Government of **Western Australia**
Department of **the Premier and Cabinet**
**Office of Digital Government**

# Cyber Security

Office of Digital Government

CISO Perth April 2023

## Points for discussion

- Executive discussions – are we safe?
- Governance principles (AICD & CSCRC)
- Risk Management
- Confidentiality, Integrity and availability of data
- Data retention
- Supply chain
- Cyber security skills
- Cyber security project vs security operations
- New Cyber Strategy
- Cyber Security Coordinator

*Cyber security is not an even playing field. Its cheap & easy for attackers and expensive and costly for defenders!*

## The Cyber Security Unit's Role

To lead, coordinate and support whole-of-government cyber security efforts to protect the WA Government's information, assets and service delivery from cyber threats.

## Responsibilities

1. Coordinating and supporting improvements to cyber security resilience across Government
2. Improving visibility of cyber security threats, vulnerabilities and controls across Government
3. Coordinating inter-agency operational responses to cyber security incidents
4. Leading the State's inter-jurisdictional cyber security engagement
5. Providing cyber security advice to Government

# WA Government Cyber Security Policy

- Role of the Accountable Authority in leading cyber security
- **Assign Cyber Security responsibilities to an Executive**

- Understand organisational Cyber Security Context
- **Assess cyber risk**
- Plan to manage cyber risk


- **Integrate Cyber Security into Business Continuity Planning**
- Ensure adequate cyber security Insurance coverage to manage impact.
- Review and share lessons learnt from incident recovery.

Implement controls to manage risk:

- **Essential 8 Controls**
- **Top Strategies to Mitigate Cyber Intrusions**
- Vulnerability Management
- Secure Software Development
- Security Awareness
- Secure overseas travel
- **Supply Chain Security**
- Physical security of relevant assets
- Safe and secure disposal of digital assets

- Plan for how to respond to cyber incidents.
- Regularly test and exercise response plans.
- **Report incidents to the Office of Digital Government.**
- Review and share lessons learnt from incident response.

- Maintain event logs for critical systems
- Implement Intrusion Detection
- Process log data through a Security Information and Event Monitoring system.
- **Integrate with the Office of Digital Government SIEM.**

# WA Government Security Operations Centre

**CAPABILITIES – Services to WA Government Organisations:**

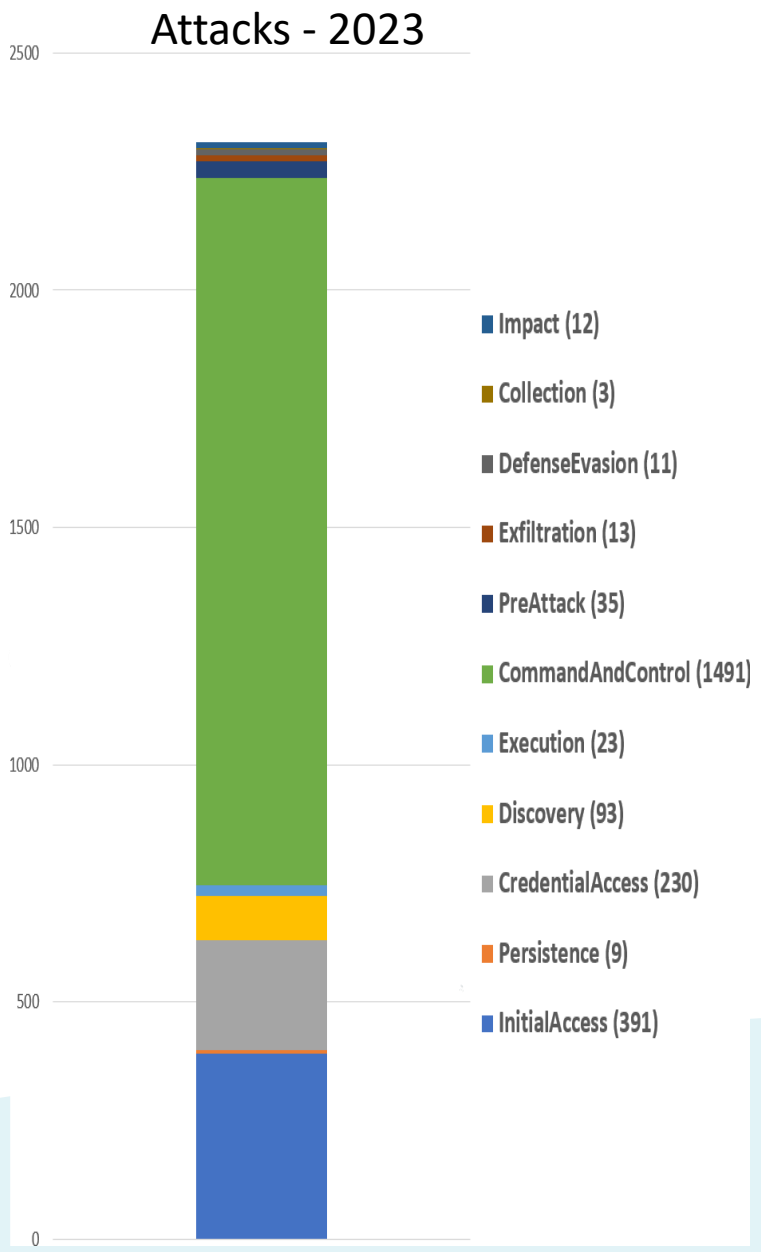
- 62 Agencies currently connected – more on the way
- Cyber security incident monitoring and analysis.
- Incident response coordination and advice.
- Threat intelligence alerts and advisories.

