EHRI

Enterprise Human Resources Integration

Office of Personnel Management (OPM)

Entrance on Duty (EOD)

Requirements Specifications

From: ENTERPRISE HUMAN RESOURCES INTEGRATION

U.S. Office of Personnel Management
1900 E Street NW, Room 3336
Washington, DC 20415

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Working for America

February 04, 2014

Change Page

Version	Date	Revision Description
1.0	05/29/2009	Initial version
1.1	06/15/2009	Incorporated information from the EOD Form Owner Assumptions document and EHRI PMO comments, including: Updated Forms Table to show the number of approvals, disapprovals, and non-responses Clarified "Use Plain Language" requirement by including an example Added requirement 4.1.4 Form Packages Added requirement 4.1.10 Form Changes and Reproductions Expanded requirement 4.1.13 Electronic Signatures to include a reference to NIST standards Revised requirement 4.1.14 Electronic Certification of Multiple Forms to include reference to OMB guidance. Added requirement 4.1.15 Electronic Certification of Single Forms Added requirement 4.2.7 Data Validation Completed section 7.0 Next Steps
1.2	06/19/2009	Incorporated information from PMO second-round review, including: Modified Requirement 4.1.13 – Electronic Signatures to remove reference to "Digital Signature" technology, and to add an additional reference to the GPEA Updated Section 3.0 – EOD Standard Forms List to include recent form owner feedback (New approvals: SF-81, SF-180, SF-256) Updated Section 7.0 – Next Steps to include reference to agencies with existing EOD solutions
1.3	06/22/2009	Completed Section 3.3 – EOD Work Group to include a group purpose and a list of participating agencies

Version	Date	Revision Description
1.4	07/23/2009	Incorporated EOD Work Group feedback to include: Modified Section 1.0 to include a more comprehensive definition of EOD vs. Onboarding and to cite the consequences of agency non-compliance with OPM EOD requirements Added EHRI EOD team goals to Section 1.3 Modified Section 3.1 to include new Form Owner acceptances for the SF-15 and DG 50 and indicated rejection of the SF-312 and pending approval for the SF-1199A and FMS-2231 Added 2 additional columns to Section 3.1 to define form Completion Period and eOPF Transfer Format and expanded Section 3.0 to include a definition of each column Added an additional Section 4.2, Electronic Form Completion and Certification, to list requirements under this item Added Terms of Reference (TOR) to Section 5.1 – EHRI System Certification Methodology Modified Section 6.3 – SORN to reflect accurate SORN requirement Modified the following sections to cite additional examples and federal guidance to support requirement: 4.1.1 – Use Plain Language 4.1.6 – HR Intervention 4.2.6.1 – Electronic Signature Block Text 4.2.7 – Electronic Certification of Multiple forms (merged with previous requirement - Electronic Certification of Single forms) 4.3.5 – Data Input Sources 4.3.7 – Data Validation 4.3.9 – Source System Identifier 4.4.3 – User Actions Audit Trail 4.5.2 – Data Export 4.5.3 – System of Record 4.5.7 – Records Retention 4.6.2 – Help Roles Added Requirements: 4.1.10 – Additional Reference Information 4.1.11 – Human Resources Role 4.1.12 – Educational Data Update 4.2.1 – Electronic Form Completion 4.2.3 – Electronic Form Changes and Reproductions 4.2.5 – Electronic Form Storage 4.2.6.2 – Electronic Signature Dates 4.5.5 – Transmission Receipt
1.5	08/05/2009	Incorporated EOD Work Group feedback (round 2 edit) to include: Modified document title from “EOD Requirements Specifications” to “OPM EOD Requirements Specifications” Modified Section 3.1 to include new Form Owner acceptances for the SF-199A and FMS-2231. Modified all references to “EHRI EOD Requirements” to “OPM EOD Requirements” Modified the following sections to provide additional detail/examples: 4.1.8 – Applicant Data Input Changes 4.2 – Electronic Form Completion and Certification 4.2.3 – Electronic Form Changes and Reproductions 4.3.9 – Source System Identifier 4.5.3 – System of Record (NOTE: Title changed to “Temporary Account Termination”) 5.1 – EHRI System Certification Methodology
1.6	08/07/2009	Updated Section 6.3 (System of Record Notice), to include OPM Forms Manager revision.

Version	Date	Revision Description
1.7	09/24/2009	Updated document to include Office of General Council (OGC) recommended changes: Revised Section 4.2.6 to include reference to OPM Policy on Electronic Signatures. Added Appendix B: OPM Steps for Conducting an Assessment of Electronic Signatures. Updated all forms to meet OPM standard format. E.g. SF-50. Replaced Terms of Reference (TOR) with EOD Self Certification in Section 5.1 and as referenced throughout document. Updated Section 3 to reflect approval of the OF 306. Added statement to Section 4.5.1 to reinforce data provider responsibility to provide accurate and complete data (Risk Mitigation action).
1.8	11/04/2009	Updated document to include OPM Office of General Council (OGC) recommended changes: Added the Privacy Act Statement as part of Section 4.2.5: Data Input Confirmation. Revised Section 4.2.6 to preclude reference to OPM Policy on Electronic Signatures. Removed Appendix B: OPM Steps for Conducting an Assessment of Electronic Signatures. Made minor edits to Sections 4.2.5: Data Input Confirmation and 4.2.6: Electronic Signatures.
1.9	11/11/2009	Incorporated Final EHRI comments to include: Minor text edits. More detailed source references in Section 4.2.6, Electronic Signatures. Removal of DRAFT Watermark.
1.10	1/11/2010	Incorporated comments from the Office of the General Counsel (OGC) as follows: Made global edits to citations Changed wet to written Changed collection to utilization Added Privacy Act Statement in Section 4.2.5 Added additional details in Section 4.2.6 Made edits to Section 4.3.7 Data Validtion Changed text to read "…younger than 18 to 16
2.0	05/28/2010	Incorporated additional comments from the OGC as follows: Corrected documentation references in sections 4.2.6, 6.0, and 6.2
2.1	06/14/2010	Corrected number in section 2.2 from "…twenty-two (23)" to "…twenty-three (23)"
2.2	08/04/2010	Changed Standard Forms List TSP-3 eOPF transfer format from Scanned PDF Image to N/A. This form is NOT stored in eOPF.
2.3	01/27/2014	Removed what was Section 1.2, “For Offical Use Only”. Updated list of EHRI PMO points of contact in Section 1.4.
2.4	02/04/2014	Removed FOR OFFICLA USE ONLY from the footer section. Removed shading in the column headers in Section 3.1. In Appeendix A, labeled ‘Data Validation’ as a *System Requirement* in the Requirement Type column and ‘Data Transmission Receipt” as *Data Transfer* in the Requirement Type column.

