U.S. Department of Transportation

Federal Aviation Administration (FAA)

Privacy Impact Assessment
MyITSM/Benefits Operation Center Case Management Module (BOC CMM)

Responsible Official
Julie Dunn
System Owner, MyITSM BOC CMM
Human Resources Management

Approving Official
Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

CLAIRE W BARRETT Digitally signed by CLAIRE W BARRETT
Date: 2020.03.25 19:59:53 -04'00'

Executive Summary

The Federal Aviation Administration's (FAA) Office of Information and Technology (AIT) implemented the My Information Technology Service Management (MyITSM)[1] system to facilitate the management of FAA's technical support services. MyITSM the *Benefits Operations Center Case Management Module (BOC CMM)*, used by the Office of Human Resource Management (AHR) Benefits Operation Center (BOC) to support the administration of FAA employee benefits and retirement programs including FAA employees who are eligible for retirement benefits and annuitants who are currently receiving benefits. The BOC CMM provides automated workflow management application to track, manage, and administer BOC services.

In accordance with E-Government Act of 2002, the FAA developed this Privacy Impact Assessment (PIA) because the BOC CMM collects personally identifiable information (PII) of FAA employees and their beneficiaries (such as spouses or children) who are members of the public.

DOT Privacy - Approved - 032520

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[2]

[1] MyITSM is comprised of three Commercial-off-the Shelf (COTS) applications; 1) Remedy Service Management Suite by BMC Software, Inc., 2) DameWare by SolarWinds Worldwide, LLC, and 3) iDashboards. MyITSM is used to facilitate FAA's management of technical support services, i.e. help desk ticketing, tracking of IT equipment, and maintenance activities performed on hardware and software. The BOC CMM is a component within the Remedy Services Management Suite.

[2] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The BOC provides benefits and retirement services to 46,000 FAA employees, annuitants, [3] and beneficiaries. BOC CMM is a workflow management system used by the BOC to support its mission and facilitates the tracking, management and administration of benefits and responding to benefits or retirement inquiries and actions. Using the BOC CMM, BOC personnel create, edit, and view existing case files, inclusive of forms, notes, journal entries, and documents, related to specific benefits or retirement inquiries and actions.

Initiating Inquiries

FAA employees may initiate contact with the BOC:

By fax at 816-329-2476 or 816-329-2418 (Kansas City BOC Office);
By postal mail at FAA/Benefits Operations Center, 901 Locust St., Rm 117, Kansas City, MO 64106; or

Privacy - Approved - 032520

[3] BOC CMM does not actively collect information about annuitants. If an annuitant were to call in, however, the BOC specialist would attempt to assist them. Typically, the BOC specialist would refer them to the Office of Personnel Management (OPM) or the Department of Interior (DOI) and then document the referral.

- In-person at FAA/Benefits Operations Center, 901 Locust Street, Room 117, Kansas City, MO 64106

Via Phone:

When the BOC specialist receives a call from an employee, the individual’s telephone number is automatically displayed in the system. The BOC specialist asks for the employee’s[4] full name, and enters it into BOC CMM. BOC CMM sends a query to the FAA’s Active Directory that populates the BOC CMM case screen with the employee’s full name, FAA email address, and office phone number. The BOC specialist asks for the date of birth (DOB) and last four digits of the caller’s social security number (SSN) to validate the caller’s identity. BOC CMM includes an interface with the Department of Transportation’s (DOT) Consolidated Automated System Time and Labor Entry/Internet Reporting (CASTLE-IR) system that allows BOC specialists to view additional information about the employee such as their line of business (LOB), date of hire, location, and job position, which are necessary to support benefit and retirement processing.[5]

After the employee is validated, the BOC specialist assists with the inquiry and annotates the conversation into the journal; a free-form text field within the BOC CMM. If the employee requests to use a personal email address for future communication, the BOC specialist annotates the journal accordingly. The BOC specialist is trained not to enter any PII, with the exception of the preferred email address, into this free-form text field. If the inquiry is resolved, the case is closed and a case number is not generated.

