

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.

Moderate ADM Support Systems (MASS)

Date: May 31, 2019

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

MASS is owned and managed by the Office of Administration (ADM). The systems operate under U.S. NRC Privacy Act systems of records NRC-39, "Personnel Security Files and Associated Records, and" NRC-40 "Facility Security Access Controls Records,"

The MASS FISMA boundary consists of Personnel Security Adjudication Tracking System (PSATS), Electronic Questionnaire for Investigations Processing (e-QIP), The Next Generation Name Check Program (NGNCP) – Law Enforcement Enterprise Portal (LEEP), Space and Property Management System (SPMS), Drug Test Tracking System (DTTS) and the ADM Support Systems (ASS) which consists of four separate systems/services:

2. What agency function does it support?

Personnel Security Adjudication Tracking System (PSATS):

PSATS supports Personnel and Facilities Security functions for the Office of Administration (ADM), Division of Facilities and Security (ADM/DFS). PSATS allows Personnel Security Branch (PSB) to monitor and manage personnel security data and (security clearances, security investigations, and access authorizations) badge data associated with the issuance of permanent and temporary badges, along with foreign travel declarations as required by the Security Executive Agent Directive 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position" (SEAD 3).

PSATS subsystem also consists of two separate systems/services, Electronic Questionnaires for Investigations Processing (e-QIP) and Next Generation Name Check (NGNCP) / Law Enforcement Enterprise Portal (LEEP) that contains PII.

Electronic Questionnaire for Investigations Processing (e-QIP)

e-QIP supports Personnel Security functions for the Office of Administration, Division of Facilities and Security (ADM/DFS). e-QIP a secure website that is owned and operated by the Office of Personnel Management (OPM). The data contained within e-QIP is sensitive but unclassified. It is designed to house all personnel investigative forms including the SF-86, "Questionnaire for National Security Positions," the SF-85P, "Questionnaire for Public Trust Positions," the SF-85PS, "Supplemental Questionnaire for Selected Positions," and the SF-85, "Questionnaire for Non-sensitive Positions." Individuals are invited into the system electronically to enter, update, and release their personal investigative data over a secure internet connection to their sponsoring agency for review, approval, and submission to our investigation provider.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

The NGNCP-LEEP supports NRC Personnel Security functions. It provides information from the Federal Bureau of Investigation (FBI) records based on name checks of the spouses/ cohabitants of NRC employees and applicants to assure there is not a security risk regarding the employees or applicants initial or continuing eligibility for NRC employment or access authorization.

Space and Property Management System (SPMS):

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.

Drug Test Tracking System (DTTS):

DTTS is operated and managed by the Drug Testing Program Office in the Office of Administration's Division of Facilities and Security, Personnel Security Branch (ADM/DFS/PSB). The purpose of the system is to manage and monitor the drug testing program at the NRC for employees and contractors.

ADM Support Services (ASS):

The ASS subsystem consists of four separate systems/services that does not contain PII. Please refer to its PTA's below for additional information.

- NRC Webstreaming Service - June 25, 2018, ML18177A311

- Postage Meter System (PMS) - September 20, 2017, ML17276A160
- Electronic Print Order Reporting Tracking System (e-PORTS) – February 29, 2016 ML16061A352
- FIX-IT/Clean-It – TBD

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

Personnel Security Adjudication Tracking System:

PSATS is used by the NRC to automate the tracking of personnel security related activities. The function of the system is to serve as a mechanism to track the status of security checks related to the processing of an individual's security clearance. This system monitors the status of personnel security clearance checks for applicants, current NRC employees, contractors, consultants, student interns, licensees and anyone who requires access to NRC facilities, classified information, sensitive NRC information and equipment, nuclear power facilities, and special nuclear material.

Electronic Questionnaire for Investigations Processing

ADM/DFS only utilizes a portion of the OPM system as detailed above. There are two sides of e-QIP, the OPM NP2 Portal Agency side <https://apollo.opm.gov> and the e-QIP Secure Applicant Website, <https://nbib.opm.gov/e-qip-background-investigations> <https://nbib.opm.gov/e-qip-background-investigations>. e-QIP is a module of the overall OPM portal and membership into this portal is by invitation only. Applicants are initiated into the system to enter their personal data to complete the required investigative paperwork listed above.

The Next Generation Name Check Program– Law Enforcement Enterprise

NGNCP-LEEP has two modules. The Customer Facing Element (CFE), used by FBI customers, provides a secure, web-based interface for customer submissions using a separate agency organizational account and individual accounts for each user. CFE allows for electronic name check submissions, name check submission status, response packages, automated billing process and reporting capability.

The Processing Element (PE), used by the FBI, provides a web-based processing element for research analysts that includes search interfaces, automated billing process, automated workflow, application replacement, application consolidation, metrics, auditing, and reporting capability.

Space and Property Management System:

The NRC uses the SPMS to manage office space, property asset inventory, visitor access requests, and employee headquarter parking assignments.

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 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.

Drug Test Tracking System:

DTTS is a case management and random drug pool generation system that is currently used to track drug testing records and generate random drug test pools. DTTS is a client application that sits on a standalone ITI workstation located in the secure Drug Testing Program office. ITI personnel perform offline updates/maintenance activities on the workstation.

DTTS key functionalities include:

- Generating random drug testing pools (Headquarter, Regional Offices, and the Technical Training Center (TTC))
- Monitoring drug test dates and results
- Providing management and statistical reports

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

Personnel Security Adjudication Tracking System:

- Executive Order 10450, as amended, "Security Requirements for Government Employment."