Table of Contents

1.0 Introduction

The Enterprise Human Resources Integration (EHRI) Program Management Office (PMO) is tasked with the development of standards and the utilization of policies for Federal Entrance on Duty (EOD) systems. This document provides the results of an initiative led by the EHRI PMO and a cross-agency work group collaboration designed to leverage the findings and recommendations prescribed in the Human Resources Line of Business (HR LOB) Entrance on Duty (EOD) Concept of Operations (CONOPS).

EOD, as defined by this document, refers to the automated utilization and distribution of information required as part of the larger employee onboarding process. Employee onboarding involves additional orientation and socialization activities that are aimed at improving employee retention and time-to-productivity. Throughout this document, the term onboarding is used to refer to the process by which an employee is brought into a new organization; however, this document does not address employee onboarding activities beyond those that are part of EOD.

A number of agencies and Personnel/Payroll Shared Service Centers are developing EOD systems with the intention of leveraging technology to streamline the employee onboarding process. Many of the forms necessary, as part of the onboarding process, are forms required for long-term retention in the electronic Official Personnel Folder (eOPF). The Code of Federal Regulations (CFR), Part 293: Personnel Records states that the Official Personnel Folder (OPF) of each employee in a position subject to civil service rules and regulations is under the jurisdiction and control of the Office of Personnel Management (OPM). For this reason, OPM has a special interest in the improvement of the efficiency of personnel records management and in the legal requirements for documentation stored in a Federal employee's eOPF.

The EHRI PMO is responsible for maintaining the integrity of the eOPF, which protects information rights, benefits, and entitlements of the employee. As such, EHRI may define the requirements for eOPF data utilization and sharing. The requirements contained in this document have been reviewed and approved by federal EOD form owners. Form owner approval to electronically complete and certify forms subject to their approval is dependent upon agency compliance with the requirements in this document. If an agency is unable to meet the requirements defined in this document, separate form owner approval to electronically complete and certify EOD forms must be obtained. In addition, agencies unable to meet the requirements defined in this document may be denied the right to send EOD documentation electronically to eOPF.

1.1 Purpose

This document provides standard requirements and direction for Federal agencies that are developing EOD systems that meet the legal requirements for documentation stored in Federal employees' eOPFs. The requirements contained in this document complement agency research and review of the HR LOB EOD Concept of Operations (CONOPS).

1.2 Background

The goal of EHRI is to leverage technology to support the Federal employee lifecycle through informed human capital decision making. EHRI is one (1) of five (5) OPM-led e-Gov initiatives designed to maximize the benefits of information technology in line with the previous Administration's Presidential Management Agenda. In the spring of 2004, OPM was tasked with managing an HR LOB to identify

approaches to improve service and reduce costs associated with information technology systems and supporting processes within Federal Human Resources. The HR LOB identified an effective and standard EOD solution as a key component in working towards inter-agency efficiency and cost savings.

An EOD system manages the automated utilization and distribution of initial employment information and is a component of the greater employee onboarding process. Onboarding includes the data utilization and provisioning tasks involved in the EOD process, as well as new employee socialization, orientation, and training. A comprehensive EOD solution leverages system interoperability and workflow to include all of the necessary steps between applicant selection and reporting for duty. Applicants may complete their pre-employment and orientation paperwork by entering information through the EOD system. An EOD solution can increase the efficiency with which new employees are hired by automating the provisioning process and alerting individuals as tasks are completed.

In January 2007, HR LOB developed an EOD CONOPS. The EOD CONOPS provides the results of a cross-agency collaboration describing a business capability that leverages technology to bring efficiencies to the employee onboarding process. The EOD CONOPS document provides a framework for Federal EOD systems that leverage best practices in compliance with the Federal Enterprise Architecture (FEA) guidelines. The CONOPS outlines a standard EOD process, common EOD data elements, and high-level functional requirements. The HR LOB EOD initiative supports the overall vision of the HR LOB to promote standardized and interoperable Human Resources (HR) solutions that provide common, core functionality to support the strategic management of human capital. A common focus on HR integration and improved efficiencies lends itself to cross-collaboration between the HR LOB and EHRI.

In November 2008, the EHRI PMO formed an EHRI EOD Team and initiated an effort to build upon the analysis documented in the EOD CONOPS, to prescribe the requirements for a system that meets the legal requirements for documentation stored in a Federal employee's eOPF. Specifically, the EHRI EOD was tasked with prescribing EOD requirements that:

- Leverage the requirements defined in the HR LOB 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 eOPF.
- Adhere to Form Owner requirements for the electronic completion and certification of forms under their management.
- Define the minimum standard requirements that must be met before EHRI accepts data from an EOD system for long-term storage in eOPF.

Over the course of seven (7) months, EHRI performed an analysis of EOD forms, including relevant policy requirements, electronic signature dispositions, and form owner acceptance of forms that are completed electronically. The team consulted with form owners from multiple federal agencies to prescribe mutually agreeable requirements for the electronic completion of federal forms. This analysis resulted in the refinement of existing HR LOB EOD CONOPS requirements, and the addition of new requirements and policy considerations necessary for the development of an EOD system that produces electronic documents suitable for transmission to eOPF.

1.3 Scope

The HR LOB EOD CONOPS summarizes four (4) primary areas where technology can be leveraged: utilization and sharing of new hire data, communication, monitoring of the process, and employee provisioning. The OPM EOD requirements document expands upon the utilization and sharing of new hire data as it relates to eOPF.