If the inquiry is not resolved, the BOC CMM generates a random case file number and assigns a BOC specialist to address the outstanding issue. The BOC specialist emails the employee and provides the case file number, name of the assigned BOC specialist, and any follow up actions required of the employee such as forms to be completed or supporting documentation to submit. Upon receipt from the employee, the BOC specialist scans, uploads, and attaches all received forms or supporting documentation to the applicable case file. All case files are encrypted and hard copy originals are stored in a locked file cabinet at the BOC office for one year after the case closes. If the employees is required to provide documentation containing medical information, the information is not scanned into the BOC CMM. This documentation is maintained in hard copy and is stored in a locked file cabinet,

[4] For ease of reading, this PIA uses “employee” to refer to anyone who engages with the BOC. However, the caller may be a former employee, beneficiary, or individual authorized to speak on behalf of the employee.

[5] For a complete list of CASTLE-IR data elements that are available upon look-up in BOC CMM, see Appendix A.

in the BOC office and is accessibly by BOC personnel only. These records are destroyed one year after the case file is closed.

Via Email:

An employee submits a benefits or retirement inquiry by emailing the BOC at 9-ACE-FAA-Bene@faa.gov. All email inquiries are automatically redirected into the BOC CMM. BOC personnel perform an advanced search function in BOC CMM daily to filter out the email inquiries for action. BOC personnel either can input, resolve, and close the inquiry or assign an open inquiry to a BOC specialist for further assistance. If the inquiry is from a FAA email address, BOC CMM is automatically populated with employee's name, FAA email address, and telephone number via an interconnection with Active Directory. If the email inquiry is from a personal email address, the BOC specialist enters the full name into BOC CMM to validate the employee and populate BOC CMM with the above referenced employee information. The process for managing the inquiry follows the process disrobed above.

Via Fax, Postal Mail, or In-Person:

Under very rare circumstances, a FAA employee may submit an inquiry by fax, postal mail, or in-person. The BOC specialist follows the same procedures as outlined above for phone

Closing Out Inquiries

Once an inquiry is completed it is marked "resolved" in the system and the case is closed and an email to the employee. A BOC specialist uploads any completed forms that are required to be included in the employee's Electronic Official Personnel Folder (eOPF) to an encrypted folder for the appropriate AHR Shared Service Centers (SSC) shared drive. AHR Human Resource specialists then upload the forms to the employee's eOPF and remove the files from the network drive. Thirty days after the case file is marked "resolved," the BOC CMM case file automatically changes to a "closed" case status. BOC CMM automatically strips all forms attached to closed cases after one year.

DOT Privacy - Ap

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) *v3*[6]*, sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*[7]*.*

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

The FAA employs multiple techniques to inform FAA employees for which the FAA collects, uses, disseminates, and retains their PII in the BOC CMM. An agency-wide message was broadcast notifying FAA employees of the requirement to provide their DOB and the last four digits of their SSN to validate the caller's identity. Individuals who call the BOC (employees, annuitants, beneficiaries, and representatives) receive notice through a voice recording to that their full name, DOB, and last four digits of the employee's SSN will be required in order to process their benefit or retirement inquiry.

FAA is required to use official OPM issued forms for the processing of benefits and retirement actions.[8] OPM has published a government-wide Privacy Act System of Records Notice (SORN), OPM/GOVT 1 – General Personnel Records (71 FR 35342, June 18, 2006), which provides notice of its privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information about an individual that may be collected for general federal personnel matters including benefits and retirement. The Privacy Act notice referenced on the majority of OPM forms used by the BOC is OPM/GOVT-1. In addition, OPM has asserted that federal agencies must manage all records maintained at the agency in accordance with OPM/GOVT-1 if those records are part of the employee official personnel file. Therefore, the FAA manages all benefit and retirement related records maintained in the BOC CMM and any hard-copy inputs and out-put in accordance with OPM/GOVT-1.

