MANUAL TRANSMITTAL

2.25.2

Department of the Treasury
Internal Revenue Service

FEBRUARY 26, 2018

EFFECTIVE DATE

(02-26-2018)

PURPOSE

(1) This transmits revised IRM 2.25.2, Managed Service for IRS, IRS Portal and Extranet Usage Standard.

MATERIAL CHANGES

(1) The information in IRM 2.25.2 has been updated to reflect the transition of the Employee User Portal to the Integrated Enterprise Portal environment.

(2) This IRM has been updated to reflect changes resulting from combining Public User Portal (PUP), Registered User Portal (RUP) and Employee User Portal (EUP) in one Managed Service contract. This change will leverage industry leading practices and innovations to improve the IRS web environment's efficiency. The Business Owner is the Deputy Commissioner Services and Enforcement, Online Services (OLS), however, this IRM is now maintained, managed, and enforced by the Information Technology (IT) Enterprise Technology Implementation (ETI) as the Portal Program Management Office has been dissolved due to the reorganization.

(3) Added Program Scope and Objectives

EFFECT ON OTHER DOCUMENTS

IRM 2.25.2, dated September 29, 2014, is superseded.

AUDIENCE

All Operating Divisions & Functions, IT organizations, Enterprise Technology Implementation (ETI) , Enterprise Operations (EOps) Enterprise Services (ES), Application Development (AD) and Cybersecurity (CS) and Application's Program Management Offices (PMO) are required to use this IRM.

S. Gina Garza
Chief Information Officer

2.25.2
IRS Portal and Extranet Usage Standard

Table of Contents

2.25.2.1 Program Scope and Objectives
2.25.2.2 Portal Definitions
2.25.2.3 Portal Standard Guidelines
2.25.2.4 Portal Identification and Assignment
2.25.2.5 IRS Portal and Extranet Usage Standard Governance
2.25.2.6 Exception Process
2.25.2.7 Information Resources Accessibility Program (IRAP)
2.25.2.8 ELC
2.25.2.9 Transition Management
2.25.2.10 Portal Security

Exhibits
2.25.2-1 Portal Identification and Assignment Checklist

2.25.2.1
(02-26-2018)
Program Scope and Objectives

(1) This section defines the standard and directs the usage of the Integrated Enterprise Portals (IEP). For all business applications in development prior to the ELC MS3 and all other new IT applications, IRS intranet users and external system interactions for these business applications shall utilize the IEP identified in this IRM. This IRM covers what a managed service contractor is required to address and what is required for both external web based users (individuals and systems) and internal web based users (individuals) that have been identified by the Enterprise Technology Implementation (ETI) and Enterprise Architecture Office (EA).

(2) It is the standard of the IRS that interactive and batch electronic connections are organized through as few portals as feasible and that the use of those portals is appropriate to the IRS' mission. The reduction in numbers of portals is important to achieve maximum integration of assets; reduction of costs; and standardization of security.

(3) IRS organizations and users in complying with this portal standard are essential to the IRS achieving enterprise goals. If there are any questions or if additional guidance on this standard is required, contact Enterprise Technology Implementation (ETI) at 240-613-4726 *PortalPMOMailbox@irs.gov or Enterprise Architecture Office at *Enterprise Architecture enterprise.architecture@irs.gov 240-613-4443.

2.25.2.2
(02-26-2018)
Portal Definitions

(1) A "Portal" as used in this standard is defined as the web based infrastructure (hardware and software) that serves as the entry point for web access to IRS applications and data. The portal provides common services such as communications services, platform services, security services and applications services, content managements services, and common services, secure methods for accessing/updating IRS application and data. The various portals are distinguished by whether their users are internal or external, by the nature of the interaction or exchange, and by the nature of threats, risks, and protections required by the data or applications, including the method of authentication and authorization.

(2) The Integrated Enterprise Portals (IEP) has combined the infrastructure of all three portals: the Public User Portal (PUP) (formerly the Digital Daily), the Registered User Portal (RUP), which allows IRS to leverage efficiencies, and the Employee User Portal (EUP), which allows IRS to streamline processes. The IEP-PUP is the IRS external or Internet portal that allows unrestricted public access to non-sensitive materials and applications, including forms, instructions, news, and tax calculators. No authentication is required for access to any materials on the IEP-PUP.