Electronic Questionnaire for Investigations Processing

- Executive Orders 9397, 10450, 10577, 10865, 12333, 12968, 13467 as amended, 13488, and 13549; 5 U.S.C. §§ 1103, 1302, 1303, 1304, 3301, 7301, 9101, and 11001; 22 U.S.C. §§ 272b, 290a, 2519; 31 U.S.C. §§ 1537; 42 U.S.C. §§1874(b) (3), 2165, 2201, and 20132; 50 U.S.C. § 3341; Public Law 108-136; and Homeland Security Presidential Directive (HSPD) 12.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

- Section 145 of the Atomic Energy Act (AEA) of 1954, as amended; Executive Order 13467 - "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information;" as amended, Executive Order 10865 - "Safeguarding Classified Information within Industry;" Executive Order 12968 – "Access to Classified Information;" as amended, and 10 CFR Part 10, Subpart B – "Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information for an Employment Clearance."

Space and Property Management 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 Facilities."

- 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) (44 U.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.

Drug Test Tracking System:

- Executive Order 12564, Section 503 of Public Law 100-71, 5 U.S.C. 7301

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

Personnel Security Adjudication Tracking System:

To track and manage the official agency records on investigations, clearances, drug testing, and credentialing that are maintained in paper as part of its Personnel and Facilities Security Programs.

Electronic Questionnaire for Investigations Processing

The Federal Government requires background investigations and reinvestigations of all Federal employees, Federal contractors, licensees, applicants, and incumbents. The Nuclear Regulatory Commission (NRC) is required to conduct national security investigations on all of its employees.

The Next Generation Name Check Program (NGNCP) – Law Enforcement Enterprise Portal (LEEP)

The purpose of the system is to electronically submit name check requests to the FBI and to receive the results (responses) electronically. The data collected will be reviewed by NRC Personnel Security to provide assurance that employees, consultants, contractors, licensees and others are reliable and trustworthy to have access to NRC facilities, classified information, sensitive NRC information and equipment, nuclear power facilities, and special nuclear material.

Space and Property Management System:

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.

Drug Test Tracking System:

DTTS provides the Drug Testing Program staff the ability to manage creating random drug test pools and tracking drug test results. This will improve accuracy, compliance, data integrity, and reporting capabilities for managing the Drug Testing Program.

6. Points of Contact:

Name	Role	Office/Division/Branch	Telephone
Mary Muessle	System Owner/Executive Sponsor	ADM	301-415-7322
Diem Le	MASS ISSO	ADM/PMAE	301-415-7114
Karen Cudd	PSATS/SPMS/DTTS Lead Project Manager	ADM/PMAE	301-415-5362
Timothy Pulliam	PSATS Business Manager	ADM/DFS	301-415-8080
Christoph Heilig	PSATS Functional Manager	ADM/DFS/PSB	301-415-7731
Jesus Sanchez	PSATS Technical Project Manager	ADM/DFS/PSB	301-415-2509
Patricia Ibanez	SPMS Project Manager	CounterPointe Solutions, Inc.	703-789-2390
Nancy Turner Boyd	DTTS Project Manager	ADM/DFS/PSB	301-415-6645
Jason Wright	Webstreaming Business Project Manager	ADM/DFS/MGSDB	301-415-5446
Jackie Nicholson	Postage Meters Project Manager	ADM/DFS/MGSB/SDT	301-415-2095
Michael Hale	ePORTS Project Manager	Innovative Software Solutions, LLC	703-405-0329
Richard Branch	FIX-IT/Clean Project Manager	ADM/DFS/FOSMB/FOT	301-415-8389
Emily Robbins	eQIP & NGNCP/LEEP Project Manager	ADM/DFS/PSB	301-415-7000

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

a. New System Modify Existing System Other (Explain)

It describes an existing FISMA boundary system, MASS. This PIA update is to combine all the PIAs for MASS' sub-systems/services into one main PIA.

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

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

Personnel Security Adjudication Tracking System:

Approval Date: March 01, 2011
ADAMS accession number: ML11066A005

Electronic Questionnaire for Investigations Processing:

Approval Date: May 23, 2007
ADAMS accession number: ML063200397

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

Approval Date: N/A - New System
ADAMS accession number: N/A - New System

Space and Property Management System:

Approval Date: October 17, 2016
ADAMS accession number: ML16291A339

Drug Test Tracking System:

Approval Date: April 20, 2017
ADAMS accession number: ML17094A841

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

No modifications have been made to the MASS FISMA boundary; the MASS PIA's have been combined and it is being resubmitted as part of a periodic review.

B. INFORMATION COLLECTED AND MAINTAINED

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

Personnel Security Adjudication Tracking System:

Yes.

Electronic Questionnaire for Investigations Processing:

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

Yes.

Space and Property Management System:

Yes.

Drug Test Tracking System:

Yes.

(1) If yes, identify the group(s) of individuals?

Personnel Security Adjudication Tracking System:

- Federal employees
- Federal Contractors
- Licensees
- Consultants
- Foreign assignees
- Employment applicants

Electronic Questionnaire for Investigations Processing:

- Federal employees
- Federal contractors
- Licensees
- General Public

The Next Generation Name Check Program (NGNCP) – Law Enforcement Enterprise Portal (LEEP)

- Federal employees
- Federal contractors
- Licensees
- Consultants

Space and Property Management System:

- Federal employees
- Federal Contractors
- Licensees
- Visitors to the NRC

Drug Test Tracking System:

- NRC employees
- Federal contractors
- Employment applicants

(2) IF NO, SKIP TO QUESTION B.2.

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

Personnel Security Adjudication Tracking System:

Demographic data, personal identification, and security clearance/access approval information, to include but not limited to: name, social security number, date and place of birth, identity verification information, credential/badge number, a subset of drug testing records (testing date, date of results, applicant test result, random test result if positive), employee and contractor foreign travel information, and classified visit data (name of visitor, agency/organization; level of clearance, dates of visit).

