An executive's guide to scaling shared services to

Enhance operational cybersecurity

CGI

The inflection point

The complexity of the federal cybersecurity environment continues to challenge federal agencies. Nation-state adversaries are conducting sustained, AI-enabled targeted campaigns against agency networks — not opportunistic intrusions, but deliberate, patient attacks on mission-critical systems and sensitive data. Adversaries now automate reconnaissance, generate phishing content at scale, and identify exploitable vulnerabilities faster than most agency security teams can respond. The result? Cybersecurity strategies and approaches from even a few years ago are vulnerabilities today.

For a growing number of federal civilian agency leaders, shared cybersecurity services have become the most compelling answer to a problem that is no longer manageable alone. The reasons are structural. A persistent workforce shortage leaves agencies competing for a limited pool of specialized talent, unable to sustain the analyst depth, threat intelligence, and incident response readiness that today's environment demands. The rising cost of cybersecurity talent runs up against flat or declining budgets, forcing difficult trade-offs between keeping legacy systems running and investing in capabilities that reduce risk. As modernization accelerates with cloud migrations, AI adoption, and hybrid architectures, the attack surface expands faster than any single agency security team can cover. Shared services don't just reduce costs. They provide access to scale, specialization, and continuity that most agencies simply cannot build on their own.

The increasing risks

Advances in AI create both opportunities and threats in cybersecurity. While advances in artificial intelligence can increase the pace at which intrusions and anomalies are detected, they also allow adversaries to be more creative and even more persistent in their attack positions. Unfortunately, the two elements do not cancel each other out and require an advanced understanding of how to deploy AI productively to address these new threats.

At the simplest, adversaries are taking advantage of the ease of access to AI, using chatbots to write better phishing emails, and more advanced efforts are crafting agents to extract online data to enhance social engineering efforts and orchestrate attacks.

Meanwhile, nation-state actors aren't waiting. They prepare the battlefield years in advance, targeting not only federal systems but also state, local, and commercial infrastructure. Regional entities such as local utilities, transportation authorities, and civic service providers often lack resources to defend against advanced persistent threats, yet their operational technology (OT) systems that manage critical infrastructure (such as water treatment plants and wastewater facilities) represent critical leverage points for disruption.

Building on this threat, we are also seeing the increasing convergence of OT with traditional IT networks. Both OT systems and IoT devices are increasingly connected to traditional enterprise networks, creating a larger attack surface for security teams to manage. At the same time, many of these devices are difficult to manage, patch and support, creating potential long term vulnerabilities when not thought out properly.

When these threats are combined with fragmented, immature and underfunded cybersecurity systems, the risks continue to rise. Organizations need a consolidated cybersecurity approach - efficient, resilient, and invisible. An established cybersecurity shared service model offers respite for organizations that want to focus on their missions and decrease their risk profile. A shared service aligns incentives and allows the provider to deliver reliable service across multiple clients, continually improving processes and leveraging technology to reduce costs while maintaining quality.

The convergence

Modernizing with AI-powered cybersecurity shared services

The advances in technology and continued development of these new threats quickly converge on the same solution: a managed cybersecurity shared services platform. The increasingly complex and fast-paced ecosystem of cybersecurity requires a different approach.

Historically, cybersecurity was seen as an expense that never slowed, with leaders throwing money at it in hopes that spending would make the problems go away. Currently, only the largest, best-funded organizations can afford top-tier security operations capable of defending against nation-state threats. Mid-sized agencies make do with less comprehensive coverage. Small critical infrastructure operators rely on basic protections that sophisticated adversaries easily bypass. The gap between what organizations need and what they can afford creates systemic vulnerability.

A managed shared services platform is a smarter way to gain new capabilities while receiving top-tier protection at a lower cost.

Security that functions with an “always on” approach, rather than a complex, bespoke in-house service that requires continual investment, training and overhaul. Protection that agencies and critical infrastructure operators can depend on without dedicating disproportionate budget or attention.

AI-enhanced shared services further impact this convergence of needs. By dramatically reducing the marginal cost of adding another organization to the platform, the shared services organization can deliver high-quality security operations—including defenses effective against nation-state actors—at price points that work for a much broader range of organizations.

Building cybersecurity that scales

5 non-negotiables for a shared services partner

Shared services have transformed federal IT by eliminating redundant capabilities, driving economies of scale, and ensuring consistent quality. In today's cybersecurity landscape, this model is no longer optional—it's essential. Agencies and enterprises need a partner that delivers security reliably, efficiently, and invisibly, enabling cost-effective security without compromise. Here are five critical features and what they look like in practice:

1

Operational trust

A proven history of delivering mission-critical services for years, not months.

Example: A partner that has supported continuous monitoring for multiple Cabinet-level agencies through multiple administrations without service interruption.

2

Proven scale

The capability to run complex cybersecurity operations for diverse clients simultaneously.

Example: Managing Security Operations Centers (SOCs) for multiple agencies while maintaining 24/7 coverage and rapid incident response.

3

Operational excellence

High-quality services at efficient costs through platform-driven approaches, not bespoke fixes.

Example: Leveraging a centralized threat intelligence platform to serve dozens of agencies, reducing duplication and accelerating detection.

4

Proven AI-enabled defense at scale

The ability to operationalize AI and machine learning in live security environments – enhancing detection, response and analyst efficiency without introducing risk.

Example: Applying AI-driven analytics and automation across centralized security operations to identify anomalies, prioritize threats and accelerate response times across multiple agencies simultaneously.

5

Strategic positioning

Cybersecurity as a core identity—not a checkbox—backed by deep delivery expertise.

