Australian Government
National Capital Authority

Customer story
National Capital Authority

Keeping file sharing secure without exposing the network.

A small agency with a big public responsibility, the National Capital Authority (NCA) plays a key role in planning and managing national land and public spaces in Canberra. Operating across both public-facing and internal government environments, it works in a space where security, simplicity and practicality all need to align.

With fewer than 100 staff, roles are often blended. Michael Wuth, who supports internal systems and security, describes his role as an "internal IT resource", managing everything from infrastructure to information handling.

But while the organisation itself is small, the network it operates within is not.

> **SigBox removes the need to give people access to our secure network.**
>
> **Michael Wuth, NCA**

The challenge.

The NCA regularly shares information with a mix of stakeholders, from government agencies to private contractors and members of the public.

Each comes with different expectations, systems and levels of trust:

- Internal government sharing is supported by existing trusted networks
- External sharing introduces more complexity and risk
- Large files regularly exceed email limits
- Sensitive environments require strict control over access

At the same time, not all information is high risk.

"A lot of the information we're sharing is either already public or will become public," Michael explains. "But we still need to be conscious of how it's handled."

Without the right tools in place, this creates a balancing act between accessibility and security, particularly when working across networks.

Why traditional approaches fall short.

While email remains the default for most teams within the organisation, it quickly breaks down when files are too large to send, external users need to provide documents securely, or there's no clear way to control access without opening up internal systems. The alternative is giving external users access to internal networks. But this isn't viable.

"SigBox removes the need to give people access to our secure network," Michael says. "That's a big part of it."

The solution.

SigBox provides the NCA with a secure way to send and receive files without exposing internal systems or overcomplicating workflows.

Rather than replacing existing tools, it fits alongside them.

- Email remains the default for everyday sharing
- SigBox is used when files are too large or require a more secure transfer
- Some teams use it as a primary intake channel for external documents

Customer story
National Capital Authority

Australian Government
National Capital Authority

"It's an additional tool rather than something that forces a whole new process," Michael says.

Supporting real-world use cases.

Across the organisation, SigBox is used in practical, everyday scenarios:

Event management: External parties submit applications and supporting documents for events held on national land.

Infrastructure and project work: Vendors share large files such as plans, drawings and image-heavy documentation.

General file transfer: Teams receive documents from contractors without relying on email limits or insecure platforms.

Making secure sharing easier.

One of the most valuable features has been the file request functionality, which simplifies how external users submit information.

Instead of creating and managing guest accounts, teams can send a file request directly via email, generate a link for external users, and automatically organise submissions into clearly labelled folders.

"SigBox allows us to manage the process a lot better," Michael says. "You don't need to create guest accounts or clean them up afterwards."

For a tool to be widely adopted, it needs to be easy to use, especially when dealing with external stakeholders.

For NCA, SigBox's simplicity has been key.

"It's not overly complicated," Michael explains. "It looks similar to other web pages, so people can use it without much trouble."

That familiarity reduces friction for both internal teams and external users, making it a practical option in day-to-day work.

A controlled environment for sensitive networks.

Unlike consumer-grade file sharing platforms, SigBox was built to be a more controlled and secure environment.

The NCA has deliberately restricted access to platforms like Google Drive due to concerns around control and data handling.

"With SigBox, there are more security controls around it," Michael says. "That's important in our environment."

This allows the organisation to:

- Maintain tighter control over how information is shared
- Reduce exposure to external risks
- Support secure transfers between different networks

Without a secure file sharing platform, the risks are clear.

"There's a reputational risk if information is exposed," Michael says. "That's a big consideration."

SigBox helps mitigate that risk by providing a consistent, controlled way to transfer information, without introducing unnecessary complexity or disrupting existing workflows.

Having used SigBox for more than a decade, the platform has become a reliable part of the NCA's toolkit.

"I think it definitely has its place," Michael says.

"There will always be a need for a secure mechanism to transfer information between different networks."

The outcome.

For the NCA, the value of SigBox comes down to one thing: practical security.

It enables teams to securely send and receive files across different networks, without opening up internal systems or forcing major process changes.

In an environment where control, simplicity and risk all need to be balanced, that's exactly what's needed.