Protecting Digital Assets In Governments

Governments are constantly targeted by state and non-state actors. Combining the size and reach of government operations with highly sensitive information in use, it's clear why increasing the security of communications is no longer "if," but rather "how."

This document provides a snapshot of the current cybersecurity landscape and best practices when it comes to assessing the security threshold of available communication platforms for the government.



Cybercrime costs global businesses & governments

$6 Trillion / Year



113 Gov. Agencies

Fell prey to ransomware in 2019 with a 90% attack success rate

Global Perceived Risks in 2020*

Economy	Risk 1	Risk 2	Risk 3
United States of America	Cyberattacks	Spread of infectious diseases	Data fraud or theft
Canada	Cyberattacks	Spread of infectious diseases	Unemployment or underemployment
United Kingdom	Cyberattacks	Fiscal crises	Extreme weather events
Germany	Cyberattacks	Involuntary migration	Asset bubble
Netherlands	Cyberattacks	Spread of infectious diseases	Failure of climate change adaptation

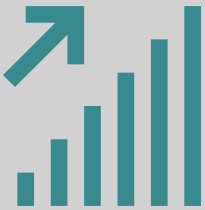
*Data collected by the World Economic Forum to determine what the world's business community is most concerned with for the next decade.

According to the World Economic Forum 'Risks For Doing Business' 2020 report, Cyber Attack comes third in the top global risks for organizations after unemployment and infectious diseases.

In the UK, USA, Germany, Canada, and the Netherlands to name a few – cyberattack is ranked as their top concern. Now more than ever, businesses need to prioritize and re-think how to protect their digital assets, and for vendors, whether they help solve or add to the problem.

5 Key Elements of a Secure Communication Infrastructure

A security-first architecture embraces the mindset that everything should be scrutinized and authenticated by implementing cutting-edge cybersecurity protocols and operating on the basis of zero-trust. This means enabling electronic communication throughout federal and government agencies with the same level of security and privacy as a face-to-face conversation.



COVID-19 has seen employees bombarded by a staggering volume of attacks with ever-more realistic imitations of messages sent out impersonating well-recognized Government agencies. In fact, FBI data suggests that cyberattacks **have increased by a whopping 400% during the pandemic.**

1. State-of-the-art Encryption

End-to-end encryption (E2EE) is no longer an add-on, it is a fundamental necessity for secure communication. But not all end-to-end encryption is created equal. Using **forward and backward secrecy** ensures that every asset is separately encrypted instead of using one key for everything. Some protocols have also been proven to be more secure than others. A decentralized solution that uses **double-ratchet E2EE** allows for every individual call, message, and file to be separately encrypted on every device, with the keys generated from the device rather than a central server. This protects the information to the smallest possible unit, creating a system that grows more complex - not more valuable - for hackers with every message.

2. Data Sovereignty

Data is crucial in every industry, but for government organizations especially, the pressure is immense and the threats complex. Organizations need to prioritize data sovereignty by implementing **Zero-trust policies** and moving systems that exchange or host data to a **private cloud or on-premise environments**.

3. Continuity of Service

A crucial (and often overlooked) element is the ability to communicate, plan, and update on what's going on should the network be compromised or under attack. If organizations fail to **provide a secure environment for critical/crisis communication** that is independent of their network infrastructure and by invitation only, they can be certain that employees will find their own ways of talking and sharing information. This will put confidential and sensitive information on the radar of third parties, fundamentally eroding the entire cybersecurity defense of the organization, not to mention potential regulatory fines for breach of compliance.

4. Federation & Messaging Layer Security

Wire™ is leading the development of a new, open global standard for secure communication technologies called Messaging Layer Security (MLS).

Partnering with industry leaders, our goal is to create a **secure, interoperable, and federated system that enables users to operate between different messaging systems with the same level of privacy and security that Wire offers.** Alan Duric, Wire's Co-Founder previously helped develop WebRTC and is leading the development of the MLS, which will establish a broader standard for all encryption.