1.4 Contacts

The following members of the EHRI PMO should be contacted for additional information regarding the requirements contained in this document.

Item	Contact / Title	Contact Information
eOPF EOD Memorandum of Understanding (MOU), Self Certification Process / Questions or additional information concerning EHRI EOD	Gladys McKenzie, OPM EHRI Entrance on Duty (EOD) Project Manager	Ph: (202) 606 1699 E: Gladys.McKenzie@opm.gov
Interconnection Security Agreement (ISA) and Authority to Operate (ATO)	Paul Burke, OPM Operations Lead	Ph: (202) 606 4809 E: Paul.Burke@opm.gov
Questions or additional information concerning EHRI and eOPF	Marie Boucher, OPM EHRI Project Manager	Ph: (202) 606 1832 E: Marie.Boucher@opm.gov
OPM Master Forms List	Richard Hoffheins, OPM EHRI Master Forms List	Ph: (202) 606 1625 E: Richard.Hoffheins@opm.gov

2.0 Requirements Definition Methodology

EHRI leveraged the requirements defined in the EOD CONOPS to formulate the analysis of existing policies and processes. Following a review of relevant Federal documentation and the United States Code, the analysis team authored an EOD Assumptions document.

The Assumptions document facilitated the consideration and acceptance of policy assumptions that improve the efficiency of Federal EOD systems. The team consulted with form owners, policy experts and functional managers to refine existing CONOPS requirements and to prescribe new ones.

Following an initial draft of the OPM EOD requirements document, the document was released to the EHRI EOD Work Group for review and validation. The team conducted two (2) EHRI EOD Work Group sessions in which seventeen (17) agencies provided comments and feedback that were incorporated into subsequent document revisions.

2.1 Document References

The following documents were reviewed and considered during the OPM EOD requirements development process:

- The Human Resources Lines of Business Entrance on Duty Concept of Operations (HR LOB EOD CONOPS)
- The Electronic Signatures in Global and National Commerce Act, Public Law 106-229 (E Signature Act of 2000)
- Government Paperwork Elimination Act (GPEA), Public Law 105-277
- Circular No. A-130, Appendix II, Implementation of the Government Paperwork Elimination Act (GPEA)
- United States Code (U.S.C.)
- Federal Information Resources Management Regulation (FIRMR) Bulletin(s)
- Circular A-130, Management of Federal Information Resources
- Office of Personnel Management Guide to Processing Personnel Actions (GPPA)
- The Code of Federal Regulations (CFR)
- The Office of Personnel Management's (OPM) Guide to Personnel Recordkeeping (GPR)
- The Federal Employees Group Life Insurance (FEGLI) Handbook for Annuitants, Compensationers, and Employing Offices
- The Privacy Act of 1974 (5 U.S.C. 552a)
- Internal Revenue Bulletin
- Summary of the Thrift Savings Plan

2.2 Entrance on Duty Assumptions and Policy Coordination

The requirements for Federal EOD system must reflect the policy and intentions associated with standard onboarding forms. For this reason, the OPM EOD requirements gathering and refinement process began with an identification of standard onboarding forms and form owners. As part of this initiative, the team identified twenty-four (24) standard EOD forms. The team conducted a thorough review of the policies affecting each form, specifically with regard to electronic form completion and electronic signatures.

The result of this review was documented in the EOD Assumptions document, which is available from the EHRI PMO upon request, and distributed to each of the standard form owners for their consideration and acceptance. Assumptions described in the document are supported by existing Federal documentation and procedures and are not intended to present new information. Rather, the document presents existing policies and regulations in a format that supports the mission of effective EOD system development.

Upon review and consideration of the Assumptions document, the EHRI EOD team received twenty-three (23) form owner acceptances. One (1) owner has provided a rejection notice and EHRI continues to work through their concerns to gain approval. A summary of form owner acceptances is provided in section 3.1. The team continues to request feedback from form owners who have yet to respond to ensure a comprehensive understanding of acceptance or non-acceptance by form owners.

However, failure to comment does not affect the progress of EOD requirements and systems development. Many of the requirements contained in this document, have been identified during the development of the Requirements Assumptions for EOD Forms document and reflect existing Federal regulations.

2.3 Entrance on Duty Work Group

2.3.1 PURPOSE

The purpose of the EHRI EOD Work Group is to:

- Review the OPM EOD Requirements Document for cohesion, relevance, and effective achievement of the key EHRI EOD team goals (see Section 1.2 for a summary of EHRI EOD Team goals).
- Validate existing requirements to ensure that prescribed methods are practical, appropriate, and support Federal policy.
- Prescribe additional requirements to promote the achievement of the key EHRI EOD team goals.
- Serve as a conduit and a liaison between members of the eOPF community and the EHRI PMO concerning issues affecting EOD systems development.
- Serve as a forum for discussion of the business processes surrounding EOD, specifically as they relate to eOPF and Federal policy.

Meetings of the EOD Work Group are held as appropriate to review and finalize requirements.

2.3.2 MEMBERS

The following agencies are represented in the EOD Work Group:

- U.S. Department of Agriculture (USDA)
- U.S. Department of Health and Human Services (HHS)
- U.S. Department of Homeland Security (DHS)
- U.S. Department of Transportation (DOT)
- U.S. Department of Veterans Affairs (VA)
- U.S. Office of Personnel Management (OPM)
- U.S. Department of Energy (DOE)
- U.S. Department of Treasury
- U.S. Department of Army
- U.S. Department of Air Force
- U. S. Department of Commerce (DOC)
- Defense Logistics Agency (DLA)
- U.S. Department of Defense (DOD)
- Securities and Exchange Commission (SEC)
- National Archives and Records Administration (NARA)
- The Department of the Interior, National Business Center (DOI NBC)
- Social Security Administration (SSA)

3.0 Entrance on Duty Standard Forms

The EHRI EOD team consulted with nine (9) Federal agencies to develop a standard EOD Forms List. The nine (9) agencies included: General Services Administration (GSA), Department of Labor (DOL), National Aeronautical and Space Administration (NASA), The Department of the Interior, National Business Center (DOI NBC), Office of Personnel Management (OPM), Department of Homeland Security (DHS), U.S Department of Agriculture Agricultural Research Service (USDA ARS), Defense Logistics Agency (DLA) and U.S Department of Agriculture Forest Service (USDA FS).

