Information Management and Technology (IMT) Project Review and Approval Handbook

(*Supplements 270 FW 2*)

November 2022

Table of Contents

Background

Requirements of the Federal Information Technology Acquisition Reform Act

Federal policy governing information technology has moved towards greater authority and accountability for agency and bureau Chief Information Officers (CIO) in several areas related to Information Management and Technology (IMT), including budget, acquisition, and portfolio management and review. This trend culminated with the passage of the Federal Information Technology Acquisition Reform Act (FITARA) in 2014 and associated Office of Management and Budget (OMB) guidance.

As part of FITARA implementation, the Department of the Interior (Department) has mandated that we—the U.S. Fish and Wildlife Service (Service)—must consolidate authority over IMT under the Associate Chief Information Officer (ACIO). This consolidation includes greater oversight over IMT spending throughout the Service, including projects within the Service's IMT portfolio. Information Resources and Technology Management (IRTM) has designed the project approval process in this handbook to achieve this goal.

In accordance with Departmental policy and delegations of authority, the ACIO has the authority to approve all "non-major" IMT projects, which are the vast majority of all proposals. **Because IMT projects that meet the threshold of "major" have to be approved by the Department's Office of the Chief Information Officer (OCIO), the ACIO's role in major projects is to decide whether or not to recommend that the OCIO approves the project.**

21st Century Integrated Digital Experience Act (IDEA)

The 21st Century IDEA requires Federal agencies to carry out a variety of actions to improve websites and other types of digital services by ensuring that they are user-friendly and accessible to individuals with disabilities, among other things. Specifically, the IDEA requires us to:

- Modernize our websites,
- Digitize services and forms,
- Accelerate use of e-signature,
- Improve customer experience,
- Standardize and transition to centralized shared services, and
- Comply with the U.S. Web Design System (USWDS) website standards and maturity model.

For the purposes of this handbook, the requirements of the 21st Century IDEA are part of the overall IMT project review and approval process. Specifically, we must evaluate all applicable IMT projects to determine if they meet the requirements set forth in the Act.

Project Review and Management

To facilitate compliance with FITARA, IRTM has developed a controlled IMT project approval process and engaged in efforts to identify, inventory, manage, and protect our IMT projects as part of a comprehensive management strategy. To further these efforts, the ACIO developed 270 FW 2, Project Management Office and Information Management and Technology (IMT) Project Management, which requires that all Service-owned or funded IMT projects and information systems, regardless of cost,

undergo an identification, evaluation, and approval process. The following principles guide the review of proposed IMT projects:

1. The ACIO will approve and IRTM will carry out IMT projects after they have gone through the IMT project review process.
2. Our IMT projects must be compliant with all applicable established and emerging requirements such as IT security, privacy, accessibility (Section 508), information collection clearance, and records management.

IMT Project Management

An IMT project refers to a temporary endeavor (with a defined start and end) with specific objectives to develop, modernize, enhance, dispose, or maintain an IMT system or investment. A project may consist of one or more components and may involve one or more acquisition- or development-related activities. This does not include technical activities done to maintain existing technical infrastructure or systems, such as configuration changes or repairs that fall into the category of operations and maintenance (O&M). Once an IMT project enters the O&M phase, the project management portion of its lifecycle is finished, until the system is modified or enhanced. This handbook does not cover overall program management and O&M requirements.

Purpose

The purpose of this handbook is to provide guidance to Business Leads, Executive Sponsors, and any other Service employee who may be involved with initiating and managing an IMT project (see 270 FW 2 for definitions of these roles). We use the terms “project originator(s)” as a generic term to describe the employee or group submitting a request, where appropriate. Any reference to “you” throughout the document refers to the project originator(s).

This handbook describes the IMT project review process and the requirements that you must meet to initiate an IMT project. While the exact requirements for authorization depend on the characteristics of the project, this handbook outlines the general process. In most cases, the IMT project review process involves the presentation of a business or mission support case for investing Service money in technology solutions.

The handbook describes:

- The IMT project review process steps and requirements;
- The roles and responsibilities of the Requirements Management Board (RMB), Information Management and Technology Requirements Committee (IMTRC), Information Management and Technology Executive Board (IMTEB), Project Management Office (PMO), and project originators for authorizing or obtaining authorization for IMT projects and related acquisitions; and
- Related review and compliance issues.

Scope

All IMT projects are subject to the IMT project review process, though the level of approval needed will differ depending on the requirements of the project. The RMB reviews and approves most projects; however, some project proposals require additional review by the IMTRC and IMTEB. More information on the level of review required, based on project characteristics, can be found in Chapter 1.

This handbook's purpose is to provide guidance on the project approval process. It does not describe any other part of the project management lifecycle. In the future, IRTM will provide additional guidance on the requirements associated with the acquisition, development, and implementation of IMT projects in this handbook or through other policy documents, as appropriate. For more IMT project and portfolio management policies, see 270 FW 2, Project Management Office and Information Management and Technology (IMT) Project Management.

Pre-Approval Best Practices

After you identify a need or a gap in our current capabilities, but prior to requesting and receiving approval for your project, undertaking certain critical tasks can help ensure project success and avoid potential issues in the future. There are currently not any formal requirements for this "pre-approval" phase; however, the following are best practices to adhere to when preparing a request.