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the BOC CMM.

DOT Privacy - Approved - 032520

[6] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

[7] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

[8] Lists of the OPM required data and forms typically maintained in the BOC-CMM may be found in Appendices B and C.

Individual Participation and Redress

DOT should provide a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Data maintained in the BOC CMM is collected directly from the employee or from the Department or FAA systems authorized for this purpose. When the BOC analyst requests the employee's full name, DOB, and last for of their SSN, the information is entered into the BOC CMM-CASTLE-IR interface and is used for identity verification against the CASTLE-IR repository; the BOC does not retain the data. Employee full name, work telephone number, and FAA email address is provided by the FAA's Active Directory and is used to track inquires and communicate with employees. As discussed in the Overview, employees may be required to provide additional PII on forms or supporting documentation necessary to process their inquiry.

FAA employees may request their benefits or retirement information be updated, amended or changed by contacting a BOC specialist by phone (1-855-322-2363), email (9-ace-FAA-bene@faa.gov), fax (816-329-2418 or 816-329-2476), or postal mail (BOC, 901 Locust Street, Kansas City, Missouri 64106). If there is an error in an employee's information on a benefits form, the individual must complete a new form and submit it to the BOC. If updates are needed to information maintained in CASTLE-IR, the employee should contact their local HR office. Corrections to Active Directory information are managed by the employee's local IT office.

Under the provisions of the Privacy Act, individuals may request searches of agency records to determine if any added records pertain to them. Individuals wishing to know if their records appear in this system may inquire in person or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Avenue, SW
Washington, DC 20591

The request must include the following information:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records
- A signed attestation of identity

DOT Privacy - Approved - 032520

Individuals seeking to contest information about them that is contained in the BOC CMM should make their request in writing, detailing the reasons their records must be corrected and addressing their letter to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Avenue, SW
Washington, DC 20591

Additional information about the Department's privacy program may be found at https://www.transportation.gov/privacy-program. Individuals may also contact the DOT Chief Privacy Officer at privacy@dot.gov.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which its collects, uses, maintains, or disseminates PII.

Any PII, such as full name, date of birth, work email address and job title, is used in BOC CMM for the purpose of assisting BOC personnel track and process benefits and retirement inquiries and actions for FAA employees.

BOC CMM uses employee information in accordance with the purposes for which it is collected under OPM/GOVT 1, discussed above.

The BOC CMM operates under the following authorities:

- *Retirement Counseling,* 5 U.S.C. § 8350 empowers the FAA, or any federal agency, to appoint a "retirement counselor to furnish information on benefits and counseling services relating to such benefits to other employees of the agency." Retirement counselor is any employee of the agency designated by the head of the agency to furnish information on employee benefits, such as retirement and insurance benefits.
- FAA Order 1100.1 B: FAA may "appoint, develop, and sustain employees through human resources programs including: compensation and benefits."

The information collected on the OPM forms maintained in the BOC CMM, is authorized by 5 United States Code, Sections 1302, 2951, 3301, 3372, 4118, Chapters 83 and 84, and Pub. L. 94-455.

DOT Privacy Approved - 032520

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only if necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The FAA manages risk by minimizing the amount of PII collected by BOC CMM to the information relevant and necessary to assist the BOC track, manage, and process benefits and retirement inquiries and actions. The BOC CMM uses the full name, DOB, and last four digits of the SSN to validate an employee's identity against the CASTLE-IR repository. CASTLE-IR also provides read-only access to additional data to assist with the processing of benefit or retirement inquiries. Active Directory information, such as the full name, work telephone number, and FAA email address of an employee is used to track the inquiry and communicate with the employee. An employee may choose to disclose their personal email address as the preferred mode of communication with the BOC specialist on open inquiries.

