ADAMS ML16291A339

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

Space and Property Management System (SPMS)

Date: October 17, 2016

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

The Space and Property Management System (SPMS) is owned and operated by the Office of Administration (ADM) to manage NRC office space, property asset inventory, visitor access requests, and employee headquarter parking assignments.

SPMS was developed using a building information modeling (BIM) software that includes infrastructure and facilities management solutions called ARCHIBUS 21.3. SPMS consist of four (4) web-based modules that manages and designs office spaces within NRC for all sites; tracks allocation and inventory of NRC property assets; allows advance visitor access and visitor parking requests to be made by NRC staff; and administers the NRC HQ employee parking assignments/permits and monthly fees.

2. What agency function does it support?

SPMS ensures that the Federal Property and Administrative Services Act is properly executed by NRC for government furnished equipment that is either sensitive or over one thousand in purchase value. Guidance for equipment is prescribed under Management Directive 13.1. SPMS is also designed to adhere to agency and Federal regulations for space and facilities management available under Management Directive 13.2. Guidance for visitor access to NRC facilities is available within Management Directive 12.1. SPMS ensures that only authorized visitors have access to NRC facilities in order to assure the safety and security of NRC facilities; and supports the NRC's policy to manage a parking program that supports the need for parking at Federal facilities.

3. Describe any modules or subsystems, where relevant, and their functions.

Property Management Module

The Property Management module tracks all government furnished equipment that is considered sensitive or is valued over one thousand dollars. Qualified equipment is tracked from purchase to disposal. The Property Management

module tracks all furniture purchases and warehouse operations. The ultimate goal of the Property Module is to ensure that all properties monitored by NRC, owned or capitalized, are managed appropriately with the sufficient level of safeguards to prevent waste, fraud, abuse, and mismanagement. Property Custodians utilize SPMS to update property information. The entire lifecycle of the equipment is tracked within SPMS.

Space and Facilities Management Module
The Space and Facilities Management module enables the efficient utilization of the NRC office space at headquarters and the four regional offices. NRC must continuously monitor the current use of NRC office space while working with the NRC offices and Regions to identify and plan for their upcoming space requirements. The space design process entails considering each office's current allocation of office space against their current and projected organizational and functional requirements in order to plan appropriate adjustments to their space allocation and/or configuration. These office representatives have online access to SPMS to review data and provide ADM with proposed information updates.

Visitor Access Request System
The Visitor Access Request System (VARS) module enables NRC guards and users to create and track visit requests. Each visitor's name and company are identified in the system. All visitors at headquarters are entered in SPMS. ADM manually verifies visitors entered against the Government Watch List to ensure that suspected felons do not have access to NRC facilities. For classified meetings, only visitors with the appropriate level of clearance are permitted to attend. A visitor's level of clearance is also verified against a separate system called Personnel Security Adjudication Tracking System (PSATS). SPMS also serves as the historical log of previous visits to ensure proper oversight of facility security.

Parking Management Module
The Parking Management module allows ADM to administer the processing and distribution of monthly employee-only parking passes for parking spaces at headquarters. This ensures an equitable assignment of onsite parking spaces and fulfills facility security requirements in accordance with Federal Management Regulations and NRC specific rules, regulations, and policies.

4. What legal authority authorizes the purchase or development of this system?

Due to the extensive features available within SPMS each of the aforementioned modules is governed by a separate set of laws and regulations.

Property Management Module
Federal Property Management Regulation (FPMR) managed by General Services Administration encompasses the following regulations:

Federal Acquisition Regulation specifically 48 CFR Part 45, Federal Acquisition Regulations System, "Government Property."

41 Code of Federal Regulation (CFR) : 101-25.100, "Use of Government Personal Property and Nonpersonal Services"; 101-25.301, "General"; 101-

25.302, “Office Furniture, Furnishings, and Equipment”; 101-26.2, “Federal Requisitioning System”; 101-45, “Sale, Abandonment, or Destruction of Personal Property”; 102-36, “Transfer of Excess Personal Property”; 102-37, “Donation of Surplus Personal Property”; and 102-38, “Sale of Personal Property”.