Start by clearly defining your requirements and scope. Developing a robust set of requirements will involve reaching out to potential users or customers within your office or throughout the Service to understand their needs. In some cases, this could also involve meeting with members of the public. To define the scope of the project, think about how you would answer the question, "What does *done* look like?" This will help ensure your project does not expand beyond what you've originally planned and will help you avoid potential cost or schedule overruns.

Once you have a good description of your requirements, you can engage the RMB to help conduct market research to investigate potential solutions. This information can assist with some of the required analyses to receive approval for your project, including a high-level alternatives analysis and an initial cost-benefit analysis. You may need to meet with Region or program leadership and RMB representatives to develop this information further. Working together with the RMB, you should identify a solution that best meets the requirements of stakeholders and provides the greatest benefit to the Service.

After identifying a technical solution to a business need, you should present it to your Regional or program leadership through established channels as determined by Regional or program policy. Leadership support is a vital component of project success as they may be asked to commit resources to the development or implementation of a project or serve as an Executive Sponsor. As a result, it is often beneficial to involve leadership early in the process.

Chapter 1 – IMT Project Review Process

This chapter defines the process IRTM uses to review IMT projects. This review process ensures that the Service is meeting its responsibility for managing risks throughout the project development lifecycle and helps the ACIO (or delegated parties) to make appropriate approval decisions and monitor project health. Project originators should work with the RMB to gather the required information and develop the necessary documentation. Review these process diagrams for a visual representation of the information in this chapter.

Note: You must receive approval for all applicable projects (as outlined in this handbook and 270 FW 2) before applying funds to a project.

Process Structure

1. RMB Review, which consists of:

   a. Request initiation and requirements development;
   b. Functional reviews for cyber security, privacy, Section 508 (accessibility), and additional reviews as determined by specific project characteristics (GIS, Records Management, information collection clearance, etc.); and
   c. Voting and approval for in-scope projects, or escalation to the IMTRC for projects outside of the RMB's scope of approval.
2. IMTRC Review (if major or enterprise project)
3. IMTEB Review (if major or enterprise project)

Employees should expect the RMB review stage of the process to take at least 2 weeks. Projects that need to be approved at a higher level than the RMB will require additional review time.

RMB Review

The RMB serves as the "front door" to the IMT project review process by assisting project originators with requirements development and providing the initial response to project proposals. In addition to assisting project originators with selecting the appropriate technical solution, the RMB helps coordinate various functional reviews to ensure that the proposed solution meets applicable compliance requirements. The RMB will ultimately make approval decisions for most project proposals once their review is complete. In this section, we've broken down the process below into subsections to show activities conducted prior to the project's technical solution being confirmed through conversations with the project originator (Request Initiation and Requirements Development) and those conducted after (Functional Review).

Review the RMB charter for additional information on how the RMB functions.

Request Initiation and Requirements Development

The process begins when project originators submit a request to the RMB by emailing imt_rmb@fws.gov. The RMB will review the request and determine the appropriate scope of the project (i.e., what is the likely level of review required) and describe initial requirements that must be met, depending on the characteristics of the project (e.g., describing requirements for cloud-based projects). Depending on the complexity of your request, you may be asked to meet with the RMB to discuss your requirements. This will help the RMB gain a thorough understanding of the project requirements in the context of the available technological solutions.

At this stage, the RMB can help you perform an alternatives analysis to help identify, compare, and assess viable IT alternatives to address the given mission need or performance gap. A sound alternatives analysis facilitates a sound decision-making process and can help with determining the best solution, as well as documenting the associated rationale. Outcomes of the analysis can also help with the future acquisition planning and market research during procurements.

Once initial requirements development is complete, and the appropriate technical solution is selected or confirmed, the RMB will begin facilitating a functional review of the project as described in the following subsection.

Functional Review Process

Functional Review Process:
- ✓ Has four core components: (1) Privacy, (2) Cyber Security, (3) Accessibility (Section 508), and (4) Information Collection Clearance
- ✓ Might include additional reviews, such as GIS, High Value Asset (HVA) assessments, or Records Management assessments, depending on project characteristics.

All projects must undergo a functional review before deployment into the Service IT environment to ensure that compliance requirements are met, or when necessary, risks of non-compliance are accepted by the ACIO. In addition, depending on the makeup of the project and what kind of information it handles, additional reviews (such as HVA or GIS reviews) may be necessary. The purpose of reviewing IMT projects for privacy, security, accessibility, information collection clearance, and other applicable requirements at this stage is to ensure that project originators are adequately considering these requirements in the design and implementation of the project and to ensure that the costs associated with complying with these requirements are accurately estimated in the project proposal. In addition, this review can help determine whether there is a fatal flaw in the proposed project where it can't be made compliant or it would be cost-prohibitive to be made compliant.

The RMB has representation from each IRTM Division (Policy and Planning, Operations, Cyber Security, Privacy, and Data Management) to help identify initial requirements and gather necessary compliance information. This may include working with the Service's Associate Privacy Officer (APO), members of the IRTM Cyber Security Division (including the Associate Chief Information Security Officer (ACISO)), the Service's Information Collection Clearance Officer (ICCO), and the National Section 508 Coordinator. Once all required functional reviews are complete, the Chair of the RMB will prepare the proposal for a vote. If the project is outside of the scope of the RMB to approve, it will instead escalate the project to the IMTRC. These criteria are described briefly in the "IMTRC Review" section and in more detail in the IMTRC charter.

