UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Human Capital Data Management and Modernization

Entrance on Duty (EOD) Requirements and System Certification

September 30, 2020

OPM.GOV

Change Page

Version	Date	Revision Description
3.0	09/09/2020	Due to an OPM reorganization, the eOPF Program is now a part of the Office of Human Capital Data Management and Modernization. References to Data Warehouse Program were changed to the appropriate designation. Updated Contact Information. Removed SF 1152, Designation of Beneficiary Unpaid Compensation of Deceased Federal Employee, from the list of approved forms for electronic signature. Changed Certification period for SF 181, Ethnicity and Race Identification; and SF 256, Self Identification of Handicap, to "On or after EOD". Removed the option to file the following forms in eOPF. These forms are filed in the agency records management system. • I 9, Employment Eligibility Verification • SF 1199A, Direct Deposit Sign-Up • FMS 2231, Fast Start Direct Deposit • W 4, Employee Withholding Allowance Changed the eOPF folder to "Permanent" and added a note to the SF 813 clarifying requirement to only file a copy of the form after it is signed by the Records Center.
2.2	04/09/2018	Updated Federal Security Standards (Sec. 5.7.1)
2.1	04/07/2017	Updated formatting
2.0	07/31/2015	Updated citation regarding Source System Identifier to the correct FIRMR Bulletin 3.
1.5	06/30/2015	This document replaces the Entry on Duty (EOD) Requirements Specifications dated February 4, 2014 and the Entrance on Duty (EOD) Self-Certification dated May 28, 2010. Reorganized and consolidated the information presented in this document. Due to OPM OCIO reorganization, the Enterprise Human Resources Integration (EHRI) is now Federal Data Solutions, Data Warehouse Program. References to EHRI were changed to the appropriate designation. Added "Getting Started" describing the steps that should be taken by federal agencies developing EOD solutions. Updated language to stress the following: • EOD is part of the larger process of On-boarding. • Inclusion of a form in the list of 24 standard forms or the list in the CONOPS does not automatically mean that an EOD provider is authorized to transmit the data to eOPF.

Version	Date	Revision Description
		• All PDF Images must comply with the guidance issued by the National Archives and Records Administration (NARA). • All EOD systems must meet the functional requirements in the HR LOB EOD CONOPS document and this document. • Assure the security and reliability of the electronic approval process is equivalent to or greater than a wet signature. • A federal EOD system assures completed forms created as a result of EOD system input and data entry contain a visible source system identifier so the source may be easily identified in either paper or digital format. • All requirements for each form must be met and the agency must certify the EOD system meets the requirements. • Changed the eOPF Folder Side of the SF 813 to Temporary.

Table of Contents

1.0 Overview

The Office of Personnel Management (OPM) policy staff, and form owners worked with a cross-agency work group to develop the standards and policies for federal Entrance on Duty (EOD) systems. Subsequent to the work group, the Human Capital Data Management and Modernization (HCDMM) eOPF Program Management Office (PMO) was tasked with prescribing EOD requirements that:

- Leverage the requirements defined in the Human Resources (HR) Line of Business (LOB) EOD Concept of Operations (CONOPS), specifically as it relates to the utilization and sharing of new hire data.
- Meet the legal and policy standards for the development of EOD systems that produce electronic documents suitable for transmission to the electronic Official Personnel Folder (eOPF).
- Adhere to Form Owner requirements for the electronic completion and certification of forms under their management.
- Define the minimum standard requirements for acceptance of data in eOPF for long-term storage in eOPF.

1.1 EOD Versus On-boarding

EOD is part of the larger process of on-boarding. On-boarding can affect the organization's ability to bring a new employee up to an expected productivity level and retain employees. On-boarding includes the tasks involved in the EOD process -- data collection and provisioning materials for a new employee -- plus the socialization and training that occur to bring the employee up to full productivity.

The EOD process described in the HR LOB EOD CONOPS begins with the employee's acceptance of the tentative offer and extends through the completion of data collection activities associated with the transfer of employee data including to primary data sources such as a Human Resources Information System (HRIS) and eOPF.

The EOD process leverages technology from four primary areas: collection and sharing of new hire data, communication, process monitoring, and, employee provisioning. Data is shared between systems to provide a reduction of data entry and manual processing tasks.

1.2 Purpose

The eOPF PMO is responsible for maintaining the integrity of the eOPF, which protects information rights, benefits, and entitlements of the employee. As such, the PMO created this document to supplement the HR LOB EOD CONOPs and provide requirements and direction for federal agencies in the use of twenty-four (24) standard EOD forms. The use of this information to complete the EOD system certification assures the agency acquires an EOD system that meets the legal requirements for documentation stored in federal employees' eOPFs.

1.3 Scope

The scope of this document specifically deals with the activities that take a selected candidate from the time the offer is accepted through pre-certification to the day the employee reports for duty and the EOD data is transferred to the permanent system of record. The federal form owners approved these EOD requirements.

Form owner approval to electronically complete and certify forms is dependent upon agency compliance with the requirements in this document. Separate form owner approval is necessary when an agency is unable to meet the requirements defined in this document. Forms submitted via an EOD system are not approved for retention in eOPF if created in a system that does not have an EOD certification or a system that lacks approval by the form owner when unable to meet the EOD requirements.

1.4 Document References

The following documents were reviewed and the information contained within them included in the OPM EOD requirements:

- The HR LOB EOD CONOPS available at: https://www.opm.gov/services-for-agencies/hr-line-of-business/standardization/conceptoperations.pdf
- The Electronic Signatures in Global and National Commerce Act, Public Law 106-229 (E Signature Act of 2000) available at: http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/html/PLAW-106publ229.htm
- Government Paperwork Elimination Act (GPEA), Public Law 105-277 available at: http://www.gpo.gov/fdsys/pkg/PLAW-105publ277/html/PLAW-105publ277.htm
- Circular No. A-130, Appendix II, Implementation of the Government Paperwork Elimination Act (GPEA) available at: https://a130.cio.gov/appendix2/
- United States Code (U.S.C.) available at: http://uscode.house.gov/
- Federal Information Resources Management Regulation (FIRMR) Bulletin(s) available at: www.gsa.gov
- Circular A-130, Management of Federal Information Resources available at: https://obamawhitehouse.archives.gov/blog/2016/07/26/managing-federal-information-strategic-resource
- OPM Guide to Processing Personnel Actions (GPPA) available at: https://www.opm.gov/policy-data-oversight/data-analysis-documentation/personnel-documentation/#url=Processing-Personnel-Actions
- The Code of Federal Regulations (CFR) available at: http://www.ecfr.gov/cgi-bin/ECFR?page=browse
- The OPM Guide to Personnel Recordkeeping (GPR) available at: https://www.opm.gov/policy-data-oversight/data-analysis-documentation/personnel-documentation/#url=Personnel-Recordkeeping-GPR
- The Federal Employees Group Life Insurance (FEGLI) Handbook for Annuitants, Compensationers, and Employing Offices available at: https://www.opm.gov/healthcare-insurance/life-insurance/reference-materials/handbook.pdf
- The Privacy Act of 1974 (5 U.S.C. 552a) available at: http://www.gpo.gov/fdsys/granule/USCODE-2010-title5/USCODE-2010-title5-partI-chap5-subchapII-sec552a/content-detail.html
- Internal Revenue Bulletins available at: http://apps.irs.gov/app/picklist/list/internalRevenueBulletins.html
- Summary of the Thrift Savings Plan available at: https://www.tsp.gov/PDF/formspubs/tspbk08.pdf
- Use of Electronic Signatures in Federal Organization Transactions developed by General Services Administration (GSA) and Federal CIO Council at the request of the Office of Management and Budget (OMB) available at: https://cio.gov/wp-

content/uploads/downloads/2014/03/Use_of_ESignatures_in_Federal_Agency_Transactions_v1-0_20130125.pdf

- OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 available at: https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html
- System of Record Notice (SORN) available at https://www.opm.gov/information-management/privacy-policy/privacy-references/sornguide.pdf
- 41 CFR, part 102-194, Standard and Optional Forms Management Program available at http://www.gpo.gov/fdsys/pkg/CFR-2010-title41-vol3/pdf/CFR-2010-title41-vol3-part102-id2104.pdf
- NARA Guidance for the file formats that may be used to store permanent electronic records at https://www.archives.gov/records-mgmt/policy/transfer-guidance.html

1.5 Contacts

The following OPM personnel should be contacted for additional information regarding the requirements contained in this document.

