Human Capital Data Management and Modernization

Entrance on Duty (EOD)
System Certification Package

EOD Certification

EOD System Certification Package 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 6.0 of the Entrance on Duty (EOD) Requirements and System Certification guidance.

- 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 all 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.

EOD 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.

Entrance on Duty Certification - System Certification Worksheet

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
Forms not on the Master Forms List	3.0	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 loading into or transmission to eOPF.			
		The EOD provider and agency must obtain approval from the eOPF PMO prior to the transmission of documents not included in the OPM Master Forms List or the list of forms contained in the EOD Requirements and System Certification guidance.			
Privacy Impact Assessment	4.1	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 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 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.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
Personally Identifiable Information on Reports	4.2	System reports containing personally identifiable information (PII) must contain an official privacy statement.			
Privacy Act Statement	4.2	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.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
Social Security Number Solicitation	4.3	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			
System of Record Notice (SORN)	4.4	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.			
Form Version	5.1	The EOD system must contain current form versions. Form owners are responsible for the dissemination of updated, unlocked form versions.			
Form Owner Acceptance	5.1	All form specific requirements as defined by the official form owner must be adhered to.			
		Agencies must thoroughly evaluate the commensurate risk and benefits associated with electronic signature technologies to assure security and reliability of the provider's electronic approval process is equivalent to or greater than a wet signature.			
Electronic Form Changes and Reproductions	5.1.1	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.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
		Agencies may not modify Federal forms without prior approval. A copy of form owner approvals for all changes must be provided to the eOPF PMO prior to initiation of electronic transmission of forms to eOPF.			
Records Retention	5.1.2	Agencies must 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.			
Electronic Signatures	5.2	Electronic signature methods are applied in compliance with the NIST Guidance for Electronic Signatures and the GPEA.			
		The electronic signature must be affixed at the time of certification and in accordance with the policy of the form it applies to.			
Electronic Signature Block Text	5.2.1	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 Authority to Operate (ATO) must be granted and a copy of the letter or memorandum is provided to OPM.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
Electronic Signature Dates	5.2.2	The electronic signature date must be affixed at the time of certification and in accordance with the policy of the form it applies to.			
Use Plain Language	5.3	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.			
Data Entry	5.3	Users enter information one time, so that data elements required on multiple forms are collected once.			
Data Collection Grouping	5.3.1	User entry is by category to simplify user entry. Categories are defined by logical information groups such as General Information or Prior Federal Service, and may be presented as separate panels or screens.			
Data Input Sources	5.3.2	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.			
Personal/Public Email Address	5.3.3	The applicant can enter a personal email address to receive EOD logon information and notifications.			
Additional Reference Information	5.3.4	All instructions and related information necessary for the user to make an informed decision relative to the respective forms are contained in the automated system.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
Educational Data Update	5.3.5	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 transmitted to OPM via an agency's Human Resources Information System.			
Real-time Updates	5.3.6	Records must be updated in real-time. The eOPF PMO interprets this requirement to preclude the use of batch processing.			
Mass Hires	5.3.7	Federal EOD system accommodates the requirement for mass hires.			
		The EOD process is capable of being initiated for multiple users simultaneously.			
Data Validation	5.3.8	Validation of the data entry occurs to the extent practicable to reduce the burden on both the appointee and the HR office.			
		Data Validation occurs at the form level to verify that the user is eligible for the completion of certain forms.			
Error Alerts	5.3.9	Tiered error alerts 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.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
		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.			
Form Preview Capability	5.3.10	EOD users are able to view forms at any time during the data utilization process. The user is provided with the opportunity to view EOD forms to which their data will apply during the data input process.			
Electronic Form Completion	5.3.11	Form completion may occur at any time; however, the electronic approval/certification of an EOD form, which is verified with the application of an electronic signature, may only occur in accordance with the certification period for each form.			
Electronic Certification of Multiple Forms	5.4	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.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
Data Input Confirmation	5.4.1	An EOD system must generate an audit trail that demonstrates 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: • 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 Government Paperwork Elimination Act (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.			
		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).			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
		• Privacy Act Statement that includes the agency's authority, purpose, routine use, and disclosure disposition for the utilization of EOD information.			
		• Following electronic approval/signature of forms, the 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.			
User Actions Audit Trail	5.4.2	A reporting capability is available to review system usage metrics such as completion and submission time stamps and applicant progress.			
		The system 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.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
		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			
Human Resources Role	5.5	The HR review process is integrated in the system. Electronic systems do not replace HR's obligation to review and approve employee documentation.			
Employment Eligibility Verification	5.5.1	Employee eligibility verification must be complete prior to federal employment. Employment eligibility requirements must be included in the design and implementation of an EOD system, and external sources, such as E-Verify, should be incorporated as appropriate.			
HR Intervention	5.5.2	Designated HR personnel should have ability to monitor user progress.			
		Intervention may be required by HR in the event that pre-determined conditions are met. Intervention may be completed manually.			
Application Data Input Changes	5.5.3	An employee cannot initiate changes to forms following approval and release of the forms.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
		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 transmitted to the final system of record, the document is destroyed or an alternate appropriate action is taken per the agency records manager.			
Electronic Form Storage	5.6	An authorized user must be able to print a completed EOD form, as it would appear if completed via the paper form prior to electronic transmission to eOPF.			
Form Package	5.6.1	A form package is used to define and store forms. 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.			
Form Library	5.6.2	A form library is used to house forms. A form library is a group of forms available for selection and completion via an EOD system.			
		System administrators must be granted the authority to add forms and documents to the form library.			
Date and Time Stamps	5.6.3	Date and time stamps are provided where appropriate and at the form level for storage in the system audit trail.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
		Appropriate instances include a record of when a form is electronically certified by the employee,			
		transmitted 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 transmitted out of the EOD system until a final EOD date is populated.			
Role-Based Rights	5.7	Role-based capabilities include viewing, printing and form completion.			
		Roles are to be defined in a way that is similar to the rights and responsibilities assigned in the paper world.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
Federal Security Standards	5.7.1	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.			
Administrator Rights	5.7.2	Designated EOD system administrators are able to add, change, and delete 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.			
Access Metrics	5.7.3	A reporting capability is available to review access metrics for all EOD users.			
		Designated administrative users are able to access a report that details which users have accessed the EOD system and the time of access.			
		The report should detail which HR Specialists have accessed a particular user account or forms and when this occurred.			
Temporary Account Termination	5.7.4	Temporary accounts are automatically terminated after notification of successful record transmission or within 90 days.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
		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. Agencies should define a business process to validate that a record has successfully transmitted within 90 days from the official EOD date.			
		Documents are purged following reconciliation of transmission. EOD is not used as a long-term system of record.			
		All EOD forms must be transmitted to either eOPF or to an alternate system of record prior to account termination.			
Data Export	5.8	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.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
		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.			
eOPF Interface Control Document (ICD)	5.8.1	File transmission from an EOD system to eOPF complies with the requirements and specifications detailed in the eOPF ICD. Agencies and data providers are required to provide accurate and complete data in compliance with the ICD. Every form must be entered into the EOD system and submitted for each transaction file type: delivery, modify.			
		Print all forms to compare the data in eOPF to the data in the EOD system and confirm it matches.			
		Validate the eOPF accounts are updated and the data is correct.			
		Validate the indexing is correct: • Form number/form type • Source system identifier (must appear on each form) • Indexing date • Effective date • Source side • Delivery side • Merge folder • Duplex or two sided form			
		Validate forms requiring an NOA contain an NOA. Vice versa.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
		Validate each form contains the minimum data that must be completed.			
		Validate all required fields contain data.			
		Using the printed copies of the forms, validate all data truncated appropriately.			
		Validate the data and indexing complies with the OPM guidance.			
		Validate the signature block contains the text "Electronically signed by: <Signer Name>".			
		Validate any agency specific requirements or custom specification.			
		Confirm provider is only submitting forms under his/her purview, e.g. an EOD provider can only submit EOD forms.			
		Confirm provider is only transmitting data entered by an employee directly into an electronic EOD system.			
		Confirm security and reliability of the provider's electronic approval process is equivalent to or greater than a wet signature.			
Data Reconciliation	5.8.2	The EOD system must capture and maintain sufficient data for reconciliation of data transmission between systems.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
Transmission Receipt	5.8.3	Administrative users are provided with a transmission receipt following the successful transmission of EOD data to eOPF or the system of record.			
Source System Identifier	5.8.4	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/Agency Sub Element Code> <Producer or Vendor Name>.			
Cycle Time Metrics	5.9	A reporting capability is available to review 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.			
508 Compliancy	5.10	In compliance with 29 U.S.C. 794d, a Federal EOD system and EOD system output must be Section 508 compliant. System output includes but is not limited to completed forms, reports, and verification pages/screens.			
Tiered Help Capacity	5.11	Federal EOD system implements a tiered help capability to include the use of online help and help desk support.			
Help Roles	5.11.1	The HR LOB EOD CONOPS requires the capability for help roles (e.g., system administrators, Help Desk) to view the EOD record.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
		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).			
Error Reporting	5.11.2	An effective EOD program office allows for the submission of System Problem Reports (SPR).			
		Reports are available. They 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, exists and may feed into a configuration control process.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
Change Requests	5.11.3	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.			
System Documentation	5.11.4	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.			
Data Warehouse Program PMO System Certification Methodology	6.0	The eOPF PMO has established that the following documents must be exchanged to ensure both parties meet acceptable conditions before data are transmitted from one system to another: • EOD Certification: The EOD Certification process is designed to foster agency accountability for systems that meet the legal sufficiency requirements for documentation stored in eOPF. The EOD Certification contains a list of requirements that must be met before an agency is permitted to transmit data to eOPF.			

