Department of Customer Service

Cyber Security NSW Local Government Engagement Plan

November 2023

Version 2.0

NSW GOVERNMENT

01 Purpose

Cyber Security NSW is focused on delivering services to support the vision of a cyber-secure NSW Government. To achieve this, Cyber Security NSW:

- delivers products, services and best practice advice and guidance to NSW Government entities, including those in the local government sector
- coordinates whole-of-government cyber security strategies
- leads the NSW Government response to significant cyber security incidents and crises.

The Cyber Security NSW Local Government Engagement Plan outlines the model for engagement between NSW local government entities and Cyber Security NSW. Engagement encompasses the delivery of a wide range of tailored products, services and best practice advice and guidance to NSW local government entities.

The plan sets out a strategic approach to local government sector engagement that includes:

- 4 streams of engagement
- expectations of local government entities
- a prioritisation strategy
- challenges to consider.

02 Scope

This plan considers all NSW local government entities at all maturity levels. It does not consider NSW Government agencies outside of the local government sector.

03 Collaboration

In addition to providing services directly to NSW Government departments, agencies and local councils, Cyber Security NSW also collaborates with an array of stakeholders to support a cyber-secure NSW Government. This involves working closely with cyber security agencies across states, territories and nationally, and other relevant bodies.

To assist cyber security uplift in the local government sector, Cyber Security NSW collaborates with the Office of Local Government (OLG) and Local Government NSW (LGNSW).

For example, in 2022 Cyber Security NSW worked with the OLG to release the first iteration of the Cyber Security Guidelines for NSW Local Government. These guidelines outline the cyber security standards and controls recommended by Cyber Security NSW for NSW local government entities. Cyber Security NSW will update the guidelines annually, in line with the NSW Cyber Security Policy review and feedback from the OLG, LGNSW and local government entities.

Cyber Security NSW has established a schedule of engagement with the OLG, to ensure their input into local government sector cyber security uplift. This includes the commencement of quarterly Executive meetings in 2024 and a series of webinars on thematic areas such as risk management and incident response, to complement the well-established Local Councils Forum.

04

Principles of engagement

Purposeful

Cyber Security NSW will focus on clearly defined objectives from initiation of each engagement. Meaningful engagement will rely on knowledge of who we need to engage with, an understanding of the outcomes to be achieved, and which activities will be most effective to reach those outcomes.

Inclusive

Engagement will be undertaken in a way that enables all NSW local government entities to participate, regardless of factors such as size, location and cyber security maturity. A flexible approach to engagement ensures the inclusion of all NSW local government entities.

Timely

NSW local government entities will be informed of how and when they will be involved. Our engagement process will be clearly explained with the inclusion of proposed timelines and schedules.

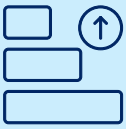
Respectful

Cyber Security NSW acknowledges and respects the expertise, perspective and needs of NSW local government entities. We will engage in a way that is open to alternative views and ideas. Our communication will be adapted to meet the needs and preferences of NSW local government entities wherever possible.

Transparent

Engagement with NSW local government entities will be open and honest. Our engagement process will be clearly explained, as will the role of NSW local government entities and how their input will inform the project. Clear expectations will be set and communicated from the outset of engagement.

Prioritised



A needs-based prioritisation process will be used to ensure engagement with NSW local government entities is effective. Engagement with NSW local government entities is prioritised to ensure outcomes are realistic, achievable and supported throughout the engagement.

Tailored

Cyber Security NSW acknowledges that each NSW local government entity has its own unique environment and circumstances. Through consultation, our approach will be tailored to enable the most efficient and productive service offerings for each NSW local government entity.

05 Levels of engagement

Dependent on the desired outcome, Cyber Security NSW will undertake the appropriate levels of engagement and service offerings. The following table provides advice on each of the engagement levels and examples of what each level might look like.

Inform	Consult	Involve	Collaborate
One-way communication to inform and educate the NSW local government entity.	Information and feedback sought from the NSW local government entity.	Cyber Security NSW works directly with the NSW local government entity through 2-way communication, ensuring the entity's issues and concerns are considered and understood.	Cyber Security NSW will work in partnership with the NSW local government entity to develop mutually agreeable solutions and a joint plan of action.
• Information disseminations • Presentations	• Surveys • Meetings	• Forums • Workshops • Inclusive decision-making processes	• Joint projects • Multi-council initiatives and partnerships

Cyber Security NSW engagement with NSW local government entities may include a single or multiple levels of engagement to meet the defined objectives.

06 Methods of engagement

Training

A key element in Cyber Security NSW engagement with local government entities is delivering cyber security awareness training for staff at all levels. Training is provided via 2 methods of engagement:

live sessions delivered virtually by Cyber Security NSW, and

e-module files that local government entities can install on their learning management system.