40 United State Code: 483 - Property Utilization; 487 - Surveys of Government Property and Management Practices; and 506 - Inventory Controls and Systems

Executive Order 12999, “Educational Technology, Ensuring Opportunity for All Children in the Next Century,” April 17, 1996, and Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” January 24, 2007.

Space and Facilities Management Module

36 CFR Part 1191, “Americans with Disabilities Act (ADA) Accessibility Guidelines for Buildings and Facilities; Architectural Barriers Act (ABA) Accessibility Guidelines.”

41 CFR: Chapter 101, “Federal Property Management Regulation,” Subchapter D, “Public Buildings and Space”; Part 102-73, “Real Estate Acquisition”; Part 102-74, “Facility Management”; Part 102-76, “Design and Construction”; Part 102-79, “Assignment and Utilization of Space”; and Part 102-85, “Pricing Policy for Occupancy in GSA Space.”

48 CFR 23.2, “Energy and Water Efficiency and Renewable Energy.” Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” January 24, 2007. Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” October 5, 2009. 13576, “Delivering an Efficient, Effective, and Accountable Government,” June 13, 2011.

5 U.S.C. 301 - Government Organization and Employees

Visitor Access Request System

Visitor access security measures are governed by The Atomic Energy Act of 1954, as amended, the Energy Reorganization Act of 1974, as amended.

10 CFR: Part 25, “Access Authorization”; Part 95, “Facility Security Clearance and Safeguarding of National Security Information and Restricted Data”; Part 160, “Trespassing on Commission Property.”

41 CFR Part 101, “Federal Property Management Regulations.”

National Industrial Security Program Operating Manual (NISPOM), Department of Defense 5220.22M, February 28, 2006, and Supplement 1, April 1, 2004.

Department of Justice’s (DOJ’s) Vulnerability Assessment of Federal Facilities, June 28, 1995.

Director of Central Intelligence Directive 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs),” November 18, 2002.

E.O. 10865, as amended, “Safeguarding Classified Information within Industry,” February 20, 1960.

E.O. 12829, “National Industrial Security Program” (NISP), January 6, 1993.

E.O.12958, as amended, “Classified National Security Information,” April 17, 1995.

E.O. 13142, “Amendment to Executive Order 12958 - Classified National Security,” November 19, 1999.

E.O. 13292, “Further Amendment to Executive Order 12958, As Amended, Classified National Security Information,” March 25, 2003.

E.O. 12968, “Access to Classified Information,” August 2, 1995.

Interagency Security Committee (ISC) Security Criteria for New Federal Office Buildings and Major Modernization Projects.

Intelligence Community Standard No. 705-1, “Physical and Technical Security Standards for Sensitive Compartmentalized Information Faculties.”

National Security Agency (NSA) performance requirements for High Security Crosscut Paper Shredders - NSA/CSS Evaluated Products List for High Security Crosscut Paper Shredders.

NACSI 4005, “Standard Criteria for Safeguarding Communications Security Material,” August 22, 1973.

FIPS PUB 201-1, Federal Information Processing Standards Publication, “Personal Identity Verification (PIV) of Federal Employees and Contractors.”

Homeland Security Presidential Directive 3, “Homeland Security Advisory System,” March 11, 2002.

Homeland Security Presidential Directive 12, “Policy for a Common Identification Standard for Federal Employees and Contractors,” August 27, 2004.

Presidential Decision Directive 63, “Critical Infrastructure Protection,” May 22, 1998.

Security Policy Board, Executive Branch Provisions of the NISP, September 19, 1996.

USC Title 18: Crimes and Criminal Proceedings (Title 18) and Electronic Communications Privacy Act of 1986 (EPCA) (18 U.S.C. 2510 et seq.).

USC Title 42: Americans With Disabilities Act of 1990 (ADA) (42 U.S.C. 12101 et seq.) and Energy Reorganization Act of 1974, as amended (42 U.S.C. 5801 et seq.).