The forms list in Section 3.1 does not contain a complete list of all onboarding forms. However, the EOD team determined that the forms included in the table below are used consistently across agencies during the onboarding process.

Section 3.1 lists twenty-four (24) standard onboarding forms along with the form owner, eOPF folder side, electronic signature disposition, and the status of the form owner's acceptance of the Assumptions document. Columns are defined as follows:

Form Owner:

Form Owner 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 their form(s) via an EOD system. For specific contact information for the form owners, please contact the EHRI PMO.

eOPF Folder Side:

The eOPF folder side 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.

Electronic Signature Disposition:

The Electronic Signature Disposition column indicates if an electronic signature is acceptable, as stated in existing Federal policies (see section 2.1 for a complete list of relevant documentation). An electronic signature disposition of "approved" also indicates the Form Owner's acceptance of an electronic signature for their form(s).

Form Owner Assumptions Document Approval:

The Form Owner Assumptions Document Approval Status column indicates if the official Form Owner has approved of 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 Form certification period 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 Transfer Format:

The eOPF Transfer Format column indicates the method by which a document should be electronically transferred to eOPF. There are three (3) ways that an EOD document can be added to eOPF:

1. **Scanned 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.

2. **PDF with Indexing Information –** If a form is generally stored in eOPF, but it is not an OPM form or does not reside in the Permanent folder, an agency may electronically transmit the PDF file with indexing information via a data feed.

3. **Data and PDF File With Indexing Information –** EHRI's long-range goal is to become data-centric. EHRI is currently configured to receive data only for a limited number of forms. However, the program is moving towards a more data-oriented approach to HR information management. In the meantime, both the data and a PDF file with indexing information should be sent for OPM forms that reside in the Permanent side. When the program moves to a data-centric approach, data collected via EOD data feeds will be available.

An eOPF Transfer Format of "N/A" indicates that the form is not stored in the eOPF. For additional information regarding EOD transfer methodology, please see the eOPF Interface Control Document (ICD).

Note: Agencies must meet the security requirements defined in the EHRI Interconnection Security Agreement (ISA) and obtain an Authority to Operate (ATO) before an electronically signed form can be transferred to eOPF. Electronic signature approval 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 data sensitivity.

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 Transfer Format
GENERAL ONBOARDING FORMS							
OF-306	Declaration for Federal Employment	Office of Personnel Management (OPM) Federal Investigative Services Division (FISD) & Strategic Human Resources Policy (SHRP)	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) Strategic Human Resources Policy (SHRP) Center for Workforce Information and Systems Requirements (CWISR)	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	N/A	Approved	Prior to EOD Date	N/A
SF-256	Self Identification of Handicap	Office of Personnel Management (OPM)	N/A	N/A	Approved	Prior to EOD Date	N/A
INS-9	Immigration & Naturalization Service Employment Eligibility Verification	Department of Homeland Security (DHS)	Optional: Deleted or Virtual I9	Electronic Signature Accepted	Approved	Prior to EOD Date	PDF with Indexing Information

Form Number	Form Name	Form Owner	eOPF Folder Side	Electronic Signature Disposition	Form Owner Assumptions Document Approval Status	Certification Period	eOPF Transfer 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	Payroll	Electronic Signature Accepted	Approved	Prior to EOD Date	PDF with Indexing Information
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	Payroll	Electronic Signature Accepted	Approved	Prior to EOD Date	PDF with Indexing Information
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	Electronic Signature NOT Accepted	Approved	On or After EOD Date	Scanned PDF Image
SF-2823	Designation of Beneficiary (FEGLI)	Office of Personnel Management (OPM)	Permanent	Electronic Signature NOT Accepted	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	Approved	On or After EOD Date	Scanned PDF Image
SF-1152	Designation of Beneficiary Unpaid Comp of Deceased Fed Emp	Office of Personnel Management (OPM)	Temporary	Electronic Signature Accepted	Approved	On or After EOD Date	Data and PDF file with indexing information
TSP-3	Thrift Savings Plan Designation of Beneficiary	Thrift Savings Plan Board (TSPB)	N/A	Electronic Signature NOT Accepted	Approved	On or After 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 Transfer Format
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
TSP-1-C	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
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
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
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
WITHHOLDING ALLOWANCES/EXEMPTION CERTIFICATE							
W4	Employee Withholding Allowance	Internal Revenue Service (IRS)	Payroll	Electronic Signature Accepted	Approved	Prior to EOD Date	PDF with Indexing Information
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

Form Number	Form Name	Form Owner	eOPF Folder Side	Electronic Signature Disposition	Form Owner Assumptions Document Approval Status	Certification Period	eOPF Transfer Format
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
SF-180	Request Pertaining to Military Records	National Archives and Records Administration (NARA)	Temporary	Electronic Signature NOT Accepted	Approved – Electronic Signature not admissible.	Prior to EOD Date	Scanned PDF Image

3.2 Data Dictionary

The EHRI PMO has developed an EOD data dictionary that cross-references standard EOD data elements with the forms to which they belong. The EOD Data Dictionary has also been cross-referenced with the Guide to Human Resources Reporting (GHRR). The EOD Data Dictionary is included as part of the eOPF ICD and available from the EHRI PMO upon request.

4.0 Entrance on Duty Requirements

The following requirements for a Federal EOD system complement the functional requirements contained in the HR LOB EOD CONOPS. The EHRI PMO applied research and analysis to the existing CONOPS requirements to include additional detail, specifically related to eOPF and OPM policy. Please refer to the HR LOB EOD CONOPS, Appendix C for a complete listing of OPM defined EOD requirements.

4.1 Functional Requirements

4.1.1 Use Plain Language

Federal EOD system requires users to enter information one time, so that data elements required on multiple forms are collected once. In order 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 so that they may 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 should be 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 should be provided via the user interface to clarify the request.

