Cyber Capability

August 2025

White Paper

Safeguarding Public Service Delivery:

Supply Chain Resilience for Australian Government Agencies

Executive Summary

Australian government agencies at both the federal and state levels are under growing pressure to maintain the continuity of public services in an increasingly unpredictable world. The supply chains that underpin health care, education, transport, emergency services and other essential functions are now exposed to a wide spectrum of risks. Disruptions can arise from natural disasters, cyberattacks, global market volatility or geopolitical events. Each of these can have an immediate and visible impact on communities and can undermine confidence in government.

The COVID-19 pandemic demonstrated how fragile certain supply chains can be, with shortages of personal protective equipment and medical devices forcing emergency procurement measures. More recently, severe flooding in parts of Australia disrupted transport routes and delayed critical infrastructure projects, while cyber incidents have affected access to citizen data and interrupted key digital services. These events have shown that supply chain resilience is not simply a technical or administrative concern. It is a strategic capability that enables governments to meet their fundamental obligation to the public: delivering essential services under all conditions.

This paper examines the nature of the risks facing government supply chains, the importance of resilience in protecting service delivery, the regulatory frameworks that shape agency obligations, and the leadership role of public sector executives. It also explores practical measures to strengthen resilience and the value of collaboration across jurisdictions and with the private sector. The central message is that resilience must be embedded into the core operations of government agencies if they are to sustain public trust and deliver on their mandates in a world of constant change.

About Cyber Capability

Cyber Capability Pty Ltd is a Canberra-based technology firm dedicated to strengthening the resilience and performance of Australian government agencies by connecting strategic business objectives with modern technology solutions. Founded with the mission of enabling lasting operational capability across the public sector, the company draws on its multidisciplinary expertise to deliver practical, outcome-focused solutions tailored to the priorities of government clients.

Its services span several critical domains relevant to contemporary public administration, including digital transformation, cyber security, data management, and supply chain resilience. These offerings are designed to support agencies in sustaining service delivery, enhancing security, and improving operational efficiency in a rapidly changing environment. Cyber Capability places a strong emphasis on aligning technical solutions with mission outcomes, sourcing professionals with specialised skills to address the unique challenges faced by public sector organisations.

Operating from Canberra, Cyber Capability works at the centre of Australia's public service and policy environment, enabling close engagement with federal and state decision-makers. This proximity facilitates agile collaboration, fosters strong working relationships, and ensures the company remains responsive to the evolving needs of government agencies and the communities they serve.

Introduction: The New Risk Reality for Government Services

Government agencies operate in an environment where uninterrupted service delivery is expected as a matter of course. Whether it is a hospital providing life-saving care, a school maintaining consistent learning programs, a transport network moving people and goods, or emergency services responding to crises, the public relies on these services to be available whenever they are needed. This expectation persists even when agencies face significant disruptions in the supply of goods, technology, infrastructure, or human resources.

The last decade has brought into focus the interconnected nature of risks facing government operations. Supply chains that once appeared robust have proven vulnerable to shocks. International dependencies mean that a disruption on the other side of the world can have cascading effects on local service delivery. Digital systems, now essential to almost every function of government, are increasingly targeted by sophisticated cyber adversaries. Extreme weather events, driven by climate change, have disrupted logistics networks and damaged critical infrastructure with little warning.

In this context, the ability to anticipate and prepare for disruption, to maintain operations during a crisis, and to recover quickly afterwards is no longer optional. It is a defining feature of modern public administration. Supply chain resilience is the mechanism through which these capabilities can be embedded into the fabric of government operations.

The Public Sector Threat Landscape

Government supply chains operate across diverse sectors and are therefore exposed to a broad and evolving range of threats. Cyber security incidents remain among the most pressing concerns. A successful attack on a government information system can halt access to essential data, disrupt payment systems or disable online service portals. In some cases, the compromise of a trusted software supplier can have wide-ranging effects across multiple agencies simultaneously.

Geopolitical tensions have also emerged as a source of disruption. Trade restrictions, sanctions, and diplomatic disputes can delay or block access to critical goods such as specialised technology components, construction materials or essential pharmaceuticals. Even when alternative sources are available, the time and cost involved in shifting supply lines can cause significant disruption to service delivery.