(3) The IEP-RUP is the IRS external portal that allows registered individuals and third party users (registration and login authentication required) and other individual taxpayers or their representatives (self authentication with shared secrets required) to access IRS for interaction with selected tax processing and other-sensitive systems, applications, and data. User interactions are encrypted from the user's workstation or system to the portal, across the Internet or via direct circuits. The IEP-RUP, via the Common Communication Gateway, also supports IRS extranets, such as the exchange of bulk files of information with the IRS and the Virtual Private Network (VPN) (both inbound and outbound), by registered and authorized external entities.

(4) The IEP-EUP is the internal IRS portal that allows IRS employee users to access IRS data and systems, such as tax administration processing systems, financial information systems, and other data and applications, including mission critical applications. Modernization registration and authentication are required for access to sensitive and mission critical applications, and all user interactions with those systems are encrypted from workstation to portal across the IRS internal network. The IEP-EUP allows IRS employee users with LAN accounts (Windows Network Login) to access Intranet sites, selected applications, non-sensitive data and selected sensitive processing where network encryption and modernization logon are not required (e.g., employee access to selected elements of their own personnel data). IRS network authentication is a basic requirement for access to any materials or services, and is also required to access modernization registration and authentication.

2.25.2.3
(02-26-2018)
Portal Standard Guidelines

(1) Commencing August 31, 2003, all proposed and design-phase business applications requiring end-user interactions (human-computer interactions) or external file transfer and system-to-system capabilities shall conform to this standard. Existing applications or systems in production are exempt from this standard until they undertake major changes or are replaced by modernized processing.

Note: All planned system development efforts in the Milestone 2 & 3 Phases or before are subject to this standard.

(2) This standard does not cover stand-alone workstation software applications (e.g., office automation) which do not interact with separate systems or applications beyond standard network file sharing. Also, this standard does not apply to top security level organizations that have exceptions or have been permitted certain access to systems with the appropriate approval.

(3) The following standard statements shall be adhered to:

1. All data and applications, which do not require authentication and are/will-be available to the general public, shall be accessed through the Integrated Enterprise Portal - Public User Portal.
2. All interaction by external entities, which requires authentication, will be accessed through the Integrated Enterprise Portal - Registered User Portal.
3. All internal tax administration processing involving taxpayer data and subject to unauthorized access (UNAX) restrictions shall be accessed through the Integrated Enterprise Portal (IEP) -Employee User Portal (EUP) and require modernization authentication and workstation to portal encryption. All other internal IRS employee interactions with processing systems and web sites should also be accessed through the IEP- EUP, with modernization logon and encryption requirements determined by their sensitivity and risk profile.

2.25.2.4
(02-26-2018)
Portal Identification and Assignment

(1) Exhibit 1 shows the Portal Identification and Assignment Checklist. The checklist is intended to facilitate analysis in determining the correct portal capabilities needed by a project. The checklist will gather the information required to make portal and capability assignments based on business and security requirements and will be submitted to EA. Completed checklists serve as the basis for determining portal assignments for specific processing within a

project or system. Completed checklists also are used as a tool in the decision making process when waivers are requested.

(2) Note that any specific project or system may use multiple portals (e.g., a project may make public data available to taxpayers via the Integrated Enterprise Portal - Public User Portal, make sensitive applications available to taxpayers and third parties via the Integrated Enterprise Portal - Registered User Portal, and make both data and applications available to employees via the Employee User Portal).

(3) Business owners proposing new applications or significant modifications to existing system interfaces shall complete a Work Request Management System (WRMS). EA personnel shall assist business owners in completing the WRMS. Business owners shall include the completed WRMS.

(4) EA shall review the completed checklists and determine the appropriate portal capabilities for the proposed application. In the event that the business owner disagrees with the portal assignment(s), the business owner may apply to EA for a waiver. The EA Standards web-address is http://it.web.irs.gov/EA/About/EA.htm.