Type of Contact	Name	Telephone	E-mail
eOPF Program Director	Vic Karcher	(202) 606-0078	Vic.Karcher@opm.gov
eOPF Points of Contact	Elizabeth Pienkoski Tom Merz	(202) 210-6753 (202) 321-0106	Elizabeth.Pienkoski@opm.gov Thomas.Merz@opm.gov
eOPF Forms Manager	Andre Smith	(202) 606-4404	Andre.Smith@opm.gov
Technical / Operations Lead Connect:Direct Connectivity Data Transmission Application Configuration Scheduling	Brian Backer	(724) 705-2462	Brian.Backer@opm.gov
Operations Lead	Paul Burke	(202) 606-4809	Paul.Burke@opm.gov
Office of the Chief Information Security Officer	Eboni Smith	(202) 606-4093	Eboni.Smith@opm.gov
Information System Security Officer (ISSO)	Ezenta Nwagwu	(202) 227-5095	Ezenta.Nwagwu@opm.gov

Type of Contact	Name	Telephone	E-mail

2.0 Getting Started

At a minimum, the following steps should be taken by agencies developing federal EOD solutions:

- Develop business rules and agency-specific requirements. Be specific about the needs of the agency; create a business case to outline the agency-specific requirements and objectives using the HR LOB CONOPS as a starting point.
- Perform a thorough review of and follow the guidance in the HR LOB EOD CONOPS document.
- Review existing agency EOD requirements and the EOD solution to ensure compliance with the requirements defined in the HR LOB CONOPS and OPM EOD Requirements document.
- For items of noncompliance, implement actions to modify existing agency requirements and/or the EOD solution.
- Evaluate agency specific EOD forms to determine if the forms are included in the OPM EOD Standard Forms List.
- If agency specific EOD forms are stored in eOPF, but are not part of the OPM Master Forms List, contact the eOPF Forms Manager to facilitate form approval and addition to the OPM Master Forms List.
- If the agency wants to submit more than the standard EOD forms identified in Section 3.1, contact the eOPF PMO to facilitate form approval and requirements.
- Contact the eOPF PMO to obtain a copy of the eOPF Interface Control Document (ICD) to prepare for testing of data transmission to eOPF.
- Contact your eOPF Oversight Manager to coordinate the submission of Memorandum of Understanding (MOU), Interconnection Security Agreement (ISA), Authority to Operate (ATO), and the EOD System Certification.
- Prepare a test plan that includes test scenarios for each of the EOD requirements for each form including file transmission to eOPF.

3.0 EOD Standard Forms

The requirements for federal EOD systems reflect the policy and intentions associated with standard EOD forms. The federal forms used for EOD are found in Appendix D, EOD Data Summary, of the HR LOB EOD CONOPS. https://www.opm.gov/services-for-agencies/hr-line-of-business/standardization/conceptoperations.pdf

Of these, there are twenty-four (24) identified standard EOD forms used throughout federal government. A thorough review of the policies affecting each of the twenty-four (24) forms, specifically with regard to electronic form completion and signatures was completed. Refer to Section 3.1 for a list of the twenty-four (24) forms. The results were documented in the EOD Assumptions document, which is available from the eOPF PMO upon request, and distributed to each of the standard form owners for their acceptance. Assumptions described in the document are supported by existing federal documentation and procedures and do not present new information.

The EOD requirements cover the collection of data and the transmission of data to eOPF and/or a system of record. **Inclusion of a form in the list of twenty-four (24) standard forms or the list in the CONOPS does not automatically mean that an EOD provider is authorized to transmit the data to eOPF.** Based on federal policies and regulations combined with the role of the provider, it may be that the data is transmitted to a system of record such as a payroll/personnel provider for processing prior to submission by that provider to eOPF. For example, for the collection and transmission of the SF 2809, TSP 1, and TSP 1C, the EOD system is authorized to collect the data, however, the payroll/personnel provider is authorized to collect the data, process the document and submit information to eOPF; therefore the EOD provider should provide the appropriate information to the payroll/personnel provider. The agency works with both providers to clearly define requirements and establish who will submit the documents to eOPF to avoid duplication and possibly conflicting documentation.

The twenty-four (24) identified EOD forms are documented on the following EOD Standard Forms List. See Table 3.1. Columns on the EOD Standard Forms List are defined as follows:

- **Form Number** - The column lists the number assigned to the form by the Form Owner.
- **Form Name** - The column lists the name assigned to the form by the Form Owner.
- **Form Owner** - The column indicates the office that owns the form including the right to approve and publish form updates, manage the policy affecting the form and approve/or deny the completion of the form(s) via an EOD system. This office also provides unlocked versions of the forms. For specific contact information for the form owners, please contact the eOPF PMO.
- **eOPF Folder Side** - The column lists the eOPF virtual folder in which the form is stored as specified in the OPM Master Forms List. An eOPF folder side of “N/A” indicates that the form is not stored in the eOPF. Digital Government (DG) form numbers are assigned to forms or documents filed in eOPF that do not have a form number.
- **Electronic Signature Disposition** - The column indicates an electronic signature is/is not acceptable, as stated in existing federal policies. An electronic signature disposition of “approved” indicates the Form Owner’s acceptance of an electronic signature.
- **Form Owner Assumptions Document Approval Status** - The column indicates if the official Form Owner approved the EOD Assumptions contained in the EOD Assumptions document. Acceptance of the Assumptions document indicates form owner acknowledgement of existing policies and a willingness to support EOD systems that

demonstrate the appropriate security and policy requirements commensurate with the level of information sensitivity.

- **Certification Period** - The column indicates when a form can be certified via an EOD system as it relates to the employee's Entrance on Duty date. Certification refers to the time at which the form may be electronically signed and routed to HR for review and approval. The utilization of data that resides on the form may occur at any time. For example, an applicant may enter the data required for the SF 3109 prior to the applicant's EOD date. However, the form cannot be electronically signed until on or after the official EOD date. The official entrance on duty date is defined as the date that the oath of office is executed (as recorded on the SF 61). Execution of the SF 61 (e.g., administration of the oaths and electronic certification of both the appointee and the designated officer) must adhere to the existing form policy. For example, an appropriate witness to the oath must be present and must apply a signature immediately following the witnessing of the oath.
- **eOPF Transmission Format -** The column indicates the three methods by which a document is stored in to eOPF.
    - **Scanned Portable Document Format (PDF) Image** – If a form is not approved for an electronic signature, it must be printed, signed and scanned into eOPF as a PDF image via the eOPF Scan/Import function or a Day Forward scanning service.
    - **Index Data Feed (IDF)** – If a form is generally stored in eOPF an agency may electronically transmit the PDF file with indexing information via a data feed.
    - **Form Data Feed (FDF)** – Preferred method for all forms; however, eOPF is currently configured to receive data only for a limited number of forms. The program is moving towards a data-oriented approach to HR information management and as additional forms become available via this process, the data providers are expected to submit data using this format.

