

Workforce Augmentation for Government

Senior cyber leadership on demand for population-scale programs and critical national infrastructure.

The problem we solve

Government cyber programs stall for one reason more than any other: the leadership and architecture roles at their core are the hardest in the market to recruit. A cyber uplift program without a program manager loses momentum; a program without a lead architect accumulates inconsistent design decisions; an enterprise security architect vacancy leaves projects queuing for design assurance. We fill these roles with experienced practitioners — embedded in your team, working under your direction, from day one.

The benefits

- Delivery momentum maintained — programs keep moving while permanent recruitment runs its course.
- Senior practitioners with decades of experience across critical national infrastructure: corrections, emergency services, utilities SCADA, government health and state government platforms.
- Familiarity with the Australian Government Information Security Manual, the Protective Security Policy Framework and the Essential Eight.
- Independent of product vendors and system integrators — advice without bias.
- A deliberately narrow service catalogue: no incentive to expand scope. When the role is filled permanently, our job is done.

The roles we fill

Cyber Program Management

An experienced cyber program manager runs your cyber uplift or remediation program — planning, budgeting, vendor and stakeholder management, risk and dependency management, and executive reporting that stands up to boards and audit committees.

Lead Cybersecurity Architect on a Cyber Program

A senior architect provides the technical security leadership on your cyber program — target state architecture, security patterns, solution design assurance and technical direction for delivery teams, so security issues are anticipated rather than discovered.

Temporary Enterprise Security Architect Role Filling

We fill a vacant enterprise security architect position on contract — maintaining architectural governance, advising project teams and keeping design assurance moving until you recruit a permanent employee, with a clean handover to the incoming architect.

How engagement works

Engagements are on a pre-agreed hourly or daily rate, with or without a retainer and associated service levels. Our people work under your direction, within your governance and security clearance processes, on your systems.

Why CyberShield Government

Why do we do this?

We make a difference to the security of the services and infrastructure that every Australian relies on.

Public sector focus

We work exclusively with the public sector, on population-scale problems — systems and programs that serve millions of citizens — and on the protection of critical national infrastructure.

Senior-led

The person you meet does the work. No pyramid of juniors — an experienced practitioner is embedded in your team from day one.

Independent

We have no affiliations with product vendors or system integrators, so we can recommend the best course of action for your agency without bias.

An understanding of the machinery of government

Australian owned and operated — we understand government procurement, budget cycles and accountability structures, and the frameworks agencies operate under.

Experience where it counts

Our track record spans maximum security prisons, emergency services dispatch, utilities SCADA, state government platforms and government health shared services.

Engagement at a glance

Role	Typical trigger	Typical duration
Cyber Program Manager	Cyber uplift or remediation program funded but unstaffed, or program leadership departure mid-delivery.	6–18 months
Lead Cybersecurity Architect	Cyber program entering design or delivery without senior technical security leadership.	6–18 months
Enterprise Security Architect	Vacancy in an established enterprise security architecture function while recruitment is under way.	3–12 months