USC Title 47: Communications Assistance for Law Enforcement Act of 1994 (CALEA) (47 U.S.C.1001 et seq.).

USC Title 50: Coordination of Counterintelligence Activities (50 U.S.C. 402a) and Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

USC Title 44: Federal Information Security Management Act of 2002 (FISMA) (44U.S.C. 3541 et seq.).

USC Title 5: Freedom of Information Act (5 U.S.C. 552); Inspector General Act of 1978 (5 U.S.C., App. 3); and Privacy Act of 1974, as amended (5 U.S.C. 552a).

Homeland Security Act of 2002 (6 U.S.C. 101 et seq.).

Electronic Communications Privacy Act of 1986 (ECPA, codified at 18 U.S.C. 2510 2522) was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. Specifically, ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute), which was primarily designed to prevent unauthorized government access to private electronic communications.

10 CFR: Part 25, “Access Authorization”; Part 95, “Facility Security Clearance and Safeguarding of National Security Information and Restricted Data.”

Parking Management Module
10 CFR Title 41, Subtitle C-Chapter 102-Subchapter C – Part 102-74-Subpart C, Code of Conduct – Federal Facilities Owned and Leased by the General Service Administration. The information is also required to administer Qualified Transportation Benefits to comply with the Americans with Disabilities Act of 1990, NRC Management Directive 13.4, “Transportation Management,” and Collective Bargaining Agreement 39.

5. What is the purpose of the system and the data to be collected?

SPMS is intended to support NRC's space management, property management, parking management and provide NRC with the means to schedule, record, and thus control visitor access to its facilities.

6. Points of Contact:

Technical Project Manager	**Office/Division/Branch**	**Telephone**
Karen Cudd	ADM/PMDA/IT	301-415-5362
Business Project Manager	**Office/Division/Branch**	**Telephone**
William Harris (SPACE)	ADM/ADSC	301-415-0072
Charlemagne Grimes (PROPERTY)	ADM/ADSC	301-415-8422
Joseph Widdup (Parking)	ADM/DAS/ASC	301-415-3316

Denis Brady (VARS)	ADM/DFS/FSB	301-415-5768
Information System Security Officer (ISSO)	**Office/Division/Branch**	**Telephone**
Diem Le	ADM/PMDA/IT	301-415-7114
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Cynthia Carpenter	ADM	301-415-8747

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ___ New System **_X_ Modify Existing System** ____ Other (Explain)

b. If modifying an existing system, has a PIA been prepared before?

Yes

(1) If yes, provide the date approved and ADAMS accession number.

ML11199A001 – PMIS 7/5/11
ML14084A009 – SPMS 3/20/14

(2) If yes, provide a summary of modifications to the existing system.

Updated to the most current PIA template and to add the Parking Management modules to the SPMS subsystem boundary.

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

Yes

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public).

Federal employees, contractors, licensees, and visitors to the NRC.

b. What information is being maintained in the system about an individual (be specific)?

Within SPMS the following information is stored only for active employees and contractors: the employee/contractor first name, middle name, last name, suffix, LAN ID, position title, employee status, organization, office telephone number, duty station, mailstop, email address, employee effective date and employee type. Retired or departing employees are purged from the system unless government owned property was lost under his/her custody. Departed contractors are immediately purged from the system.

The following information is stored only for employees and is not available for contractors: grade, employee number, pay plan, grade, occupational series, supervisor's status, and bargain unit indicator.

All visitors must furnish the following information when being registered in SPMS: first name, last name, company, start date of visit, end date of visit, NRC contact name, NRC contact phone number, location of the visit, nationality, visitor type, meeting access level, and when feasible a scanned copy of the identification card used such as a driver's license.

With the addition of Parking Management the following information is maintained office telephone number, vehicle tag number, office work hours, NRC service computation date, and check box indicating need for handicap assigned space.

c. Is information being collected from the subject individual?

Yes

(1) If yes, what information is being collected?