Environmental hazards are another critical factor. Floods, bushfires, cyclones and severe storms can sever transport routes, damage facilities and interrupt communication networks. For agencies responsible for emergency services or infrastructure maintenance, these hazards can create simultaneous challenges of increased demand and reduced capacity.

In many cases, supply chain vulnerabilities stem from a concentration of suppliers or over-reliance on a single region. This leaves agencies exposed to market fluctuations, industrial disputes or localised disruptions that can quickly escalate into service delivery crises.

Finally, inter-jurisdictional dependencies add a layer of complexity. State and territory agencies often rely on federal systems or share suppliers with other jurisdictions.

A disruption affecting one agency or jurisdiction can therefore have a ripple effect, spreading quickly and affecting services far beyond the original point of failure.

The Case for Resilience in Government Supply Chains

Resilience in the public sector context is about more than operational efficiency. It is about the capacity to ensure that essential services to the community continue even when faced with significant disruption. This requires a shift in mindset from simply managing procurement processes to embedding resilience into the strategic and operational planning of every agency.

The benefits of resilience are both practical and reputational. Agencies that can continue delivering services during a crisis preserve public trust and avoid the reputational damage that accompanies visible service failures. Communities are more likely to remain confident in their government when they see a rapid and well-coordinated response to disruption.

Financially, proactive resilience measures are more cost-effective than reactive crisis management. Emergency procurement, unplanned overtime, and the costs associated with recovering from prolonged service outages can be far greater than the investment needed to prepare for disruption in advance. The true return on investment, however, lies in the protection of community wellbeing, which is the ultimate measure of public sector performance.

Regulatory and Policy Environment

Government agencies operate within a complex framework of legislation and policy that influences their approach to supply chain resilience. The Security of Critical Infrastructure Act 2018 imposes specific obligations on operators of designated critical infrastructure, which can include certain government-owned or operated assets. Agencies subject to the Act must have risk management programs in place, report incidents, and ensure executive accountability for resilience measures.

The Protective Security Policy Framework establishes mandatory requirements for security governance, the protection of people, information, and physical assets. Its provisions apply to all non-corporate Commonwealth entities and are a key reference point for resilience planning.

The Australian Government Information Security Manual provides detailed technical guidance for safeguarding systems and data, including measures to secure supply chains. Compliance with the ISM is essential for agencies that rely on digital systems to deliver services, which now includes almost every function of government.

At the state and territory level, procurement frameworks often set out requirements for supply risk management, supplier vetting, and contract terms that address security and continuity. Sector-specific regulations also apply in areas such as health, transport, and emergency services, reflecting the unique demands and risks of each domain.

While these frameworks set important minimum standards, agencies that treat them as the starting point rather than the ceiling of their resilience planning will be better positioned to meet real-world challenges.

Governance and Leadership in the Public Sector

Strong governance is at the heart of supply chain resilience. Public sector leaders, whether they are agency heads, senior executives or board members of government-owned corporations, must view supply chain risk as a matter of strategic importance. This responsibility extends beyond compliance to an active role in shaping an organisational culture that values preparedness and foresight.

Leadership commitment begins with embedding resilience objectives into the agency's strategic plan. Resilience should not be treated as an occasional project or a one-off audit activity, but as a standing priority that is monitored, reviewed and resourced. Decision-makers must be provided with regular and comprehensive reports on supply chain vulnerabilities and the effectiveness of measures in place to address them.

Contract management is another critical area where leadership must exert influence. Supplier agreements should clearly outline expectations for resilience, continuity, and security. These requirements must be enforceable and subject to regular review to ensure they remain relevant as the risk landscape evolves.

Governance also requires investment in capability. Agencies must allocate resources to training programs, scenario-based planning, and simulated exercises that test their ability to manage disruption. By doing so, leaders not only strengthen operational readiness but also send a clear signal to staff, suppliers, and the community that resilience is a core value of the organisation.

Building and Sustaining Resilient Supply Chains

A resilient supply chain is one that can absorb shocks, adapt to changing conditions, and recover quickly when disruption occurs. For government agencies, achieving this requires a deliberate and sustained effort across several areas.

The first is visibility. Agencies must understand the structure and dependencies of their supply chains in detail. This includes mapping not only direct suppliers but also the subcontractors, distributors and offshore partners that may be involved in the provision of goods or services. Without this insight, vulnerabilities can remain hidden until they cause real harm.