Forums

Forums provide a valuable opportunity for local government staff to exchange information relating to issues, trends and threats encountered through presentations and discussions. There are 3 forums available to local government entities:

Community of Practice (CoP): The quarterly CoP may be joined by any staff across NSW Government entities (including those in the local government sector) and is supported through a dedicated Teams channel.

Local Councils Forum: The Local Councils Forum is held twice a year and is similar to the CoP, but tailored with information relevant to local councils.

Cyber Security Awareness Working Group (CSAWG): The CSAWG meets quarterly. Membership is comprised of representatives from across NSW Government, including local government. It is designed for staff across NSW Government to discuss cyber awareness problems and solutions.

06

Consultation

Consultation is a vital part of Cyber Security NSW engagement with local government entities across the whole range of services provided. Consultation is undertaken via 2 main methods:

meetings and informal discussions – these may be face to face or virtual, and range from initial consultation with scoping and kick-off sessions, through to regular meetings for the duration of service provision, and review sessions at service conclusion

email – this includes correspondence providing guidance and advice, consultation around proposed or current service offerings, and reporting of cyber security incidents.

Disseminations

Information is regularly shared via document dissemination. This includes:

- intelligence and vulnerability products
- awareness materials
- policies and arrangements
- the Cyber Security NSW monthly newsletter.

Teams channels

There are 2 Teams channels – for the CoP and Local Councils – available to local government staff. These are used to support the forums and for the timely sharing of relevant updates and materials of interest to members.

Reporting cyber security incidents

NSW Government entities must report cyber security incidents to Cyber Security NSW via email or phone (reporting channel details are shared directly with local government entities).

06

Cyber Portal

The Cyber Portal is the front door for all NSW Government entities to request information and support from Cyber Security NSW. Through the platform, local government entities can:

request guidance, assessments, intelligence, resources, training, support and more

report cyber security incidents, receive updates and exchange files with the response team

access advanced dashboards that utilise built-in reporting mechanisms to better understand each entity's environment and allow for the tailoring of services.

Presentations

Cyber Security NSW staff present threat briefings and other cyber security presentations to specific local government areas or regions, at council conferences and at other relevant forums.

Events

Each year, Cyber Security NSW holds a number of events to which local government entities are invited to attend. These events include panel discussions, presentations and professional development opportunities, such as:

- CoP forums
- NSW Government Capture the Flag
- Cyber Security Awareness Month
- NSW Government Cyber Security Summit.

07 Streams of engagement

Cyber Security NSW engagement with local government entities falls under 4 streams. Thorough consultation with local government entities will be undertaken to identify which streams are most suitable. The application of the streams will be tailored to each entity.

Information on each of the services offered can be found in the Cyber Security NSW Service Catalogue.

Readily available

These services are readily available to all NSW local government entities:

- live cyber security awareness training
- cyber security awareness training e-modules
- adaptable training deck for in-house use
- access to an external learning platform
- awareness campaigns and materials
- templates and resources
- NSW Cyber Security Policy guidance
- Local Government – Cyber Security Guidelines
- whole-of-government advice
- best practice advice and guidance
- domain-based message authentication, reporting and conformance (DMARC) support
- threat assessments
- intelligence products (alerts, advisories, briefs and reports)
- vulnerability identification and remediation products
- CoP and other forums, including the Local Councils Forum.

07

Incidents

The incident stream is targeted at local government entities that are having or have had a cyber security incident. The following services focus on incident response and are provided as required:

- incident triage and containment, including assistance, coordination and advice
- team augmentation, such as providing resources for a dedicated amount of time to support security operations activities
- digital forensics
- dark web monitoring.

Risk and resilience

The maturity stream focuses on the long-term uplift of cyber resilience and risk management. This stream may be utilised either on the request of a local government entity or approach by Cyber Security NSW when an entity is identified as requiring assistance. Maturity services and products include:

- passive and intrusive external scanning
- internal vulnerability scanning
- penetration testing
- Essential Eight (E8) Health Checks
- password hygiene assessments
- key website monitoring
- open-source intelligence (OSINT)
- access to a vulnerability risk management platform
- assessment of vendor security risk
- ACSC vulnerability data, e.g. CHIPs and HOTCHIPs
- exercise-as-a-service (EaaS)
- policy advice
- strategic cyber security assurance
- strategic cyber security contract advice.

Executive

The executive stream focuses on improving the awareness and buy-in of the executive teams of local government entities. Executive services include:

- proactive engagement by Cyber Security NSW with local government executives, including through the Audit Risk and Improvement Committee
- guidance on how to promote awareness of cyber security issues within local councils and other local government entities.