All visitors must furnish the following information when being registered in SPMS: first name, last name, company, start date of visit, end date of visit, NRC contact name, NRC contact phone number, location of the visit, nationality, visitor type and meeting access level. If the visitor is attending a meeting where sensitive or classified information is shared, the visitor must be marked as having the sufficient level of clearance in order to obtain a badge. The visitor is encouraged, but not required, to furnish the following data: middle initial, visitor cell phone, visitor email address, purpose of visit, car make, license plate, NRC escort, parking spot reservation duration (All Day, AM-Parking, PM-Parking) and additional comments. If an NRC visitor furnishes his/her driver's license as identification, then, when feasible, the guard attaches the image to the visitor's record within SPMS. The driver's license images are automatically deleted six years after each visit by a prescheduled cron job. An image of the visitor's driver's license (which is Personally Identifiable Information (PII)) is kept in the system for six years in cases of inquiries regarding the visitor

subsequent to the visit.

For employee parking requests, applications are required to fill out the NRC Form 505, “Application for Parking”, which includes: individual’s name, vehicle tag number, office organization, office mail stop, office telephone number, office e-mail, office work hours, NRC service computation date, and check box indicating need for handicap assigned space.

d. Will the information be collected from 10 or more individuals who are <u>not</u> Federal employees?

Yes

(1) If yes, does the information collection have OMB approval?

The information collected does not require OMB approval. The information collection is limited to the information necessary to identify a visitor and therefore, no OMB clearance is needed. In addition, a request for a driver’s license is exempt from Paperwork Reduction Act requirements, because it is a physical object.

e. Is the information being collected from existing NRC files, databases, or systems?

Yes

(1) If yes, identify the files/databases/systems and the information being collected.

On a weekly basis the Office of the Chief Human Capital Officer (OCHCO) extracts from Federal Personnel/Payroll System (FPPS), two pipe-delimited files containing NRC employee and NRC organization information in downloadable form to an SPMS directory. FPPS and SPMS are not integrated into SPMS but their files are loaded into SPMS. On a nightly basis, SPMS also uploads an Active Directory file furnished by Office of the Chief Information Officer (OCIO) containing the LAN identification and email address of users classified as NRC employees and contractors.

On a weekly basis, FPPS provides a pipe-delimited file containing organizational code, employee name, employee number, pay plan, grade, occupational series, supervisor status, bargaining unit indicator, email address, first name, middle name, last name, suffix, LAN ID, employee status, employee title, duty station, employee effective date and employee type. FPPS also furnishes another pipe-delimited file containing organization codes, office divisions and branch codes. SPMS also uploads an Active Directory file containing the LAN identification and email address of users categorized as NRC employees and contractors on a nightly basis. The data is made available from OCIO.

f. Is the information being collected from external sources (any source outside of the NRC)? No

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

OCHCO will verify the employee data and the organization data following Federal and NRC regulations and requirements. OCIO will verify all LAN account and email address following Federal and NRC requirements.

h. How will the information be collected (e.g. form, data transfer)?

All files containing NRC employee and NRC organization information in downloadable form will be transferred to an SPMS directory then loaded into SPMS through prescheduled cron jobs.

Parking Management Module
All applicants are required to complete and submit NRC Form 505, "Application for Parking," or the NRC Form 505A, "Application for Handicap Parking," as applicable. Information is manually entered into the Parking Management by ADM/DAS.

2. INFORMATION NOT ABOUT INDIVIDUALS

a. Will information not about individuals be maintained in this system?

Yes

(1) If yes, identify the type of information (be specific).

FPPS furnishes a pipe-delimited file containing organization codes, office divisions and branch codes. CAD drawings of NRC facilities are imported in SPMS and can be viewed within SPMS. CAD drawings contain the following data elements: location, building, floor, room number, room area, and room area standards. The **Property Module** maintains information regarding Government Furnished and Government Leased Equipment such as: office, organization code, building, floor, room number, purchase order number, property tag number, item description, serial number, model number, acquisition cost, acquisition date, Major/Minor class number, manufacturer, property custodian, document reference number, requisition and/or purchase order number and Organizational Account Code. VARS stores information about parking spaces.

