



Suburban Land Agency

Suburban Land Agency

Cyber Security Strategy

February 2024



Ngunnawal Country

We acknowledge the Ngunnawal people as traditional custodians of the ACT and recognise any other people or families with connection to the lands of the ACT and region. We acknowledge and respect their continuing culture and the contribution they make to the life of this city and this region.



ACT
Government

Suburban Land
Agency

Contents

04 Foreword

05 Overview

06 Why this Strategy is Needed

07 External and Internal Influences

08 Main Cyber Risks to SLA

09 How We're Going to Improve

10 What We're Going to Do

11 Our Vision

12 Cyber Security Strategic Pillars

17 Future State



Foreword

The Suburban Land Agency (SLA) is a trusted member of the Canberra community. The community in which we all live and work. To maintain this public trust, we must protect the information we hold and the services we provide. It's therefore a good time for SLA to review our cyber security readiness.

The importance of strong cyber security is essential for the successful operation of Government. SLA is no exception. Cyber criminals are becoming increasingly sophisticated in targeting governments and agencies. Therefore, we must respond through building our capability, innovation, enabling our people, and strengthening our partnerships.

For us to get to where we need, we must:

- Assess and fix potential weaknesses;
- Improve our security culture; and
- Meet ACT Government and community expectation with the secure conduct of business.

Therefore, I have commissioned this *Cyber Security Strategy* to ensure we achieve our objectives.

This Strategy will set in place a co-ordinated and holistic approach in strengthening SLA's defence against cyber-attacks. To continue to create great places where communities thrive, we must work together to protect SLA's place as a leader in delivering sustainable urban environments that bring people together and help our community.

Craig Gillman
A/g CEO
Suburban Land Agency



Craig Gillman



Overview

Organisations across the world are responding to the increasing volume and sophistication of cyber security threats. Criminal and nation-state actors continue to exploit the value of an organisation's data and systems to achieve their own ends. In response, SLA is undertaking a change program to uplift cyber security throughout the enterprise to fortify our defences and respond to the evolving threat environment. This change program will be driven by the Strategy and delivered according to four pillars of work. We will ensure that our governance, risk management and incident response is fit-for-purpose. We will explore new and innovative methods to harden the environment and strengthen investment in people and partnerships to deliver cyber secure outcomes into the future.

SLA is responsible for substantial transactions which attract interest from many financially motivated threat actors. SLA uses technology to secure financial transactions related to land sale, land lease, auctions and tender processes. To achieve these outcomes, we have digital engagement strategies to gather feedback, address concerns and incorporate community aspirations into land development plans.

SLA needs to align with the ACT Government cyber security policies and the evolving regulatory environment. By doing so, we can protect the sensitive Government and personal information we collect, receive and develop in the course of our work. This maintains the trust of the ACT Government and the ACT community, to conduct our operations with professionalism and integrity.

This cyber security change program supports our overarching Digital Transformation Program to ensure SLA responds to the evolving technological landscape.

Why this Strategy is Needed

According to the *2021-2022 Annual Cyber Threat Report*, the Australian Cyber Security Centre (ACSC) identified and reported the following trends:

- Over 76,000 cyber crime incidents were reported, which is an increase of 13 per cent from the previous financial year.
- During this period, common cyber incidents included fraud, financial and identity theft, and Business Email Compromise (BEC).
- BEC has caused cumulative financial losses of over \$98 million with an average loss of \$64,000 per report.
- There was a 25 per cent increase in the number of publicly reported software vulnerabilities.

It is becoming increasingly important for agencies to incorporate cyber security awareness and employ effective mitigation strategies. This has been a continued threat at SLA. SLA staff and Digital Solutions team have been successfully mitigating minor risks as and when it arises. As the bad actors become more sophisticated in their attacks, more needs to be done with the support of technology, resourcing and training to be proactive in our approach to keep up with, identify and block the malicious actors to protect our customer data and revenue streams .



External and Internal Influences

The following principles protect SLA from cyber threats and enable us to respond and recover if they occur.



Comply with Regulation

Regulations and frameworks evolve in response to the changing cyber landscape. SLA complies with these to protect our business, information, and reputation.



Meet Expectations of our People

Our people will be provided timely information and training to respond to cyber threats and incidents to protect SLA's business.



Protect our Third-Party Relationships

SLA collaborates with external stakeholders during day-to-day operations, like the purchasing and selling of land. We need to effectively manage risk to secure our information.



Respond to the Evolving Threat Landscape

SLA will instill a security-aware culture and cyber-safe practice as a part of our Business-As-Usual approach.



To Assure Business Continuity

SLA needs to ensure business continuity and improve our ability to plan for, respond and recover from cyber security incidents.








Protecting Public Trust

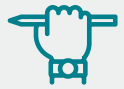
SLA has a commitment to Government and the public to protect sensitive information and enable land transactions and other day-to-day operations to occur securely.