Example: A provider whose primary mission is security, with decades of federal experience, has cultivated long-term partnerships with world-class vendors and systems and made investments in continuous innovation.

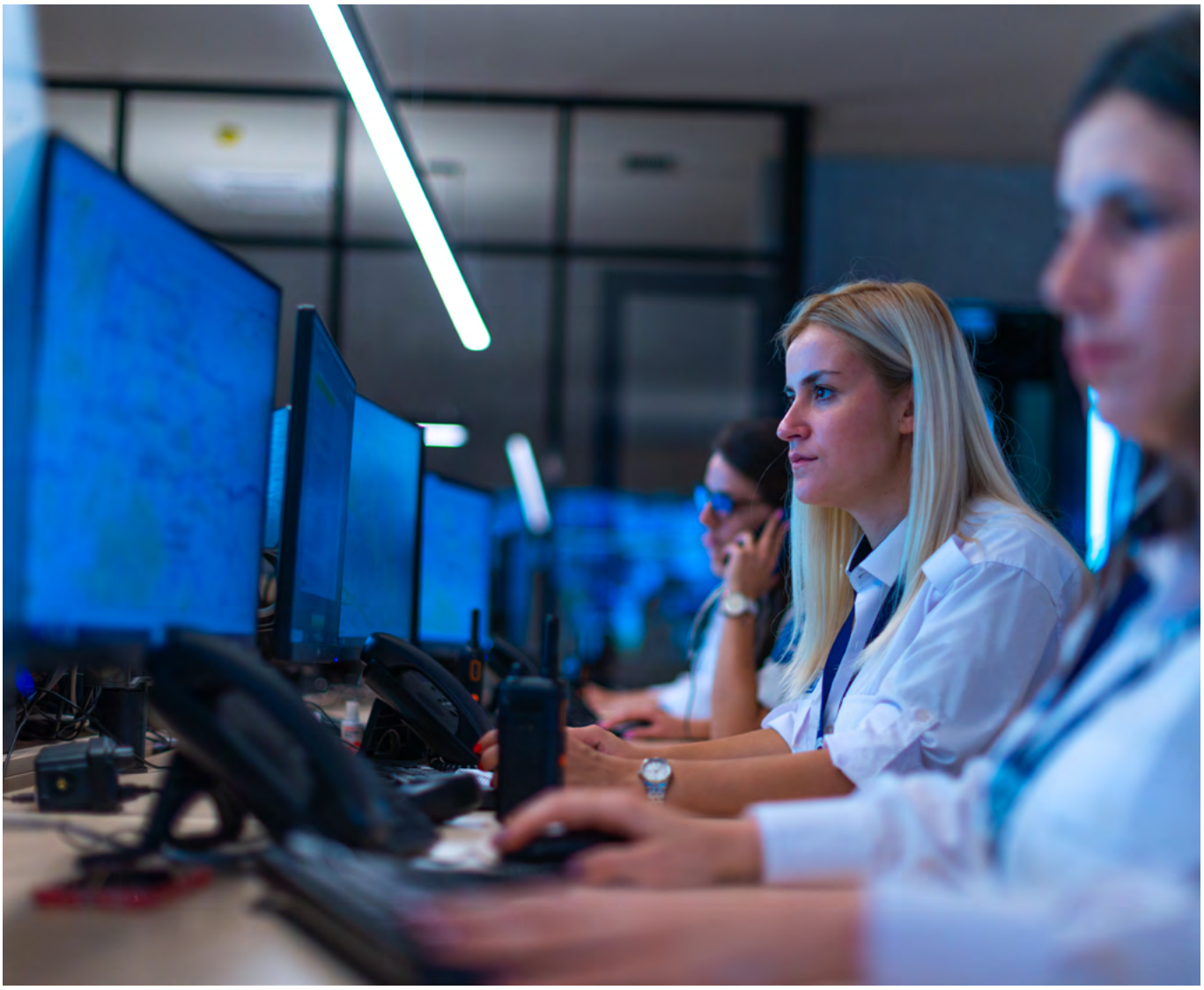
Having the right partner

Why expertise and alignment matter for cybersecurity strength

Cybersecurity should be more than a compliance requirement — it should be the invisible foundation that enables mission success and enterprise resilience. Agencies need more than tools or advice; they need an operational partner who delivers security as a shared service at scale — reliably, efficiently, and seamlessly, built on top while defending against sophisticated threats underneath.

A partner must have deep federal delivery expertise and a proven track record of operational trust — one who can run complex cybersecurity operations for multiple clients simultaneously, at efficient costs, through platform-driven approaches rather than bespoke solutions. This partner must bring nation-state defense capabilities to detect and counter advanced persistent threats, not just commodity malware, and position cybersecurity as a core identity, not an add-on.

As agencies seek to modernize, consolidate, or operationalize cybersecurity, they should look for a partner with an ecosystem mindset — one who understands security as an integrated system of capabilities, not a collection of point solutions. The right partner helps avoid fragmented efforts and drives sustainable, enterprise-wide and future-focused impact.



Looking to optimize cybersecurity defense through shared services?

For federal agencies: See how CGI helps agencies maintain a strong cybersecurity posture in the age of AI. Learn more here.

About CGI Federal

CGI Federal Inc. (CGI), a wholly owned U.S. operating subsidiary of CGI Inc., is a leading technology and professional services company that serves Federal agencies across defense, civilian, healthcare, justice, intelligence and international affairs. With nearly 8,000 professionals, we work with our clients to modernize government through innovative technology solutions, flexible delivery models and a commitment to achieve mission outcomes.

For more information
cgifederal.com

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

cgi.com