Note: All PDF Images must comply with the guidance issued by the National Archives and Records Administration (NARA) found at https://www.archives.gov/records-mgmt/policy/transfer-guidance.html. At a minimum, the images must be black and white, 300 dots per inch.

An eOPF Transmission Format of "N/A" indicates the form is not stored in the eOPF. For additional information regarding EOD transmission methodology, see the various eOPF ICDs.

3.1 Entrance on Duty Standard Forms List

Form Number	Form Name	Form Owner	eOPF Folder Side	Electronic Signature Disposition	Form Owner Assumptions Document Approval Status	Certification Period	eOPF Transmission Format
GENERAL ENTRANCE ON DUTY FORMS							
OF 306	Declaration for Federal Employment	Office of Personnel Management (OPM)	Permanent	Electronic Signature Accepted	Approved	Prior to EOD Date	Data and PDF file with indexing information
SF 61	Appointment Affidavit	Office of Personnel Management (OPM)	Permanent	Electronic Signature Accepted	Approved	On EOD Date	Data and PDF file with indexing information
SF 144	Statement of Prior Federal Service	Office of Personnel Management (OPM)	Permanent	Electronic Signature Accepted	Approved	Prior to EOD Date	Data and PDF file with indexing information
SF 181	Ethnicity and Race Identification	US Equal Employment Opportunity Commission (EEOC)	N/A Form is not filed in eOPF	N/A	Approved	On or after EOD Date	N/A
SF 256	Self Identification of Handicap	Office of Personnel Management (OPM)	N/A Form is not filed in eOPF	N/A	Approved	On or after EOD Date	N/A
I 9	Employment Eligibility Verification	Department of Homeland Security (DHS)	N/A Form is not filed in eOPF	Electronic Signature Accepted	Approved	Prior to EOD Date	N/A

Form Number	Form Name	Form Owner	eOPF Folder Side	Electronic Signature Disposition	Form Owner Assumptions Document Approval Status	Certification Period	eOPF Transmission Format
SF 312	Classified Information Non Disclosure Agreement	National Archives and Records Administration (NARA)	Permanent	Electronic Signature NOT Accepted	Not Approved	On or After EOD Date	Scanned PDF Image
SF 1199A	Direct Deposit Sign-Up	Department of the Treasury	N/A Form is not filed in eOPF	Electronic Signature Accepted	Approved	On or After EOD Date	N/A
FMS 2231	Fast Start Direct Deposit	Department of the Treasury Financial Management Services (FMS) Note: the SF-1199A may be used in place of the FMS-2231	N/A Form is not filed in eOPF	Electronic Signature Accepted	Approved	On or After EOD Date	N/A
SF 3109	FERS Election of Coverage	Office of Personnel Management (OPM)	Permanent	Electronic Signature Accepted	Approved	On or After EOD Date	Data and PDF file with indexing information
DESIGNATION OF BENEFICIARY FORMS							
SF 2808	Designation of Beneficiary (CSRS)	Office of Personnel Management (OPM)	N/A Form is not filed in eOPF	Electronic Signature NOT Accepted	Not Approved	On or After EOD Date	N/A
SF 2823	Designation of Beneficiary (FEGLI)	Office of Personnel Management (OPM)	Permanent	Electronic Signature NOT Accepted	Not Approved	On or After EOD Date	Scanned PDF Image
SF 3102	Designation of Beneficiary (FERS)	Office of Personnel Management (OPM)	Permanent	Electronic Signature NOT Accepted	Not Approved	On or After EOD Date	Scanned PDF Image

Form Number	Form Name	Form Owner	eOPF Folder Side	Electronic Signature Disposition	Form Owner Assumptions Document Approval Status	Certification Period	eOPF Transmission Format
SF 1152	Designation of Beneficiary Unpaid Comp of Deceased Fed Emp	Office of Personnel Management (OPM)	Temporary	Electronic Signature NOT Accepted	Not Approved	On or After EOD Date	Scanned PDF Image
TSP 3	Thrift Savings Plan Designation of Beneficiary	Thrift Savings Plan Board (TSPB)	N/A Form is not filed in eOPF	Electronic Signature NOT Accepted	Not Approved	On or After EOD Date	N/A
EMPLOYEE ELECTIONS							
TSP 1	Thrift Savings Plan Enrollment	Thrift Savings Plan Board (TSPB)	Permanent	Electronic Signature Accepted	Approved	On or After EOD Date	Data and PDF file with indexing information, scanned PDF image, FDF
TSP 1C	TSP Catch-Up Contribution	Thrift Savings Plan Board (TSPB)	Permanent	Electronic Signature Accepted	Approved	On or After EOD Date	Data and PDF file with indexing information, scanned PDF image, FDF
DG 60	Premium Conversion Waiver/Election Form (Benefits Admin Letter – BAL)	Office of Personnel Management (OPM)	Permanent	Electronic Signature Accepted	Approved	On or After EOD Date	Data and PDF file with indexing information, scanned PDF image, FDF

Form Number	Form Name	Form Owner	eOPF Folder Side	Electronic Signature Disposition	Form Owner Assumptions Document Approval Status	Certification Period	eOPF Transmission Format
LIFE/HEALTH INSURANCE/BENEFITS							
SF 2809	Employee Health Benefits Election	Office of Personnel Management (OPM)	Permanent	Electronic Signature Accepted	Approved	On or After EOD Date	Data and PDF file with indexing information, scanned PDF image, FDF
SF 2817	Life Insurance Election	Office of Personnel Management (OPM)	Permanent	Electronic Signature Accepted	Approved	On or After EOD Date	Data and PDF file with indexing information, scanned PDF image, FDF
WITHHOLDING ALLOWANCES/EXEMPTION CERTIFICATE							
W 4	Employee Withholding Allowance	Department of Treasury, Internal Revenue Service (IRS)	N/A Form is not filed in eOPF	Electronic Signature Accepted	Approved	Prior to EOD Date	N/A
MILITARY SERVICE FORMS							
SF 15	Application for 10-Point Veterans Preference	Office of Personnel Management (OPM)	Permanent	Electronic Signature Accepted	Approved	Prior to EOD Date	Data and PDF file with indexing information
SF 813	Verification of a Military Retiree's Service in Nonwartime Campaigns or Expeditions	Office of Personnel Management (OPM)	Permanent	Electronic Signature Accepted	Approved	Prior to EOD Date	Data and PDF file with indexing information NOTE: File only the copy signed by the Records Center in the OPF.

Form Number	Form Name	Form Owner	eOPF Folder Side	Electronic Signature Disposition	Form Owner Assumptions Document Approval Status	Certification Period	eOPF Transmission Format
SF 180	Request Pertaining to Military Records	National Archives and Records Administration (NARA)	N/A Form is not filed in eOPF	Electronic Signature NOT Accepted	Not Approved	Prior to EOD Date	N/A

4.0 Privacy Requirements

The Privacy Act of 1974 (5 U.S.C. §552a) defines a system of record as “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” Under this definition, a federal EOD system is part of the GOVT-1, General Personnel Records.

Pursuant to Section 208 of the E Government Act of 2002 and the Privacy Act (5 U.S.C. §552a), each agency that maintains a system of records, among other things, must:

- Complete a Privacy Impact Assessment (PIA).
- Inform each individual asked to provide information of the elements required for a Privacy Act Statement.

Agencies should work with their Privacy Policy Office to complete the required tasks appropriately.