Federation is especially important for government branches to be able to communicate with one another using their own intranet while remaining secure.

5. Hyper-Transparency

Organizations that are interested in implementing platforms that prioritize protecting their digital assets will see security, privacy and transparency go hand-in-hand. There is no true security if there is a violation of privacy, and **the best way to prove real privacy is through an open-source code.** Open source demonstrates that a vendor is truly focused on taking a proactive and less opaque approach in sharing its security measures and enables third-party auditing of the software.

By having the ability to examine the source code of any technology you evaluate, you can determine precisely how the vendor treats data, integrations, encryption key storage, and other potential sources of security risks.

Selecting a Secure Communication Service

With all the communications and collaboration solutions available today, the choice seems difficult. We encourage governmental organizations to follow these guidelines in order to mitigate the risks posed by malicious cyberthreat actors.

Communication Solution Comparison*

	E2EE Text Chat	E2EE Voice Calls	E2EE Video Calls	E2EE File Sharing	E2EE Screen Sharing	Open-source Code	Certified Service
Wire	✓	✓	✓	✓	✓	✓	FedRAMP In Progress
Cisco Webex	✓	✓	✓	✓	✓	X	FedRAMP
Dust	✓	N/A	N/A	N/A	N/A	X	None
Google G Suite	X	X	X	X	X	X	FedRAMP
GoToMeeting	✓	✓	✓	N/A	N/A	X	None
Jitsi Meet	✓	✓	✓	✓	✓	✓	None
Mattermost	X	X	X	N/A	X	✓	None
Microsoft Teams	X	X	X	X	X	X	FedRAMP
Signal	✓	✓	N/A	✓	N/A	✓	None
Skype for Business	X	X	X	X	X	X	FedRAMP
Slack	X	X	X	X	X	X	FedRAMP
WhatsApp	✓	N/A	✓	✓	N/A	X	None
Wickr	✓	✓	✓	✓	✓	✓	None
Zoom	✓	X	X	✓	X	X	FedRAMP

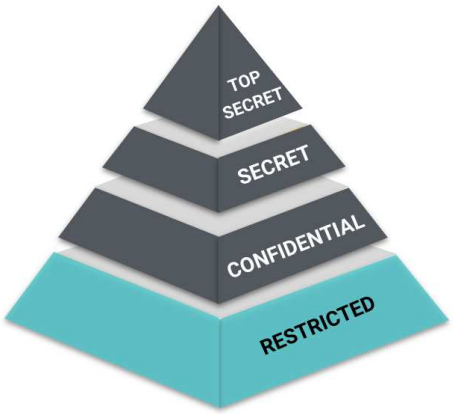
Legend: N/A = Not Applicable

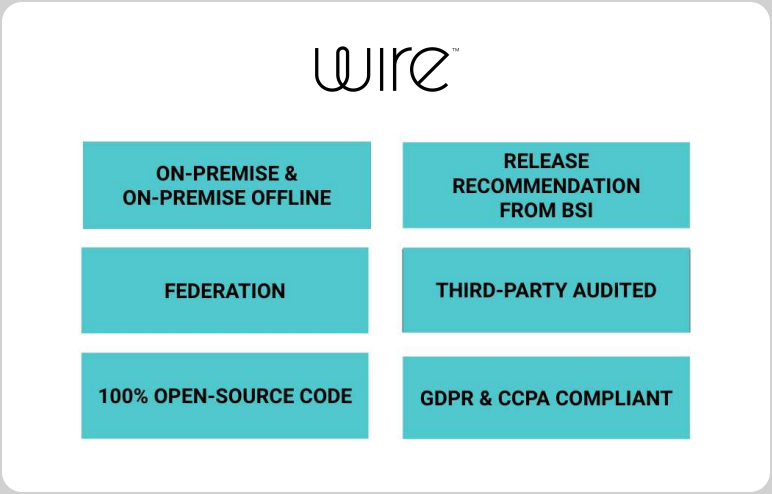
*Data based on cybersecurity information by the NSA - Selecting and Safely Using Collaboration Services for Telework

Why Wire is The Choice For Governments

Government institutions use Wire to ensure sensitive information remains under their control and to offer employees a secure communication channel. Whether at home, on-the-road or abroad, users can instantly place audio & video calls, send messages, and share files without putting mission-critical information at risk.