Cyber Threats to SLA

SLA is exposed to the below threats and needs to effectively manage risk through education and mitigations that protect our systems and enable our operations.

Threat	Description	Mitigation Strategies
 <p>Business Email Compromise</p>	<p>BEC is a common attack vector where an adversary gains access to an organisation’s business email accounts. Compromised accounts are then often leveraged to steal sensitive information and to facilitate further phishing attacks against an organisation’s users or customers.</p>	<p>Implement phishing training for employees to identify suspicious emails. Leverage security awareness products to detect compromised user accounts for remediation.</p>
 <p>Insider Threat</p>	<p>Insider threats are users who may cause harm to an organisation by abusing their trusted access. They may cause harm through intentional or unintentional actions. This could be corporate espionage, negligence or inadequate training, such as users leaving devices unlocked, reusing passwords across accounts, or not adhering to IT policies.</p>	<p>Build a cyber-secure culture to recognise signs of malicious insiders. Ensure compliance with ACT Protective Security Framework and SLA’s acceptable use and IT policies.</p>
 <p>Data Breaches</p>	<p>A data breach is the loss of any amount of an organisation’s sensitive data. Data breaches vary in severity depending on the sensitivity of the information lost, such as classified or confidential information, financial data, or personally identifiable information.</p>	<p>Implement the SLA Cyber Security Incident Response Plan. Ensure appropriate data handling policies are implemented.</p>
 <p>Ransomware</p>	<p>Ransomware is a prevalent malware that encrypts an organisation’s documents to cause disruption to business operations. A ransomware group then attempts to extort an organisation into paying a ransom to have their files decrypted. If the organisation fails to pay the ransom this results in an organisations documents being published.</p>	<p>Maintain appropriate data backups. Ensure an organisation’s IT systems align with the recommended Essential 8 maturity levels set out in the Protective Security Framework. Implement the SLA Cyber Security Incident Response Plan.</p>
 <p>Supply Chain Compromise</p>	<p>Organisations who leverage third-party IT services may introduce vulnerabilities into their environment or risks to their sensitive data in the event of a compromise of a supplier’s IT systems.</p>	<p>Ensure all third-party systems are sufficiently secure and have had a cyber security assessment performed to assess any risk that may be posed.</p>

How We Are Going to Improve



Take Advantage of our Agility

The nature and smaller size of SLA provides us a unique opportunity. Through our business model, SLA is self-funded, being able to implement organisational changes and initiatives more rapidly than regular Government agencies. As a result, SLA is presented with the opportunity to streamline and self-govern business improvements and change programs.



Lay a Good Foundation

To effectively mitigate an incident, we must establish foundational security capabilities compliant with policy requirements and maintain trusted relationships with the ACT Government. We must leverage existing capability and information to access up-to-date threat advice. We will continue to work closely with strategic partners to further develop these foundations and be aware of our third-party dependencies to avoid unnecessary risk and loss of trust.



Building on Existing Governance

SLA developed four strategic pillars for this Strategy using key themes from each of the ACT Government's policies and legislative requirements.

What We're Going to Do

This Strategy is supported by a strategic vision statement to align with our organisational mission and remind us, at a high level, why this is important.



Our Vision



*Securing our agency and **thriving community** through cyber-safe innovation, leveraging **strong relationships** and enhancing our **security culture**.*

SLA is driven to enable and promote inclusive communities

SLA being a self-funded, smaller organisation allows for agility in moving towards an innovative approach to lead cyber security capability across **Government**

Through rigorous cyber security we can ensure **SLA's** business is respected, trusted and meets community and Government expectations.



Cyber Security Strategic Pillars

We will deliver against the vision through four strategic pillars to guide change and the future work program for our cyber security.



1

Fit-for-Purpose

- Ensure SLA's governance framework, policies, and Standard Operating Procedures (SOPs) consider ACT Government cyber security protocols including ACT Protective Security Framework.
- Conduct a gap-analysis to assess current SLA cyber security posture against industry standards.
- Apply cyber security protocols proportionate to the threat to maintain operational tempo and organisational efficiency.
- Assess SLA's ability to respond and then recover from a cyber crisis event.



2

Innovation

- Develop bespoke cyber policies, training and response to cultivate our own capability within SLA.
- Establish a risk assessment function to monitor cyber threats and trends, assess relevance to SLA and inform mitigations and risk tolerance.
- Seek opportunities to collaborate with industry peers nationally and potentially internationally.
- Explore the introduction of new capabilities including SIEMs, artificial intelligence, tool monitoring, and phishing campaigns.



3

People

- Promote a proactive cyber safe culture within the agency.
- Ensure employees are kept informed on cyber security issues through regular internal communications.
- Ensure SLA is appropriately resourced with a skilled workforce to respond to a rapidly evolving cyber landscape.
- Establish an annual cyber security training model for all staff.
- Ensure cyber security protocols and risk management is enshrined in the governance and performance framework with clear accountability.