Electronic Questionnaire for Investigations Processing:

The type of information collected includes: name, date of birth, place of birth, social security number (SSN), other names used, identifying information (hair, weight, height, eyes, sex), work/home phone numbers,

citizenship, mother's maiden name, current/previous home addresses, education, employment history, name/address/phone number of references, marital status, spouse information (name, DOB, place of birth, SSN, other names used, citizenship, date/place married, separation date, address), former spouse information (name, DOB, place of birth, citizenship, date/place married, divorced/date/place, widowed/date, address), relative info (name, DOB, country of birth, citizenship, address), military history, foreign activities, foreign countries visited, medical info, police record, drug activity, alcohol use, investigations info, financial info, civil court actions.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

Personal identification, to include the employee or applicant's spouse/cohabitant's name, social security number, date and place of birth, present address, and citizenship. Spouse/cohabitant's parents' names, date and place of birth, present address, and citizenship. Criminal history record of spouse/cohabitant based on name check.

Space and Property Management System:

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.

Drug Test Tracking System:

- Name
- D.O.B.
- SSN
- Office
- Position
- Drug Test Dates
- Drug Test Results

c. Is information being collected from the subject individual?

Personnel Security Adjudication Tracking System:

Yes.

Electronic Questionnaire for Investigations Processing:

Yes.

The Next Generation Name Check Program (NGNCP) – Law Enforcement Enterprise Portal (LEEP)

No.

Space and Property Management System:

Yes.

Drug Test Tracking System:

No.

To the greatest extent possible, collect information about an individual directly from the individual.

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

Personnel Security Adjudication Tracking System:

The information is not collected directly by PSATS. It is collected from the subject individuals through the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) system and/or the completion of standard government forms used for personnel security.

Electronic Questionnaire for Investigations Processing:

Everything required on the forms identified above is collected from the subject individuals.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

N/A

Space and Property Management System:

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, applicants 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 email, 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 not Federal employees?**

Personnel Security Adjudication Tracking System:

Yes.

Electronic Questionnaire for Investigations Processing:

Yes.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

Yes.

Space and Property Management System:

Yes.

Drug Test Tracking System:

Yes.

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

Personnel Security Adjudication Tracking System:

The information collection does not have OMB approval directly by PSATS. Information that will be maintained in PSATS is collected by a variety of tools. OMB Clearances already exist for those tools. Therefore, no additional OMB Clearance is required.

Electronic Questionnaire for Investigations Processing:

Yes, the information collected has an OMB approval.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

Yes, the information collected has an OMB approval.

Space and Property Management System:

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.

Drug Test Tracking System:

Yes, however information is NOT being obtained directly from the individual. PSB receives this information from the security authorization form and information is transferred to the donor's chain-of-custody form during testing.

(a) **If yes, indicate the OMB approval number:**

Personnel Security Adjudication Tracking System:

N/A.

Electronic Questionnaire for Investigations Processing:

SF 86 - OMB No. 3206-0005

SF 85 - OMB No. 3206-0261

SF 85P - OMB No. 3206-0191

SF 85PS – OMB No. 3206-0191

Space and Property Management System:

N/A.

Drug Test Tracking System:

The authority for authorization for this form is OMB No. 0930-0158.

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

Personnel Security Adjudication Tracking System:

Yes.

Electronic Questionnaire for Investigations Processing:

No.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

No.

Space and Property Management System:

Yes.

Drug Test Tracking System:

Yes.

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

Personnel Security Adjudication Tracking System:

Information will be manually entered and/or scanned from the official agency records on investigations, clearances, drug testing, and credentialing maintained in paper as part of the Personnel, Facility Security, and Drug Testing Programs.

Electronic Questionnaire for Investigations Processing:

N/A

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

N/A

Space and Property Management System:

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.

Drug Test Tracking System:

Data will be extracted from the Department of Interior's (DOI) FPPS and loaded into DTTS.

f. Is the information being collected from external sources (any source outside of the NRC)?

Personnel Security Adjudication Tracking System:

Yes.

Electronic Questionnaire for Investigations Processing:

No.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

No.

Space and Property Management System:

No.

Drug Test Tracking System:

Yes.

(1) If yes, identify the source and what type of information is being collected?

Personnel Security Adjudication Tracking System:

OPM is the Investigative Service Provider. They provide completed investigation products such as fingerprints results and clearance information.

Electronic Questionnaire for Investigations Processing:

N/A

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

N/A

Space and Property Management System:

N/A.

Drug Test Tracking System:

Information is collected about an individual's drug test results by NRC's Medical Review Officer (MRO).

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

Personnel Security Adjudication Tracking System:

The e-QIP signature page acts as the certification from the individual that the information they submit as part of their investigation is current, accurate, and complete. OPM and/or NRC then conduct a thorough review to ensure completeness and accuracy.

Electronic Questionnaire for Investigations Processing:

There are numerous checks done within the e-QIP system to verify the structure of the data. NRC PSB initiates a new e-QIP request for an applicant inviting them into the system to complete their form online. The applicant completes the form online and before submitting it to PSB, the system requires each applicant to validate and certify with electronic signature that the form is accurate before submitting it to PSB. PSB reviews the online application for accuracy and completeness and rejects it back to the applicant if it is missing data or requires corrections. If the form is accurate, PSB validates the form within the system and releases the e-QIP request to their ISP. If there are validation errors, the system will not allow the form to be submitted to the ISP.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

The NRC Form 354, Data Report on Spouse is signed by the employee or applicant and also signed by the spouse or cohabitant and this should certify that the Information on the form is current, accurate, and complete.

Space and Property Management System:

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.

Drug Test Tracking System:

Individual identifying information is cross checked from chain-of-custody form (OMB No. 0930-0158). The multi-part form contains specimen ID number and donor information that ties the urine specimen with the correct donor, this information is verified by the donor at the time of collection.