Employees may be required to provide forms or supporting documentation to process their inquiry as discussed in the Overview. BOC CMM temporarily stores these forms as part of the record for processing benefits and retirement actions.

to the applicable case file. All case files are encrypted and hard copies are stored in a locked file cabinet at the BOC office for one year after the case has been closed. Employees may be required to provide documentation containing medical information. This documentation is maintained in hard copy form only and is stored in a locked file cabinet at the BOC office for

BOC CMM retains case management records for employee benefits and retirement action requests in accordance with NARA General Records Schedule (GRS) 5.2, *Transitory and Intermediary Records*, item 10. Records are destroyed when no longer needed for business use, or according to agency predetermined time period or business rule. FAA has implemented an automated rule to purge all attachments one year after the case is set to "closed" status in BOC CMM (case status changes to "closed" 30 days after it is "resolved"). The case file is maintained indefinitely for service continuity because employees may continue to have inquiries throughout their retirement.

Records related to operational use of the network by FAA employees (BOC and other HR related staff) are retained in accordance with item 20 of NARA, GRS 3.1, *General Technology Management*. These records destroyed 3 years after project, activity, or transaction is completed, but may be retained longer if required for business use.

DOT Privacy Approved 032620

Information about users of the system generated as part of the BOC CMM security systems including login credentials, audit trails, and security monitoring are retained until business use ceases in accordance with NARA GRS 3.2, September 2016, *Information Systems Security Records, System Access Records.*

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

BOC CMM is a workflow management application used to track, manage, and administer the processing of the benefits and retirement inquiries and actions for FAA employees. PII collected by BOC CMM is used only for the purposes of validating the FAA employee's identity and to track, manage, and process an employee's benefit and retirement inquires and actions upon an employee's request.

BOC CMM maintains records in accordance with OPM/GOVT-1 - General Personnel Records. Records in BOC CMM are routinely shared with OPM for the purposes of finalizing benefit and retirement-related actions. In addition to other disclosures generally permitted under 5 U.S.C. § 552a (b) of the Privacy Act, all or a portion of the records or information contained in this application may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a (b) (3) as provided in the SORN.

An interim Memorandum of Understanding (MOU) between the FAA (MyITSM) and DOT (CASTLE-IR) exists and is in effect until March 2020. This sharing agreement allows the BOC CMM to display PII listed in the Appendix A to validate an employee's identity and to assist in the processing of the benefits or retirement inquiry.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

Employees are responsible for ensuring the accuracy of their information on their forms and supporting documentation. The BOC specialist manually enters the full employee's name. The full name must be spelled correctly and validated by the caller.

Active Directory information, such as the employee's full name, FAA email address, and work telephone number is updated daily and populates the BOC CMM case screen when the employee's full name is entered into BOC CMM. The BOC specialist does not revalidate Active Directory information once displayed in the BOC CMM case screen. CASTLE-IR

DOT Privacy - Approved - 032520

information is also updated daily displays into BOC CMM when the caller validated and the case is opened. These updates in Active Directory and CASTLE-IR ensure the accuracy of information that is displayed in BOC CMM. Finally, the BOC CMM provides supervisors with the means to conduct quality reviews by examining case files to ensure they were properly handled and contain accurate information.

Security

DOT shall implement administrative, technical, and physical measures protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

Reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure are in place to protect PII. These safeguards incorporate standards and practices required for Federal information systems under the Federal Information System Management Act (FISMA), and as detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and NIST Special Publication (SP) 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

BOC CMM is a component of MyITSM, which has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. These safeguards strive to achieve the following objectives:

- Ensure the security, integrity, and confidentiality of PII
- Protect against any reasonable, anticipated threats or hazards to the security or integrity of PII
- Protect against unauthorized access to or use of PII

Records in BOC CMM are secured in accordance with applicable rules and policies, including all applicable DOT automated system's security and access policies. Strict controls exist to minimize the risk of compromising the information that is being stored. All BOC CMM cases files, including uploaded forms and attachments, reside in an encrypted database. Access to the computer system containing the records and hard copy forms is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. All access to BOC CMM is logged and monitored.

