work spaces to FCC employees and contractors following the FCC/National Treasury Employees Union (NTEU) space assignment policy. In the event of an emergency, the Space Management Center (SMC) will have to pull information from this system to create the space requirements for alternative work location(s) in other buildings to be used to relocate FCC employees and/or contractors. The information may be shared with other Federal agencies, *i.e.*, General Services Administration, as part of the FCC's Reconstitution Plan.

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

The Cadapult Space Management System is maintained by the FCC's Space Management Center in the Office of the Managing Director, Associate Managing Director–Administrative Operations (OMD–AO).

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 FCC manages its space holdings via this information.

If yes, 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:

The Cadapult Space Mangement System has not been assigned a Security Classification.

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

44 U.S.C. 3101, 5 U.S.C. 301.

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 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, GSA
☐ Labor relations (NTEU)
☐ Law enforcement and investigations
☐ Program partners, e.g., WMATA, *etc.*
☐ Others "third party" disclosures, please specify:

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?

The CSMS information is stored on the FCC's secure network servers and access rights are limited.

1.26 How is information in this system retrieved?

Information, *e.g.*, records, in the Cadapult Space Management System are retrieved by employee name, workspace location, and organizational unit.

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

The FCC maintains information about the FCC employees and/or contractors only as long as the employee and/or contractor works at the FCC. The records in this system are deleted entirely upon the FCC employee's retirement, voluntary resignation, transfer, or re-assignment outside the FCC, and when the contractor is no longer working at the FCC.

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 Space Management Center's (SMC) staff utilize a sign-out procedure to delete the information whenever the FCC employee or contractor's is no longer working at the FCC.

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 FCC is in the process of determining the appropriate NARA records retention and disposal schedule for this new SORN.

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 Space Management Center staff is working with PERM to determine the appropriate records retention and disposal schedule, *etc.*, which will be included in the forthcoming system of records notice (SORN).

If this is a new System of Records Notice (SORN), please skip to **Section 3.0 Development, Management, and Deployment/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 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 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 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 SOR 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 in the SOR?

☐ Yes
☐ No

Please explain your response:

2.6 Have there been any changes to the purposes for collecting, maintaining, and using the information in the SOR?

☐ 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 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:
☐ Others Routine Use disclosures not listed above:

2.8 Have there been any changes to whether the FCC will permit the information to 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 in this SORN?

☐ Yes
☐ No

Please explain your response:

2.10 Have there been any changes to how the information in the 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 in the SORN?

☐ Yes
☐ No

Please explain your response:

Please note that you should 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, and 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/Sharing of the Information:

3.1 Who will develop the information system(s)?

☐ 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, please specify:

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 Space Management Center (SMC) staff has responsibility for access and proper use of the information.
☐ 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 SMC works with the appropriate senior management to determine users and access rights.

3.5 How much access will users have to data in the information system(s)?

- ☐ Access to all data:
- ☒ Restricted access to data, as determined by the information system manager, administrator, and/or developer:
- ☒ Other access policy: The Space Management Center's staff determines the appropriate level of access based on a "need to know" basis and functional requirements.

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:
- ☐ Information system administrators:
- ☐ Information system developers:
- ☒ FCC staff in this bureau/office:
- ☒ FCC staff in other bureaus/offices: The Assistant Bureau Chief for Management (ABC) in the bureau/office that provides the information.
- ☐ FCC staff in other bureaus/offices in FCC field offices:
- ☒ Contractors: The contractors who manage the IT systems that hold the information.
- ☐ Other Federal agencies:
- ☐ State and/or local agencies:
- ☐ Businesses, institutions, and other groups, please specify which group(s):
- ☐ 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 contractors.

3.8 Has the Office of the General Counsel (OGC) signed off on any Section M contract(s) for the database?

- ☐ Yes
- ☐ No

Please explain your response:

3.9 Does the information system 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 information in the FCC's Cadapult Space Management System (CSMS) is limited to FCC's space management data needs and uses–there is no data sharing with other parties.

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 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:

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
☐ Revised matching agreement

Please explain your response:

3.15 Has the matching agreement been review and approved (or renewed) by the FCC's Data Integrity Board, which has administrative oversight of 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 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 was collected.
☐ Information is reliable for its intended use(s).
☐ Information is accurate.
☐ Information is complete.
☐ Information is current.
☒ Not applicable.

Please explain any exceptions or clarifications:

The CSMS information is provided via intra-agency uses. The FCC's Space Management Center staff rely on the bureaus and offices to provide accurate information, and any errors in the information that they provide will be recognized quickly.

