Making the Internet work better

Infrastructure Services

A Request for Proposals issued on 2023-07-18

IETF Executive Director
exec-director@ietf.org

About the IETF

The Internet Engineering Task Force (IETF) is the premiere Internet standards body creating open protocols to ensure that the global Internet is built on the highest-quality technical standards. These standards, shaped by rough consensus and informed by running code, are developed by a large volunteer community of leading engineering and technical experts from around the world. IETF processes are open and transparent, and IETF standards are freely available to anyone.

Standards and protocols developed at the IETF provide a core framework for today's online world. Everything from video conferencing, to email, to cloud storage is built on standards developed in the IETF community. In short, our work makes the Internet work.

Overview

The current contract for IETF IT infrastructure services is a black box contract - we specify the systems to be maintained along with a very basic SLA, and the provider is responsible for the underlying infrastructure on which those systems operate, including the system administration strategy. This underlying infrastructure consists of a small number of managed servers with most applications installed directly onto those servers though more recently containers have been used.

The IETF Administration LLC has consulted with the community to develop a new operational strategy for how the infrastructure should be operated. This strategy sets goals for the infrastructure to move to the cloud and to be managed very differently. As well as providing for a more modern infrastructure, this new strategy also lays the foundations for a change to the architecture of our in-house applications to take advantage of modern scaling and hosting capabilities.

This RFP is for a service provider to design the new cloud based infrastructure, migrate the existing services to that infrastructure and then manage the infrastructure. It is likely that this management will involve occasional projects to support major changes in application deployment.

Timeline

18 July 2023	RFP Issued
8 August 2023	Questions and Inquiries deadline
15 August 2023	Answers to questions issued and RFP updated if required
5 September 2023	**Bids due**
19 September 2023	Preferred bidder selected and negotiations begin
6 October 2023	Contract execution and work begins

RFP Process

The process for the RFP is as follows:

1. The RFP is publicly issued, posted to our website[1] and announced to the RFP Announcement mailing list[2], which anyone can subscribe to.

[1] https://www.ietf.org/about/administration/rfps-and-contracts/
[2] https://www.ietf.org/mailman/listinfo/rfp-announce

2. Potential bidders have until 8 August 2023 to submit any questions by email to ietf-rfps@ietf.org. Questions will be treated as anonymous but not private, as explained below. If you do not receive confirmation that your questions have been received within 24 hours then resend until you do.

3. A written response to all questions is provided on or before 15 August 2023, direct to those parties that sent questions, by email to the RFP Announcement Mailing List and posted on our website[3]. The response will include the questions asked and the answers, but will not identify the company asking the question. If required, the RFP may be updated to correct or clarify any issues identified.

4. Bids are due by **5 September 2023** by email to ietf-rfps@ietf.org. If you do not receive confirmation that your bid has been received within 24 hours then please resend until you do. The bid should include the following information:

    a. Executive summary

    b. Standard approach to infrastructure management and infrastructure project management including any assumptions.

    c. Proposed new infrastructure, including the proposed cloud provider(s), proposed cloud products and proposed architecture in outline.

    d. Project plan and schedule for all the deliverables that must include when the work will begin and end, and any other milestones, as well as any dependencies that may delay delivery.

    e. Statement confirming that you can deliver the deliverables and meet all the listed requirements, along with any additional information needed to substantiate this.

    f. Key personnel experience and projected availability for the expected lifetime of the contract.

    g. Fee and payment schedule. Fixed priced bids are preferred but if that is not possible then a maximum fee must be specified.

    h. A warranty including a proposal for fee reduction or refund due to late- or non-delivery.

5. The IETF Administration LLC and designated contractors and volunteers will select a preferred bid and notify the bidder by 19 September 2023. The selection process may include questions by email and/or conference call.

[3] https://www.ietf.org/about/administration/rfps-and-contracts/

6. The IETF Administration LLC then enters into contract negotiation with the preferred bidder, based on its standard contract and using the relevant sections of the Statement of Work below. If contract negotiation fails then a different preferred bidder may be chosen.

    a. For contracts of this nature, the standard proposed terms are an initial term of two years followed by two renewals by mutual agreement, each for a further two years, giving a possible total of six years.