In some cases, it is possible that the functional review process will reveal that the project can't meet applicable requirements or that it would be cost-prohibitive to make it compliant, so it will fail to move forward as originally conceived. In these cases, the RMB will assist you with selecting an alternative solution that still meets your requirements.

See Chapter 3 "Functional Reviews Necessary for Approval" for more information about the required functional review processes and specific contacts in each area.

RMB Vote and Decision

Once all functional reviews are complete, the RMB will conduct a vote in accordance with the RMB charter. The RMB may vote to either approve, disapprove, or escalate the project to the IMTRC (if it is out of scope). Approval votes must be unanimous. If the RMB votes to approve the project, any related procurement and project activities may proceed. See the "Following Approval" section below for more information. If the RMB votes to disapprove the project, you can appeal the decision to the IMTRC.

IMTRC Review

The IMTRC is a higher-level technical review board within IRTM that has the authority to review certain complex or costly IMT projects and initiatives and adjudicate appeals of decisions made by the RMB. IMT projects will be reviewed by the IMTRC in the following scenarios:

- The project meets at least one of the criteria established in the IMTRC charter that places it outside the scope of the RMB's approval authority (e.g., it meets the threshold of a major investment as defined in Departmental guidance) and the RMB votes to escalate the project.
- The project originator appeals a disapproval decision by the RMB.

The IMTRC charter describes the IMTRC review process in more detail. For appeals, the IMTRC will vote on whether to approve the project. Once approved, you may proceed with project or procurement activities (see the "Following Approval" section). If disapproved, you may appeal the decision to the IMTEB or otherwise work with the RMB to revise and resubmit the request or investigate other alternatives, if desired.

For projects that represent potential major investments or meet one of the other criteria established in the IMTRC and IMTEB charters for triggering automatic higher-level review, the IMTRC will instead escalate the project to the IMTEB (with recommendations) for additional review.

IMTEB Review

The IMTEB brings together the ACIO, the Assistant Director for Management and Administration (AD-MA), and other senior Service leadership to review, approve, and monitor IMT projects that have enterprise-wide mission or business impacts, require cross-program or Regional budget coordination, or meet the threshold of a major investment as defined by the Department. The IMTEB charter provides more information on how the IMTEB functions.

The IMTEB reviews in-scope projects after they have been reviewed by the IMTRC as well as appeals of IMTRC decisions. The charter describes requirements for project originators, Executive Sponsors, and the appropriate program and Regional leadership. Following the review, the ACIO will determine whether to hold a vote or make a unilateral decision on the project in accordance with the charter. If the IMTEB does not approve a request, the project originator can work with the RMB to revise and resubmit it through the IMTRC and IMTEB, or they can consider an alternative solution.

Following Approval

Once a project is approved by the appropriate governance body, the PMO will assign a project manager (if necessary) to help develop the necessary project documents and initiate the project, which may include a Privacy Impact Assessment (PIA), Business Impact Assessment (BIA), and other documentation (see Chapter 3). The project manager will continue to work with Business and Technical Leads, Executive Sponsors, and IRTM staff throughout project development.

IMT projects should meet all obligatory privacy, security, and information collection clearance requirements before deployment. Project managers will work with the IRTM Investment Management, Risk Management, and Compliance Branches to ensure that project data is entered into the appropriate systems. Project managers must follow the PMO's guidelines to define implementation schedules and resource allocation as project implementation moves forward. The PMO is responsible for collecting and storing all the necessary project-related documentation. Executive Sponsors should keep a copy of the approved project proposals for their own records.

Acquisition Program Advisory Council

Some high-cost project proposals will require approval from the Department's Acquisition Program Advisory Council (APAC), in addition to the IMTEB, before the project can move into the acquisition/development phase. The APAC is a strategic and operational acquisition oversight body and serves as a forum for key stakeholders within the Department to make decisions regarding enterprise purchasing solutions and for reviewing complex acquisitions to ensure compliance with applicable law, regulations, and policy.

In accordance with the Department's Acquisition, Assistance, and Asset Policy- 60 (DOI-AAAP-60), the APAC must review any acquisition that meets the defined APAC threshold. This includes, but is not limited to, acquisitions that:

- Have total contract lifecycle costs that exceed $50,000,000;
- Include an enterprise-level contract **and** will be used to procure a category of products or services for more than two Departmental bureaus or offices with a total dollar value of $5,000,000 or more;
- Require an analysis of alternatives or a business case in accordance with OMB M-19-13, Category Management: Making Smarter Use of Common Contract Solutions and Practices;
- Are highly sensitive or important, considering political implications, connection to the Department's mission goals, connection to critical Governmentwide programs and priorities, or any other relevant factors; or
- Are associated with a current or potential major IMT investment, as defined in Departmental capital planning guidance.

For projects that meet this threshold, the ACIO, assigned PMO representative, and Contracting Officer (if applicable) will coordinate with the project originator and Executive Sponsor to develop an acquisition strategy and the other documentation needed to make a presentation before the APAC. The APAC will review the project according to the process in DOI-AAAP-60.

