GO.gov Customer Briefing

IBC & GSA

April 15, 2026

Agenda

- Connect.gov for GO.gov Information
- Key Agency FOC-B Dates
- Travel Management Center (TMC) Authorization Options
- Agency Security Controls (ATO/ATU)
- Agency Security Controls Single Sign On (SSO)
- Service Access Fee (SAF)
- GO.gov Training Strategy
- FM Integration Status

Connect.gov for GO.gov Information

- Register and establish a MAX.gov account to access Connect.gov
- Log into Connect.gov to search for and access GO.gov useful information and updates:
  - Past and future GO.gov meeting details and materials
  - Transition Toolkit
  - Training materials
  - Change Management Network materials
  - Security information
- Ensure Agency Travel Superuser POCs *establish a MAX.gov* account to access Connect.gov
- Contact MAX.gov Support for assistance
- All Agency GO.gov meeting schedule is available on the resources above

Contact MAX Support: Email: maxsupport@max.gov | Phone: 202-395-6860

MAX Support Hours: Weekdays - 8:30 AM - 6:30 PM ET

Site Maintenance: Sundays, 2-8:00 AM ET

Key Agency FOC-B Dates

Key Agency FOC-B Dates

FOC-B Timelines

27 May 2026

Projected GO.gov FedRAMP Award

Nov 2026

Issue Agency ATO/ATU for TMC

Nov 2026

Issue agency ATO/ATU for GO.gov

2 Dec 2026 – 15 Jan 2027

User Acceptance Testing (UAT)

Dec 2, 2026 – Jan 15, 2027
(Holiday blackout: Dec 16 – Jan 3)

Projected TMC Security Package Available including SSPP and SAR

03 June 2026

Issue Agency ATO/ATU for OFF Interface

Nov 2026

System Integration Testing (SIT)

FM: Aug 24 – Sept 21, 2026
Travel: Nov 2-20, 2026

2–20 Nov 2026

FOC3 Go-Live

March 2027

TMC Authorization Options

TMC Authorization Options

Travel Management Center (TMC)

- GSA selected two TMC's for the IBC Customer Agencies in TMC Acquisition Group 1 (less than 10,000 Air Transactions …) as follows:
  - CI Travel
  - Duluth Travel

- Each IBC Customer Agency has been assigned **one of these two TMCs** to support their transition to GO.gov
  - Agencies will coordinate with their assigned TMC during onboarding.

TMC Authorization Options (1/2)

1. **Agency inherits the GSA MFR** in alignment with OMB A - 130 "Managing Information as a Strategic Resource" and 02/2026 CISO Council Briefing - (**Recommended Approach**)
    a. Issue ATU for Customer Responsible Controls(**Optional**)

2. Agency separately funds and conducts Independent Assessment (**NOT RECOMMENDED**)
    a. Agency issues interim **AOR/ATU/ATO/** based upon the GSA MFR
        i. conducts independent assessment while onboarding to GO.gov.
    b. Two Assessment Types
        i. Independent Assessment of the gap between NIST 800-53 & the GSA SSPP (NIST 800-171, 800-172, 800-53) - **Additional Cost to the Agency**
    c. Independent Assessment of the Full NIST 800-53 for a FISMA Moderate Solution - **Additional Cost to the Agency**

TMC Authorization Options (2/2)

Authorization of the TMC: Each agency could authorize the TMC in order for production data to be sent to the TMC's GDS.

- GSA Recommends **Acceptance of the MFR**
  - Agency can issue an ATU for the Customer Responsible Controls
  - Template available on Connect.gov

Authority to Use (ATU) - Option 1

An Authority to Use allows an agency to leverage or "reuse" an existing authorization—typically from another agency or a cloud service provider—rather than undergoing the full ATO process from scratch.

Purpose: It is designed to accelerate approvals for shared systems or software, such as cloud-hosted platforms.

Requirement: A MFR, the GSA CISO equivalent to an ATO must already be on file for the offering before another agency can issue an ATU or ATO.

Efficiency: It is often described as a "lightweight" package because it focuses on the minimum compliance details required for onboarding onto a pre-authorized platform.

Authority to Operate - Option 2

An Authority to Operate is a formal declaration by a designated senior official that a specific information system is approved to function within an agency.

Purpose: It signifies that the system's security and risk posture meet the agency's requirements after a comprehensive assessment.

Process: The system owner must complete the full Risk Management Framework (RMF) process, which includes categorizing the system, selecting and implementing security controls, and conducting a thorough security assessment.

Responsibility: The Authorizing Official (AO) personally accepts the residual risk of operating the system.