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

Personnel Security Adjudication Tracking System:

Information is manually entered and/or scanned into PSATS, and electronically sent from OPM through e-Delivery (.pdf documents). Executive Order 10450, as amended, "Security Requirements for Government Employment." To track and manage the official agency records on investigations, clearances, drug testing, and credentialing that are maintained in paper as part of its Personnel and Facilities Security Programs.

Electronic Questionnaire for Investigations Processing:

The information is collected via individual's data entry on the electronic forms which are then submitted to e-QIP, hiring agency accesses/reviews/verifies, then submits to OPM for investigation.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

The information collected on the NRC Form 354 is entered directly into LEEP secure website by a NRC PSB employee or contractor.

Space and Property Management System:

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.

Drug Test Tracking System:

Medical Review Officer receives results from the drug testing laboratory and mails chain-of-custody forms to the NRC DTP.

2. INFORMATION NOT ABOUT INDIVIDUALS

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

Personnel Security Adjudication Tracking System:

No.

Electronic Questionnaire for Investigations Processing:

N/A

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

No.

Space and Property Management System:

Yes.

Drug Test Tracking System:

No.

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

Personnel Security Adjudication Tracking System:

N/A

Electronic Questionnaire for Investigations Processing:

N/A

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

N/A

Space and Property Management System:

FPPS furnishes a pipe-delimited file containing organization codes, office divisions and branch codes. Computer Aided Drawings (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.

Drug Test Tracking System:

N/A.

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

Personnel Security Adjudication Tracking System:

OPM is the Investigative Service Provider. They provide completed investigation products such as fingerprints results and clearance information.

Electronic Questionnaire for Investigations Processing:

N/A

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

N/A

Space and Property Management System:

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.

Drug Test Tracking System:

Information is collected about an individual's drug test results by NRC's Medical Review Officer (MRO).

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.**

Personnel Security Adjudication Tracking System:

PSATS tracks and manages the personnel security (security clearances, investigative and access authorizations), drug program data associated with applicant drug testing and employee random drug testing, and incoming and outgoing classified visit data. The information is used for reporting, statistics, forecasting, history tracking, validation, etc. Credentialing data will be used to

enable reciprocal acceptance of personal identity verification (PIV) credential determinations across agencies. Classified visit data will be used to validate an individual's clearance level and show access approval for the specific visit.

Electronic Questionnaire for Investigations Processing:

The information is used for background investigations. NRC also uses the information during the application process for updating an existing application.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

Data will consist of criminal record checks based on name checks only. If there is no criminal record, the data will reflect no record. If there is a criminal record, the record will be revealed. The information revealed permits ADM DFS to make security determinations as to whether or not any information on a specific individual has an impact on an employee or applicant's initial or continued eligibility for access authorization or employment clearance.

Space and Property Management 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 are 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.

Drug Test Tracking System:

Data in this system will be used to determine if an employee or contractor in a sensitive position is suitable for Government employment.

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

Personnel Security Adjudication Tracking System:

Yes.

Electronic Questionnaire for Investigations Processing:

Yes.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

Yes.

Space and Property Management System:

Yes.

Drug Test Tracking System:

Yes.

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

Personnel Security Adjudication Tracking System:

ADM/DFS authorized staff ensures proper use of the information.

Electronic Questionnaire for Investigations Processing:

NRC and OPM.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

NRC and FBI.

Space and Property Management 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.

Drug Test Tracking System:

Drug Testing Program staff.

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?

Personnel Security Adjudication Tracking System:

The PSATS Data Dictionary and User's Guide contains this information and is located in Rational ClearCase.

Electronic Questionnaire for Investigations Processing:

Yes, with OPM.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

N/A.

Space and Property Management System:

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

Drug Test Tracking System:

DTTS User Guide, located on DTTS workstation NRC-35 Drug Testing Program Records.

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

Personnel Security Adjudication Tracking System:

No.

Electronic Questionnaire for Investigations Processing:

No.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

No.

Space and Property Management System:

No.

Drug Test Tracking System:

No.

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

a. If yes, how will aggregated data be maintained, filed, and utilized?

Personnel Security Adjudication Tracking System:

N/A.

Electronic Questionnaire for Investigations Processing:

N/A

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

N/A

Space and Property Management System:

N/A.

Drug Test Tracking System:

N/A.

b. How will aggregated data be validated for relevance and accuracy?

Personnel Security Adjudication Tracking System:

N/A.

Electronic Questionnaire for Investigations Processing:

N/A

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

N/A

Space and Property Management System:

N/A.

Drug Test Tracking System:

N/A.

c. If data is consolidated, what controls protect it from unauthorized access, use, or modification?

The sub-systems in the MASS FISMA boundary complies with organizational defined computer security controls. These controls are applied to “harden” the system against unauthorized access, insider threat, compromise, or disaster.

They also comply with the change management procedures of the Office of Chief Information Officer (OCIO) to make sure only authorized work is performed on the system.

The systems comply with the policies and procedures of the OCIO Computer Security Organization (CSO) and undergoes independent continuous monitoring assessments to secure the system.

The data in the systems is restricted to application administrators in the ADM facilities security branch. These administrators have undergone rigorous background screening and are trained in their administrator duties to secure the MASS sub-systems.

The system owner has also assigned primary and alternate information system security officers to the MASS FISMA boundary to make sure system security controls are operating as designed and intended.

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

Personnel Security Adjudication Tracking System:

Information about an individual will be retrievable by name or social security number. Information can also be retrieved via the PSATS reporting tool (standard reports and queries).