Existing Projects and Investments

The review process in this handbook ensures that new IMT projects meet minimum necessary requirements. While these projects and systems must remain compliant with our privacy, security, accessibility, etc. requirements throughout their lifecycle, this handbook and its associated Service Manual chapter (270 FW 2) do not specifically address any compliance-related issues once the system meets requirements and begins operation. In certain circumstances an existing investment with an Authorization to Operate (ATO) may have to undergo one of the reviews described here. If a modification or enhancement to an existing Service investment requires a new expenditure of funds of over $1 million and/or leads to changes that may affect privacy, security, accessibility, information collection, etc., that modification may require review through the IMT project review process. This will generally only be necessary for major modifications, such as upgrading a legacy system to a new technology platform.

For instance, an in-house development project to upgrade an existing Service system that handles or manages Personally Identifiable Information (PII) that will modify how that PII is managed or secured would require the submission of a new project proposal before IRTM can approve the project and apply funds. Depending on the context of the modifications, the functional review process should be much faster, as reviewing officials might only need to approve changes in a specific functional area.

Chapter 2 – Requirements for Specific Types of IMT Projects

TYPES

The purpose of this chapter is to provide additional guidance about the requirements for specific categories of IMT projects. It describes additional steps that employees must take when considering specific use cases, including Commercial, Off-the-Shelf (COTS) packages, cloud-computing applications, mobile applications, and in-house or contracted application development. In addition to the review process described in Chapter 1 of this handbook, certain categories are governed by additional Federal and Departmental requirements. Employees should use this guidance as a supplement to the overall approval process described in the preceding chapter.

Commercial, Off-the-Shelf (COTS) Applications

COTS is a term used to describe the purchase of existing software solutions that are either used directly "out-of-the-box" or that are bought and configured to meet organizational needs. We purchase or license them from third-party vendors (for example, Microsoft Office). Applications that are on the Service's approved software list do not require any additional approvals outside of an Information Technology Purchase Approval (ITPA) request. COTS packages that are not on the approved list will require some additional analysis and approval from the RMB. However, a project involving a COTS application may require the full IMT project review process if the RMB believes that the request represents a project or if it contains a cloud component.

Generally, a COTS application will only require the IMT project review process if it is proposed for Servicewide use and will be established through an Enterprise Licensing Agreement or a Blanket Purchase Agreement. When initiating such a request, employees should reach out to an IT contracting specialist within the JAO (see list of contacts) on how to set up such an agreement.

Open-Source or Free Software

The review requirements outlined in this handbook can apply to both proprietary and open-source software and applications. For the purposes of this handbook, the term open-source software refers to software programs using an "open" license, which means that anyone can access, use, modify, and share them. Open-source software may be free to download, or there may be a fee. Regardless of whether the requested software is free, the RMB may need to review it in a similar fashion as we do proprietary COTS applications to ensure it meets our compliance requirements. We will treat these requests in the same manner as proprietary COTS software described above.

Cloud-Based Projects

The Department sets the standards for the Service's cloud procurement process. Departmental policy, as outlined in the Departmental Memorandum, "Acquisition of Information Technology Cloud

Services/Mandatory Use of Pre-approved Cloud Hosting Services and Contracts; August 7, 2018"
requires that:

- The Service must obtain cloud-based services using approved enterprise-wide cloud hosting solutions or contracts, as shown on the DOI Cloud Intranet site;
- All cloud procurements, including those that are issued against one of the approved enterprise-wide cloud hosting solutions, must be approved by the ACIO; and
- The Department's CIO and Senior Procurement Executive must approve any acquisition of a cloud-based product outside of approved solutions and contracts.

All cloud-based solutions (including applications, subscription services, etc.) must meet these requirements. Projects that include cloud-based components that have not been approved by either the Department or the Service will require an extensive investment into cyber security assessments and hence must go through the IMT project review process no matter the cost. As a result, even acquiring "smaller" cloud-based applications or web tools or services used by a limited number of employees may require a very expensive, lengthy IT security review and approval process. IRTM recommends consulting with the RMB's Cloud Point of Contact (POC) by emailing imt_rmb@fws.gov prior to initiating any cloud procurement request.

When considering whether to procure a cloud-based solution or migrate an existing Service application or system to the cloud, it is important to gather and understand stakeholder requirements as part of the planning process to determine if a cloud-based solution is appropriate and which cloud provider is a good fit. For instance, it is important to consider network reliability and the volume of data involved. The RMB Cloud POC can help collect and use this information to guide a project originator to analyze potential solutions and make a business case for the project that is based on the technical and business-related needs of stakeholders.

Cloud-based Project Approval Requirements

The approval requirements are as follows:

A. Prior to making any planning and/or financial arrangements, contact the RMB at imt_rmb@fws.gov for assistance with reviewing and providing feedback on the potential project idea. The RMB's Cloud POC has broad knowledge of applying technology options to solving business or process automation problems across the Service and within the Department. They can share this knowledge and expertise with the project originator and help find the most optimal solution in terms of costs, risks, and efficiency.

B. After gathering the information necessary to formulate a business case for the potential cloud solution, the project originator, with help from the Cloud POC, will submit the cloud project proposal to the RMB. This serves as the initial request. The RMB will conduct a functional review, as described in Chapter 1. This will ensure that the proposal incorporates the appropriate compliance requirements.