4.1.2 Employment Eligibility Verification

As authorized in the 8 CFR 274a.2, agencies must ensure that employee eligibility verification is complete prior to federal employment. The Employment Eligibility Verification Program (E-Verify) has been implemented to meet the requirements of an employment verification system. Employment eligibility requirements should be considered during the design and implementation of an EOD system, and external sources, such as E-Verify, should be incorporated as appropriate.

4.1.3 Data Utilization Grouping

Federal EOD system groups data utilization 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.

4.1.4 FORM PACKAGES

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

4.1.5 FORM LIBRARY

Federal EOD system provides the capability to house 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 be granted the authority to add forms and documents to the form library.

4.1.6 HR INTERVENTION

Federal EOD system provides designated staff with the ability to monitor user progress and notifies designated Human Resources (HR) personnel that intervention may be required in the event that pre-determined conditions are met. Intervention may be completed manually.

Examples of pre-determined conditions may include specified completion timeframes or required supporting documentation. For example, if an applicant does not complete the EOD input within a specified period–of-time, the system notifies the HR servicing office. An example of required supporting documentation may include additional requirements associated with the SF-3109, FERS Election of Coverage; for example, if 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). Then 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 in order to modify court order. If the employee fails to meet the preceding conditions, an EOD system should notify HR of a required intervention.

4.1.7 FORM OWNER ACCEPTANCE

OPM and EOD form owners support the Government Paperwork Elimination Act (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.

Federal EOD systems adhere to form specific requirements as defined by the official form owner. Agencies must thoroughly evaluate the commensurate risk and benefits associated with electronic signature technologies.

4.1.8 APPLICANT DATA INPUT CHANGES

Federal EOD system does not allow an employee to initiate changes to forms following approval and release of the onboarding forms. Following an employee's electronic signature certifying completion of standard onboarding forms, the employee releases ownership of the forms and can no longer initiate changes via the EOD system. After the employee release, 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. If the HR representative reviews and accepts a form, it is transferred to the final system of record (e.g., eOPF, Human Resources Information System [HRIS]), the document is destroyed or an alternate appropriate action is taken per the agency records manager. In this case, 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 (section 8d):

> 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.

4.1.9 Personal/Public Email Addresses

Federal EOD system enables the manual entry of an applicant's personal email address to receive EOD logon information and notifications. The provision of secure information via email follows the National Institute of Standards and Technology (NIST) guidelines for information security. During the onboarding forms completion phase, the applicant may not yet be a Federal employee and may not have a government issued email address. Appropriate security considerations and precautions must be implemented to meet this requirement.

4.1.10 Additional Reference Information

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, then they should be made available via an EOD application. The implementation of this requirement will vary by system design, and may be as simple as providing a link to associated documentation on an external site.

4.1.11 Human Resources Role

Federal EOD system requires that HR review is integrated as appropriate to promote the integrity of employee onboarding forms. 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 create and maintain all records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual.

Efficiencies should be built into EOD systems to reduce the burden on applicants and staff as appropriate. However, agencies have an obligation to promote the integrity of onboarding forms before they are sent to eOPF.

4.1.12 EDUCATIONAL DATA UPDATE

Federal EOD system captures employee Educational Data as defined in the Guide to Human Resources Reporting (GHRR). Required data elements include Instructional Program Code, Educational Level Code, and Degree Year. Data is transferred to the EHRI Data Warehouse via an agency's HRIS system.

4.2 Electronic Form Completion and Certification

For the purposes of this section, 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. Form completion may occur at any time. However, form certification may only occur in accordance with the certification period for each form indicated in Section 3.1. 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.

4.2.1 ELECTRONIC FORM COMPLETION

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. For additional information regarding form certification period, please see Section 3.1.

4.2.2 FORM PREVIEW CAPABILITY

Federal EOD system provides the capability for 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 their data will apply during the data input process. This stresses the importance and the implications of the transaction.

4.2.3 ELECTRONIC FORM CHANGES AND REPRODUCTIONS

EOD system developers do not modify a Federal form. Form reproductions displayed in Federal EOD systems are complete and accurate reproductions of the official form. Pursuant to 41 CFR, part 102-194, General Services Administration (GSA) authorizes agencies to create electronic personnel forms without obtaining prior approval from GSA or the Office of Personnel Management. Provided the electronic reproduction 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 Guide to Processing Personnel Action (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 EHRI PMO prior to initiation of electronic transfer of forms to eOPF.

4.2.4 ELECTRONIC FORM STORAGE

Federal EOD systems must enable an authorized user to print completed EOD forms, as it would appear if completed via the paper form prior to electronic transmission to eOPF. According to the GPPA, an agency that stores Official Personnel Folder forms electronically must store them in such a way that, when a paper copy is needed, that copy looks essentially like the original approved Office of Personnel Management, standard, or agency form.

4.2.5 DATA INPUT CONFIRMATION

Confirming accuracy and user acceptance of data input is a critical step in ensuring the validity of forms populated via an EOD system. An effective data input certification process involves multiple steps and requires appropriate tracking. In the event that an employee contests the certification of certain forms and/or data, a system must generate an audit trail that demonstrates that the individual adequately viewed the data input and was provided with the sufficient notice and review tasks prior to the release of the information. At a minimum, the following certification steps must occur:

1. Federal EOD system provides an electronic read-only Portable Document Format (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.

2. Prior to electronic approval/signature of a form(s), the user must be presented with a certification statement containing:

    - Certification that the individual has reviewed the information provided in the form(s) and acknowledges that electronic approval is the equivalent of signing each form.

    - Implications if information has been stated fraudulently.

    - 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.

3. Following electronic approval/signature of forms, Federal EOD system must provide users with a confirmation page containing a list of forms electronically completed and signed, date/time of certification transaction, and a copy of the certification text agreed to, prior to electronic approval. Users must be prompted to either save and/or print this page for their own records.

4.2.6 ELECTRONIC SIGNATURES

Federal laws and policies support the use of electronic signatures. Accordingly, 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. Electronic signature methods are applied in compliance with the NIST Guidance for Electronic Signatures and the GPEA.