Electronic Questionnaire for Investigations Processing:

Information is retrieved from e-QIP by social security number, name, or investigation request number.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

A unique identifier number is assigned to each name check request. The Personnel Security user will click on a link on a returned name check to see the report. If the name check located any sensitive information at all, the report will be sent via Federal Express back to the original requester.

Space and Property Management System:

SPMS monitors the location of government furnished equipment, space allocation to employees and space utilization. The aforementioned information is not PII. 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.

Drug Test Tracking System:

Information about an individual will be retrieved using their Name and/or SSN.

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

Personnel Security Adjudication Tracking System:

No.

Electronic Questionnaire for Investigations Processing:

No.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

No.

Space and Property Management System:

No. SPMS does not provide real-time data that could identify and locate an employee. 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.

Drug Test Tracking System:

No.

- a. **If yes, what controls will be used to prevent unauthorized monitoring?**

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

Personnel Security Adjudication Tracking System:

There are over 75 specific reports and an ad hoc capability available from the PSATS reporting tool. Reports are run on an as-needed basis.

Electronic Questionnaire for Investigations Processing:

Reports include the following:

How many individuals have been initiated

How many have not accessed the system after being invited

How many forms were rejected

How many forms are in review

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

N/A

Space and Property Management System:

There are over 30 specific reports and an ad hoc capability available from the SPMS reporting tool. Reports are run on an as needed basis.

Drug Test Tracking System:

- A list of employees/contractors who must report for random drug testing
- A report of the number of drug test conducted, dates, & results
- Notification of drug test results

a. What are the reports used for?

Personnel Security Adjudication Tracking System:

Reports will be used for security information, budgetary purposes, resource planning, and quality control purposes.

Electronic Questionnaire for Investigations Processing:

System management

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

The reports are role-based and provide the names that were either submitted or still unsubmitted. The other type of report is for billing purposes for the role that handles the payments for the name checks.

Space and Property Management System:

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

Drug Test Tracking System:

The list of employees will be used to have those people on the list report for drug testing. The report on the number of drug tests conducted, dates, and results will be used for reporting up to Management. Notification of drug test results will be sent to the person being tested.

b. Who has access to these reports?

Personnel Security Adjudication Tracking System:

Staff from the Personnel Security and Facilities Security Branches, the System Administrator, and ADM IT Coordinator will have need-to-know access based on a roles and responsibilities.

Electronic Questionnaire for Investigations Processing:

System administrator

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

The reports are role-based and only NRC staff with accounts can access the reports.

Space and Property Management System:

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.

Drug Test Tracking System:

- Drug Testing Program staff
- ADM Managers with need to know.

- OGC
- Attorneys with need to know.
- OCHCO
- Management with need to know.

D. ACCESS TO DATA

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

Personnel Security Adjudication Tracking System:

GRS 1, Item 36, Federal Workplace Drug Testing Program Files; GRS 1, Item 10, Temporary Individual Employee Records; GRS 18, Item 17, Visitor Control Files; GRS 18, Item 22, Personnel Clearance Files; and GRS 24, Item 6, User Identification, Profiles, Authorizations, and Password Files (excluding records relating to electronic signatures).

Electronic Questionnaire for Investigations Processing:

ADM/DFS/PSB - Has access to review, approve, and submit to OPM.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

ADM/DFS/PSB

Space and Property Management 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/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.

Drug Test Tracking System:

ADM Drug Test Program staff

a. For what purpose?

Personnel Security Adjudication Tracking System:

For reporting, validation, statistics, forecasting, history tracking, etc.

Electronic Questionnaire for Investigations Processing:

The system's completed forms are used to initiate background investigations. NRC also uses the information during the application process for updating an existing application.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

To make security determinations as to whether or not any information on a specific individual has an impact on their initial or continued eligibility for access authorization or employment clearance.

Space and Property Management System:

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.

Drug Test Tracking System:

Management of the NRC Drug Testing Program.

b. Will access be limited?

Personnel Security Adjudication Tracking System:

Yes. Limited by need-to-know based on roles and responsibilities.

Electronic Questionnaire for Investigations Processing:

Yes, access restricted by roles.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

Yes, limited by need-to-know based on roles and responsibilities.

Space and Property Management System:

Yes.

Drug Test Tracking System:

Yes.

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

Personnel Security Adjudication Tracking System:

Yes.

Electronic Questionnaire for Investigations Processing:

No.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

No.

Space and Property Management System:

Yes.

Drug Test Tracking System:

Yes.

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

Personnel Security Adjudication Tracking System:

Other NRC systems will not have direct access (connection) to PSATS. However, there will be imports of current data from other NRC systems, such as Human Resources Management System, Employee Drug Test Tracking System, and Access Control and Computer Enhanced Security System.

Electronic Questionnaire for Investigations Processing:

N/A.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

N/A.

Space and Property Management System:

Pandemic System located at Region II.

Drug Test Tracking System:

There is no direct access since DTTS is a standalone workstation. All file sharing will be performed through manual file importing and exporting.

Personnel Security Adjudication Tracking System (PSATS) Department of Interior's (DOI)

Federal Personnel/Payroll System (FPPS)

b. How will the data be transmitted or disclosed?

Personnel Security Adjudication Tracking System:

Information will be transmitted via secure file transfer.

Electronic Questionnaire for Investigations Processing:

The information is transmitted electronically through a secure portal within OPM. The transmission is secured with 128-bit encryption.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

N/A.

Space and Property Management System:

Open Database Connectivity - (ODBC) export

Drug Test Tracking System:

Data about an individual will be extracted from DTTS onto an NRC MXI Thumb Drive and loaded into PSATS only for the pre-employment drug test type.

Data about an individual will be extracted from FPPS onto an NRC MXI Thumb Drive and loaded into DTTS.

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

Personnel Security Adjudication Tracking System:

No external agencies will have direct access to the information in PSATS. However, a flat file (batch loading of data in a specific layout for agency reporting) is produced monthly to verify security clearances with OPM's Clearance Verification System (CVS).