7. Contract negotiation is anticipated to complete by 6 October 2023 and result in the award of the contract. All RFP contract awards are posted on our website and announced to the RFP Announcement mailing list. The terms of the contract are later posted publicly on our website, with the fee information and signatures (where possible) redacted. In addition any Conflict of Interest declarations required of the preferred bidder are also posted publicly on our website. This transparency is non-negotiable.

8. Work generally begins immediately after award of the contract, unless specified otherwise in the Statement of Work or negotiated contract.

Jay Daley
IETF Executive Director
IETF Administration LLC

Statement of Work: Infrastructure Services

Deliverables

The service provider will be contracted to deliver the following:

Part 1 - Pre-transition planning

The service provider must deliver the following within six weeks of the start of the contract:

1. A full architecture for the new infrastructure, agreed with the IETF, including:
    - Specification of the deployment environment(s) including
        - Infrastructure access controls
        - Management interfaces
        - Monitoring and alarming systems
        - Secrets management
        - Other architectural components described in this RFP
    - Details of how the architecture will ensure service availability and data integrity in the event of a range of failures.
    - Detailed initial deployment plan for each service
    - Process for deploying new versions of each service, in an automated manner
2. A detailed plan for transition, agreed with the IETF. The plan must include:
    - Timetable for the transition
    - Individual technical transition plan for each service
    - Downtime requirements for each service
    - Process for engaging with the existing service provider(s) and resolving any issues during the transition.
    - Test plan for assuring a successful transition
    - Risk analysis with mitigations for key risks
3. Full cost estimate, including:
    - Third party costs for the infrastructure provision (i.e. how much should the IETF expect to be recharged for third party cloud services)
    - Service provider fees for the transition, unless already agreed on a fixed price basis.

Part 2 - Transition of existing services to new infrastructure

The service provider must complete a successful transition in line with the architecture, transition plan and cost estimates, by 31 March 2024, including:

1. All services successfully transitioned
2. Timetable met
3. Agreed downtime not exceeded
4. All tests pass

Part 3 - Managed infrastructure

From the time the first service transitions, the service provider must deliver a managed infrastructure that meets the requirements, on an ongoing basis.

Requirements

Part 1 - Service provider requirements

Nature of service

The IETF requires a service provider to provide managed infrastructure services based on top of one or more third-party cloud services. The key personnel identified to work with the IETF must have extensive experience in providing these services.

The IETF does not require the service provider to be accredited by the proposed third-party cloud services, but will consider any accreditations when assessing RFP responses.

Scope of responsibility

Service provider is responsible for the IETF infrastructure and the delivery of the goals, including:

1. Infrastructure components, including:
    a. “as a service” services, including compute, storage, database and network
    b. Operating systems and containers
    c. Network functions
    d. Production, development and test environments
2. Management and operation of the infrastructure, including:
    a. Resource allocation
    b. Configuration and upgrades

    c. Change control
    d. Instrumentation
3. Management of any third party infrastructure providers, including
    a. All of 2 above
    b. Billing
4. Outcomes for the infrastructure, including:
    a. Availability
    b. Performance
    c. Security
    d. Visibility (i.e. of data collected by instrumentation)
    e. Value for money

Behaviors

IETF requires the Service Provider to actively practice the following behaviors:

- Open and communicative by default, particularly in pre-emptive communications.
- Flexible attitude, open and receptive to new ideas, not defensive.
- Always looking for ways to improve the infrastructure and take advantage of new features/services.
- Aware of and continually aiming to adopt and further industry best practices.

These behaviors are particularly important if the Service Provider is to work successfully with the IETF. The IETF operates in a highly transparent manner, with strong engagement with a highly technical community numbering in the tens of thousands, and even small details can be subject to extensive discussion and analysis. It will work best if the Service Provider fully embraces the IETF way of working.