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

SPMS does not obtain data from an external source. Floor plans such as CAD drawings are compiled by the Space Design Branch within the Office of Administration. Information regarding Government Furnished and Government Leased Equipment is furnished by the Property Management

Branch based on invoices, purchase agreements, and packing slips.

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

SPMS data is used for space design and allocation; property management inventory tracking; NRC visitor monitoring and employee parking assignments. The functionalities of each module is discussed in more detail below:

Space and Facilities Management Module

The Space Design Branch staff use the data on a daily basis in conjunction with their duties as space planners and designers. The Space Management Domain is broken down into two different activities: Space Inventory and Performance, compiling an inventory of spatial locations with maps, and Personnel and Occupancy, assigning of people to spatial areas. The space planning system focuses on two components of general-purpose office space: the primary (or people occupied) areas, and the office support areas. SPMS contains data needed to perform a space requirements analysis. This analysis identifies the functions to be performed in the space and triggers the space allocation formula and design criteria from the databases. Also identified in the analysis are: (1) any special organizational requirements; (2) existing architectural and design conditions; and (3) adjacency requirements. By automating the process of constructing the space requirements analysis, space planners can respond quickly to customer requests for space changes in the near term as well as conduct an iterative "what-if" scenario involving large blocks of space composed of many workstations and multiple organizations. The primary system users consist of the DFS/SPPMB management and design staff, but each program office has a representative who can access the data in the system.

Property Management Module

Equipment records from purchase to disposal are monitored within the Property Module. The following types of transactions are tracked under Property: equipment, furniture, and supplies. The ultimate goal of the Property Module is to ensure that all properties monitored by NRC, owned or capitalized, are managed appropriately with a sufficient level of safeguards to prevent waste, fraud, abuse, and mismanagement. SPMS provides controls to prevent duplication of property tag numbers and audit trails for all property transactions, including the identification of the individual entering a record in the system, and including the capability to archive all such transactions. User roles and workflow are available within SPMS to safeguard against unauthorized access and to ensure that only authorized users have access to the assigned equipment.

SPMS also calculates depreciation for capitalized equipment. Reports and ad hoc queries can be generated from SPMS.

Visitor Access Request System

The VARS collects data about requests for visits, visitor parking, and arrivals and departures of visitors at NRC. The goal of VARS is to ensure that Level Four

Facility guidelines are properly executed at NRC. Visitor information is captured and verified manually against the Criminal Watch List or Terror Watch List. For classified meetings, VARS checks that only visitors with the appropriate level of clearance are permitted to attend. The Facilities and Security Branch is immediately notified when a foreign national is registered in VARS. Badges have time limits which ensure that they cannot be used longer than the duration permitted.

Parking Management Module
The information is used to determine the utilization of parking spaces, fees collected, and prioritization of applicants. NRC captures office telephone numbers, and vehicle tag number in case the owner of the vehicle needs to be contacted.

2. Is the use of the data both relevant and necessary for the purpose for which the system is designed? Yes

3. Who will ensure the proper use of the data in this system?

The System Owner, Business Project Manager, Information System Security Officer, System Administrator, and Network Administrators will ensure proper use of the information in the system.

4. Are the data elements described in detail and documented? Yes

a. If yes, what is the name of the document that contains this information and where is it located?

Yes, the SPMS Data Dictionary is stored in the NRC Rational Jazz.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier? (Be specific.)

SPMS monitors the location of government furnished equipment, space allocation to employees and space utilization. The aforementioned information is not Personally Identifiable Information. Data will be retrieved by requesting one of the standard reports available to authorized users. NRC employees and authorized contractors can also locate the official duty station of the employees and this information is publicly available. Only a very limited user community has access to visitors and their visits. User access is reviewed on a quarterly basis.

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No, this system does not provide real-time data that could identify and locate an employees. Within the Visitor Access Request Module, the option exists to see

whether the visitor is still on site at NRC, however, specific location, such as building or room is not available.

8. List the report(s) that will be produced from this system.

a. What are the reports used for?