**COMMON ATTACKS – Targeting sensitive information, and disruption of services:**

- Targeting of internet facing services exploiting unpatched systems.
- Sophisticated phishing emails targeting staff to divulge their usernames and passwords.
- Business Email Compromise seeking to redirect payroll and payments to suppliers.
- New malware attacks using advanced tactics and techniques to bypass traditional defences.
- Accidental exposures of data.

**KEY INITATIVES**

- Improving detection capabilities.
- Central vulnerability scanning service to promptly identify exposed systems.
- Threat Intelligence Sharing Platform - between agencies, federal and interstate counterparts.
- Promotion of the secure internet connections - Australian Protective DNS service.



# Efforts to improve cyber security maturity

## Cyber Uplift Team

- Newly formed team that builds on existing efforts to assist agencies by:
  - Offering a catalogue of cyber security services, informed by the reported data.
  - Proactively engaging with agencies to help address their issues on a case-by-case basis; and
  - Create whole-of-sector solutions and guidance to solve issues at scale.

## Cyber Assurance

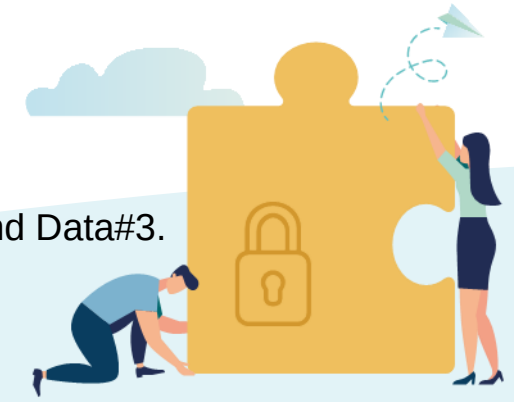
- Combined effort from the varied skills of the Cyber Security Unit:
  - Assessments against the Cyber Security Policy.
  - Design reviews for new systems and applications.
  - Cyber security testing and vulnerability assessments.

## Security Operations Centre

- Assist agencies with detecting and responding to cyber threats.
  - New centralised services to address common issues
  - Assist agencies in maturing their own processes, not just offering a central service.

## Data#3 Partnership (Project Fortify )

- Partnership between DGov, the Department of Finance, and a major ICT supplier, Data#3
- Three work streams designed to increase agency cyber maturity and understanding, developed by DGov and Data#3.
- 30 agencies are engaged with Fortify, most in multiple steams..
- Almost 60 projects are underway or have been completed, valued at $2.2m.
- Fortify 2.0 – Implementation time!



# Western Australian Government Cyber Security Incident Coordination Framework

Roles and responsibilities
Principles
State Emergency Management Arrangements
Interjurisdictional Coordination
Reporting incidents
Support to Ministers
Exercising

| | |
|---|---|
| NCSA-5 **Normal Conditions** | NCSA-5 is the baseline NSCA Level which establishes a normal state of readiness. NCSA-5 is typical of a normal day-to-day cyber threat that is managed with existing capability and capacity, with no additional resources or capability required. |
| NCSA-4 **Lean Forward** | A cyber threat that necessitates precaution via increased monitoring and analysis, and strategic coordination and engagement at the national level. |
| NCSA-3 **Alert** | A cyber threat that requires immediate monitoring, analysis and strategic coordination at the national level. The situation may also require incident, preparation and response activity in one or more jurisdictions. |
| NCSA-2 **National Cyber Incident** | A cyber threat that significantly impacts or has the potential to impact multiple Australian jurisdictions, and/or requires an immediate and coordinated inter-jurisdictional response, including potential for national resource sharing. |
| NCSA-1 **National Cyber Crisis** | A significant cyber threat that necessitates a collective, strategic approach to response. Requirement for nation-wide crisis management. |

## Cyber Event

**Agencies and MSPS**
- Periodic reporting to agency's Corporate Executive
- Reporting to DGov of abnormal increases in cyber events

## Cyber Incident

**Agencies and MSPS**
- Manage incident in accordance with its incident management plan
- Notify DGov of incident within 24 hours of detection
- Report applicable incidents to WA Police and ACSC and coorperate with any investigation
- Inform RiskCover of Incident

**DGov**
- Notify ACSC of incidents (and liase if required)
- Liase with WA Police and ACSC
- Coordinates interagency information sharing on reported incidents and inter-jurisdictional coordination, if required.
- Supports coordinated public information, if required.

## Significant Cyber Incident

**Agencies and MSPS**
- Manage incident in accordance with its incident management plan
- Notify DGov of incident as soon as practicable
- Report applicable incidents to WA Police and ACSC and coorperate with any investigation
- Inform RiskCover of Incident

**DGov**
- Notify ACSC of incidents (and liase if required)
- Liase with WA Police and ACSC if required
- Coordinates interagency responses to significant incidents or crises
- Provides inter-jurisdictional coordination, if required
- Provides Ministerial-level coordination, if required
- Provides coordinated public information, if required

**DG ICT Council**
- Strategic-level coordination by GC ICT Council, if required

## Cyber Crisis

**Agencies and MSPS**
- Manage incident in accordance with its incident management plan
- Notify DGov, WA Police and ACSC of significant developments

**DGov**
- Notify and liase with the ACSC
- Liase with WA Police and ACSC if required
- Leads the coordination of operational-level incident
- Inter-jurisdictional coordination
- Ministerial-level coordination
- Coordinated public information

**DG ICT Council**
- Strategic-level coordination by GC ICT Council, if required

# Cyber Security Unit
## Office of Digital Government