Wire **for Federal Government**

Wire is a comprehensive workspace for secure government collaboration. Wire provides integrated and frictionless worker productivity with audio, video, messaging, and file sharing protected by the industry's most stringent security. Wire makes it possible to foster the open, productive collaboration that users want while ensuring the data privacy, protection, and compliance that government ministries and agencies need.

wire

The Security vs. Productivity Challenge in Government Agencies

Federal and national government ministries and agencies must balance security with productivity. On one hand, they must enforce the highest security standards to safeguard sensitive and classified data. At the same time, compliance with data privacy regulations is crucial due to their access to citizen information. These security and privacy mandates often lead to unintended challenges:

- → Long procurement cycles and high costs for specialized, secure IT equipment
- → App fatigue and productivity loss due to many separate tools needed to work and stay secure
- → Tool abandonment and rogue use of dangerously insecure consumer tools like WhatsApp due to user unfriendliness and security friction

Wire eliminates these challenges by providing a seamless, secure, and scalable collaboration platform designed for government agencies. It is the only enterprise-class solution secured at scale by the Messaging Layer Security (MLS) standard*[1], while ensuring end-to-end encryption, privacy compliance, and support for thousands of teams.

10+
Years of experience

>1800
Customers world wide

Zero
Knowledge Architecture

100%
Ease of use

[1]* Messaging Layer Security (MLS) is the only global open standard for end-to-end encrypted communication. Wire, along with other organizations like Meta, Google, Mozilla, Oxford University, co-founded MLS as the standard for next-gen information security and efficiency for groups in the tens of thousands.

For more information go to: **wire.com/en/government**

Federal Government - High Security

Secure and seamless online workspace for government operations and sensitive topics

Administrator and Operator Shielding

IT admins and operations personnel can't see any message content, preventing security breaches due to human error.

Full Data Ownership

Available via private cloud and on-premises deployments, with installation services and SLA-backed support. Since Wire doesn't require specialized equipment, it can be configured to fit in your existing IT environment.

Open, Closed Federation

Wire allows separate government organizations to own and operate their own back-end and federate with other agencies' closed backends to call, text, conference, and share files with others outside their organization as if they were on the same backend. Each back-end administrator has full management control and can also extend connectivity to users on Wire Cloud.

ID Shield

Wire offers a painless identity and device verification function called ID Shield, ensuring that users only communicate with intended recipients. Users can authenticate, renew, or revoke identity and device verification using a certification process.

Real-World Use Cases

Secure and seamless online workspace for government operations and sensitive topics

Intelligence & National Security
Secure cross-border communication and classified operations while enforcing strict access controls.

Military Operations
Empower tactical teams with secure messaging, video, and file sharing, ensuring operational privacy.

Parliaments & Judiciary
Enable confidential collaboration between political bodies, legal professionals, and court administrators.

Foreign Ministries & Border Security
Facilitate encrypted diplomatic communications and safeguard sensitive immigration data (passport details, biometrics, and immigration history).

Public Health & Emergency Response
Securely manage communications during pandemics, natural disasters, and cybersecurity incidents.

Remote & High-Risk Operations
Protect data exchange in unstable or high-security regions with end-to-end encryption.

Data Sovereignty & Compliance
Ensure total control over sovereign data through private cloud and on-premises deployment.

The Wire Secure Communications Promise

No matter the use case, Wire always brings you these benefits

E2EE Everything

Next-gen End-to-end encrypted (E2EE) makes security invisible and easy for large and complex orgs

✓ Every piece of data is encrypted, no one – not even Wire – can access your content

Productivity without Risks

Enjoy all the features of well-known collaboration platforms, without the pitfalls of compromised security design choices, and it's configurable to meet your needs

✓ Wire is the only workspace that provides security and productivity in one app

Open Source Transparency

Don't just "trust us", Wire's source code is available on GitHub, frequently independently audited

✓ Transparent by design, the only collaboration platform endorsed by the German government

Zero Trust Architecture

Every piece of data is fully authenticated, authorized, and encrypted before granting access

✓ Never trust, always verified – protects against impersonators and other bad actors

For more information go to: **wire.com/en/government**