4.1 Privacy Impact Assessment

The E-Government Act of 2002 requires agencies to conduct a PIA before developing or procuring IT systems or initiating projects that collect, maintain, or disseminate Personally Identifiable Information (PII) data from or about members of the public, or initiating, consistent with the Paperwork Reduction Act, a new electronic utilization of PII. Upon initiation of EOD system development, agencies should commence a PIA. The PIA must be reviewed by a senior level reviewing official and made available for public review and comment via the Federal Register. The PIA must include:

- The information to be collected (e.g., nature and source).
- Reason the information is collected (e.g., to determine eligibility).
- Intended use of the information (e.g., to verify existing data).
- With whom the information will be shared (e.g., another agency for a specified programmatic purpose).
- The opportunities available to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.
- How the information is secured (e.g., administrative and technological controls).
- Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 provides additional information regarding the completion of a PIA.

4.2 Privacy Act Statement

In accordance with 5 U.S.C. § 552a(e)(3), agencies are required to provide a Privacy Act Statement to all persons asked to provide personal information that goes into a system of record. EOD system owners must ensure that the following elements are present and accessible via an EOD interface:

- Authority - The legal authority for collecting the information, (e.g., statute, executive order, or regulation).
- Purpose - The purpose(s) for collecting the information and how the information will be used.

- Routine Uses - To whom the information may be disclosed outside of the Utilization Department and for what purposes.
- Mandatory or Voluntary Disclosure - Whether providing the information is mandatory or voluntary. Information utilization can only be made mandatory when a federal statute, executive order, regulation, or other lawful order specifically imposes a duty on the person to provide the information, and the person is subject to a specific penalty for failing to provide the requested information.

A federal EOD system must contain an official privacy statement on all reports containing PII.

4.3 Social Security Number Solicitation

Solicitation of an applicant's Social Security Number (SSN) requires additional notice. The following elements should be incorporated into the EOD PIA:

- The law or authority for collecting the SSN.
- How the SSN will be used.
- Whether disclosure is mandatory or voluntary.

4.4 System of Record Notice

Federal EOD systems used to furnish information that resides on Personnel Forms are covered under the GOVT-1 System of Record Notice (SORN). Agency EOD systems that disclose information outside of the already existing routine uses of GOVT-1 must contact OPM to coordinate the amendment of GOVT-1 to include any new routine uses before disclosing EOD information.

5.0 EOD Requirements

All EOD systems must meet the EOD functional requirements contained in the HR LOB EOD CONOPS Appendix C and this document. The eOPF PMO researched and analyzed the existing CONOPS requirements and included additional detail specifically related to eOPF and federal policy. At a minimum, the agency must test and provide documentation to the eOPF PMO for these requirements.

5.1 Form Owner Acceptance

A federal EOD system adheres to form specific requirements as defined by the official form owner. A federal EOD system must contain current form versions and instructions. Refer to Section 3.1 for form owner information.

EOD form owners supply EOD system owners and the eOPF PMO with an update in the event of a form change. Form owners also provide updated, unlocked copies of forms needed by the EOD providers. EOD system owners are not authorized to make any changes to the content or format of federal forms.

OPM and EOD form owners support the GPEA. Circular A-130, Management of Federal Information Resources, section 8 Policy:(g), requires that agencies identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.

5.1.1 Electronic Form Changes and Reproductions

EOD system developers or other personnel cannot modify a federal form. Form reproductions displayed in federal EOD systems must be complete and accurate reproductions of the official form. Pursuant to 41 CFR, part 102-194, GSA authorizes agencies to create electronic personnel forms without obtaining prior approval from GSA or OPM provided the electronic reproduction meets the following criteria:

- The form is complete (contains all instructions and questions);
- The wording and punctuation of all items, instructions, and identifying information match the current official form; and
- The sequence and format for each item on the form must be reproduced to the highest degree possible.

Agencies may not modify federal forms without prior approval. According to OPM's GPPA, requests for additions or deletions of form data must be sent through an agency's Standard and Optional Forms Liaison to the OPM Reports and Forms Manager, as part of the Plans and Policy Group Center for Information Services and Chief Information Officer. A copy of form owner approvals must be provided to the eOPF PMO prior to initiation of electronic transmission of forms to eOPF.

5.1.2 Records Retention

A federal EOD system provides the capability to store, protect, archive, classify, retrieve, and retire documents in compliance with the NARA disposition schedules available at http://www.archives.gov/about/records-schedule/. According to the GPPA, the agency must certify that all NARA disposition schedules are/will continue to be met by the electronic forms system.

5.2 Electronic Signatures

Federal laws and policies support the use of electronic signatures. A federal EOD provider must use electronic signature methods that comply with the Government Paperwork Elimination Act (GPEA) and the National Institute of Standards and Technology (NIST) Guidance for Electronic Signatures available at http://www.nist.gov/itl/csd/fips-072313.cfm.

The GPEA specifically provides that electronic records and their related electronic signatures are not denied legal effect, validity, or enforceability merely because they are in electronic form. OMB guidance implementing this Act does not limit electronic signature transactions to a particular group, (e.g., applicant, appointee, witness, etc.) and is therefore deemed applicable to required Appointing Officer signatures, whenever practicable. OMB guidance states:

> *Sometimes a notary or other third party signs as witness to the signature. When converting these transactions to electronic systems, agencies should ensure that the selected technology and its implementation are able to provide similar functions.*

Agencies should strive to permit individuals or entities the option to submit information or transact with the agencies electronically and to maintain records electronically, when practicable. Most form owners allow their forms to be electronically signed if the agency deems the security and reliability of its electronic approval process to be equivalent or greater than that of a written signature, and the utilization of an electronic signature is practicable.

Agencies are tasked with implementing the appropriate electronic signature solution in accordance with GPEA and related guidance. Agencies must thoroughly evaluate the commensurate risk and benefits associated with electronic signature technologies and certify the approval process is equivalent to or greater than a wet signature. Each agency must ensure that all appropriate requirements and guidance were followed in assessing and implementing electronic signature alternatives before approving the use of an electronic signature for a particular form. The following sections of the GPEA contain valuable information related to the use of Electronic Signatures:

- Section 1703: Procedures for Use and Acceptance of Electronic Signatures by Executive Agencies
- Section 1706: Study on Use of Electronic Signatures
- Section 1707: Enforceability and Legal Effect of Electronic Records

Additionally, Circular No. A-130, Appendix II, Implementation of the GPEA provides guidance for implementing electronic signature systems.

According to OMB guidance on the implementation of GPEA and the use of electronic signatures:

> *Agencies may institute the use of electronic signatures for personnel records, business applications, and information utilization whenever the use of electronic transactions is practicable and equal to a written signature; the use is not prohibited by law or regulation; or the document containing the electronic signature is not required to be retained in paper format.* ***In addition, OPM has identified the following documents that may not be signed electronically at this time****:*
>
> - *SF-2823 Designation of Beneficiary under FEGLI Program*
> - *SF-3102 Designation of Beneficiary (FERS)*
> - *SF-2808 Designation of Beneficiary (CSRS)*
> - *RI-76-10 Assignment of Federal Employees, Group Life Insurance (FEGLI) (must be witnessed)*

- *SF-1152 Designation of Beneficiary Unpaid Compensation of Deceased Federal Employee*

Agencies must contact the form owner for additional information regarding form specific electronic signature dispositions and related policy. Forms requiring a written signature must be printed from the EOD application, signed, and processed according to the current paper process.

5.2.1 Electronic Signature Block Text

For the development of federal EOD system, the applicant signature block on an electronically signed form must contain the text "Electronically signed by <Signer Name>". Alternate signature blocks (Witness, Agency Official, etc.) must contain the signer's name and title, regardless of whether or not the signee title is present in a separate field.