Designed To Operate In Classified Environments





Built to safeguard every critical mobile communication. Wire's security is recognized by IDC as unique.

German Government Use Case

With a large number of government workers operating from their home office, protecting sensitive communications outside of the IT firewalls grew critical.

The German government uses Wire's secure communication platform to facilitate working from anywhere while drastically reducing security risks. The Federal Office for Security in Information Technology (*Bundesamt für Sicherheit in der Informationstechnik* or *BSI*) issued a release recommendation for Wire's secure solution making it an official tool for handling classified information.

Offering audio and video conferencing, messaging, screen-sharing, and file-sharing, Wire's is also well-appreciated by users, meeting their collaboration needs in a modern and intuitive platform.

Best-in-class Security

- NSA and BSI Recommended
- Perfect Forward/Backward Secrecy
- Mission-first System
- Minimal Metadata Footprint
- Developed by former Skype Technologists

Feature-rich

- Full Collaboration Suite
- Configurable Ephemeral Messages
- Secure External Guest Rooms
- 25 Participants on Audio & 12 on Video
- Works in Low Bandwidth

User-friendly

Wrapped in a clean and intuitive design that users love, Wire is as easy to use as consumer applications, and available on iOS, Android, Windows, Mac, and Web App with up to 8 devices/user.

Government, Ministries, and Military Use Cases



Safeguard Mission-Critical Information



Cyber Espionage Protection



Secure Mobile Communication



Immediate Incident Response

Wire Enterprise

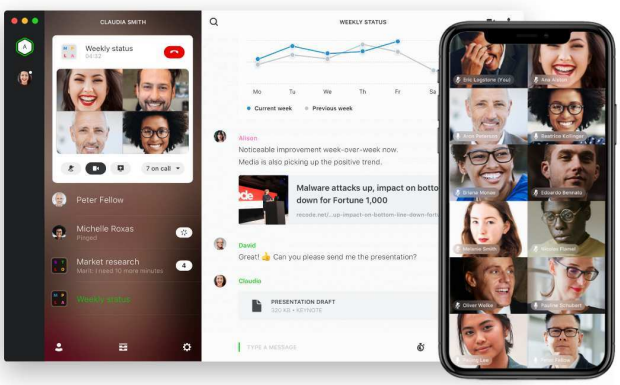
Fully customizable self-hosted platform for secure collaboration across your entire organization. Ensure your communication is in compliance with the highest security standards.

CONTACT US ▶

Wire Pro

End-to-end encrypted SaaS platform. Set up an account, invite members, and start communicating and collaborating securely in minutes.

GET STARTED ▶



> Wire was the clear choice as a partner - not only is their collaboration platform secured with the highest level of end-to-end encryption, they are built upon principles of transparency and privacy that many others lack.
>
> Tomas Nystrom, IT Director at Fortum.

About Wire™

Wire™ is the most secure collaboration platform, transforming the way businesses communicate at the same speed that our founders disrupted telephony with Skype. Headquartered in Berlin with offices in Switzerland and San Francisco, Wire's award-winning collaboration and communication platform counts over 1,800 enterprise customers worldwide. Recognized by IDC, Forrester, and Gartner as one of the most secure collaboration platforms, Wire offers messaging, audio/video conferencing, file-sharing, and external collaboration - all protected by the strongest end-to-end encryption.

Visit wire.com to learn about Wire's secure communication solution for governments.

Award-Winning Choice

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2020

Capterra BEST EASE OF USE 2019

G2 Leader FALL 2020

Capterra TOP 20 2020

CYBER SECURITY EXCELLENCE AWARDS WINNER 2020

Trusted by our Partners

INTELLIGENT WAVES LLC

DELL Technologies

BYLIGHT

SVA