08 Prioritisation and expectation

Services offered by Cyber Security NSW will be prioritised on an as-needed basis. In consultation with local government entities, Cyber Security NSW will assess risk and help determine what entities are most in need of support and which services will be most beneficial.

It is acknowledged that each local government entity has its own unique set of circumstances and needs. To ensure cyber risks are properly identified and prioritised, local government entities are expected to engage fully in the consultation process at the outset and throughout the entirety of the engagement. In some instances, the engagement will include a service level agreement.

09

Benefits of working with Cyber Security NSW

Effective governance controls

- Enhanced trust in government
- Strong cyber security foundation
- Effective, risk-based strategy

Reduced likelihood of compromise

- Improved cyber risk management
- Cyber-aware workforce
- Preventing cost of recovery

Proactive detection

- Vulnerabilities identified across assets
- Prioritisation of remediation actions
- Mitigation to prevent exploitation

Rapid response

- 24/7 support when incidents occur
- Expert advice and technical support
- Efficient and speedy remediation

Without Cyber Security NSW

- Poor cyber risk management
- Inconsistent approach to cyber security
- Under-resourced teams and controls
- Inexperienced cyber security incident responders
- Lack of centralised cyber security guidance

10

Council contacts

A central point of contact will be gathered from local government entities and saved in a central location. It is the responsibility of local government entities to ensure primary contact details are updated in the event of any changes.

11 Risks to effective engagement

The following potential barriers to effective engagement should be considered when enacting this plan.

Potential issue	Mitigation strategy
Large number of local government entities	Cyber Security NSW will work with local government entities to prioritise where assistance is most needed.
Differing capacity of local government entities	Cyber Security NSW will offer modified or different models of engagement according to what is identified during thorough scoping and consultation with each local government entity at the start of engagement.
Unclear purpose	The first stage of engagement will include thorough scoping and defining of services and intended outcomes. This process will be done in consultation with the local government entity.
Failure to review and evaluate	To assess if the approach is working, a review and evaluation of the engagement will be completed. This will enable ongoing improvement of engagement through lessons learnt. The broader Cyber Security NSW Local Government Engagement Plan will also be reviewed and its approach adjusted if needed.

12 Case studies

Case study 1:
Incident response

Cyber Security NSW received a notification from the ACSC that a local council had been subject to a ransomware attack. The local council had limited personnel resources and their IT was managed by a third-party organisation.

Liaising directly with the local council, Cyber Security NSW ensured the council had adequate incident response processes and resources. This involved collaborating with the ACSC and engaging contacts from the NSW Police Force Cybercrime Squad. Cyber Security NSW developed a profile on the threat actor and delivered the brief to the local council's responders, and conducted dark web monitoring of the threat actor's leaks site for exposed information.

Cyber Security NSW also liaised with ID Support NSW to manage the impact of personal information exposure. The local council rebuilt their systems, and investigation reports by the ACSC and the third-party incident responder were shared with Cyber Security NSW to supplement intelligence on the threat actor's methodologies.

Case study 2:
E8 Health Check

In May 2021, Cyber Security NSW informed a small regional local council of its vulnerability service offerings. The entity had recently been victim of business email compromise and was keen to take advantage of services they were unable to fund internally. Included was the E8 Health Check, which assesses an entity's cyber security maturity against the E8 mitigation strategies. The service covered 3 mitigation strategies: patch operating systems, patch applications and regular backups.

The E8 Health Check service involves the collection of data via forms, interviews, document analysis and authenticated vulnerability scanning data. This data is then analysed and a maturity assessment performed, with actionable findings identified to move towards a higher E8 maturity level. This is presented in a detailed report for the entity.

In June 2021, the entity requested our E8 Health Check service, with the primary focus being assessing their patching efforts. The engagement spanned several months due to the entity's limited capacity. In October 2021, Cyber Security NSW was able to begin analysis of all the data for the E8 Health Check assessment.

The assessment identified positive findings but the overall maturity of the 3 assessed mitigation strategies had a maturity level of 0. The report was provided to the entity, which detailed the findings, with quick wins in addition to longer-term, tailored improvement opportunities for the entity. The report was well received, and the entity was in full agreement with the findings.

In November 2022, Cyber Security NSW engaged with the entity to review progress made since the report findings. Cyber Security NSW was pleased to hear the entity had already actioned several of the suggestions and was working to complete all others. This included implementing a tool to assist with application and operating system patch management, improving vulnerability and asset management, scheduling backup restoration tests and decommissioning end-of-life operating systems. All of these mitigations will help the entity improve its cyber resilience.

Department of Customer Service

2/24 Rawson Place
Haymarket NSW 2000

Office hours:
Monday to Friday
9am - 5pm

E: info@cyber.nsw.gov.au
W: digital.nsw.gov.au/policy/cyber-security

NSW GOVERNMENT