For a system to be considered "certified" an ATO must be granted and a copy of the letter or memorandum is provided to the eOPF PMO. A certified system also assumes that an agency and EOD provider complies with the terms and conditions outlined in this document.

5.2.2 Electronic Signature Dates

The electronic signature date must be affixed at the time of certification and in accordance with the policy of the form to which it is applied For example, an SF 61 must be certified on an employee's EOD date and an SF 2817 cannot be certified until after the Oath of Office (SF 61) is administered.

5.3 Data Entry

A federal EOD system requires users to enter information one time, so that data elements required on multiple forms are collected once. As prescribed in the 44 U.S.C. § 3506, a system designed for the utilization of personnel information must reduce:

> *…to the extent practicable and appropriate the burden on persons who shall provide information to or for the agency, including with respect to small entities, as defined under section 601(6) of title 5, the use of such techniques…44 U.S.C. § 3506 (c)(3)*
>
> *…as the clarification, consolidation, or simplification of compliance and reporting requirements…44 U.S.C. § 3506(c)(3)(C)(ii)*
>
> *…to the maximum extent practicable, uses information technology to reduce burden and improve data quality, agency efficiency and responsiveness to the public…44 U.S.C. § 3506(c)(3)(J)*

To comply with this requirement, some agencies may elect to implement a questionnaire-like user interface to collect required data. Via this method, questions contained on more than one (1) form must be combined into a single clear and unambiguous question to fulfill the intent of multiple forms. For example, the data elements, "Name", "Surname, First Name", "Family Name, Given Name" are rephrased to state "Full Legal Name." Questions that are unique to a single form are not restated to avoid compromising their original intent.

This requirement is supported by Title 44 U.S.C, section 3506, which prescribes the government obligation to refine data utilization so that it:

> *…is not unnecessarily duplicative of information otherwise reasonably accessible to the agency; section 3506(B)*
>
> *…is written using plain, coherent, and unambiguous terminology and is understandable to those who are to respond; section 3506(D)*

The HR LOB EOD CONOPS translates this directive into a requirement to use plain language. In all cases, questions must adhere to the intent of the form(s) on which the response resides. Systems are designed with sufficient consideration as to whether or not a question is subject to multiple interpretations. For example, if a question is subject to interpretation, additional information is provided via the user interface to clarify the request.

5.3.1 Data Utilization Grouping

A federal EOD system groups data by category so that user input is simplified. Categories are defined by logical information groups such as General Information or Prior Federal Service, and may be presented as separate panels or screens. Categories are determined by pre-identified criteria (position-driven requirements) to define and simplify the data utilization. For example, if an EOD system uses a questionnaire approach to data utilization, the user may be guided through a series of panels containing multiple questions. In this case, each panel represents a category of data utilization.

5.3.2 Data Input Sources

A federal EOD system automatically populates EOD required data elements from applicable sources and requires a verify data input from external sources prior to the completion of additional data input. Applicable sources may include, but are not limited to, E-Verify, e-QIP and USA Staffing. Technical requirements are coordinated through the appropriate data providers. Agencies should review the EOD CONOPS, which prescribes an integrated approach to EOD for additional information regarding input sources.

5.3.3 Personal/Public Email Address

A federal EOD system allows the manual entry of an applicant's personal email address and uses the email address for EOD logon information and notifications as the applicant may not yet be a federal employee with a government issued email address. The EOD system must provide secure information via email following the NIST guidelines for information security.

5.3.4 Additional Reference Information

A federal EOD system includes all instructions and related information necessary for the user to make an informed decision relative to the respective forms. For example, if benefits brochures and booklets are generally provided to assist the employee with making elections to complete the SF 2809 form then they are available via an EOD application. The implementation of this requirement varies by system design, and may be as simple as providing a link to associated documentation on an external site.

5.3.5 Educational Data Update

A federal EOD system captures employee Educational Data as defined in the Guide to Human Resources Reporting (GHRR) for transmission to OPM via an agency's HRIS system. Required data elements include Instructional Program Code, Educational Level Code, and Degree Year.

5.3.6 Real-time Updates

The HR LOB EOD CONOPS states that a federal EOD system must update records in real-time. The eOPF PMO interprets this requirement to preclude the use of batch processing. Electronic signatures must be affixed at the time of certification.

5.3.7 Mass Hires

A federal EOD system accommodates mass hires for the same position or multiple positions. The EOD process is capable of being initiated for multiple users simultaneously.

5.3.8 Data Validation

A federal EOD system validates data entry to the extent practicable to reduce the burden on both the appointee and the HR office. Examples include:

- An EOD system prompts a user to check the dates if an employee's birth date is later than the date of the employee's last federal appointment;
- An EOD system prompts a user to check the marital status when an employee selects unmarried (as required for the SF 15, SF 2809 and W4) but the employee attempts to register a spouse for Health Benefits.
- An EOD system prompts a user to check the birth date when an individual's birth date indicates the person is younger than 16, making the person ineligible for federal employment.

Data Validation also occurs at the form level to verify the user is eligible for the completion of certain forms. Examples are:

- When an individual is not appointed as a federal employee, the signature does not appear in the "appointee's signature" space of the OF 306.
- When an employee has not completed the certification of the SF 61, Oath of Office, the employee is ineligible to submit an SF 3109 or an SF 2809 because the employee is not eligible for benefits as a federal employee.

5.3.9 Error Alerts

A federal EOD system provides error alerts or messages to ensure users thoroughly review entered data. Error alerts occur when specified edits are required at field level, prior to category completion and prior to final data submission. Prior to final data review, an EOD system displays a list of errors associated with data submission and provides the ability for the user to return to the correct page(s) to correct the errors.

5.3.10 Form Preview Capability

A federal EOD system allows EOD users to view forms at any time during the data utilization process. OMB's guidance for the implementation of the GPEA stresses the importance of minimizing the likelihood of repudiation. The user is provided with the opportunity to view EOD forms to which the data will apply during the data input process. This stresses the importance and the implications of the transaction.

5.3.11 Electronic Form Completion

A federal EOD system allows form completion to occur at any time. However, form certification may only occur in accordance with the certification period for each form on the EOD Standard Forms List. Electronic form completion refers to the process by which a user enters data that is applied to an EOD form. Electronic form certification refers to the electronic approval of an EOD form, which is verified with the application of an electronic signature.

For example, the applicant data entry required for completion of the SF 61 may occur prior to the EOD date. However, electronic certification (i.e., application of the electronic signature for both the applicant and witness) cannot take place until the official EOD date.

The completion of forms via an EOD system does not modify the policy surrounding a form; it simply modifies the method with which the form is administered. For example, an SF 61 still requires a witness to the administration of the Oath of Office; however, the witness may indicate approval electronically.

The appropriate certification period associated with forms is not modified for completion via an EOD system. For example, eligibility for federal benefits and the completion of the associated election forms (e.g., SF 2809 and SF 3109) cannot be certified prior to employee and witness certification of the Oath of Office.

5.4 Electronic Certification of Multiple Forms

A federal EOD system allows the electronic approval (signature) of multiple forms in a manner consistent with the guidance contained in Circular No.A-130, Appendix II, Implementation of the GPEA, section 6(c) states:

> *Users should be able to decide how, when, and what type of electronic authentication to use of those made available by the agency. If none are acceptable the user should be able to opt out to a paper process. If a user wants a certain mechanism for authentication to apply only to a single agency or to a single type of transaction, the user's desires should be honored, if practicable. Conversely, if the user wishes the authentication to work with multiple agencies or for multiple types of transactions, that should also be permitted where practicable. Specifically, it should be consistent with how the agency employs such means of authentication and with relevant statute and regulation and only if it conforms to practicable costs and risks.*

A federal EOD system must allow for a variety of user constraints and requirements as practical. For example, if a user does not wish to certify multiple forms simultaneously, the user is allowed to select the forms to which the user's approval will apply. If a user is unable to complete an electronic EOD process, an alternative paper process is available. As stated in Circular No.A-130, Appendix II, Implementation of the GPEA, a user may apply an authentication mechanism for a single transaction.