Requirements		Reference Section and Description	EOD System Meets Requirement for Each Form Yes/No? If yes, include documentation	If no, what is the action plan for correcting system?	Proposed Implementation Date?
		• 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 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 ATO.			
		• Authority to Operate (ATO): Prior to data acceptance, an agency must provide OPM 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.			

The _(EOD System Name)_____ complies with all functional, security, auditing, reporting and data retention requirements as defined in the OPM EOD Requirements and other OPM guidance.

_____
Signature of EOD Provider Representative

_____
Date of Signature

_____
Print Name, Title, Email Address and Telephone Number of EOD Provider Representative Completing Review and Testing of EOD Software

As the _____ Program Manager for my agency, I acknowledge responsibility for and hereby certify that__(EOD System Name)_____complies with all functional, security, auditing, reporting and data retention requirements as defined in the OPM EOD Requirements and other OPM guidance.

_____
Signature of Agency Representative

_____
Date of Signature

_____
Print Name, Title, Email Address and Telephone Number of Agency Representative Completing Review and Testing of EOD Software

The _(EOD System Name)_____System is hereby authorized for three years from _(Effective Date)_____. The EOD system must be recertified at the end of three years or at any time EOD software changes that affect the forms used by the agency. Recertification includes complete testing. Failure to meet the EOD requirements or comply with the OPM

_____
Signature of OPM eOPF Representative

_____
Date of Signature