Space and Facilities Management Module
To determine occupancy levels and where offices are located as well as for future space scenarios such as:

- Office specific workstations Report
- Office specific employees Report
- Office specific square footage Report
- Office specific vacant offices Report

Property Management Module
To be able to track all information concerning property and equipment purchased by the NRC such as:

- Acquisition Report
- Requisitions Report
- Active Records Report
- Excess Report
- Depreciation Report

Visitor Access Request System
Visitor Access Module tracks all visit requests and visitor arrivals and departures. The reports are developed to ensure that only authorized visitors have access to NRC facilities.

- Visitor Parking Report
- Visitor Log (by Name, Date, Location, etc.)
- Visitor by Country (not USA)
- Classified Visitor
- Prox Cards Not Returned
- NRC Contact Visited

Parking Management Module
Since there is a limited inventory of parking spaces, reports are utilized to perform reconciliation to ensure that Management Directives 13.4 and Article 39 Collective Bargaining Agreement have been adhered to regarding the distribution of monthly parking spaces to NRC employees and contractors.

- Permits by Request Type
- License Tags
- Carpool Members
- Parking Applicants by Request Type
- Handicap Report
- Monthly Parking Collection Totals
- Schedule of Parking Collections
- Lost Permit Log

- Monthly Parking Ticket Distribution
- Monthly Parking List by Name
- Monthly Parking List by Permit
- Current Month Non-Payers
- Monthly Parking Log

b. Who has access to these reports?

Depending on user roles which are reviewed by the System Administrator every quarter, user will have access to different reports. Users with elevated access will have access to additional reports.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

***Space and Facilities Management Module*:** Individuals from ADM/Directorate for Space Planning and Consolidation (DSPC) with assigned duties.

Property Management Module: Individuals from ADM/Division of Facilities and Security (DFS) with assigned duties, such as IT Coordinators and Property Custodians. User access is monitored by the Property Labor Services Branch within Office of Administration.

Visitor Access Request Module: All NRC employees and approved contractors with the privilege to escort visitors have the ability to enter a visitor entry. Their level of access to the system will depend upon their roles.

Parking Management Module: Individuals from ADM/Division of Administrative Services (DAS) with assigned duties.

a) For what purpose?

Space and Facilities Management Module is utilized by Space Coordinators to determine occupancy levels and where offices are located as well as for future space scenarios.

Property Management Module is used to track all information concerning the entire life cycle of equipment purchased by the NRC in compliance with agency mandates and federal regulations.

Visitor Access Request System is used to track all visit requests and visitor arrivals and departures. The reports are developed to ensure that only authorized visitors have access to NRC facilities.

Parking Management Module is used to prioritize and assign employee parking spaces and monitor monthly fee collections.

b) Will access be limited?

Yes

2. Will other NRC systems share data with or have access to the data in the system?

Yes

a) If yes, identify the system(s).

Pandemic System located at Region II

b) How will the data be transmitted or disclosed?

ODBC export

3. Will external agencies/organizations/public have access to the data in the system?

No

E. RECORDS RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and are required under 36 CFR 1234.10. The following questions are intended to determine whether the records in the system have an approved records retention schedule or if one will be needed.

1. Can you map this system to an applicable retention schedule in NUREG-0910, or the General Records Schedules at http://www.archives.gov/records-mgmt/grs ?

Yes

a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished. For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to a file for transfer based on their approved disposition?

Space Module

GRS 11.1 - "Space and Maintenance General Correspondence Files"

- Destroy when 2 years old. (N1-GRS-96-1, item 1c)

GRS 11.2 – "Agency Space Files"

Records relating to the allocation, utilization, and release of space under agency control, and related reports to GSA.

a) Building plan files, surveys, and other records utilized in agency space planning, assignment, and adjustment.
   - Destroy 2 years after termination of assignment, or when lease is canceled, or when plans are superseded or obsolete. (GRS 11, 1952, item 2a)

b) Correspondence with and reports to staff agencies relating to agency space holdings and requirements.