Agency Security Controls (ATO/ATU)

GO.gov Security Workstreams

Objective: Ensure all GO.gov integrations meet security and authorization requirements

Workstream	Description	Owner	Projected Completion Date
FedRAMP Moderate GO.gov	GO.gov will obtain a FedRamp Moderate ATO which is an authorization of a cloud system that has been assessed by a 3PAO and successfully met the applicable 323 NIST 800-53 Rev. 5 baseline control requirements.	IBM	05/27/2026
Agency Authority to Operate (ATO)	To effectively utilize GO.gov, each federal agency is required to formally authorize its own CRM Agency ATO. The Agency CRM ATO consist of 60 customer responsible controls and 146 total customer responsible control requirements. These CRM Agency ATOs must leverage the GO.gov Moderate FedRAMP ATO. This requirement ensures a baseline level of security and compliance across all implementations of GO.gov. *In accordance with their agency policies and procedures	Agency Customer	Nov 2026

Customer Security Requirements – GO.gov ATO/ATU

Recommend Agencies Consult with their IT Security Department to understand Requirements

GO.gov Interface Shared Service Provider – Interior Business Center (IBC)

- IBC will establish an ATO with GO.gov for FM Interface

GO.gov Customer Agency Security Authorization Tasks

- Customer Agencies to identify Security POCs
- Review draft GO.gov FedRAMP and TMC's Memorandum For Record (MFR/ATO) documentation on Connect.gov.
  - GSA Chief Information Security Officer will provide documentation as it is approved and available, which will then be shared on Connect.gov for agency access.
- Conduct assessment of agency implementation of GO.gov FedRAMP Customer Responsibility Matrix (CRM) controls in support of Authority to Operate (ATO)/Authority to Use (ATU) issuance
- Complete and sign Interconnection Security Agreement (ISA) or Information Exchange Agreement (IEA) addressing customer connectivity to GO.gov
- Issue agency CRM Artifact ATO/ATU for agency implementation of GO.gov
- Authorization for agency Travel Management Company (TMC)

Agency Security Controls Single Sign On (SSO)

Single Sign On (SSO)

- Recommend that agencies: consult with their IT Security Department to understand specific Agency requirements
  - Meets federal identity requirements and is already FedRAMP authorized
  - Improves UX by reducing passwords and providing a unified login
  - Minimizes risk and complexity when connecting agency systems to GO.gov

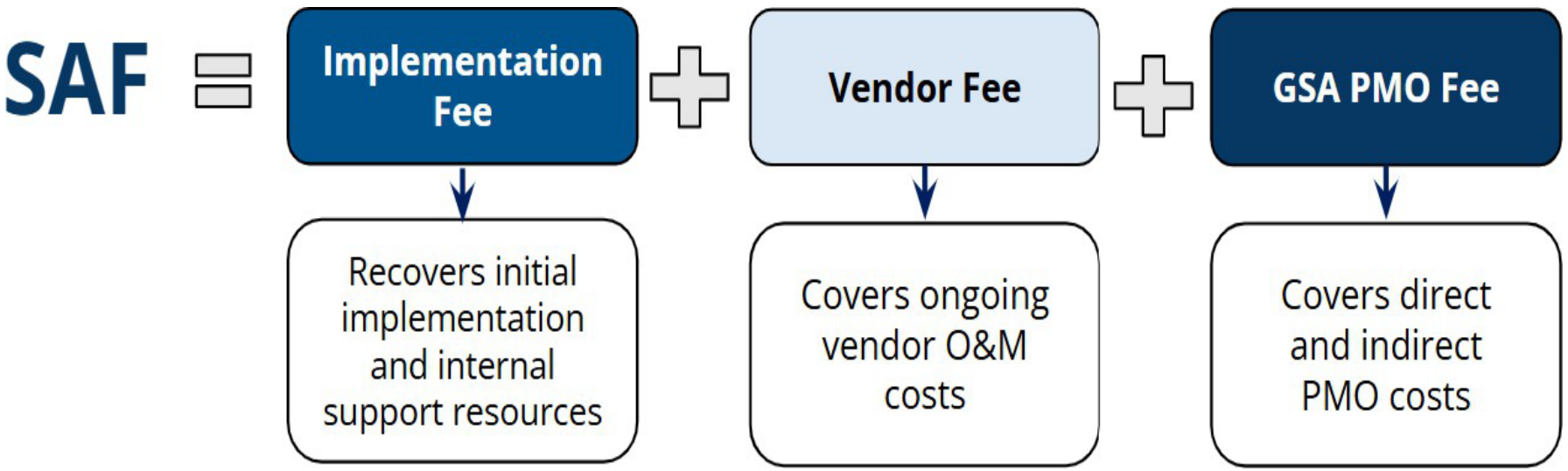
- Integration Steps
  - Select ICAM/SSO solution with MFA
  - Document SSO in the ATO/ATU package
  - Enable SSO in GO.gov test environment
  - Validate in SIT and UAT
  - Enable SSO in GO.gov production
  - Users able to sign into GO.gov