Certain EOD forms can be authenticated (electronically signed) prior to an applicant's EOD date, and some cannot be authenticated until after an applicant's EOD date. An applicant may decide to submit certain forms during a data input session, but to check remaining data elements and to enter them at a later date. EOD systems must accommodate this requirement. For these reasons, a federal EOD system must allow for the electronic approval of selected single forms as appropriate.

5.4.1 Data Input Confirmation

A federal EOD system assures the user confirms, certifies and accepts the data. At a minimum, the following certification steps must occur:

- The federal EOD system provides an electronic read-only PDF of the populated forms prior to the user's certification of completion. The Electronic Signatures in Global and National Commerce Act, Public Law 106-229 (E Signature Act of 2000) and the GPEA support the requirement that an individual who is asked to apply an electronic signature to a document must be allowed to see the form in full before applying the signature.
- The federal EOD system provides, prior to electronic approval/signature of all forms, a certification statement containing:
    - Certification that the individual reviewed the information provided in the form(s) and acknowledges the electronic approval is the equivalent of signing each form.
    - Implications for submission of fraudulent information.
    - Consent to the electronic release of information as appropriate (e.g., to HR Staff or Federal Investigators).

    - Privacy Act Statement that includes the agency's authority, purpose, routine use, and disclosure disposition for the utilization of EOD information.
- The federal EOD system provides a confirmation page containing the list of forms electronically completed, certified and signed; the date/time of certification for each form; and a copy of the certification text following electronic approval/signature of forms.
- The federal EOD system must prompt the user to either save and/or print the confirmation page for own records.

5.4.2 User Actions Audit Trail

A federal EOD system must generate an audit trail that demonstrates the individual was provided with sufficient notice and review time to verify the data input prior to certification and release of the information.

According to the GPPA, for each form that is cleared or signed electronically, there must be an audit trail to show when and who:

- Signed/approved the data/form,
- Cleared the data/form,
- Input data to, and/or
- Changed data on the form.

In the event an employee contests the certification of certain forms/data, a federal EOD system must be able to produce an audit trail demonstrating that the employee viewed the data input and was provided with the information prior to the release of the information. While the forms created as a result of data input must be transmitted to a system of record within 90 days, an EOD audit trail containing sufficient data to justify the legal sufficiency forms completed via the system is maintained indefinitely. The application and depth of this requirement will vary by agency.

5.5 Review

An EOD solution allows managers and HR personnel to monitor the EOD process, preferably through a dashboard type view. Compliance with legal, regulatory, and policy requirements must be considered when designing what to monitor; the privacy and security of personal data must be carefully safeguarded. Issues around compliance could be tied to manager notifications or reminders. EOD tasks are monitored for completion and the appropriate notifications are sent when timelines are not met. A federal EOD system integrates the HR review as appropriate to promote the integrity of employee EOD forms and reduce the burden on applicants and staff. However, electronic systems do not replace HR's obligation to review and approve employee documentation. Per the 5 U.S.C. 552a (e)(5) agencies must

> *...maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination…*

Actions by HR Specialists are tracked at the form field level and are traceable to the individual HR Specialist who completes a specific action.

5.5.1 Employment Eligibility Verification

A federal EOD system allows agencies, as authorized in the 8 CFR 274a.2, to complete employee eligibility verification prior to federal employment. The Employment Eligibility Verification Program (E-Verify) meets the requirements of an employment verification system.

Employment eligibility requirements must be considered during the design and implementation of an EOD system, and external sources, such as E-Verify, are incorporated as appropriate.

5.5.2 Monitoring

A federal EOD system allows HR to monitor user progress through the EOD process and allows HR to send notifications to remind the user of required actions when certain pre-determined conditions exist. Pre-determined conditions include the failure of a user to meet specified completion timeframes or submit required supporting documentation. An example of required supporting documentation may include additional requirements associated with the SF 3109, FERS Election of Coverage, etc.. When an employee indicates via an EOD system that the employee has a living former spouse to whom a court order, on file at OPM, awards a portion of the employee's annuity (see SF 3109, Question 5), the employee must also complete OPM Form 1556, Former Spouse's Consent to FERS Election, request for waiver of consent requirement, or request for extension of election deadline to modify court order. If the employee fails to meet the preceding conditions, an EOD system should notify HR.

A federal EOD system also monitors the progress of the user entry through the process and where practical the system issues automatic notifications. For example, when an applicant does not complete the EOD input within a specified period–of-time, the system automatically notifies the HR servicing office that follow-up is necessary.

5.5.3 Applicant Data Input Changes

A federal EOD system does not allow an employee to initiate changes to data or form contents following approval and release of the EOD forms. The employee releases ownership of the forms and can no longer initiate changes via the EOD system following an employee's electronic signature certifying completion of standard EOD forms.

After the employee applies an electronic signature certifying completion of the forms, an HR representative must review the forms and may reject any forms deemed inadequately completed. At this time, the employee may edit the information to re-populate the rejected form and submit a new form via the EOD system.

When the HR representative reviews and accepts a form, it is transmitted to the final system of record such as eOPF or the HRIS and the document in the EOD system is destroyed or an alternate appropriate action is taken per the agency records manager. At this point, employee changes or revisions must be coordinated with the HR servicing office.

The process described above mirrors the current paper process in which an employee cannot make corrections to an existing form, but can submit a revised form through the HR servicing office. This process is supported by Circular No. A-130, Implementation of the GPEA:

> *Carefully control access to the electronic data, after receipt, yet make it available in a meaningful and timely fashion. Security measures should be in place to ensure that no one is able to alter a transaction, or substitute something in its place, once it has been received by the agency unless the alteration is a valid correction contained in an electronically certified re-transmission.*

5.6 Electronic Form Storage

A federal EOD system allows an authorized user to print completed EOD forms, as they appear when completed via the paper form prior to electronic transmission to eOPF or the agency HRIS. According to the GPPA, an agency that stores Official Personnel Folder (OPF) forms electronically, must store them in such a way that, when a paper copy is needed, that copy looks essentially like the original approved OPM standard, or agency form.

5.6.1 Form Packages

A federal EOD system provides the capability to define and store form packages. A form package is a set of forms necessary for completion based on the type of appointment and occupation. The content of the form package may be different by agency. For example, if a "temporary assignment" form package is defined, it may not include the completion of an SF 2809 as temporary employees are ineligible for health benefits. Additional examples of such packages are "seasonal" hires, "occupational" grouping and "type of appointment".

5.6.2 Form Library

A federal EOD system supports form libraries. A form library is a group of forms available for selection and completion via an EOD system. Libraries may be defined by form packages and are grouped by logical categories (e.g., agency-specific, standard forms, etc.). System administrators must have the ability to add forms and documents to the form library.

5.6.3 Date and Time Stamps

A federal EOD system provides date and time stamps where appropriate and at the form level for storage in the system audit trail. Appropriate instances include but are not limited to a record of when a form is electronically:

- Completed, certified and submitted by the employee,
- Transmitted to HR,
- Approved by HR,
- Transmitted to a system of record (A form cannot be transmitted out of the EOD system until a final EOD date is populated.), and
- Transmitted to eOPF.