Electronic Questionnaire for Investigations Processing:

Yes, but only to the individual agency's data.

The Next Generation Name Check Program (NGNCP) – Law Enforcement Enterprise Portal (LEEP)

Other FBI customers would have access to their own name check information.

It is possible that other agencies would be seeking information on the same individuals as the NRC.

Space and Property Management System:

No.

Drug Test Tracking System:

No.

a. If yes, who?

Personnel Security Adjudication Tracking System:

N/A.

Electronic Questionnaire for Investigations Processing:

Each agency has access to data on their employees/applicants.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

The FBI determines the user accounts by accrediting the users and requiring them to sign user agreements.

Space and Property Management System:

N/A.

Drug Test Tracking System:

N/A.

b. Will access be limited?

Personnel Security Adjudication Tracking System:

N/A.

Electronic Questionnaire for Investigations Processing:

N/A

The Next Generation Name Check Program (NGNCP) – Law Enforcement Enterprise Portal (LEEP)

Yes.

Space and Property Management System:

N/A.

Drug Test Tracking System:

N/A.

c. What data will be accessible and for what purpose/use?

Personnel Security Adjudication Tracking System:

The information uploaded into the secure portal at OPM's CVS includes the social security number, last name, active clearance level, and date and city and state/country of birth. Since OPM already has the information about an individual, NRC is just communicating the clearance information.

Electronic Questionnaire for Investigations Processing:

If an employee changes agencies or applies to an agency and already has an electronic form on file, the employee may grant the agency permission to begin the application process.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

Criminal history records based on name checks only. This information will assist NRC Personnel Security in making determination if employees, consultants, contractors, licensees and others are reliable and trustworthy to have access to NRC facilities, classified information, sensitive NRC

information and equipment, nuclear power facilities, and special nuclear material.

Space and Property Management System:

N/A.

Drug Test Tracking System:

N/A.

d. How will the data be transmitted or disclosed?

Personnel Security Adjudication Tracking System:

This information is uploaded electronically to the secure portal within OPM. The transmission is secured with 128-bit encryption.

Electronic Questionnaire for Investigations Processing:

Individual agencies are not able to transmit or disclose information.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

The data will be available to the NRC Personnel Security users with accounts in the system. If the data is non-sensitive, it will be available within the application. If the data is sensitive, it will be sent via Federal Express back to the original requester.

Space and Property Management System:

N/A.

Drug Test Tracking System:

N/A.

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?

(See table next page)

<u>Record</u>	<u>Schedule</u>	<u>Disposition</u>
Personnel Security Adjudication Tracking System		
Employee drug test plans, procedures, scheduling records	GRS 2.7 item 100	Temporary. Destroy when 3 years old or when superseded or obsolete.
Employee drug test acknowledgment of notice forms	GRS 2.7 item 110	Temporary. Destroy when employee separates from testing-designated position.
Employee drug testing specimen records	GRS 2.7 item 120	Temporary. Destroy 3 years after date of last entry or when 3 years old, whichever is later.
Employee drug test results. Positive results.	GRS 2.7 item 130	Temporary. Destroy when employee leaves the agency or when 3 years old, whichever is later.
Employee drug test results. Negative results.	GRS 2.7 item 131	Temporary. Destroy when 3 years old.
Employee Acquisition Records. Job vacancy case files. One-time competitive and SES.	GRS 2.1 item 050	Temporary. Destroy 2 years after selection certificate is closed or final settlement of any associated litigation; whichever is later.
Employee Acquisition Records. Job vacancy case files. Standing register competitive files for multiple positions filled over a period of time.	GRS 2.1 item 051	Temporary. Destroy 2 years after termination of register.
Employee management records. OPF/eOPF Short-term records.	GRS 2.2 item 041	Temporary. Destroy when superseded or obsolete, or upon separation or transfer of employee, whichever is earlier.
Employee management records. Employment eligibility verification records.	GRS 2.2 item 060	Temporary. Destroy 3 years after employee separates from service or transfers to another agency.
Security records. Visitor processing records. Areas requiring highest level security awareness.	GRS 5.6 item 110	Temporary. Destroy when 5 years old, but longer retention is authorized if required for business use.
Security records. Visitor processing records. All other facility security areas.	GRS 5.6 item 111	Temporary. Destroy when 2 years old, but longer retention is authorized if required for business use.

Personnel security records. Personnel security investigative reports. Personnel suitability and eligibility investigative reports.	GRs 5.6 item 170	Temporary. Destroy in accordance with the investigating agency instruction.
Personnel security records. Personnel security and access clearance records. Records of people issued clearances.	GRS 5.6 item 181	Temporary. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use.
Personnel security records. Index to the personnel security case files.	GRS 5.6 item 190	Temporary. Destroy when superseded or obsolete.
System access records. Systems not requiring special accountability for access.	GRS 3.2 item 030	Temporary. Destroy when business use ceases.
System access records. Systems requiring special accountability for access.	GRS 3.2 item 031	Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.
E-QIP	GRS 5.6 item 181	Temporary. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use.
Next Generation Name Check Program – Law Enforcement Enterprise Portal. Personnel Clearance Files	GRS 5.6 item 181	(retentions provided above)
	GRS 5.6 item 170	
	GRS 5.6 item 190	
Space and Property Management System		
Facility, space vehicle, equipment, stock and supply administrative and operational records. Agency Space Files.	GRs 5.6 item 010	Temporary. Destroy when 3 years old or 3 years after superseded, as appropriate, but longer retention is authorized if required for business use.