(1) Agency reports to the GSA, including Standard Form (SF) 81, Request for Space, and related documents.
   - Destroy when 2 years old. (GRS 11, 1952, item 2b1)

(2) Copies in subordinate reporting units and related work papers.
   - Destroy when 1 year old. (GRS 11, 1952, item 2b2)

<u>Property Module</u> - GRS 4.1 - "Property Disposal Correspondence Files"
- Destroy when 2 years old. (GRS 4, 1952, item 4)

<u>Visitor Access Module</u> - GRS 18.17a&b - "Visitor Control Files"
Registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers.

a. For areas under maximum security.
   - Destroy 5 years after final entry or 5 years after date of document, as appropriate. (GRS 18, 1960, item 18)

b. For other areas.
   - Destroy 2 years after final entry or 2 years after date of document, as appropriate. (GRS 18, 1960, item 18)

<u>Parking Management</u> – GRS 11.4 – "Credential Files"
Identification credentials and related papers.

a. Identification credentials including cards, badges, parking permits, photographs, agency permits to operate motor vehicles, and property, dining room and visitors passes, and other identification credentials.
   - Destroy credentials 3 months after return to issuing office. (GRS 11, 1952, item 4a)

b. Receipts, indexes, listings, and accountable records.
   - Destroy after all listed credentials are accounted for. (GRS 11, 1952, item 4b)

b. If the answer to question E.1 is yes, skip to F.1. If the response is no, complete question E.2 through question E.7.

2. If the records <u>cannot</u> be mapped to an approved records retention schedule, how long do you need the records? Please explain.

3. Would these records be of value to another organization or entity at some point in time? Please explain.

4. How are actions taken on the records? For example, is new data added or updated by replacing older data on a daily, weekly, or monthly basis?

5. What is the event or action that will serve as the trigger for updating, deleting, removing, or replacing information in the system? For example, does the information reside in the system for three years after it is created and then is it deleted?

6. Is any part of the record an output, such as a report, or other data placed in ADAMS or stored in any other location, such as a shared drive or MS SharePoint?

7. Does this system allow for the deletion or removal of records no longer needed and how will that be accomplished?

F. TECHNICAL ACCESS AND SECURITY

1. Describe the security controls used to limit access to the system (e.g., passwords).

The system resides behind the NRC network firewall. The user must first gain access to NRC network via valid user name and password. Single sign on via Active Directory is implemented and access is further restricted by user role. User must be cleared with a minimum of IT II system access to gain access to NRC network and the role will determine the amount of information the user can access. The role is reviewed every quarter and access is deactivated for contractors not logging into SPMS within any 90-day period.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

Password protection and assignment of all users to role-based access groups.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

Yes

a. **If yes, where?**

Security measures are partly described in a Security Plan for Moderate ADM Support Systems (MASS). In addition to the Security Plan, the procedures are described in the user procedure.

4. Will the system be accessed or operated at more than one location (site)?

Yes

a. If yes, how will consistent use be maintained at all sites?

SPMS is accessible via the NRC Intranet. The level of access for each module is managed through role-based access privileges.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

System Administrators, space coordinators, property custodians, parking administrators, and NRC staff who submit visit requests or check visitors in and out.

The following are SPMS-defined access groups:

System Administrator
NRC No Role
NRC System Administrator
Parking Admin
Parking Admin – Daily
Parking Admin – Monthly
Parking Applicant
Parking Attendant
Property Custodian, Space Coordinator
Property Custodian, Space Coordinator and VARS Security
Property Administrator
Property Custodian
Property Custodian and VARS Administrative Services
Property Custodian and VARS Security
Property Group
Property Other
Space Administrator
Space Coordinator
Space Coordinator and VARS Commission Staff
Space Coordinator and VARS Security
Space Group
Space Group and no VARS Access
Space Other
Space Other – No VARS
Space Property Administrator
Space Property Administrator and VARS Security
Space Property Other
VARS
VARS Administrative Services
VARS Commission Staff
VARS Parking Attendant
VARS Security
VARS Service Desk
VARS Staff
VARS Visitor
Warehouse
Warehouse and Property Custodian

6. Will a record of their access to the system be captured?

Yes

a. If yes, what will be collected?