Circular No. A-130, Appendix II, Implementation of the GPEA (http://www.whitehouse.gov/omb/fedreg/gpea2.html) 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)

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

The Government Paperwork Elimination Act specifically provides that electronic records and their related electronic signatures are not to be 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 are tasked with implementing the appropriate electronic signature solution in accordance with GPEA and related guidance. Each form owner must ensure that all appropriate requirements and guidance were followed within their agency 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

4.2.6.1 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 with a certified EOD system” or “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.

In order for a system to be considered “certified” an Authority to Operate (ATO) must be granted and a copy of the letter or memorandum is provided to the EHRI PMO. A certified system also assumes that an agency complies with the terms and conditions outlined in the EOD Self Certification procedure. Please see Section 5.1 for additional information regarding system certification.

4.2.6.2 Electronic Signature Dates

The electronic signature date, must be affixed at the time of certification and in accordance with the policy of the form, it applies to. 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) has been administered.

4.2.7 Electronic Certification of Multiple Forms

Federal EOD system allows for 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.

The certification method must be implemented in a manner that applies adequate opportunities for a user to view and change the forms. For example, at the completion of data entry, the applicant must be prompted to view the form recreations to certify that the completed forms include all user supplied data entries and are accurate. Once the applicant is satisfied with all required data elements, the applicant must be presented with a statement that indicates the implications of the electronic approval of a single form or multiple completed forms.

Federal EOD systems must consider and account for a variety of user constrains and requirements as practical. For example, if a user does not wish to certify multiple forms simultaneously, the user should be 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 should remain established. 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 (see Section 3.1 for a list of standard EOD forms and their associated completion periods). 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, Federal EOD system must allow for the electronic approval of selected single forms as appropriate.

4.3 System Requirements

4.3.1 Form Tracking

Federal EOD system tracks forms by version. The EOD system must contain current form versions. Form owners are responsible for the dissemination of updated, unlocked form versions. However, it is the EOD system owner's responsibility to ensure that form owners are aware of this requirement.

4.3.2 Administrator Rights

Federal EOD system allows designated EOD system administrators to add, change, and deletes form packages within the system. A form package is defined as a set of forms necessary for completion based on the type of appointment and occupation. Additional administrative tasks, such as user account management, role assignments, reports generation and workflow management, must be granted to the administrator.

4.3.3 Real-time Updates

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

4.3.4 ROLE-BASED RIGHTS

Federal EOD system uses role-based capabilities to include viewing, printing and form completion. For example, HR Specialists and employees should have view and print capabilities assigned to their roles at the form level. When appropriate, roles are to be defined in a way that is similar to the rights and responsibilities assigned in the paper world. For example, HR Specialists are granted the right to modify effective dates, following employee data submission.

4.3.5 DATA INPUT SOURCES

Federal EOD system automatically populates EOD required data elements from applicable sources. A user must 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 should be 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.

4.3.6 DATA ENTRY

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)

4.3.7 DATA VALIDATION

Federal EOD system validates data entry to the extent practicable to reduce the burden on both the appointee and their HR office. For example, if an employee birth date is later than the date of the employee's last Federal appointment, an EOD system prompts the user to check the dates. Additional examples may include if an employee indicates that the employee is unmarried (as required for the SF-15, SF-2809 and W4), the employee cannot register a spouse for Health Benefits. If an individual's birth date indicates that they are younger than 16, they are ineligible for federal employment. If an individual has not yet been appointed as a Federal employee, their signature will not appear in the "appointee's signature" space of the OF-306.

Data Validation should also occur at the form level to verify that the user is eligible for the completion of certain forms. For example, if an employee has not yet 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 yet eligible for benefits as a Federal employee.

4.3.8 Error Alerts

Federal EOD system provides tiered error alerts 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 an error.

4.3.9 Source System Identifier

Completed forms created as a result of EOD system input and data entry must contain a visible source system identifier so that 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 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, it is important that a visible source system identifier appear on the form itself. The FIRMR Bulletin B-2 (part 12g) 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.

4.3.10 Mass Hires

Federal EOD system accommodates the requirement for mass hires. The EOD process is capable of being initiated for multiple users simultaneously.

4.4 Reporting Requirements

4.4.1 Date and Time Stamps

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 a record of when a form is electronically certified by the employee, transferred to HR, approved by HR and transmitted to a system of record. The system captures the date of tentative offer extension and acceptance, as well as the scheduled EOD date and actual EOD date. A scheduled EOD date must be provided before an applicant is granted access to the EOD system. An actual EOD date must be entered to verify employee eligibility for Federal benefits. A form cannot be transferred out of the EOD system until a final EOD date is populated.

4.4.2 Access Metrics

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 have accessed the EOD system

and the time of their access. Similarly, a report should detail which HR Specialists have accessed a particular user account or forms, and when this occurred.

4.4.3 User Actions Audit Trail

Federal EOD system provides a reporting capability for system usage metrics, such as completion and submission time stamps and applicant progress. The system also capture when users view the recreations of their forms, certification statements, and form input data. The certification date should be captured and maintained at the form level. According to the GPPA, for each form that was cleared or signed electronically, there must be an audit trail to show when and who:

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

In the event that an employee contests the certification of certain forms/data, the system is able to reproduce 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 transferred 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 should be maintained indefinitely. The application and depth of this requirement will vary by agency.

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

4.4.4 Cycle Time Metrics

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 are likely to include:

- Time from recruiting to EOD system
- Time to access EOD system
- Time to complete condition (Applicant)
- Time to complete condition (HR)
- Time from completing conditions to Report for Duty date
- Time from acceptance to Report for Duty date

Additional information regarding cycle time metrics, definitions, and measurement criteria is available in the HR LOB EOD CONOPS, Appendix E Performance Indicators.

4.4.5 PERSONALLY IDENTIFIABLE INFORMATION ON REPORTS

System reports containing personally identifiable information (PII) must contain an official privacy statement.

4.5 Data Transfer Requirements

4.5.1 EOPF INTERFACE CONTROL DOCUMENT (ICD)

File transfer from an EOD system to eOPF complies with the requirements and specifications detailed in the eOPF Interface Control Document (ICD). Agencies and data providers are required to provide accurate and complete data in compliance with the ICD. The accuracy and validity of eOPF is dependent upon the submission of appropriate data. The eOPF ICD is available upon request from the EHRI PMO.