Part 2 - Goals and associated requirements

The following goals are extracted and updated from the IETF infrastructure strategy. The Service Provider should expect these goals to be reviewed annually or biennially and the IETF community to play an active role in that review. The Service Provider is required to adapt as these goals change over the life of the contract.

The IETF IT infrastructure must be operated to meet the following goals and associated requirements, each of which is described in more depth in the sections below. It is recognised that some of these goals overlap or are interdependent.

1. **Fit-for-purpose service availability**
2. **Fit-for-purpose service performance**
3. **Separated, cloud-first services**
4. **Automated, transparent and accessible infrastructure management**

5. **Secure and enduring services and data**
6. **Comprehensive service monitoring**

Fit-for-purpose service availability

The IETF requires its IT infrastructure to support a fit-for-purpose service availability, which means:

- Minimal unplanned downtime.
- Infrastructure designed to eliminate planned downtime (i.e. no planned downtime required for management of the infrastructure, such as OS upgrades).
- Planned downtime only needed for
    - Application deployment, recognising that the IETF aims to re-architect its own applications to remove this need
    - Transition of services
    - Major projects
- Where planned downtime is required, then:
    - It must not be during or during the preparation phase of IETF meetings or other key events..
    - Should be able to be scheduled for any day of the week at any time, to meet IETF operational requirements.

Fit-for-purpose service performance

The IETF requires its IT infrastructure to provide a fit-for-purpose service performance, which means:

- Excellent infrastructure performance.
- All relevant and potentially relevant performance/utilization data collected.
- An infrastructure that scales to match load, particularly during key events, with minimal manual intervention.
- An infrastructure designed to support the global nature of the IETF and ensures excellent performance to all end users.
- An evidence based approach used in setting all resource limits.
- A strategy for rapidly addressing performance bottlenecks.

Separated, cloud-first services

The IETF requires its IT infrastructure to operate cloud-first and support IaaS, PaaS and SaaS, which means:

- All services run in the cloud on public cloud platforms.
- All cloud platforms to support orchestration (preferably Kubernetes), including automated deployment, scaling and management, except where the application itself cannot support this.

- All services to be containerised (and managed via orchestration) so that they are entirely separated at the filesystem/package level and any one can have any supporting package upgraded without any other service being affected.
- Any service can be customized, upgraded and migrated to another platform / cloud provider with either no dependency or only entirely unavoidable dependency, on any other service or component of any other service. (no vendor lock-in when possible)
- All services to support operation behind Cloudflare Web Application Firewalls, Content Delivery Networks and other front end services.

Automated, transparent and accessible infrastructure management

The IETF requires the management of its infrastructure to be automated, transparent and accessible, which means:

- All build and configuration managed through an automated configuration management and deployment platform (e.g. Ansible).
- Automation scripts in a public GitHub repository.
- Credentials and other secret information used in automation scripts / deployments to be properly protected in our HashiCorp Vault instance.
- A full test environment with the expectation that wherever possible, deployment involves first deploying to test, validating efficacy of changes, and then deploy to production.
- Where reasonable, it should be possible for any member of the IETF community to build a replica of any IETF service, with placeholder information available to replace any confidential information.

Secure and enduring services and data

The IETF requires its services and data to be secure and enduring, which means:

- An embedded risk-aware culture, with regular peer review and external audit of all strategies, processes and systems.
- Security-first network/service design and network/service management.
- A formal access control model with centralized observability.
- Clear compartmentalisation of confidential information.
- A patch management process that minimizes the threat from unpatched systems.
- A backup and restore strategy that provides strong assurance of data integrity and high confidence of system rebuild.
- Active management of nuisance traffic.

Comprehensive service monitoring

The IETF requires comprehensive, standards-based service monitoring, which means:

- Every part of the infrastructure is instrumented.
- Centralized collection of monitoring data to enable cross-service analysis.
- Controlled publication of monitoring data that maintains operational security while providing maximum access to the IETF community.
- Where possible, standards based data collection and distribution, and where proprietary APIs need to be used then these must be open and documented APIs.