User access will be captured in the audit logs along with time and date of transaction.

7. Will contractors be involved with the design, development, or maintenance of the system?

Yes

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or PII contract clauses are inserted in their contracts.

- *FAR clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*
- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

8. What auditing measures and technical safeguards are in place to prevent misuse of data?

Audit logs capture the date and time an entry is processed in SPMS. The Employee table has fields recording when a record was updated last by Active Directory. For each module, there exists only one point of entry. NRC Data Center conducts nightly tape backups of the system. All data imported from external systems is stored for historical auditing purposes.

9. Are the data secured in accordance with FISMA requirements?

SPMS is within the boundary of the Moderate ADM Support Systems (MASS) which has received an Authority to Operate (ATO). MASS is categorized as a Moderate sensitivity Information Technology System. Classified and Safeguards information processing are not permitted.

a. If yes, when was Certification and Accreditation last completed?

May 6, 2013. This security authorization will remain in effect as long as the System Owner satisfies the Periodic System Cybersecurity Assessment (PSCA) requirement. The most recent assessment was performed on January 12, 2016.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/CSD Staff)

System Name: Space and Property Management System (SPMS)

Submitting Office: Office of Administration

A. PRIVACY ACT APPLICABILITY REVIEW

___ Privacy Act is not applicable.

_X_ Privacy Act is applicable.

Comments:
Visitor Access Request System (VARS) module records are covered by Privacy Act System of Records NRC 40, Facility Security Access Control Records; Parking Management module records are covered by Privacy Act System of Records NRC 1, Parking Permit Records.

Reviewer's Name	Title	Date
Sally A. Hardy	Acting Privacy Officer	10/27/2016

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

___ No OMB clearance is needed.

_X_ OMB clearance is needed.

___ Currently has OMB Clearance. Clearance No._____

Comments:
Paragraph B.1.c.(1) states that visitors are asked to voluntary provide information that goes beyond that which is needed for self-identification per OMB Guidance. The additional information is covered by the Paperwork Reduction Act. In addition, Paragraph B.1.d.(1) improperly cites the exemption in 5 CFR 1320.3(h)(8)(1) regarding the request for a driver's license.

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	10/27/16

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

__X__ Needs to be scheduled.

__X__ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:
Information and data (records) fall under NARA approved General Records Schedules (GRS) **except** for the retention of copies of driver's licenses in the SPMS system. A schedule needs to be created or identified (in the GRS) in coordination with ADM to manage the retention and disposition of all copies of driver's licenses in SPMS (verifying or changing the current six year retention). The SPMS data dictionary retained in NRC Rational Jazz will also need to be researched and an appropriate retention schedule applied for the SPMS data in that system.

Reviewer's Name	Title	Date
Marna B. Dove	Sr. Information Management Analyst (Electronic Records Manager)	10/25/16

D. BRANCH CHIEF REVIEW AND CONCURRENCE

____ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

__X__ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ Date **10/28/16**

Kimyata MorganButler, Chief
FOIA, Privacy, Info Collections Branch
Customer Service Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Cynthia Carpenter, Director, Office of Administration**	
Name of System: **Space and Property Management System (SPMS)**	
Date CSD received PIA for review: **October 17, 2016**	Date CSD completed PIA review: **October 27, 2016**
Noted Issues: Visitor Access Request System (VARS) module records are covered by Privacy Act System of Records NRC 40 and the Parking Management module records are covered by Privacy Act System of Records NRC 1.	
Kimyata MorganButler, Chief FOIA, Privacy, and Info Collections Branch Customer Service Division Office of the Chief Information Officer	Signature/Date: **/RA/ 10/28/16**
Copies of this PIA will be provided to: *John Moses, Director* *Solutions Develop Division* *Office of Chief Information Officer* *Kathy Lyons-Burke* *Senior IT Security Officer (SITSO)* *FISMA Compliance and Oversight Team* *Computer Security Office*	