Property Module		
Property Disposal Correspondence Files. Excess personal property, equipment, and vehicle records.	GRS 5.4 item 040	Temporary. Destroy when 3 years old, but longer retention is authorized is required for business use.
Visitor Access Module		
Visitor Control Files. Visitor processing records. Areas requiring highest level security awareness.	GRS 5.6 item 110	Temporary. Destroy when 5 years old, but longer retention is authorized if required for business use.
Visitor Control Files. Visitor processing records. All other facility security areas.	GRS 5.6 item 111	Temporary. Destroy when 2 years old, but longer retention is authorized if required for business use.
Parking Management		
Credential Files. Personal identification credentials and cards. Application and activation records.	GRS 5.6 item 120	Temporary. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use.
Credential Files. Local facility identification and card access records.	GRS 5.6 item 130	Temporary. Destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to near expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is authorized if required for business use.

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.

1. If the records cannot be mapped to an approved records retention schedule, how long do you need the records? Please explain.

2. **Would these records be of value to another organization or entity at some point in time? Please explain.**
3. **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?**
4. **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?**
5. **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?**
6. **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).**

Personnel Security Adjudication Tracking System:

PSATS uses a user ID and encrypted password to access the system. The password must be reset every 90 days. PSATS automatically locks a user's access after 3 unsuccessful tries and the user is also logged out of the system after 15 minutes of inactivity. The system will be PIV enabled using an individual's badge and PIN for access.

Electronic Questionnaire for Investigations Processing:

The Agency Administrator is responsible for creating accounts for agency employees (Users). The Agency Users are first approved access into the secure web portal by OPM officials. Then a profile is created for each Agency User in relation to their roles and responsibilities.

A person (agency users and applicants) must be invited into the system before access is granted. An email is then generated to the new user with a registration code and instructions to log in. The user then goes to the secure website and enters their social security number. Three special 'golden' questions (NAME, DOB, Place of Birth(POB)) then appear and the user must know these answers to verify their identity along with the registration code. It is then the user's responsibility to create a username and password for future logins. The user must also create three challenge questions and answers specifically created by them. This will ensure that no one can attempt to impersonate the user on the eQIP system.

The Agency Administrator is the only individual who can reset the 'golden' questions back to the default identifiers when a user gets locked out. A lock out occurs after a user encounters three unsuccessful login attempts.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

FBI customers must be accredited and sign a user agreement to use the application. The end user applies for a user account and password and the password must be reset at least every 90 days. If the end user has not logged in within 90 days, the account will automatically expire. The password must be between 8-12 characters, include upper case, lower case, at least one special character and a number. The password cannot use two consecutive characters back to back.

The end user chooses a passcode picture and passcode that will appear each time the end user logs into the application. Once the user logs into the first part of the application, a one-time password email will be automatically sent to the registered email of the user. The user has 60 minutes from the email timestamp to use the passcode to log the rest of the way into the application.

Space and Property Management System:

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.

Drug Test Tracking System:

The workstation is standalone and located in the locked Drug Testing Program office. Only Drug Testing Program staff will have keys/combo to the office and content.

Access to DTTS will be limited to the Drug Testing Program staff. Staff must login to the system with a User ID and password.

The ADM System Administrator will have access to the workstation to apply operating system patches, security patches, and software updates and to assist with SQL statements for adhoc reporting.

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

Personnel Security Adjudication Tracking System:

An audit log tracks modifications to certain data fields within PSATS. All access to data in PSATS is restricted to a need-to-know based on roles and responsibilities.

Electronic Questionnaire for Investigations Processing:

There are built in audit logs to monitor disclosures and determine who had access. The audit log tracks to whom the form is assigned at each step in the process. These logs are checked regularly to ensure that the system is accessed appropriately.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

The NRC users only have access to the NRC data for their role-based account and that they specifically requested.

Space and Property Management System:

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

Drug Test Tracking System:

NRC Information Technology Rules of Behavior and there is an audit trail of system access, data insert, update and delete.

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

Personnel Security Adjudication Tracking System:

Yes.

Electronic Questionnaire for Investigations Processing:

Yes.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

Yes.

Space and Property Management System:

Yes.

Drug Test Tracking System:

No.

If yes, where?

Personnel Security Adjudication Tracking System:

The date and time of the last login is captured. Certain fields are also captured in an audit log as the data is modified.

Electronic Questionnaire for Investigations Processing:

The roles are documented within e-QIP in the user roles set up area. User accounts are automatically deleted if not accessed within 90 days.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

Each user must read and acknowledge the FBI Systems User Rules of Behavior Agreement Form before access is granted to the system.

Space and Property Management System:

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.

Drug Test Tracking System:

N/A.

The criteria, procedures, controls, and responsibilities regarding access to the system is documented for the subsystems in —

- FY18 Annual MASS System Security Plan (SSP), July 9, 2018 (ADAMS accession number: ML18191B003)

This document is reviewed yearly.

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

Personnel Security Adjudication Tracking System:

Yes.

Electronic Questionnaire for Investigations Processing:

OPM controls which agencies can access the system. NRC utilizes this system at headquarters. The individuals may access this system wherever the internet can be accessed.

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

The end users will be NRC headquarters users.

Space and Property Management System:

Yes.

Drug Test Tracking System:

No.

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

Personnel Security Adjudication Tracking System:

PSATS will be a web-based system that will operate from the NRC Headquarters Data Center. User access is through authorized network connectivity. Log in requirements and access levels remain the same no matter from what location an approved user attempts to access the system.

Electronic Questionnaire for Investigations Processing:

N/A

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

N/A

Space and Property Management System:

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

Drug Test Tracking System:

N/A.

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

Access to the data is strictly controlled and limited to those with an operational need to access the information.