Part 3 - Detailed operational requirements

Third-party cloud services

The proposed third-party cloud services must meet the following requirements:

- At least two regions in the continental US, one to be the primary region for the IETF infrastructure and one as backup. Additionally, at least one region in Europe and one in Asia for possible future expansion.
- Open and transparent pricing model enabling high quality cost estimates to be made.
- Proven track record of stability and reliability.
- Full range of features necessary to meet IETF requirements.

Covered services and environments

The IETF has a wide variety of services, a high rate of change/growth in services, increasing integrations between services, significant fluctuations in usage with an underlying increase, and a wide variety of deployment models.

What follows is the list of services that operate on the current infrastructure and are required to be transitioned. While efforts have been made to ensure that this is a comprehensive list, there may be additional services that need to be included after the commencement of the contract. Many of these services rely on Docker.

- Datatracker. An internally developed workflow management system written in Python/Django, using PostgreSQL. This also provides an OAuth server for SSO across our applications.
- www.ietf.org Wagtail website.
- Interactive tools at author-tools.ietf.org. A web interface to a set of custom tools, mostly in Python.

- Satellite websites (rfc-editor.org, iab.org, iesg.org, irtf.org, trustee.ietf.org, and more) using a mix of direct manual construction, Wagtail, Dokuwiki and Wordpress with the latter being phased out in favor of Wagtail.
- Wikis (wiki.ietf.org, authors.ietf.org and others) using wiki.js with custom plugins.
- Groupchat using Zulip.
- Ephemeral notes (notes.ietf.org and special purpose instances) using Hedgedoc.
- A bibliographic content service (bib.ietf.org) that provides information about RFCs, Internet-Drafts, documents from several other SDOs, and any document with a DOI.
- Mailarchive. A custom mail archive tool.
- Analytics (using Matomo) across most web services.
- We also make a considerable number of files/documents available via direct HTTP and RSYNC.[4]

In addition, the IETF operates multiple development and testing environments that are required to be operated on the new infrastructure.

In addition, the IETF uses Cloudflare for a CDN with a regularly expanding usage. Cloudflare provide their services to us free of charge under their Galileo project[5]. The service provider is required to incorporate and manage relevant Cloudflare services as part of the new infrastructure. We currently also manage DNS using Cloudflare, and utilize R2 for static assets served at static.ietf.org. We anticipate using R2 and potentially other S3 compatible bucket stores for many of the artifacts (such as the content of Internet-Drafts and RFCs) managed by the datatracker.

In addition, the IETF operates a significant set of high-volume mail processing services. The operation of these services are the subject of a separate RFP and the outcome of that will determine which of those services are to operate on the IETF infrastructure. Notwithstanding that decision, the IETF infrastructure is required to operate the Mailarchive service and to ensure that applications can reliably connect to mail gateways with successful delivery.

In addition, the IETF operates YANG Catalog[6] a custom website for YANG (a technology developed by the IETF). While this operates on AWS, this is currently outsourced as a complete service and there are currently no plans to move it to the IETF infrastructure.

[4] https://www.ietf.org/about/open-records/
[5] https://www.cloudflare.com/en-gb/galileo/
[6] https://yangcatalog.org

Databases

The IETF uses PostgreSQL as its standard backend database for its applications. This is currently managed by a combination of our existing service provider, development staff and a specialist database services company.

It is expected, though not required, that the new infrastructure proposed by the Service Provider will see these operated on a PostgreSQL-as-a-service offering. The IETF will support this transition both internally and through its specialist database services company.

The IETF requires any proposed use of PostgreSQL-as-a-service to be carefully planned to minimize latency between that service and the applications.

Incident resolution

Service provider is responsible for the resolution of all incidents that originate in the infrastructure, and all incidents that originate in applications where a pre-agreed resolution strategy exists. For all other incidents, service provider responsibility is to support the IETF, as needed, for the IETF to resolve the incident.