2.25.2.5
(02-26-2018)
IRS Portal and Extranet Usage Standard Governance

(1) The IRS Portal and Extranet Usage Standard will be managed and enforced by Enterprise Architecture Office within the Information Technology (IT).

(2) EA will:

- Facilitate communication and information flow across the Enterprise for the three IRS portals.
- Provide guidance and communication to stakeholders across the PUP, RUP, and EUP.
- Ensure decisions regarding the three IRS portals are executed in a timely manner.
- Ensure that appropriate procedures, processes, and guidelines are in place for the management of the three IRS portals and other special extranets at the IRS.
- Ensure IRS employees can access IRS data and systems and those IRS employees with LAN accounts can access Intranet sites, depending on their rights and permissions.

(3) EA is responsible for the standards and guidelines as it relates to portal web sites and will:

- Provide standards and guidance to IRS users submitting web applications to the IEP - PUP, IEP - RUP, and IEP - EUP.
- Ensure correct hosting environments are used based on Security standards and guidance for IRS application security levels.
- Provide guidance to IRS users for portal environments and ensure that consistent reviews apply appropriate criteria. Support all portal standards and guideline documentation governed by IT.

2.25.2.6
(02-26-2018)
Exception Process

(1) Waivers to portal access assignments(s) may be granted by the Enterprise Architecture (EA) Office if critical business needs cannot be met.

(2) Critical business needs and/or Congressional Mandates with schedule constraints that cannot be met by the standard mandated portal(s). Waivers with a get-well plan will be required and evaluated by EA.

(3) This exception process applies to in-flight .NET applications while there is no available hosting environment in the Integrated Enterprise Portal (IEP) - Employee User Portal (EUP).
EA Office Enterprise Services (ES) explored and recommended enhancements to the current IEP - EUP to enable .NET hosting capabilities. However, due to budgetary constraints and directional changes, ES executive management authorized the use of "Current Production Environment with Active Directory-base authentication " as a hosting environment (hereafter referred to as CPE .NET Environment) outside of the Portals.

The CPE .NET Environment is a temporary hosting solution for in-flight .NET applications intended for IRS-internal users. All in-flight .NET-based intranet applications (applications for internal use only) are granted temporary permission to be hosted in the CPE .NET Environment until a portal infrastructure with .NET capabilities is available. For other application hosting standards, please refer to the Application Hosting Guidance posted in ETI web site at: http://ppmo.goportal.web.irs.gov/progress.aspx

EA will implement the migration of hardware/software/application from the CPE .NET to the IEP - EUP (or new portal) after .NET capabilities in the portal infrastructure are available.
Java-based applications must adhere to this IRM, specifically section 2.25.2.1, unless otherwise granted waiver by ES executives.
.NET-based intranet applications hosted in the CPE .NET Environment must:

- Complete migration or transition to the IEP -EUP (or the new portal infrastructure) in a reasonable timeframe after .NET capabilities are made available in the IEP -EUP (or the new portal infrastructure).
- Accept and be responsible for transition costs incurred from migrating to the IEP-EUP (or the new portal infrastructure) after .NET capabilities are made available in the IEP- EUP (or the new portal infrastructure).
- Conform to the .NET Application Design Pattern set forth by EA and make the transition-to-IEP - EUP (or the transition-to-new portal infrastructure) smoothly.

2.25.2.7
(02-26-2018)
Information Resources Accessibility Program (IRAP)

(1) The primary roles and responsibilities for IRS accessibility guidance belong to IRAP. The IRAP Program Manager serves as the official Section 508 Coordinator for the IRS. As such, IRAP will:

- 1. Proactively seek and bring together Section 508 related updates (laws, regulations, policies, guidelines, etc.).
- 2. Notify Integrated Enterprise Portal (IEP) directly of these updates.
- 3. Promulgate and market accessibility requirements throughout the agency, as necessary.
- 4. Assist the Managed Service contractor or the application in preparing the accessibility portion of a web development life cycle framework that can be integrated into day-to-day operations.
- 5. Participate with Managed Service contractors or the application in the evaluation of automated testing tools that support 508 web accessibility for possible use in the web development life cycle.