4.5.2 DATA EXPORT

The HR LOB EOD CONOPS describes the requirement for an EOD system to export data (real time or batch) to other applicable sources. Applicable sources may include eOPF, agency payroll offices, or agency HR Information Systems (HRIS). Data export to eOPF cannot take place until the agency has verified that an employee account has been created in eOPF. This may be established by setting up an automated check for whether or not an eOPF account exists or by verifying account creation by accessing eOPF. 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.

4.5.3 TEMPORARY ACCOUNT TERMINATION

Federal EOD system automatically terminates temporary accounts after notification of successful record transfer, or within 90 days. Termination of temporary accounts should include the denial of further employee access to the EOD system and the deletion of forms created as a result of data entry. Data entered as part of the EOD process may remain in the system at an agency's discretion. Employee records (i.e., the forms created as a result of data entry) should not be maintained in more than one system. Per Circular No.A-130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individual "Agencies should not publish systems of records that wholly or partly duplicate existing government-wide systems of records."

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

4.5.4 DATA RECONCILIATION

Federal EOD system must capture and maintain sufficient data to provide for reconciliation of data transfer between systems. Refer to the eOPF ICD for data transfer specifications.

4.5.5 TRANSMISSION RECEIPT

Federal EOD system provides administrative users with a transmission receipt following the successful transfer of EOD data to external sources (eOPF, HRIS, etc.)

4.5.6 Forms Not Included on the OPM Master Forms List

EOD documents that are not included in the OPM Master Forms List (e.g., medical documents), are coordinated with the agency's Records Manager and Privacy Officer before transmission to eOPF. The EOD system developer must obtain approval from the EHRI PMO prior to the transfer of documents not included in the OPM Master Forms List.

4.5.7 Records Retention

Agencies meet the retention guidelines for standard onboarding forms in accordance with their Records Manager. According to the GPPA, the agency must certify that all National Archives and Records Administration (NARA) disposition schedules are/will continue to be met by the electronic forms system.

4.6 Security and Accessibility Requirements

4.6.1 508 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.

4.6.2 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 should only be allowed to see certain forms, access should be 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. Persons furnishing information must be made aware that their information may be accessible to persons other than their HR Specialist (if applicable).

4.6.3 Tiered Help Capability

Federal EOD system implements a tiered help capability to include the use of online help and help desk support.

4.6.4 Federal Security Standards

Federal EOD system provides user access that complies with Federal standards and regulations. Federal standards include Federal Information Processing Standards (FIPS) Publication 112 and the National Institute of Standards and Technology (NIST), Federal Information Security Management Act of 2002 (FISMA), and Circular No.A-130.

4.7 Management Requirements

4.7.1 Error Reporting

An effective EOD program office allows for the submission of System Problem Reports (SPR). Reports may be generated and submitted outside of an EOD system (e.g., Help Desk or Customer Support application). An error reporting and resolution process, as defined by program management, may feed into a configuration control process.

4.7.2 CHANGE REQUESTS

An effective EOD program office allows for the submission of Change Requests (CR). This is a business process decision that may be made outside of an EOD system. A Change Request submission and resolution process, as defined by program management, may feed into a configuration control process.

4.7.3 SYSTEM DOCUMENTATION

EOD system managers maintain, and make 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

4.8 Form Owner Requirements

4.8.1 FORM TEMPLATE UPDATES

EOD form owners supply known EOD system owners and the EHRI PMO with an update in the event of a form template change. It is also assumed that form owners provide an updated, unlocked copy of any and all new form templates. Note: An unlocked PDF form allows for EOD system owners to apply the correct data elements during electronic form completion. EOD system owners are not authorized to make any changes to the content or format of Federal forms.

5.0 Entrance on Duty File Transmission Methodology to eOPF

5.1 EHRI System Certification Methodology

The EHRI 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 ICD. Agencies must contact the EHRI PMO to obtain the appropriate documentation and approvals before data can be sent via a data feed to eOPF. An agency is considered certified when EHRI is provided with documentation confirming that an acceptable agency self-certification is complete and that an Authority to Operate (ATO) is granted. If an agency is unable to comply with the requirements defined in this document, separate form owner approval must be granted and the electronic transfer of documents to eOPF may be denied.

The EHRI PMO has established that the following documents must be exchanged to ensure both parties meet acceptable conditions before data are transferred from one system to another:

- **EOD Self-Certification:** The EOD Self-Certification process is designed to foster agency accountability for systems that meet the legal sufficiency requirements for documentation stored in eOPF. The EOD Self Certification contains a list of requirements that must be met before an agency is permitted to transmit data to eOPF.
- **Memorandum of Understanding (MOU)**: This is a business-level agreement between two (2) parties in the form of a legal contract. For EOD, the MOU specifies the quality of data to be sent, as well as specifics regarding adherence to EHRI requirements.
- **Interconnection Security Agreement (ISA)**: This is an agreement between parties that will be exchanging data. For EOD, this document specifies EOD security considerations, rules of behavior, formal standards and audit trail responsibilities. This document also outlines the requirement for a system Certification and Accreditation (C&A) and a letter that indicates the system's Authority to Operate (ATO).
- **Authority to Operate (ATO)**: Prior to data acceptance, an agency must provide the EHRI PMO with a letter or memorandum from the agency's senior official indicating its ATO. An ATO indicates the successful completion of the C&A process, including a plan to continue to mitigate problems and sustain operations.

5.2 Interface Control Document (ICD)

Data transfer from Federal EOD system to eOPF conforms to the requirements and specifications contained in the eOPF ICD.

6.0 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 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.
- Inform each individual asked to provide information of the elements required for a Privacy Act Statement.

This section provides a high-level overview of the requirements associated with the Privacy Policy directive. Agencies should work with their Privacy Policy Office to complete the required tasks appropriately.