Service provider incident resolution must meet the timescales set out below:

	Services	**Condition**	**Resolution**
1	Services necessary for the delivery of an IETF meeting.[1]	Service is unusable[2], during an IETF meeting (From morning of Saturday the meeting starts until afternoon of the following Friday, all in local meeting timezone).	Full service restoration within 30 minutes.
2	Services necessary for meeting preparation.[1]	Service is unusable[2], in the week before the IETF meeting. (From Monday morning ET timezone until the meeting starts).	Resolution within 2 hours, with extension of an additional 1 hour for exceptional circumstances.[3]
3	Services defined as Primary in-between meetings	Service is unusable[2], any time except during the periods in 1 and 2 above.	Resolution within 4 hours, with extension of an additional 4 hours in exceptional circumstances.[3]

4	Services defined as Primary in-between meetings	Service is usable but operating incorrectly, any time except during the periods in 1 and 2 above	Resolution within 24 hours, with extension of an additional 24 hours in exceptional circumstances.[3]
5	Services defined as Secondary in-between meetings	Service is unusable[2], any time except during the periods in 1 and 2 above.	Resolution within 24 hours, with extension of an additional 24 hours in exceptional circumstances.[3]
6	Services defined as Secondary in-between meetings	Service is usable but operating incorrectly, any time except during the periods in 1 and 2 above	Triage within 24 hours. Resolution within 72 hours, with extension of an additional 72 hours in exceptional circumstances.[3]

NOTES:

[1] Services in this category will have been subject to a change freeze, except for emergency fixes, for at least one week before the meeting.

[2] Unusable means that the service is unavailable, or its performance is unacceptable, or it is operating incorrectly with the risk of data corruption or the risk of any other serious problem.

[3] Service provider is free to make this determination on a case-by-case basis. All such determinations to be recorded and discussed with IETF at scheduled review meetings.

Cost management

It is expected (though not a requirement) that the IETF is directly recharged by the Service Provider for the cost of third-party cloud services. The IETF needs to keep these costs within budget and so requires the Service provider to:

- Provide reasonably accurate cost estimates on a quarterly basis
- Continually monitor incurred costs and alert the IETF of any significant deviations from previously supplied estimates.
- Aim to keep third-party costs within the agreed budget limits

As the Service Provider is required to continuously monitor the performance of the infrastructure and rapidly adjust resources as necessary to maintain an acceptable level of performance, it is recognised that this may lead to costs exceeding budget

and that the priority may be for these adjustments to be made without prior estimation of the impact on costs.

Developers and developer support

The IETF has a core set of staff developers and long-term development contractors (fewer than 10 in total) who write the bulk of our software. Our infrastructure includes a substantial set of development/testing environments and automated build chains. We expect this infrastructure transition to include shifting completely to Continuous Integration-driven automated deployments of each service.

The development team members are also the primary operators/superusers of each service. While globally distributed, the development team responds to issues during regular working hours for their location and are not otherwise on call.

Service provider is required to support staff and contractors as needed, particularly with management of infrastructure (such as databases) that the services rely on.

There is also a strong set of community developers, some of whom develop adjacent tools for community use and some of whom contribute code to IETF tools. These developers are active throughout the year and particularly at 'codesprint' sessions, held at each IETF meeting, where 10+ community developers meet and work on the IETF applications for a day.

The IETF supports these community developers with pre-built development environments for them to run locally, and live integrations to development instances running on IETF infrastructure.

Application architecture

Most IETF developed applications are not capable of operating without planned downtime for deployments or horizontally scaling to meet performance targets. The IETF is in the process of re-architecting these applications to remedy this. The Service Provider is required to provide advice to the development team as needed, in support of this objective.

Community engagement

The IETF is a community-led organization and regular communication with the community is key to the success of this contract. Service provider is required to engage with the community as follows:

- Participate in regular community calls.
- Monitor key community mailing lists and respond as required.

- Monitor and respond to issues or PRs raised against GitHub repositories that service provider manages.

Part 4 - Transition specific

URL continuity

Most IETF web services require URL continuity - as services move, redirects have to be maintained. This is currently accomplished with a mix of bulk redirects in Cloudflare and logic at origin servers. The transition to the new infrastructure must maintain this preservation of continuity.