C. Once the functional review is complete, the RMB will vote on whether to approve the proposal unless it falls outside the scope of RMB approval (as described in Chapter 1). If it is out of scope, the RMB will escalate it to the IMTRC and IMTEB.

D. After the project originator receives final approval, the PMO may assign a project manager to the project, signaling the beginning of the project management process.

Mobile Applications

This section of the handbook covers applications written for mobile devices and not the mobile device (e.g., iPhone, or a tablet PC) itself. Generally, requests to purchase mobile applications do not require the full IMT project review process. Instead, they require approval from a supervisor and will be evaluated by the RMB and approved via an Information Technology Purchase Approval (ITPA) request. However, a project involving development of a new mobile application will require going through the IMT project review process.

Mobile Application Development (In-House or Contracted) Requirements

A. Mobile applications developed by, on behalf of, or in coordination with the Service, and that are made available to the public and advertised as Service or Federal Government mobile applications using a Service logo or other means must:

(1) Meet applicable National Institute of Standards and Technology (NIST) guidelines, including NIST 800-37, NIST 800-53, Revision 5, and 800-163;

(2) Undergo the IMT project review process described in this handbook;

(3) Meet the baseline security and privacy requirements outlined in DOI OCIO Directive 2016-003, Department of the Interior Mobile Applications Privacy Policy, including undergoing a compliance review prior to deployment and receiving an ATO to clear the application under NIST guidelines and the Federal Information Security Management Act (FISMA);

(4) Pass periodic compliance reviews by IRTM privacy and cyber security personnel following initial deployment; and

(5) Must comply with information collection clearance requirements and renewals, as appropriate.

These requirements apply if the Service has paid for or otherwise sponsored the application (i.e., the application uses the Service logo), even if a concessionaire, contractor, partner, or other third-party group distributes the application.

B. Mobile applications do not need to clear vetting under FISMA or undergo the IMT project review process described in this handbook if a concessionaire, contractor, or partner provides it directly to the public, if it uses its own privacy statement, and if it is not:

(1) Advertised as a Federal mobile application,

(2) Funded by the Government,

(3) Using any Service intellectual property or data, and

(4) Going to be used to share data with the Service.

These applications:

(1) Are typically the type companies, such as outfitters and guides, provide; and

(2) Are not considered Service-owned or sponsored applications.

Once the Service pays for a mobile application, it becomes subject to the requirements in section A above and it is considered a Federal application.

C. The mobile application development or modification process also requires ongoing review, monitoring, and evaluation. Following are the Service's processes:

(1) Mobile application development or modification proposals must go through the IMT project review process described in Chapter 1.

(2) After approval and during development, the application will be monitored by Service privacy, cyber security, information collection clearance, and other IRTM management officials who will work with application developers and the project originator to ensure that security, privacy, and information collection clearance requirements are met, risk is appropriately identified and mitigated, and adequate controls are implemented to safeguard user PII and the Service environment.

(3) Upon deployment, the application is subject to periodic privacy and security reviews and must undergo a functional review any time there is a change made to the application that affects or potentially affects user PII or the handling of data.

(4) Applications must comply with information collection clearance requirements and renewals, as appropriate.

Custom In-House Applications

In-house applications are those developed using a programming language, such as Java, C++, JavaScript, etc. These typically reside within the Service's network boundary, but not necessarily. In-house applications can range from mobile device apps to full-blown client-server applications running on top of a database. This includes applications developed by Service staff and applications where development is outsourced via a contract. All projects aimed at delivering custom, in-house-developed applications must go through the IMT project review process. IRTM's Application Development and Web Services Branch oversees the processes involved in developing most in-house applications.

Chapter 3 - Functional Reviews Necessary for Approval

This chapter provides additional information about the Service's functional review process and some of the mandatory compliance areas, including privacy, security, Section 508, and information collection clearance. IRTM strongly encourages project originators to consult with the RMB to clarify requirements and expectations for any of the functional review areas. The functional review is a collaborative process between project originator, the RMB, and IRTM personnel.

See Appendix B, Additional Review Information, for a description of the other reviews that may be necessary depending on project characteristics, including GIS, Records Management, HVA review, and Capital Planning and Portfolio Management reviews.

Privacy Review and Privacy Impact Assessments (PIA)

The privacy review portion of the functional review process ensures that we can meet our requirements under the Privacy Act of 1974, the E-Government Act of 2002, and other applicable laws dealing with privacy. These laws collectively require that we take steps to protect the privacy of employees and the public when performing mission activities, including adequately securing PII when purchasing or developing an information system. The Associate Privacy Officer (APO) leads the Service's privacy program. The APO will assist project originators with ensuring that they have adequately addressed privacy requirements in any solicitation or statement of work and that proposed information systems handle PII according to applicable standards. As part of the functional review, the APO will assist with carrying out a Privacy Threshold Analysis (PTA) to determine the exact privacy requirements that the project will need to meet.

Privacy Review Considerations

A key question regarding any system is whether it will contain, handle, or otherwise use information subject to privacy laws, such as PII. If not, the privacy review will typically be short. If it will, then additional review by the APO may be necessary to ensure that the appropriate privacy controls are in place to protect that information. The privacy review portion of the functional review will be commensurate with the size of the system and the type and sensitivity of information handled.

PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to an individual. Some PII is not sensitive and does not require special handling, such as information on a business card or in an email signature block. However, some PII is considered sensitive and requires stricter handling requirements. This is due to the fact it could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual if lost, compromised, or inappropriately disclosed. Examples of sensitive PII on their own include Social Security numbers, Tribal enrollment numbers, financial account numbers, date of birth, and biometric identifiers (e.g., fingerprint, facial image). Examples of PII that may become sensitive in conjunction with an individual's identity are citizenship or immigration status, medical or health information, or performance ratings. If you have questions about whether your application, system, or information collection project contains PII, contact the Service's APO.

We must implement privacy controls for all Federal information systems that contain PII to ensure the protection and proper handling of PII throughout the information lifecycle. You can find required privacy controls in the current version of NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. Implementing these controls is a requirement for receiving an ATO. The

privacy functional review helps identify what controls are required. As projects move forward, you must work with the APO to ensure that appropriate privacy requirements are incorporated into contracts and solicitation language as needed. We must implement provisions into contracts related to acquisitions, as appropriate, to ensure that contractors who develop, operate, or provide systems and applications work with us to meet privacy requirements. This includes providing access to records in accordance with an established System of Records Notice (SORN), conducting a PIA or developing a new SORN, and implementing appropriate privacy controls.

Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA)

The PTA is the tool used by the APO to identify projects and systems that are privacy sensitive. Once complete, the APO can use the PTA results to advise project originators and other officials regarding what privacy compliance requirements need to be met, including whether a full PIA is required. During the RMB process, you will need to work with the privacy representative from the RMB to complete the PTA by filling out the DI-4012 PTA form and submitting it to the APO, who will assess it further. For more information on the PTA process, review the Department's PTA Guide.

A PIA is an analysis of how a system collects, uses, maintains, and disseminates privacy information (such as PII) and how the system complies with applicable privacy laws and regulations. Completing a PIA at the beginning of the project helps us make informed system design and/or procurement decisions based on the privacy risk associated with the system and the options available for mitigating that risk. It also creates accountability for and provides documentation that we considered privacy from the beginning stages of system development and procurement. PIAs generally will not be completed prior to project approval. However, you should begin collecting the information required for a PIA so that you can begin the process once your project is approved (if necessary). See the Department's PIA Guide for more information.

System of Records Notices (SORNs)

If, through the PTA, the APO determines that the project includes a Privacy Act system because information is retrieved from the system via a personal identifier, we may need to publish a new SORN.

A SORN is a notice published by a Federal agency in the *Federal Register* upon the establishment and/or modification of a system of records. It describes the existence and character of the system. The SORN identifies the system of records, the purposes of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details as required. SORNs are required for all information systems that contain Privacy Act records. While we must conduct PIAs if the system collects or maintains PII, a SORN is only necessary when we retrieve information from the system by a personal identifier. The APO will assist project originators with determining whether a SORN is required. See OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act for more information.

IT Security Assessments

We are required to secure all Government-owned information systems to ensure the confidentiality, integrity, and availability of Federal information. As a result, on behalf of the project originator, the security representative on the RMB will coordinate with IRTM Cyber Security Division personnel during the functional review process, as necessary, to review the project for compatibility with the Service network and workstation platforms as well as the inclusion of appropriate security controls. A security

review helps ensure security controls are incorporated throughout the system development lifecycle and acquisition process and helps us to meet applicable security requirements. This includes authoring appropriate compliance provisions in contract documents to ensure that contractors developing, operating, or providing applications and information systems to the Service or on behalf of the Service are compliant with applicable Federal and Departmental security requirements. The security review will also determine if some aspect of the proposed project may be inconsistent with Federal, Departmental, and/or Service policies and requirements.

As part of the security portion of the functional review process, you may be asked to provide information on how the system will be hosted, potential interconnections with other Service systems, and additional characteristics of the request. Once Cyber Security personnel are satisfied that all applicable security requirements have been incorporated into the project proposal and that no fatal flaws exist, they will pass it through the security functional review. IMT projects will undergo further security compliance review throughout the lifecycle of the project.

During the functional review process, the system will receive an initial security categorization as determined in Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. This is used to help determine what security controls apply to the system. Ultimately, all applications, systems, and IMT projects must implement the appropriate security controls outlined in the latest version of NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, as consistent with their security categorization and any applicable Departmental guidance. The Risk Management representative on the RMB will work with project originators to carry out the FIPS-199 assessment.

Additional Security Considerations

Prior to deployment into production, all information systems must have a valid ATO established through the security Authorization and Accreditation (A&A) process. The ACIO is the Service official with the authority to give the ATO. Personnel from the IRTM Cybersecurity Risk Management Branch will consult with project originators and managers to make sure that the Service's security requirements are incorporated and that the appropriate documentation is developed. In cases where a contract is used, appropriate provisions must be included to direct the contractor to work with IRTM to complete the required A&A documentation, which includes a system security plan, risk assessment, security test and evaluation, continuous monitoring plan, disaster recovery plan, and continuity of operations plan.