The second is diversification. Relying on a single supplier or sourcing region creates a single point of failure. Diversification, whether through multiple suppliers, alternative transport routes, or flexible procurement arrangements, provides options when the unexpected occurs.

Preparedness is the third essential element. Agencies need to have contingency plans that can be activated without delay.

These plans should identify alternative suppliers, stockpiling strategies for critical items, and processes for reallocating resources during an emergency. The best-prepared agencies do not wait for disruption to occur before considering these options; they plan and test them in advance.

Security assurance completes the resilience picture. Cyber security, physical security, and personnel vetting requirements must be applied consistently across all tiers of suppliers. This integrated approach ensures that the resilience of the supply chain is not compromised by a weak link in the network.

Collaboration Across Jurisdictions and Sectors

Government supply chains rarely operate in isolation. Federal agencies, state departments, and local councils often share suppliers, infrastructure, and even information systems. This interconnection creates opportunities for collaboration that can greatly enhance resilience.

Collaboration can take many forms. Joint procurement initiatives allow agencies to negotiate stronger contractual terms for resilience and security. Shared threat intelligence improves the ability to detect and respond to emerging risks. Cooperative planning ensures that agencies can provide mutual support during a crisis, pooling resources to maintain essential services.

Engaging with the private sector is equally important. Suppliers, logistics providers, and technology partners bring valuable expertise and operational capacity. By involving these partners in resilience planning and response exercises, agencies can create a more cohesive and effective network for managing disruption.

The most resilient public sector supply chains are those where collaboration is not an afterthought but a built-in feature of governance, procurement, and operational planning.

Incident Response and Service Recovery

When disruption occurs, the ability to respond quickly and decisively is critical to limiting its impact. Incident response is not simply about fixing the immediate problem; it is about managing the consequences for service delivery and public confidence.

An effective response begins with early detection. Agencies must have systems in place to identify disruptions as they emerge, whether through monitoring supply flows, maintaining real-time communication with suppliers, or tracking cyber and environmental threats. Once a disruption is identified, clear escalation pathways are essential. Decision-makers need accurate information quickly in order to choose the most effective course of action.

Service recovery planning should identify which services are most critical and must be restored first. It should outline alternative delivery channels, resource reallocation strategies, and communication plans for keeping the public informed. Transparency during recovery is vital. Citizens are more likely to accept temporary inconvenience if they understand what has happened, what is being done, and when normal services will resume.

Agencies that regularly rehearse their incident response and recovery processes are better prepared for the real thing. Each exercise provides an opportunity to identify gaps, improve coordination, and strengthen confidence in the agency's ability to handle future disruptions.

Looking Ahead: Preparing for the Next Generation of Risks

The threat environment facing government supply chains will continue to evolve. Technological change is creating both new opportunities and new vulnerabilities. The increasing use of artificial intelligence, for example, offers ways to improve supply chain visibility and forecasting, but also presents fresh targets for cyber adversaries.

Global geopolitical competition is likely to continue influencing access to key resources. Disruptions to the supply of semiconductors, rare earth minerals, or medical products can have far-reaching effects on public sector projects and services.

Climate change will remain a major driver of risk. The increased frequency and severity of extreme weather events will challenge infrastructure resilience, logistics planning, and community recovery efforts. Agencies must anticipate these impacts and factor them into long-term planning.

Resilient agencies will be those that invest in foresight. This means monitoring emerging threats, engaging with experts across disciplines, and adapting plans to reflect new realities. The future will belong to those organisations that treat resilience as a continuous process rather than a one-time achievement.

Conclusion: Service Continuity as a Public Mandate

For government agencies, supply chain resilience is about safeguarding the continuity of public services under any circumstances. It is about ensuring that communities can depend on essential services regardless of the challenges facing the systems that deliver them.

Building resilience requires leadership commitment, robust governance, informed planning, and a culture that values preparedness. It calls for strong relationships with suppliers, collaborative networks across jurisdictions, and a willingness to invest in capabilities that may never be fully tested until a crisis occurs.

The rewards of resilience are measured not just in operational efficiency, but in the trust and confidence of the citizens served. In an era where disruption is inevitable, that trust is one of the most valuable assets any government can hold. By embedding resilience into the heart of supply chain management, agencies can uphold their public mandate and deliver on their promise to protect and serve the community.