Current installations and separation of services

All of the servers listed below are owned and maintained by the existing service provider. There are four physical servers in two separate locations. Each server has 32 logical CPUs and 128Gb of RAM. The OS for each instance is OpenSuse, installed in a virtual server using Xenserver.

- Most services run on IETFA, with a warm backup maintained via database replication and rsync at IETFC.
- Newer services, such as wikis and the bibxml service, run on IETFX, with a warm backup at IETFY.

Applications on these servers are installed directly by the current service provider using a custom directory plan to provide some degree of application separation. A few applications are installed in Docker containers.

The IETF requires the new infrastructure to run Linux but does not require any specific Linux distribution. Commonly used distributions will be favored over those with little market presence.

The IETF requires each application to be transitioned to its own containerised environment on the new infrastructure in order to achieve the goals outlined above.

The transition will be considered complete when the IETF has no dependency on these existing servers and they can be repurposed by the owner as they see fit.

Additional Details

The following sections are provided for information only and are not requirements or any form of commitment by the IETF. They are not intended to form part of any contract.

Demand for services

The IETF is a global community with an uneven geographic spread, and the community uses the IETF infrastructure 24x7x365. During IETF meetings, both the triannual plenaries and the many interim meetings, demand on services is high and uninterrupted availability is expected. At other times, the activities are not so time critical that they cannot tolerate a delay of a few hours if planned and sufficient warning is given.

Also, there are a number of services intended for users to pull large amounts of data (1-10 GB) in order to maintain local copies of large datasets. While service performance can be adversely affected by a bottleneck at a level of the stack above the IT infrastructure, the IT infrastructure should not become the bottleneck.

Community participation in the development and operation of IT services

The IETF is a community-led organization and there are several mechanisms for the community to participate in the development and operation of IETF IT services. These may change over time:

- Monthly open Tools Team call of 1-1.5 hours.
- Participation on the Tools-discuss[7] mailing list. This is a low volume mailing list with occasional spurts of high volume. However, it should be noted that the community may raise relevant matters on other lists, including the general IETF list and the admin-discuss list.
- Formal consultations with the community on aspects of our IT strategy. These are rare, possibly twice a year, lasting for a few weeks, with community feedback provided by email.
- Occasional workshops or special meetings to discuss specific issues or plans.
- Contributing via public GitHub repositories. All IETF software is open source and available this way.

IETF Meetings and the IETF Network

The IETF meets three times a year on a global rotation. Each meeting will have 1000+ onsite participants and 400+ remote participants. These meetings are crucial to the operation of the IETF and therefore the expectation for IETF IT systems is that they are highly available both during the meetings and in the preparatory periods.

The IETF provides its own network in the IETF Meeting venues, which is installed and managed by the NOC team, a combination of contractors and volunteers. This network, its equipment and its management are out of scope for this contract.

[7] https://www.ietf.org/mailman/listinfo/Tools-discuss

The IETF utilizes a highly specialized remote participation tool during its meetings, with an onsite team managing this throughout the meeting. This operates on AWS under the management of the remote participation tool provider. This tool requires Datatracker to be functioning as its authentication provider.

The IETF uses a third party registration system for its meetings, which is integrated with both Datatracker and Salesforce.

Additionally, the IETF hosts interim meetings of individual Working Groups, using one of a number of remote participation options. The IETF generally avoids scheduling any application downtime or major upgrades near the time of an interim meeting.

Specialist providers

The IETF is supported by a number of specialist providers in the following areas: UI/UX research and design, database management, security auditing and customisation of off-the-shelf applications (e.g. Wagtail and Salesforce).

Threat model

The IETF is vulnerable to the same threats as any other organization and needs to mitigate those at many levels. The threat model for the IETF is unusual with more of an emphasis on data integrity and preserving the accuracy and availability of historical data, than on protecting confidential information. Where the IETF does collect highly confidential information, such as for the NomCom process, every effort is made to compartmentalize that. Additionally, the IETF receives significant nuisance traffic (as a proportion of overall traffic).

ENDS