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:
  ☐ Information is processed and maintained only for the purposes for which it was collected:
  ☐ Information is reliable for its intended use(s):
  ☐ Information is accurate:

☐ Information is complete:
☐ Information is current:
☐ No information comes from non-FCC sources:

4.3 If the information is being aggregated or consolidated, what controls are in place to insure that the information is relevant, accurate, and complete?

☐ Not applicable.

Please explain your response:

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?

☐ Not applicable.

Please explain your response:

4.4 What checks are used to verify that the Data Quality guidelines are met?

4.5 How often are these policies and procedures checked routinely—what type of annual verification schedule has been established?

Section 5.0 Safety and Security Requirements:

5.1 How is the information in the information system stored and maintained?

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

5.3 Is the information system part of another FCC information system that collects personally identifiable information (PII)?

☐ Yes
☒ No

Please explain your response:

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 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:

Lack of the information in the Cadapult Space Management System (CSMS) would impact the FCC's daily operations, space management needs.

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 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:

The Capadult Space Mangement System does not include any external access portals.

If there are no externally facing information system portals, please skip to Question 5.10.

5.9 If the information is collected via 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:
☐ 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—specifies 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 a customer-facing web site not on www.fcc.gov?

☒ Yes
☐ No

Please explain your response:

The Cadapult Space Management System has a intra-FCC customer-facing data entry portal that is not accessable outside the FCC IT network.

If there is no customer-facing web site(s) please skip to Question 5.15.

5.12 If the information system has a customer-facing web site, does this web site(s) have a Privacy Act Notice and how is it displayed?

☒ Yes
- ☒ Notice is displayed prominently on this 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—specifies 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:

5.14 If information is collected from FCC employees and contractors on line via the FCC Intranet, which of these applicable:

- ☒ Not applicable
- ☐ Link to the FCC's privacy policies via www.FCC.gov.
- ☐ Privacy notice displayed on the webpage
- ☐ Privacy notice is printed at the end of the FCC form
- ☐ Website uses other method(s) to alert users to the Privacy Act Notice, as explained below:

☐ No link or notice, please explain why not:

If information is not collected via the FCC Intranet, please skip to Question 5.16.

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

- ☐ Not applicable
- ☐ 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—specifies 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:

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

☐ Privacy notice is on the document.
☐ Statement on the document notifies the recipient that they may read the FCC Privacy Notice on www.fcc.gov.
☐ Other, please specify:
☒ Not applicable, as personal information will not be collected.

If there is no access to the information system from outside the FCC, please skip to Question 5.18.

5.17 If consumers may access the information and/or the information system on-line, does it identify ages or is it directed to people under 13 years old?

☐ Yes
☐ No

Please explain your response:

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

☐ Yes
☒ No

Please explain your response:

5.19 Do individuals have the right to decline to provide personal information?

☐ Yes
☒ No

Please explain your response:

The FCC's Cadapult Space Management System (CSMS) is an administrative management tool to manage space holdings.

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

☐ Yes
☒ No

Please explain your response:

If individuals do not have the right to consent to the use of their information, please skip to Question 5.24.

5.21 If so, how does the individual exercise this right?

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

5.23 What kinds of reports can the information system and/or the information be used to produce on the individuals whose data are in the system?

The Cadapult Space Management System (CSMS) can provide information on scheduled moves by date and history; vacancy reports; occupancy data by bureau/office; occupancy by building and floor; and organization report data.

5.24 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, please explain your response:
- ☐ 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, please explain your response:

5.25 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 work with the Cadapult Space Management System are required to complete privacy training. In addition the Space Management Center (SMC) staff emphasizes to those with access that this information is not to be shared or disclosed.

5.26 How often are security controls reviewed?

- ☐ Six months or less
- ☒ One year
- ☐ Two years
- ☐ Three years
- ☐ Four years
- ☐ Five years
- ☐ Other, please explain your response:

5.27 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
- ☐ Two years
- ☐ Three years
- ☐ Four years
- ☐ Five years
- ☒ Other, please explain your response: 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 5.29.

5.28 What are the safeguards to insure that there are few opportunities for disclosure, unavailability, modification, damage to the information system, and/or prevention of timely performance of FCC operations if operational training is not provided?

5.29 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
- ☐ Two years
- ☐ Three or more years
- ☒ Other re-certification procedures: The FCC's Space Management Center staff periodically emphasizes to those who work with the Cadapult Space Management System (CSMS) database that the CSMS and its information fall under the Privacy Act.

5.30 Do the Commission's training and security requirements for this information system conform to the requirements of the Federal Information Security Management Act (FISMA)?

- ☒ Yes
- ☐ No

Please explain your response:

The FCC's Space Management Center's Cadapult Space Management System and its procedures will conform to FISMA requirements.

If the Privacy Threshold Assessment was completed recently as part of the information system's evaluation, please skip to Question 5.35.