4

Partnerships

- Leverage relationships with the relevant ACT Government stakeholders (ACTCSC and DDTS) and vendors.
- Continue to share responsibility for cyber security with ACT Government partners such as ACTCSC and DDTS.
- Manage any cyber risks within SLA's Standard Operating Procedures .
- Bolster risk mitigation by bringing cyber security to the forefront of Corporate risk and not be labelled as just an ICT issue.



Fit-for-Purpose

- SLA will invest in logical processes to manage relevant and likely cyber threats for any new cyber security measures.
- SLA will improve our incident response readiness through a risk-based approach that has a purposeful and resource-efficient application.
- SLA requires a risk assessment which will assess the effectiveness of current risk mitigations and tolerance for residual risk.
- SLA will review our governance framework, including the cadence of security reports to decision-making committees, clear accountability, and measure the effectiveness of risk mitigations.
- SLA will conduct a gap analysis and the Responsible, Accountable, Supportive, Consulted and Informed (RASCI) matrix to determine current cyber vulnerabilities.
- SLA's framework will need to incorporate incident response readiness, including crisis response, with clear reporting lines to enable accountability in the event of any potential compromise. This framework will improve the incident response readiness across SLA.



ACT
Government

Suburban Land
Agency





Innovation

- SLA will embed cyber security into initiatives to fortify our defences from the design stage through to implementation.
- SLA will review its business systems catalogue and architecture to ensure it is consistent with the ACT PSF's policy regarding ICT systems and system hardening.
- SLA will review and update current access control, onboarding and offboarding arrangements, administrator privileges, and a standardised approach to updates.
- SLA will investigate the use of emerging technologies, such as artificial intelligence options for reviewing and reporting of cyber incidents and analysing the viability of generative artificial intelligence to enhance SLA's business operations.
- SLA will explore opportunities to collaborate with industry peers to identify new and innovative approaches to common challenges.



People

- SLA is committed to establishing a cyber-safe culture across the agency whereby security behaviours and attitudes are reflected by all employees.
 - This will provide a human firewall to fortify security.
 - People are the first line of defence.
- We will enable our people through a comprehensive training and awareness campaign, in addition to the ACT Government Cyber Security Policy.
 - SLA will incorporate the recommendations from the *Cyber Resourcing Plan and Cyber Training Roadmap* to ensure the workforce and resourcing is cyber mature.
- SLA will refresh the approach to training in conjunction to strategic partnerships across Government. SLA will aim to uplift cyber training to reflect the technological knowledge and understanding of cyber risk that is required in today's interconnected world.
- SLA will conduct a review of roles and responsibilities to ensure cyber threats will be effectively managed.
- SLA will ensure that all employees are kept informed regarding cyber risks and recommended treatments.





Partnerships

- SLA will seek to strengthen partnerships in recognition of dependencies on shared services with ACT Government.
- SLA will need to leverage our strategic partnerships to collaborate on crisis response from the ACTCSC.
- Strong relationships will act as a force-multiplier in sharing crucial cyber security related information and managing threats.
- SLA will create a more robust governance structure with defined roles and responsibilities.
- SLA will investigate our cyber vulnerabilities posed through shared services and third-party vendors to prepare for a third-party compromise.
- SLA will take responsibility for its cyber security posture, leveraging its reliance on the ACT Government. This will require reviewing the policies and support from ACT Government to identify gaps in the requirements of SLA. SLA will work to address these gaps with bespoke initiatives to harden our own defenses.



ACT
Government

Suburban Land
Agency

Future State



Fit-for-Purpose

- SLA has become a leader in cyber security modelling best practice to other ACT Government stakeholders.
- SLA has developed and exercised an incident response that includes crisis communications.
- SLA has instituted cyber security into the governance framework with clear accountabilities and reporting to support effective management of risk.



Innovation

- SLA has harnessed innovation to fortify security with emerging technologies.
- SLA is an ACT Government leader in cyber security processes.
- SLA is actively exploring opportunities to collaborate with industry peers to share experiences and challenges.



People

- SLA has implemented the *Resourcing Plan and Training Roadmap* to help build cyber security awareness and culture.
- SLA has a cyber-secure work culture with a high level of cyber literacy.
- Staff are informed of cyber risks and understand the required treatment methods.
- SLA has conducted a gap analysis and built a RASCI matrix to identify key roles and responsibilities.



Partnerships

- SLA has strengthened our relationship with ACT Government.
- SLA has mapped our arrangements with third-party vendors to understand our dependencies.
- SLA has identified the gaps in the DDTS managed systems and SLA's own systems and implemented bespoke initiatives to address vulnerabilities.