6.1 Privacy Impact Assessment

The E-Government Act of 2002 requires agencies to conduct a Privacy Impact Assessment (PIA) before developing or procuring IT systems or initiating projects that collect, maintain, or disseminate 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 Privacy Impact Assessment (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:

- What information is to be collected (e.g., nature and source)
- Why the information is being 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)
- What opportunities individuals have 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 will be secured (e.g., administrative and technological controls), and
- Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a

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

6.2 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.

Disclosure: Mandatory or Voluntary: 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.

6.2.1 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 Privacy Act Statement:

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

6.3 System of Record Notice (SORN)

As stated above, 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 the Office of Personnel Management to coordinate the amendment of GOVT-1 to include any new routine uses before disclosing EOD information.

7.0 Next Steps

Federal EOD systems will bring dramatically improved efficiencies and cost savings to the Federal onboarding process. Agencies should consider the implementation of an EOD system that meets OPM requirements as a way to leverage their existing investment in EHRI eOPF. The publication of this document provides a complement to existing Federal EOD documentation in addition to Federal standards, such as the National Institute of Standards and Technology (NIST) guidelines. The following steps should be considered by agencies developing Federal EOD solutions and agencies that have implemented Federal EOD solutions:

1. Perform a thorough review of the HR LOB Concept of Operations (CONOPS) document, available at: http://www.opm.gov/egov/documents/EOD/index.asp

2. Review existing agency EOD requirements and/or EOD solution to ensure compliance with the requirements defined in the HR LOB Concept of Operations (CONOPS) and OPM EOD Requirements document. For items of noncompliance, implement action to modify existing agency requirements and/or EOD solution.

3. Evaluate agency specific onboarding forms list to determine if forms are included in the EHRI EOD team analysis (see Section 3.1 for a complete list). Review existing forms in relation to the EOD Assumptions document to determine whether or not a similar analysis is required for additional forms. If agency specific onboarding forms are stored in eOPF, but are not part of the OPM Master Forms List, contact the EHRI PMO to facilitate form approval and addition to the OPM Master Forms List.

4. Obtain a copy of the eOPF Interface Control Document (ICD) to implement necessary preparations for data transfer to eOPF.

5. Contact the EHRI PMO to coordinate the appropriate agreements (MOU, ISA, and ATO) and a copy of the EOD Self-Certification outline prior to the transfer of data to eOPF.

Appendix A: Requirements Checklist

The following table summarizes the requirements contained in this document that complement the functional requirements contained in the HR LOB EOD CONOPS. As defined in the EOD Self Certification Outline, agencies are required to perform a self-assessment to determine whether or not their system meets OPM EOD requirements. This table may be used as a quick reference to determine if an EOD system meets the EHRI requirements for EOD data that is to be transferred to eOPF. Please refer to the HR LOB EOD CONOPS, Appendix C, for a complete listing of OPM defined EOD requirements.

Requirement Type	Item	Document Reference
Functional Requirement	Use Plain Language	4.1.1
Functional Requirement	Employment Eligibility Verification	4.1.2
Functional Requirement	Data Utilization Grouping	4.1.3
Functional Requirement	Form Packages	4.1.4
Functional Requirement	Form Library	4.1.5
Functional Requirement	HR Intervention	4.1.6
Functional Requirement	Form Owner Acceptance	4.1.7
Functional Requirement	Applicant Data Input Changes	4.1.8
Functional Requirement	Personal/Public Email Addresses	4.1.9
Functional Requirement	Additional Reference Information	4.1.10
Functional Requirement	Human Resources Role	4.1.11
Functional Requirement	Educational Data Update	4.1.12
Electronic Form Completion	Electronic Form Completion	4.2.1
Electronic Form Completion	Form Preview Capability	4.2.2
Electronic Form Completion	Electronic Form Changes and Reproductions	4.2.3
Electronic Form Completion	Electronic Form Storage	4.2.4
Electronic Form Completion	Data Input Confirmation	4.2.5
Electronic Form Completion	Electronic Signatures	4.2.6
Electronic Form Completion	Electronic Certification of Multiple Forms	4.2.7
System Requirement	Form Tracking	4.3.1
System Requirement	Administrator Rights	4.3.2
System Requirement	Real-Time Updates	4.3.3
System Requirement	Role-Based Rights	4.3.4
System Requirement	Data Input Sources	4.3.5
System Requirement	Data Entry	4.3.6
System Requirement	Data Validation	4.3.7
System Requirement	Error Alerts	4.3.8
System Requirement	Source System Identifier	4.3.9
System Requirement	Mass Hires	4.3.10

Requirement Type	Item	Document Reference
Reporting Requirement	Date and Time Stamps	4.4.1
Reporting Requirement	Access Metrics	4.4.2
Reporting Requirement	User Actions Audit Trail	4.4.3
Reporting Requirement	Cycle Time Metrics	4.4.4
Reporting Requirement	Personally Identifiable Information on Reports	4.4.5
Data Transfer	eOPF Interface Control Document (ICD)	4.5.1
Data Transfer	Data Export	4.5.2
Data Transfer	Temporary Account Termination	4.5.3
Data Transfer	Data Reconciliation	4.5.4
Data Transfer	Data Transmission Receipt	4.5.5
Data Transfer	Forms Not Included on the OPM Master Forms List	4.5.6
Data Transfer	Records Retention	4.5.7
Security and Accessibility Requirements	508 Compliancy	4.6.1
Security and Accessibility Requirements	Help Roles	4.6.2
Security and Accessibility	Tiered Help Capability	4.6.3
Security and Accessibility	Federal Security Standards	4.6.4
Management Requirements	Error Reporting	4.7.1
Management Requirements	Change Requests	4.7.2
Management Requirements	System Documentation	4.7.3
Form Owner Requirements	Form Template Updates	4.8.1
File Transmission Methodology	Memorandum of Understanding (MOU)	5.1
File Transmission Methodology	EOD Self Certification	5.1
File Transmission Methodology	Interconnection Security Agreement (ISA)	5.1
File Transmission Methodology	Authority to Operate (ATO)	5.1
Privacy Requirements	Privacy Impact Assessment	6.1
Privacy Requirements	Privacy Act Statement	6.2