The system also captures when users view the recreations of their forms, certification statements, and form input data. The certification date is captured and maintained at the form level.

The system also captures the:

- Date of tentative offer extension,
- Date of acceptance,
- Scheduled EOD date which is provided before an applicant is granted access to the EOD system, and
- Actual EOD date which is used to verify employee eligibility for federal benefits.

5.7 Role-Based Rights

A federal EOD system provides levels of secured access based on the role of the user. Role-based capabilities allow viewing, printing, and form completion. When appropriate, roles are defined in a way that is similar to the rights and responsibilities assigned in the paper world.

For example, HR Specialists and employees are assigned view and print capabilities to their roles at the form level and are granted the right to modify effective dates, following employee data submission.

5.7.1 Federal Security Standards

Federal EOD system provides users access that complies with Federal standards and regulations. Federal standards include Federal Information Processing Standards (FIPS)

Publication 200, Federal Information Security Modernization Act of 2014 (FISMA), and Office of Management and Budget (OMB) Circular No. A-130.

5.7.2 Administrator Rights

A federal EOD system allows designated EOD system administrators to:

- Add, change, and delete form packages within the system;
- Manage user accounts, role assignments, reports generation and workflow management; and
- Perform other additional administrative tasks deemed necessary by the agency.

5.7.3 Access Metrics

A federal EOD system provides a reporting capability for access metrics concerning all EOD users. Administrative users are able to access a report that details which users accessed the EOD system and the time of the access. Similarly, a report indicates which HR Specialists accessed a particular user account or form, and when the access occurred.

5.7.4 Temporary Account Termination

A federal EOD system automatically terminates temporary accounts after notification of successful record transmission, or within 90 days. Termination of temporary accounts includes the denial of further employee access to the EOD system and the deletion of forms created as a result of data entry.

5.8 Data Export

A federal EOD system exports data to other applicable sources . Applicable sources may include eOPF, agency payroll offices, or agency HRIS. An EOD application is not a long-term system of record. Forms not delivered to eOPF must be transmitted to a system of record, as defined by the agency's Record Manager, within 90 days from the date of HR office approval.

Employee records (i.e., the forms created as a result of data entry) are not maintained in more than one system, per Circular No. A-130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, available at https://www.digitalgov.gov/resources/appendix-i-to-omb-circular-no-a-130-federal-agency-responsibilities-for-maintaining-records-about-individuals/ .

> "*Agencies should not publish systems of records that wholly or partly duplicate existing government-wide systems of records*."

5.8.1 eOPF Interface Control Document (ICD)

A federal EOD system transmits files to eOPF that comply with the requirements and specifications detailed in the various eOPF ICDs. Agencies and data providers are required to provide accurate and complete data in compliance with the ICDs. The accuracy and validity of eOPF is dependent upon the submission of appropriate data. The agency may request a copy of the eOPF ICDs from the eOPF PMO.

Data transmission to eOPF cannot take place until the agency verifies an employee account is created in eOPF. This may be established by setting up an automated check for whether or not an eOPF account exists or by HR manually verifying the account creation by accessing eOPF.

5.8.2 Data Reconciliation

A federal EOD system must capture and maintain sufficient data to provide for reconciliation of data transmission between systems.

Agencies must define a business process to validate a record successfully transmitted within 90 days from the official EOD date. Documents are purged following reconciliation of transmission data. EOD is not used as a long-term system of record. All EOD forms must be transmitted to either eOPF, HRIS or to an alternate system of record, prior to account termination.

5.8.3 Transmission Receipt

A federal EOD system provides administrative users with a transmission receipt following the successful transmission of EOD data to external sources (e.g., eOPF, HRIS, etc.) and provides error messages for the data in the files that do not successfully transmit.

5.8.4 Source System Identifier

A federal EOD system assures completed forms created as a result of EOD system input and data entry contain a visible source system identifier so the source may be easily identified in either paper or digital format. The source system identifier must appear on the face page below or near the form number. The required source system identifier format is:

`EOD:<Agency/Agency Sub Element Code>.`

For example, the OPM source system identifier is EOD:OM00. A list of agency sub-element codes may be found in the Guide to Personnel Data Standards, located at: http://www.opm.gov/feddata/guidance.asp.

If a form is later questioned or contested in a court of law, it is important to trace data entry to the source system to determine whether the system requirements comply with federal policy. If a form is printed and the paper copy is deemed the official record, meta-data associated with the source system may be lost. For this reason, a visible source system identifier must appear on the form itself. The FIRMR Bulletin B-3 included the following guidance relative to electronic systems producing optional and standard government forms:

> *The name and producer/vendor (if any) of the software used to create the electronic form must appear on the face page below or near the form number. Form users and agencies need a way to identify electronic versions of forms from printer versions, in determining the quality and accuracy of the software, and in the overall performance of the producer/vendor.*

5.9 Cycle Time Metrics

The full Performance Indicators or Cycle Time Metrics can be found in Appendix E, Performance Indicators, of the HR LOB EOD CONOPS. A federal EOD system provides a reporting capability for cycle time metrics for all administrative EOD users. Cycle time metrics are used to analyze EOD process efficiency and compliance with the OPM End-to-End Hiring Initiative. Performance indicators include but are not limited to:

- Time from recruiting to EOD system – From the date of the tentative offer acceptance to the date the record is built in EOD.
- Time to access EOD system – From the time the record is built in EOD to the time the prospective employee receives access to log on.
- Time to complete condition (Applicant) – From login notification to date all conditions are met.
- Time to complete condition (HR) – From date received the record for HR documentation to the date returned to the Applicant.
- Time from completing conditions to Report for Duty date – The number of days from all conditions being satisfied until the report for duty date.

- Time from acceptance to Report for Duty date – The number of days from acceptance of formal offer by prospective employee to the report for duty date.

5.10 508 Compliancy

In compliance with 29 U.S.C. 794d, a federal EOD system and EOD system output must be Section 508 compliant. System output may include completed forms, reports, and verification pages.

5.11 Tiered Help Capability

A federal EOD system contains a tiered help capability to include the use of online help and help desk support.

5.11.1 Help Roles

The HR LOB EOD CONOPS requires the capability for help roles (e.g., system administrators, help desk) to view the EOD record. Security and rights associated with help roles must be strictly controlled and restricted to a read-only privilege. Whenever possible, form-level user restrictions are applied. For example, if a user assigned to a help role only allowed to view certain forms, access is restricted to the appropriate form-level access. EOD system owners must thoroughly evaluate the commensurate risk and benefits associated with help roles and develop a process for the assignment of such roles.

5.11.2 Error Reporting

A federal EOD system displays a list of errors associated with data entry and provides hyperlinks back to page(s) to enable correction of errors. A federal EOD system also allows System Problem Reports (SPR). An error reporting and resolution process may feed into a configuration control process.

5.11.3 Change Requests

A federal EOD system allows Change Requests (CR). A Change Request submission and resolution process, as defined by program management, may feed into a configuration control process.

5.11.4 System Documentation

A federal EOD system maintains, and makes available upon request, complete descriptions of:

- The electronic generation and storage system, including all procedures relating to its use.
- The indexing system, which permits the identification and retrieval for the viewing or reproducing of relevant records maintained in an electronic storage system.
- The business processes that create, modify, and maintain the retained forms, and establish the authenticity and integrity of the forms, such as audit trails.

6.0 eOPF System Certification

The eOPF PMO is committed to maintaining the integrity of eOPF, which protects information rights, benefits, and entitlements of the employee. Agencies that send documents to eOPF from federal EOD systems are subject to the requirements defined in this document and the eOPF ICDs.