- 6. Endorse selected Section 508 software tools that assist site owners in making their web sites compliant with this IRM.
- 7. Support Managed Service contractor or the application Accessibility Plan for technical support by partnering in plan formulation and endorsement.

(2) For additional guidance please refer to the IRAP web address – http://irap.web.irs.gov/

(3) The links are: for Section 508 – http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards

2.25.2.8
(02-26-2018)
ELC

(1) The Integrated Enterprise Portal (IEP) uses the ELC Managed Service Path. The Managed Services Path is designed to capitalize on the benefits of Managed Services provided by either an outside service (3rd party); internal intra-business processes; and/or existing infrastructure (operational) service provider. This could include software package(s), integrated software packages, shared-services and/or infrastructure components (assets) e.g., servers, web hosting, network centric, workstations, support services and/or web hosting. The managed service is: (a) proprietary; and/or, (b) not maintained by the IRS. The standard detailed reviews required in the development of new solutions or the purchase of a service is not required when the solution is being provided and maintained by a service provider. The Managed Services Path is oriented toward selection and acceptance of the managed services solution, i.e., outside source (3rd party), intra-business processes, and/or infrastructure (operational) service provider.

(2) For additional guidance please refer to the ELC web address – http://elc.nc.no.irs.gov/elcpmoweb/index.asp

2.25.2.9
(02-26-2018)
Transition Management

(1) Integrated Enterprise Portal (IEP) is a Managed Service contract and therefore meets the Transition Management (TM) level I support requirement. IEP is responsible for the following:

- Identify and Manage Project TM Team members
- Coordinate TM Training for Project TM Team
- Lead Organization Alignment
- Lead Gap Identification
- Schedule and Conduct Readiness Workshops
- Write the TMP and submit to TMO Project Office
- Submit to Organization for approval
- Monitor Gap Closure/TMP implementation

(2) For additional guidance please refer to the ETMO web address -http://it.web.irs.gov/ES/BRSD/ETMO/default.htm.Monitor Gap Closure/TMP implementation.

2.25.2.10
(02-26-2018)
Portal Security

(1) Security of the IEP Managed Service Environment

(2) Managed service providers conducting business with IRS are responsible for providing the minimum NIST 800-53 (latest revision) security controls to protect Federal information and information systems at the FIPS categorization level applicable to the acquisition

(3) The IRS consumer organization acquiring a managed service shall ensure the solution meets FISMA requirements. To meet those requirements the IRS consumer can use the following guidance:

- Ensure the acquisition includes the FISMA security requirements, at an appropriate FIPS categorization level. Include any necessary customizations such as additional security requirements of organizationally defined parameters (e.g. patch application deadlines).
- Ensure the acquisition defines the security assessment method that will be used to achieve an IRS Authority to Operate, prior to the go-live production date. Ensure the acquisition includes the minimum continuous monitoring requirements defined by IRS Cybersecurity during the authoring of the solicitation. Ensure the acquisition includes any additional continuous monitoring or reporting requirements, as needed by the IRS consumer.

(4) While a managed service solicitation is being written, the IRS consumer works with IRS Cybersecurity to understand and document acceptable assessment methods, as well as continuous monitoring requirements. The available options will vary depending on the acquisition. Each acquisition has a unique scope.

(5) Some acquisitions require the service provider to deliver a new, highly customized version of their service. This type of service may not have undergone a FISMA security control assessment in the past, thus IRS Cybersecurity may require that an assessment is performed before an Authority to Operate is recommended.

(6) Other acquisitions require a proven, existing, out-of-the-box solution, that has minimal customization. For this type of service, IRS Cybersecurity may request to review evidence that the provider received an Authority to Operate from a previous IRS contract, or from another agency.

(7) Acquisitions also vary in hosting requirements. Some acquisitions require the provider to manage their solution at an agency datacenter. Other acquisitions allow the provider to manage their solution in their own datacenter, or in a cloud environment, outside the agency datacenter. Again, IRS Cybersecurity will provide different assessment options, depending on the scenario.

- For cloud acquisitions, IRS Cybersecurity may request that the service provider have an existing FEDRAMP Provisional Authority to Operate, or that the provider undergo FEDRAMP certification.