BOC specialists access the BOC CMM via their PIV card. BOC specialists are required to complete annual security and privacy awareness training and role based training. The training allows individuals to understand how privacy influences their role and perform their

DOT Privacy - Approved - 032520

duties properly and securely in situation involving the use of PII. Necessary clearances and completion of required security and privacy training allows for access to the BOC CMM for BOC users.

BOC personnel are informed of the FAA Rules of Behavior (ROB) for IT Systems and must acknowledge them prior to having access to the BOC CMM. Additionally, AHR has developed an incident response plan for the BOC CMM, which includes procedures for detection of an incident, remediation, and response where appropriate, to protect and inform affected individuals.

BOC CMM, a component of MyITSM, is assessed in accordance with the OMB Circular A-130 Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources* and the DOT Certification and Accreditation Guidance. The MyITSM is approved through the Security Authorization Process under the National Institute of Standards and Technology (NIST).

MyITSM, with the BOC CMM, was issued a three-year authority to operate (ATO) on November 9, 2017. MyITSM is categorized as a moderate risk system in accordance with NIST Federal Information Processing Standards (FIPS) 199.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FAA is responsible for identifying, training, and holding Agency personnel accountable for adhering to FAA privacy and security policies and regulations. FAA follows the Fair Information Principles as best practices for the protection of information associated with the BOC CMM module. The FAA ROB for IT systems governs the BOC CMM module. FAA's Office of the Chief Information Officer, Office of Information Systems Security, Privacy Division, is responsible for governance and administration of FAA Order 1370.121, FAA Information Security and Privacy Program & Policy.

Mandatory annual security and privacy training, as well as FAA ROBs and periodic staff meetings, provides necessary guidance to the handling of data by FAA employees and contractors within BOC CMM. The FAA ROB for IT Systems must be read, understood, and acknowledged by each user prior to a user's authorization to access FAA information systems, including BOC CMM. The FAA conducts regular periodic security and privacy compliance reviews consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*.

DOT Privacy - Approved - 032520

BOC CMM contains audit provisions to ensure proper usage by authorized users and monitoring for unauthorized usage. Authorized BOC supervisors conduct quality control reviews for case files in BOC CMM. Supervisors review files to insure all security and privacy protocols are adhered and followed by BOC personnel.

Responsible Official

Julie Dunn
System Owner, MyITSM BOC CMM
Human Resources Management
1-855-FAA-BENE (322-2363)

Approving Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer

DOT Privacy - Approved - 032520

Appendix A: CASTLE-IR Data Elements

The following data elements are available as read-only data from CASTLE-IR.

- Name
- SSN (look up only)
- EIN
- DOB (look up only)
- Age
- Years of Service
- Job Series
- Position Title
- Special Program Office (SPO)
- Org Code
- Duty Location
- Line of Business
- Supervisor Level
- Supervisor Description
- Statistical Specialty Code
- Statistical Specialty Description
- Bargaining Unit Status (BUS) Code
- Salary
- Retirement Plan Code
- Retirement Plan Description
- Health Benefits Plan Number
- Health Benefits Plan Description
- Federal Employee’s Group Life Insurance (FEGLI) Code
- Federal Employee’s Group Life Insurance (FEGLI) Description
- Date of Accession
- Work Schedule
- Service Computation Date (SCD) for Leave
- SCD for Retirement
- Date Retirement Eligible
- Veterans Status
- Employee Mailing Address (street, city, state, zip)

DOT Privacy - Approved - 032520

Appendix B: Potential PII in MyITSM BOC CMM

The following data elements may be present in the BOC CMM on forms and other documentation provided by the employee

