

Provider Intake Form

eOPF Index Data Feed (IDF) External API — Access Request

Version 1.3 — September 2026

Return to: eOPFOperations@opm.gov

Contains no secrets

Complete this form and return it to the **OPM eOPF integration team** (eOPFOperations@opm.gov) to begin provisioning access to the eOPF Index Data Feed (IDF) external API. Fields marked **(required)** must be filled in before provisioning can start. This form contains no secrets — credentials are issued separately through a secure channel after approval.

1. Provider system

Field	Your answer
System / application name (required) e.g. USA Staffing	
Short code used in naming (required) e.g. <code>USAS</code> , <code>USAP</code>	
Owning agency / program office (required)	
Purpose / use case summary	

2. Environment(s) requested

Check all that apply. Providers integrate and validate in TST first, promote to UAT for sign-off, and receive production access after UAT sign-off.

- ☐ TST **(start here)**
- ☐ UAT
- ☐ PRD (requires prior UAT sign-off)

3. Tier & app registration naming

OPM provisions a Microsoft Entra ID app registration for your system per tier, following the `SP-EOPF-<SYSTEM>-<TIER>-IDF` scheme, where `TIER` = `NP` for non-production (shared by TST/UAT) or `P` for production.

Field	Your answer
Requested app registration name(s) e.g. <code>SP-EOPF-USAS-NP-IDF</code> , <code>SP-EOPF-USAS-P-IDF</code>	
Existing Entra app registration to reuse (if any)	

4. Authorized subagencies (required)

List every 4-character subagency code your system will submit documents for. These gate which documents your system may submit; documents for any other subagency are rejected (eOPF 939). The eOPF integration team will return the matching AgencyAccountName value to send for each subagency (e.g. OM00 → OPM , TR93 → IRS).

#	Subagency code	Description (optional)
1		
2		
3		
4		
5		
6		

Attach an additional sheet if you need more rows.

5. Roles requested

Role	Needed?	Notes
Standard submit (Add/Update)	Yes (default)	Add/Update documents.
IDF.Delete	☐	Required only if your system deletes documents.

6. Technical contacts (required)

Role	Name	Email	Phone
Primary technical contact			
Secondary technical contact			
Security / secrets custodian			

7. Secrets delivery

How should OPM deliver your **client secret** and **APIM subscription keys**?

- ☐ Shared Key Vault — vault name/URI: _____
- ☐ Secure secrets manager / one-time-secret link

☐ Other (describe): _____

Secrets are **never** sent over plain email.

8. Source IP addresses for allow-listing (required)

List the **public** IPv4 addresses or CIDR ranges your system will call the API from — the egress addresses OPM sees (NAT gateway, firewall, or outbound proxy), not internal RFC 1918 addresses. These are recorded so OPM can allow-list your system at the network layer; traffic from an address that is not on the list can be blocked. Keep ranges as narrow as possible (/32 per host where you can), and list non-production and production separately — they use different allow-lists.

Environment	Public IPv4 address / CIDR	Source (NAT gateway, proxy, data center, cloud region)
Non-production (TST/UAT)		
Non-production (TST/UAT)		
Non-production (TST/UAT)		
Production (PRD)		
Production (PRD)		
Production (PRD)		

Attach an additional sheet if you need more rows.

Field	Your answer
IPv6 addresses / prefixes (if your egress is IPv6)	
Cloud-hosted egress — provider, region, and service tag (if any) e.g. Azure East US NAT gateway, AWS us-east-1 NAT	

Egress addresses change when your hosting does. Email **eOPFOperations@opm.gov** as far in advance as you can before addresses change or are added — allow-list updates are change-controlled, and calls from an unlisted address can fail until the update is deployed.

9. Expected volume (optional, helps sizing)

Field	Your answer
Estimated documents per day	
Peak burst rate (docs/minute)	
Typical PDF size	

What happens next: once received and approved, OPM provisions your Entra app registration, provider authorization, and APIM subscription (primary + secondary keys), then delivers credentials through your selected secure channel. Verify connectivity with `GET /v1/me` — a `200` with your identity JSON confirms both credential layers end to end.