Applicable IMT projects must also have an Information Systems Security Officer (ISSO) appointed prior to deployment to ensure implementation of and help to monitor system-level security controls and maintain system documentation. For more information about how to appoint an ISSO, contact the IRTM Division of Cyber Security.

In addition to the documentation described above, all information systems must complete a Business Impact Assessment (BIA) prior to receiving an ATO. Per NIST, a BIA is an analysis of an information system's requirements, functions, and interdependencies that is used to characterize system contingency requirements and priorities in the event of a significant disruption. The project manager, Business Lead, and ISSO will need to work together to complete the BIA as early as possible after the project is approved.

The ACISO is the Service official with primary responsibility for the Service's overall information security. The ACISO or other members of the IRTM Division of Cyber Security assist with the completion of any necessary security-related activities and receiving an ATO, including the development of any necessary documentation.

Section 508

Section 508 of the Rehabilitation Act of 1973 requires that we make sure our Information and Communication Technology (ICT) is accessible to all employees and members of the public. To both comply with legal requirements and to meet our goals for accessibility, we must ensure that any time we develop, procure, maintain, or use ICT we follow Section 508 standards and guidelines. Project originators are accountable for researching the proposed technology solutions and ensuring they are Section 508 compliant prior to submitting a request for review.

As part of any necessary procurement process, you must work with the RMB, applicable Section 508 Coordinator, and later, contracting staff to ensure that accessibility requirements are incorporated into project planning documents and to develop necessary documentation. The National Section 508 Coordinator can assist in identifying and meeting the requirements for unique and complex requests.

A full list of the current Section 508 Coordinators are available on the Section 508 SharePoint site, which is also the main repository for Section 508 information. You can also review the United States Access Board's Section 508 standards directly (36 CFR Part 1194).

Role of the Requiring Official in the 508 Review Process

In terms of Section 508, as soon as you decide to procure or develop ICT, such as an application or IMT project, you become the "Requiring Official." The Requiring Official owns the need that the proposed project will meet and is responsible for identifying the applicable Section 508 technical and performance requirements. Refer any unique or complex cases to your applicable Section 508 Coordinator for their assistance in identifying applicable requirements.

Once you identify the applicable Section 508 requirements, you must incorporate them into the procurement or the development of ICT. You should begin by conducting market research to determine which commercial products and services are available that meet (or come closest to meeting) your needs. This could include requesting accessibility conformance information from the vendor, in the form of an Accessibility Conformance Report (ACR).

If the request will use a contract, required solicitation language must be included in the statement of work. The General Services Administration (GSA) provides tools for developing solicitation language on their Section 508 website. Any testing or evaluation criteria should also be included. Any documents provided to the Contracting office for inclusion in a solicitation must also be Section 508 compliant.

The RMB will work with the National Section 508 Coordinator and project originators during the functional review to identify applicable 508 standards and incorporate the appropriate contract language to require vendors and service providers to meet those standards. It is possible that given the requirements of the project that full compliance with the applicable standards cannot be determined until the vendor or developer delivers the application or system. This handbook does not cover this type of conformance testing.

Exceptions to Section 508

It is possible that a project meets one of the exceptions to Section 508 (undue burden, fundamental alteration, commercial non-availability, or one of the "general exceptions"). In this case, you can submit an exception request in accordance with section 4.8 of 270 FW 4. The National Section 508 Coordinator will maintain a catalog of approved requests.

21st Century IDEA Accessibility Requirements

The 21st Century IDEA further emphasizes that digital services, including websites and other web-based services, must be accessible to individuals with disabilities in accordance with Section 508. You can review the U.S. Web Design System principles for additional information.

Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. 3501 *et seq.*) was enacted to reduce, minimize, and control the paperwork and information collection burden imposed by the Federal Government and to maximize the utility of creating, collecting, disclosing, maintaining, using, sharing, and disseminating that information. To do this, the PRA imposed controls on "collections of information," which is defined as the obtaining, causing to be obtained, or disclosure of facts or opinions by or for an agency by 10 or more non-Federal "persons," regardless of whether the collection is voluntary or mandatory (or 1 or more when contained in regulations). To guarantee compliance, we must ensure that the Service's Information Collection Clearance Officer (ICCO) reviews proposed applications or systems that will collect information from the public to determine whether the collection will need further review from OMB.

If the proposed project or system will involve collecting information from any member of the public (including individuals, partnerships, corporations, universities, nonprofit organizations, and any element of a State, territory, local, and Tribal government), the ICCO must be involved in the functional review process. The ICCO will determine the appropriate next steps. They may ask you to provide more information about which members of the public you will collect information from and how many responses/submissions you estimate per year for each of those entities. The RMB will arrange the ICCO review process during the functional review to avoid delays caused by OMB reviews. For more information see 281 FW 4 and 281 FW 5.

Appendix A- Acronyms/Terms

Following are some common IT acronyms and terms that we use in this Handbook.