Service Access Fee (SAF)

Service Access Fee (SAF)

An overview of Service Access Fee (SAF)

- **What is the Service Access Fee (SAF)?** The SAF is a transaction-based fee applied to each approved expense report (formerly known as vouchers) in GO.gov. It enables GSA to recover the costs of launching and operating GO.gov as a governmentwide shared service.
- **Who pays the SAF?** All customer agencies using GO.gov.



An overview of Service Access Fee (SAF)

- **Who pays the SAF?** All customer agencies using GO.gov.
- **How is it applied?** The fee is charged per approved expense report. Or applied for approved, uncancelled authorizations with no expense report 60 days after the trip has ended.
- **Why is the SAF being charged?** The SAF funds centralized services that were previously handled independently by each agency in ETS2, such as:
  - Contract and vendor management
  - Configuration management and release testing
  - API Maintenance
  - Reports Maintenance
  - Training support
  - Service desk and user support

Note: The SAF does not include fees for TMCs.

An overview of Service Access Fee (SAF)

- **How is it managed?**
  - The SAF is outlined in each agency's Interagency Agreement (IAA).
  - It is reviewed annually and adjusted as needed based on overall government travel volume.
  - The final rate is set annually in August, following a review of May–June travel data, for the upcoming fiscal year.
  - The fee is designed to be recovered over a 15-year period, minimizing the annual cost burden on agencies.
  - SAF fees paid for approved, uncancelled authorizations 60 days after trip ends will be paid by GSA and absorbed into the SAF. Agencies will not pay twice for the same voucher, if a voucher is subsequently paid.
- **How will payment be collected?**
  - Until G-Invoicing is fully implemented, the Service Access Fee (SAF) will be automatically added to each approved travel authorization and expense report and collected by GSA. Agencies will receive SAF usage reports at an agreed-upon frequency and will remit payment via Electronic Funds Transfer (EFT) or Corporate Billing Account (CBA).
- **In the future, GSA expects to transition SAF collection to G-Invoicing for billing and payment. Under this model:**
  - Agencies will use a 15-year General Terms and Conditions (GT&C) agreement
  - GSA is currently evaluating whether the Standard Order or EZ function is the most appropriate for SAF reimbursement through G-Invoicing

GO.gov Training Strategy

GO.gov Training Strategy

- GSA/IBM will primarily offer self-paced, End-User training and deliver it to customer LMS. This includes:
  - Micro Videos by Role
  - Training Session Recordings by Role
  - Training Materials by Role (User Guides & Quick Reference Guides)
- IBM will provide Train-the-Trainer training to IBC and a limited number of agency superusers
- IBM will offer end-user training in addition to the GSA/IBM provided resources.
  - Change Champion Network materials
  - End-User Communications Workbook

FM Integration Status

FM Integration Status

FM Integration Status

- IBC is enhancing the current out-of-the-box eTravel FM integration solution from SFTP to Real-Time integration.

- The Go.Gov Interface solution will be developed, as a real-time interface, using Oracle Integrated Cloud (OIC) services to interface Travel transactions from Go.Gov to Oracle Federal Financials (OFF) and interface Travel Acknowledgments and Funds Check statuses from OFF to Go.Gov.
  - Travel Authorizations
  - Travel Vouchers
  - Funds Check
  - Acknowledgments

FM Integration Status Cont.

Development Status:

- Travel Authorizations, Funds Check, Acknowledgments
  - Completed the initial development using the existing documentation and sample generic payload files.
  - Unit testing is in progress.
  - Identified solution gaps and design questions have been communicated to GSA FM team.
  - As per the current GSA time, the Integrated Testing phase with GSA is scheduled for August 2026.
  - IBC has requested to start the integrated testing from May 2026.
  - Travel Vouchers
    - Development for Travel Vouchers is in progress.

Communications & Next Steps

- Frequency we will communicate to them
- How to ask questions – Meredith Day (mday@ibc.doi.gov)
- Next meeting
- Homework
  - Attend monthly GO.gov All Agency meetings
  - Respond to data calls and emails
  - Review materials on Connect.gov
  - Document business processes that are unique to your agency for Gap Analysis

Open Floor Questions