Members of the FAA Employee Workforce

- Name
- Incident number
- Pager number
- Social Security Number (SSN)
- EIC
- FAA email address
- FAA phone number
- Mailing address
- DOB
- Age
- Years of service
- Job series
- Position title
- Special program office
- Organization code
- Duty location
- Line of business
- Supervisor level
- Supervisor description
- BUS code
- Salary
- Retirement plan code
- Retirement plan description
- Health benefits plan number
- Health benefits plan description
- Federal Employee's Group Life Insurance (FEGLI) Code
- FEGLI description
- Date of accession
- Work schedule
- Service Computation date for leave/retirement
- Date retirement eligible
- Veterans status
- Medicare claim number
- Insurance policy number
- Office of Workers Compensation Program (OWCP) Claim Number
- Medical Information (yes/no answers to questions regarding medical conditions. Open text field request condition, dates, duration, kind of treatment)
- Gender
- Height/weight, blood pressure, pulse, yes/no questions related to abnormalities, blank text field to describe abnormalities
- Military serial number
- Compensation numbers
- Enrollment code
- Military service numbers, branch of service
- Military service dates
- Military badges, citations, education
- CSA/CSF/CSI Claim number
- Thrift Savings Program (TSP) Account Number
- Challenge questions

DOT Privacy - Approved - 032520

Members of the Public

- Name
- SSN
- DOB
- Sex
- Marital status (divorce decree, dates)
- Home address
- Medicare claim number
- Insurance policy number
- Email address
- Telephone number
- Relationship code
- Estate/Trust/Tax ID/EIN number
- Account number

DOT Privacy - Approved - 032520

Appendix C: Common Forms in BOC CMM

The table below represents the most common forms found in the Human Resource Case Management (HRCM) for BOC CMM. This table is not exhaustive and is provided to give the reader an understanding of the types of transactions and data managed in the system.

Form ID	Form Name
SF 50	Notification of Personnel Action
SF 1152	Designation of Beneficiary -- Unpaid Compensation of Deceased Civilian Employee
SF 1153	Claim for Unpaid Compensation of Deceased Civilian Employee
SF 2801	Application for Immediate Retirement (Civil Service Retirement System)
SF 2803	Application to Make Deposit or Redeposit
SF 2804	Application to Make Voluntary Contributions, CSRS
SF 2806-1	Notice of Correction of Individual Retirement Record
SF 2808	Designation of Beneficiary, CSRS
SF 2809	Employee Health Benefits Registration Form
SF 2810	Notice of Change in Health Benefits Enrollment
SF 2817	Life Insurance Election: FEGLI
SF 2822	Request for Insurance
SF 2823	Designation of Beneficiary, Federal Employees' Group Life Insurance Program
SF 3100	Individual Retirement Record (FERS)
SF 3102	Designation of Beneficiary, Federal Employees Retirement System
SF 3104B	Documentation and Elections in Support of Application for Death Benefits when Deceased was an Employee at the Time of Death
SF 3107	Application for Immediate Retirement (Federal Employees Retirement System)
SF 3108	Application to Make Service Credit Payment (Federal Employees Retirement System)
SF 3112	Documentation in Support of Disability Retirement Application
SF 3116	Phased Employment/ Phased Retirement Status Elections
OPM 1514	Military Deposit Worksheet

DOT Privacy Approved - 03520

Form ID	Form Name
OPM 1515	Military Service Deposit Election
RI-10-125	Federal Employee Retirement Coverage Corrections Act (FERCCA) Election Form
RI-20-97	Estimated Earnings During Military Service
RI-20-124	Certification of Service Performed as a Law Enforcement Officer, Firefighter, Nuclear Materials Courier, Customs and Border Protection Officer (535 Service), or Air Traffic Controller
FE-6	Claim for Death Benefits, Federal Employees' Group Life Insurance Program
FE-6 DEP	
FAA 2730-71	Cash Award Payment Authorization
FAA 3300-30	Creditable Service Computation
DD-214	Certificate of Release or Discharge from Active Duty
TSP-1	Election Form
TSP-1-C	Catch-Up Contribution Election
TSP-3	Designation of Beneficiary
TSP-17	Information Relating to Deceased Participant
W-4P	

DOT Privacy Approved - 0323