Acronym	Description
A&A	Authorization & Accreditation, authority for boundary
ACIO	Associate Chief Information Officer
ACISO	Associate Chief Information Security Officer
APAC	Acquisition Program Advisory Council
APO	Associate Privacy Officer
ATO	Authorization to Operate
BIA	Business Impact Assessment
CIO	Chief Information Officer
COTS	Commercial, Off-the-Shelf
FCHS	Foundation Cloud Hosting Services contract
FedRAMP	Federal Risk Authorization and Management Program for cloud services
FITARA	Federal Information Technology Acquisition Reform Act (FITARA)
FISMA	Federal Information Security Management Act (FISMA) and related OMB requirements
GIS	Geographic Information System
GSA	General Services Administration
HVA	High Value Assets
ICT	Information and Communication Technology (usually used in the context of Section 508)
IMT	Information Management and Technology
IMTEB	Information Management and Technology Executive Board
IMTRC	Information Management and Technology Requirements Committee
IRTM	U.S. Fish and Wildlife Service Office of Information Resources and Technology Management
ISSO	Information Systems Security Officer
ITPA	Information Technology Purchase Approval
NIST	National Institute of Standards and Technology
OCIO	Department of the Interior Office of the Chief Information Officer
O&M	Operations and Maintenance
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PMO	Project Management Office
PTA	Privacy Threshold Assessment
RMB	Requirements Management Board
SORN	System of Records Notice

Appendix B - Additional Review Information

While all IMT projects must go through the reviews we describe earlier in this handbook, some additional reviews apply only to a subset of requests. This appendix describes these reviews and includes links to other sources of guidance.

Capital Planning and Portfolio Management

We must ensure that our IMT acquisitions and projects are managed effectively and that all IT spending can be reported as necessary, in accordance with portfolio management policy. During this review, the IRTM Investment Management Branch will work with the project originator to determine the funding plans for the request and to classify the proposed investment according to Departmental regulations and ensure that all investment information is properly recorded.

GIS

Some projects may contain spatial data components or datasets that require review from the Service's National GIS Coordinator (IRTM's GIS Branch Chief). These involve the acquisition, consumption, processing, distribution, use, or maintenance of location-based data. Examples of projects or project components that need GIS review include maps, imagery, point locations, spatial databases, and position information within non-geographic databases.

If a project contains spatial data components, the Service's National GIS Coordinator must perform an analysis to determine whether there are similar systems within the Department or the Service that consume or produce this type of information. This helps to ensure that there is no duplication of effort or wasted funds.

High Value Asset (HVA)

HVA systems and data refer to those assets, systems, and data that require a higher level of control because of the sensitivity of the information and data processed or maintained. They may contain sensitive data used in critical Federal operations, or unique collections of data (by size or content) that make them of interest to criminal, politically motivated, or state-sponsored attackers. These are typically assets used for overall Federal Government operations, not for those used by a field station or Regional office, for example.

During the functional review stage, the RMB will work with the Cyber Security Division to determine whether the proposed investment is an HVA in accordance with OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program. Project originators should be prepared to answer questions about the sensitivity of information in the system, the quantity of sensitive information stored or handled, and the uniqueness of the dataset or capability, among other questions.

Records and Information Management

The Service is required by Federal law, regulation, and policy to create and preserve records that are evidence of its organization, functions, policies, decisions, procedures, operations, transactions, and other official activities. The Records and Information Management Branch within IRTM, led by the Service's Chief Records Officer, is responsible for establishing records and information management policies and procedures and for ensuring that all Service employees carry out their responsibility to manage records throughout their lifecycle, including creation, maintenance, use, and disposition.

As part of these responsibilities, the Chief Records Officer helps ensure that records management requirements and controls are adequately implemented within proposed projects and systems. In certain circumstances, the Chief Records Officer may work with the RMB to conduct a review of a project proposal during the functional review phase. This review will focus on identifying records that the system will produce, the appropriate disposition of those records according to the Department's and Service's Records Schedules, and records controls that need to be implemented to ensure that the records are protected from unauthorized removal or loss.

For more information about records and information management requirements, see the Records and Information Management SharePoint site and 280 FW 1, Records and Information Management Policy and Program.

Grants and Cooperative Agreements

The review processes discussed in this handbook outline the necessary approvals to receive authorization to apply funding to an IMT project through the contracting process. However, there may be circumstances where an alternative agreement, such as a grant or cooperative agreement, may require the use of Federal IT resources or generate Federal information.

In these cases, the Wildlife and Sport Fish and Restoration (WSFR) Financial Assistance Policy and Oversight (FASO), Policy and Compliance Branch and IRTM may need to review the project. This is true for all agreements that would require a recipient, or their subrecipient(s) or contractor(s), to:

- Create an IT system such as a website or database in which Federal information will be collected or stored; or
- Otherwise create, collect, handle, process, store, share, maintain, or dispose of information for the Federal Government, in any medium or form.

The project originator must submit any such requests to the WSFR, FASO-Policy and Compliance Branch Chief by email for review prior to award (see the Policy and Oversight Branch SharePoint site for contact information). The email must include a copy of the complete application received from the intended recipient and provide any additional details regarding the system to be created/maintained or the information it will generate and how the Service will use it. The email subject line should read "FA Policy & IRTM Review Request." This review will determine whether the appropriate funding instrument is being used and if further review is required.

If a contract is the more appropriate vehicle, the project may be subject to the IMT project review process. Otherwise, the RMB will coordinate with the project originator to ensure that necessary compliance requirements are incorporated into the language of the agreements.

For more information about these requirements, please see IT Bulletin 2018-001, Guidance and Review Requirements for Contracts and Agreements Involving Information Management and Technology.