5.31 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:

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

☐ Yes
☐ No

Please explain your response:

5.33 Has a "Certification and Accreditation" (C&A) been completed?

☐ Yes
☐ No

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

5.34 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:

5.35 Is the system using technology in ways that the Commission has not used previously, *i.e.*, Smart Cards, Caller-ID, *etc*?

☐ Yes
☒ No

Please explain your response:

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

The information in the Cadapult Space Management System database is limited to very minimal data to manage the FCC's space holdings. There is no effect on the general public's privacy and little affect on the privacy of FCC employees and contractors. Access is limited by IT security measures and those who have been given authorization.

5.37 Will the information system include a capability to identify, locate, and/or monitor individuals?

☒ Yes
☐ No

Please explain your response:

While the Cadapult Space Management System (CSMS) does include information on the location of employees and contractors in FCC space, the CSMS does not possess any technology, "electronic" or otherwise, to monitor individuals in their offices and workstations.

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):**

5.38 If the information system includes these capabilities identified in Question 5.36 above, what kinds of information will be collected as a function of the monitoring of individuals?

5.39 Does the information system 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 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, *e.g.*, fill out forms and/or licensees; participate in surveys; and or maintain records

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:

☒ 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 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 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 system of records notice (SORN), do the form(s) 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 the system of records 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:

7.2 Are the procedures for individuals to gain access to their own information in this system of records notice 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:

This is a new SORN. Individuals seeking access to the information about them in the Cadapult Space Management System (CSMS) should contact the system manager or their assistant chief for management in their bureau/office, which is consistent with FCC policies and rules under 47 CFR §§ 0.554 – 0.555.

7.3 Are the procedures for individuals seeking to correct or to amend information about them in this system of records notice 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:

This is a new SORN. Individuals who wish to be notified of the procedures for amending or correcting information about them in the Cadapult Space Management System (CSMC) should contact the system manager or their assistant chief for management in their bureau/office.

7.4 Does the FCC provide any redress to amend or correct information about an individual in this system of records notice, 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:

Not applicable, as this is a new 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 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:

The Cadapult Space Management System is a new system of records notice. There are no exemptions to the notification, access, and corretion/amendment procedures.

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 SORN that is being updated or revised?

The Space Management Center (SMC) has posted notices that the information in the Cadapult Space Management System database is "non public for internal use only." The SMC also issues reminders periodically to those granted access to the information that they are to keep the information confidential and to safeguard any printed materials.

7.8 How often is the 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 bureaus/offices are responsible for ensuring the accuracy and completeness of the information that they provide to the Space Management Center staff that maintains the Cadapult Space Management System. The Space Management Center staff sends out e-mail notices periodically to remind them of the sensitivity of the data.

Section 8.0 Consumer Satisfaction:

8.1 Is there a customer satisfaction survey included as part of the public access to the information?

☐ Yes
☐ No
☒ Not applicable

Please explain your response:

The Cadapult Space Management System (CSMS) is an administrative information system that is used solely to manage the FCC space holdings. The CSMS is also used in the event that an emergency or other situation arises that requires the FCC to relocate its employees and/or contractors to other building and facilities.

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, and what practices and procedures have you adopted to minimize them?

Risks:	Mitigating factors:
a. B/Os not updating data.	a. Periodic reminders to update data.
b. Personally Identifiable Information (PII) is stored in this information system	b. Information is protected on PCs requiring login's and access rights; and there is little impact to individual privacy since the PII that is stored in this system is "low security"s
c. Access to information on a laptop	c. Password protected
d.	d.

9.2 What deficiencies did the bureau/office find in its procedures for evaluating the information system(s) and what remedies did the bureau/office enact following this PIA?

Deficiencies:	Remedies:
a. Privacy information	a. Periodic training/notice to be implemented on a standard basis
b.	b.
c.	c.
d.	d.
e.	e.

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

Initial implementation: On-going since Fall 2005
Secondary implementation:
Tertiary implementation:
Other implementation:

9.4 Are there any ancillary and/or auxillary information system applications linked to this information system that also require a Privacy Impact Assessment?

☐ Yes
☒ No

If so, please state what the application is, if a Privacy Impact Assessment has been done, and the date that the Privacy Impact Assessment was completed:

Certification:

I as the information system owner or custodian will ensure that the FCC's information security and privacy policies, guidelines, and procedures are followed in the development, integration, operation, and maintenance of this information system.

Mary Kay Welch Mgr, Space Management Center 3/27/07
[Information System Owner or Custodian, Title, and Date (MM/DD/YYYY)]

Leslie F. Smith 03/23/2007
[Privacy Analyst and Date (MM/DD/YYYY)]