Personnel Security Adjudication Tracking System:

- PSATS Administrator
- Security Manager
- Senior Adjudicator
- Adjudicator
- Processor

- Facilities Security Specialist
- Station Guard
- Drug Manager
- Drug Tester
- View Only

Electronic Questionnaire for Investigations Processing:

- Agency Administrator
- System Administrator
- Functional Administrator
- Initiators
- Reviewers
- Approvers
- Applicant/user

The Next Generation Name Check Program – Law Enforcement Enterprise Portal

Personnel Security users and ADM PMDA billing users will have access to the system. Each role is segregated. The billing users will not have access to the name check data.

Space and Property Management 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

Drug Test Tracking System:

- Drug Testing Program Staff
- ADM System Administrator

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

Yes.

a. If yes, what will be collected?

Personnel Security Adjudication Tracking System:

The date and time of the last login is captured. Certain fields are also captured in an audit log as the data is modified.

Electronic Questionnaire for Investigations Processing:

Name and role(s) held

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

User access is captured, all requirements pertaining to CNSSI 1015 (for NSS systems) auditing requirements are being captured.

Space and Property Management System:

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

Drug Test Tracking System:

Audit Trail of system access, data insert, update, delete.

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

Personnel Security Adjudication Tracking System:

Yes.

Electronic Questionnaire for Investigations Processing:

Yes.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

No. The application is owned by a non-NRC agency.

Space and Property Management System:

Yes.

Drug Test Tracking System:

Yes.

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

Personnel Security Adjudication Tracking System:

An audit log tracks modifications to certain data fields within PSATS.

All access to data in PSATS is restricted to a need-to-know based on roles and responsibilities.

Electronic Questionnaire for Investigations Processing:

Individuals only have access to e-QIP for a defined period of time. The applicant's access is removed when the time has expired, or the applicant has certified and released their data. The e-QIP system administrators, security administrators, IT specialists, Investigation Service Providers, and analysts have access to the system in order to perform their duties in managing, upgrading, and using the system. Role-based access controls are employed to limit the access of information by users and administrators based on the need to know the information for the performance of their official duties. The e-QIP system enforces separation of duties, preventing unauthorized disclosure or modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system.

The Next Generation Name Check Program– Law Enforcement Enterprise Portal

The system allows you to track submission detail, tracking dates, and current stage of processing. All data can be sorted and filtered. NRC users only have access to the NRC data based on roles and responsibilities.

Space and Property Management System:

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.

Drug Test Tracking System:

Log into system with USERID/Password.

Audit trails of system activity built into the application.

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

Yes.

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

May 6, 2013 (ADAMS accession number: ML13093A075).

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 December 20, 2017.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL

(For Use by OCIO/ISB Staff)

System Name: Moderate ADM Support Systems (MASS)

Submitting Office: Office of Administration (ADM)

A. PRIVACY ACT APPLICABILITY REVIEW

Privacy Act is not applicable.

Privacy Act is applicable.

Comments:

PSATS will maintain personally identifiable information and is covered under NRC-39, Personnel Security Files and Associated Records and NRC-40, Facility Security Access Control Records; **LEEP** – is covered under NRC-39, Personnel Security Files and Associated Records; **e-QIP** system does maintain PII and is covered under NRC system of records NRC-39, Personnel Security Files and Associated Records. **Visitor Access Request System (VARs)** module records are covered by NRC 40; **Parking Management module records** are covered by Privacy Act System of Records NRC 1, Parking Permit Records and Information in **DTTS** is covered by Privacy Act systems of records: NRC-35, Drug Testing Program Records

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	10/04/2019

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

No OMB clearance is needed.

OMB clearance is needed.

Currently has OMB Clearance. Clearance No. _____

Comments:

As previously noted in the prior SPMS PIA and again June 2019 the following issues continue. Paragraph B.1.c.(1) (SPMS) states that visitors are asked to voluntarily 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) (SPMS) improperly cites the exemption in 5 CFR 1320.3(h)(8)(1) regarding the request for a driver's license.

Also, a number of clearance numbers in Paragraph B.1.d.(1)(a) are incorrect. Corrected clearance numbers were provided in previous PIAs. The program office was informed in June 2019 that this issue still existed but no changes were made.

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	9/18/19

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

- No record schedule required.
- Additional information is needed to complete assessment.
- Needs to be scheduled.
- Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	6/18/19

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.
- 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/_____
 Anna T. McGowan, Chief
 Information Services Branch
 Governance & Enterprise Management
 Services Division
 Office of the Chief Information Officer

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

TO: Mary Muessle, Director, Office of Administration (ADM)	
Name of System: Moderate ADM Support Systems (MASS)	
Date ISB received PIA for review: May 31, 2019	Date ISB completed PIA review: October 4, 2019
<p>Noted Issues:</p> <p>PSATS will maintain personally identifiable information and is covered under NRC-39, Personnel Security Files and Associated Records and NRC-40, Facility Security Access Control Records;</p> <p>Next Generation Name Check Program LEEP – is covered under NRC-39, Personnel Security Files and Associated Records;</p> <p>e-QIP system does maintain PII and is covered under NRC system of records NRC-39, Personnel Security Files and Associated Records;</p> <p>Visitor Access Request System (VARS) module records are covered by Privacy Act System of Records NRC 40;</p> <p>Parking Management module records are covered by Privacy Act System of Records NRC 1 , Parking Permit Records;</p> <p>DTTS is covered by Privacy Act systems of records: NRC-35, Drug Testing Program Records.</p>	
Anna T. McGowan, Chief Information Services Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: /RA/ October 11, 2019
<p><i>Copies of this PIA will be provided to:</i></p> <p><i>Thomas Ashley, Director IT Services Development & Operation Division Office of the Chief Information Officer</i></p> <p><i>Jonathan Feibus Chief Information Security Officer (CISO) Governance & Enterprise Management Services Division Office of the Chief Information Officer</i></p>	