(8) In addition to the minimum continuous monitoring reports required by IRS Cybersecurity, the IRS consumer may decide to require the provider to submit additional security reports on a regular basis. This additional oversight may be applicable to systems that process sensitive data or support critical IRS capabilities.

(9) Depending on the size of the acquisition and the sensitivity of the data being processed, it may be necessary to establish a security section of the program office. This will ensure agency officials are dedicated to maintaining oversight of the managed service provider's security posture over time. Routine activities for individuals in the security office may include:

- Meeting regularly with the service provider to review status of their security posture
- Reviewing vulnerability remediation reports

- Reviewing incident investigation reports
- Reviewing and monitoring updates to correct security weaknesses

(10) The Security Control Assessment for the current IEP was performed by IRS Cybersecurity following the NIST-800-53 Revision. 3.

(11) Security process for deploying an application in the IEP environment please follow the guidance.

(12) Typically, an application project manager will submit a Security Change Request to the Cybersecurity IT FISMA Services group who will profile a Level of Assessment to determine the level of risk to the IEP, the of impact on the existing infrastructure and testing required for the application to deploy. The level of assessment results will vary widely with the risk and size of the application.

(13) Since the IEP infrastructure has an existing set of security controls, a prospective application can inherit many of the infrastructure controls. The inheritance of infrastructure security controls helps an IRS application reduce its time to market since it is not necessary to design and build all the controls from scratch. An application can also operate with controls that were already tested and proven over time.

(14) The IEP infrastructure offers the following types of controls for an application to inherit:

- IEP monitors for vulnerabilities and deploys security patches for the operating system and middleware
- IEP conducts auditing of systems administration activity using a Security Incident and Event Management System (SIEM) and investigates suspicious activity
- IEP reports infrastructure security incidents to IRS authorities
- IEP grants and monitors systems administration access to the system
- IEP securely configures operating systems, middleware and network devices using NIST and vendor hardening standards
- IEP offers authentication mechanisms for end-user access to applications

(15) To gain a detailed understanding of the existing infrastructure controls, a prospective application can consult the IEP System Security Plan, IEP Security Patch Management Plan, IEP Incident Handling Monitoring and Response Plan, IEP Security Audit Plan, IEP Continuous Monitoring Plan, IEP Security Configuration and IEP Change Management Plan and the IEP Systems Access Process.

This Page Intentionally Left Blank

Exhibit 2.25.2-1 (02-26-2018)
Portal Identification and Assignment Checklist

I. Project Description

Project Name:_____

Project Acronym:_____

Date:_____

Submitter:_____

Submitter Office:_____

Submitter Phone Number:_____

Description of Business Requirements:

Description of Project Interface Requirements:

II. Please check all organization/user types your proposed project supports:

Individual Taxpayer

Business Taxpayer

IRS Employees/Contractors with IRS Equivalent Access

Government Entities

Third Parties

Trusted Third Parties (e.g., Contractors such as CSC or Vendors such as Sun who receive a network extension to their site on a permanent or temporary basis).

Other

If you check “Other,” please provide a description of the other users below:

III. How will your users or user systems access IRS systems? Please check all methods that your users will connect to IRS systems from the list below:

Internet

Workstations/Servers on the IRS Intranet

VPN over the Internet

Fixed Point-to-Point Lines

Exhibit 2.25.2-1 (Cont. 1) (02-26-2018)
Portal Identification and Assignment Checklist

Dialup to IRS

Other

If you check “Other,” please provide a description of the other methods below:

IV. What types of services do you expect your application to provide?

Bulk Data Transfer

Interactive Applications (Dynamic)

Static Information Presentation and Retrieval

Web Services

Other

If you check “Other,” please provide a description of the other services below:

V. What is the sensitivity of the data your application processes or accesses? Please check all data classifications your users will access from the list below:

Taxpayer Data

Other Sensitive but Unclassified (SBU) Data

Access to Personal Sensitive but Unclassified (SBU) Data

Non-Sensitive

VI. Are your applications and/or data mission critical to functioning of the IRS? Please check below if your system is mission critical:

Non-Sensitive