The completion of appropriate documentation by the agency, the Data Provider, and eOPF PMO is required before data is transmitted for the first time. An agency is considered certified when the eOPF PMO is provided with documentation confirming that all requirements in the ICDs and the EOD guidance are complete. If an agency is unable to comply with the requirements defined in this document and the ICDs, separate form owner approval must be granted and the electronic transmission of documents to eOPF will be denied until all criteria are met.

The following documents are required to ensure all parties comply with established conditions:

- **Memorandum of Understanding (MOU)** – A business-level agreement or contract between OPM and the agency. The MOU specifies the quality of data and requirements for adherence to OPM standards and guidelines.
- **EOD System Certification** – A list of requirements an agency must meet before transmitting EOD data to eOPF. The agency must test the functionality of the EOD system and provide a certification indicating the EOD requirements in this document and the HRLOD EOD CONOPS are met.
- **Terms of Reference (TOR) Addendum** – When sending data containing electronic signatures, agencies must obtain approval to use an electronic signature in lieu of personally signed paper SF 50s in accordance with the GPR, Ch. 1 and the GPPA, Ch. 3. The agency must complete a TOR and provide it to the eOF PMO when the agency uses an electronic signature on its SF 50s without OPM approval.
- **Interconnection Security Agreement (ISA)** – An agreement between two parties who plan to exchange data. The ISA specifies the technical and security requirements of the interconnection, and the MOU defines the responsibilities of the participating organizations. Any two systems that share a connection, VPN or otherwise, require an ISA in place. The caveat is when two OPM systems interconnect, only a MOU is needed.
- **Authority to Operate (ATO)** – A letter or memorandum from the agency's senior official indicating the successful completion of the Security Assessment and Authorization (SA&A) process, including a plan to continue to mitigate problems and sustain operations.
- **Test Plan** - The agency and Data Provider must provide a complete test plan for review and approval by the eOPF PMO. The plan must include accuracy analysis with feedback for all EOD requirements and the Data Provider's test data submissions.

7.0 EOD System Certification

This section provides criteria for a "System Certification" on an EOD system for electronic transmission of data and/or index data feed/PDF files to an agency's eOPF instance. The system certification is a means for the eOPF PMO and agency to evaluate whether there is reasonable assurance that an EOD system meets the legal sufficiency requirements, which includes relevant policy requirements, electronic signature dispositions, and form owner acceptance of forms that are completed electronically.

7.1 EOD Certification - System Certification Worksheet

The System Certification Worksheet is prepared by the agency with the assistance of the Data Provider. The System Certification is performed by the eOPF PMO.

7.2 EOD Certification - System Certification Worksheet Definitions

The following definitions apply to the column headings on the System Certification worksheet.

- **Requirements:** EOD requirements.
- **Reference Section and Description:** Identifies the section containing details of the requirement.
- **EOD System Meets Requirement for Each Form Yes/No:** For each requirement, determine whether the EOD system being evaluated meets the requirement, partially meets the requirement, or does not meet the requirement.
- **If no, what is the action plan for correcting system?** When the EOD system partially meets the requirement or does not meet the requirement, document the action plan by the EOD provider and/or agency to meet the requirement. Include supporting documentation, the Form Number, the requirement, explanation of issue and course of action to meet the requirement. When the action plan is completed, the agency must retest and certify the requirements are met.
- **Proposed Implementation Date** – Provide a commitment date for each requirement that partially meets the requirement or does not meet the requirement. All requirements for all forms must be met prior to certification.

The implementation of the EOD system and transmission of forms to eOPF must occur within 45 – 60 days after certification of the EOD system. If it does not, the PMO will not accept any transmissions until a review is completed.

7.3 EOD Certification - System Certification Worksheet Completion Instructions

The following instructions apply to the completion of the EOD System Certification Worksheet for each form. **All requirements for each form must be met** as indicated in Section 5.0 of this document.

- Review each requirement.
- Determine a test scenario to test the requirement in the EOD system.
- Complete the test.
- Evaluate the results.
- Document the results for each form that will be entered into the EOD system
- Capture screen prints.
- Collect other documentation that supports the EOD system meets each requirement for each form.

- When the EOD system does not pass the test, work with the EOD provider and/or other agency personnel to resolve the issues.
- Email the completed certification package with supporting artifacts/documentation to your PMO contact.

The main goal of the reviews and testing is to assure the EOD system is set up to protect the rights, benefits and entitlements of federal employees and complies with federal laws and relevant policies.

EOD requirements such as compliancy with the NIST Guidance for Electronic Signatures are technical in nature and may require assistance from your agency IT personnel to determine if the EOD software meets the federal regulations and guidance in these areas.

Requirements for 508 compliancy and PIA compliancy may also require assistance from other agency personnel to determine if the EOD software meets the federal regulations and guidance in these areas.

Appendix A. EOD System Certification Package

A completed EOD System Certification Package includes:

- The Cover Sheet
- List of forms submitted to eOPF
- EOD System Certification Worksheet which includes the EOD System Certification Signature Page

Appendix B. Acronym List

Acronym	Definition
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ATO	Authority to Operate
BAL	Benefits Administration Letter
C&A	Certification and Accreditation
CFR	Code of Federal Regulations
CONOPS	Concept of Operations CONOPS
CWISR	Center for Workforce Information and Systems Requirements
DCPDS	Defense Consolidated Personnel Data System
DG	Digital
DHS	Department of Homeland Security
DOB	Date of Birth
DocGUID	Document's Globally Unique Identifier
DOE	Department of Energy
EDF	Employee Data Feed
EEOC	Equal Employment Opportunity Commission
EHRI	Enterprise Human Resources Integration
EOD	Entrance On Duty
eOPF	Electronic Official Personnel Folder
FDF	Form Data Feed
FEGLI	Federal Employees Government Life Insurance

Acronym	Definition
FEHB	Federal Employee Health Benefits
FIPS	Federal Information Processing Standards
FIRMR	Federal Information Resources Management Regulation
FISD	Federal Investigative Services Division
FISMA	Federal Information Security Management Act
FMS	Financial Management Services
GDS	Guide to Personnel Data Standards
GHRR	Guide to Human Resources Reporting
GPEA	Government Paperwork Elimination Act
GPPA	Guide to Processing Personnel Actions
GPR	Guide to Personnel Recordkeeping
GSA	General Services Administration
GUID	Globally Unique Identifier
HR	Human Resources
HRIS	Human Resources Information System
IBC	Interior Business Center
ICD	Interface Control Document
IDF	Index Data Feed
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
LOB	Line of Business
MOU	Memorandum of Understanding

Acronym	Definition
NARA	National Archives and Records Administration
NBC	National Business Center
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NOA	Nature Of Action
OMB	Office of Management and Budget
OCIO	Office of Chief Information Officer
OPF	Official Personnel Folder
OPM	Office of Personnel Management
PA	Privacy Act
PDF	Portable Document Format
PIA	Privacy Impact Assessment
PMO	Program Management Office
POC	Point of Contact
POID	Personnel Office Identifier
SBU	Sensitive But Unclassified
SDD	System Design Document
SHRP	Strategic Human Resources Policy
SA&A	Security Assessment and Authorization
SORN	System of Record Notice
SSI	Source System Identifier
SSN	Social Security Number

Acronym	Definition
TLS	Transport Layer Security
TOR	Terms Of Reference
TSP	Thrift Savings Plan
TSPB	Thrift Savings Plan Board
USC	United States Code
UUID	Universal Unique Identifier
VPN	Virtual Private Network
W3C	World Wide Web Consortium
XML	Extensible Markup Language