Australian Government
Australian Signals Directorate

ASD

The Commonwealth Cyber Security Posture in 2023

REPORT TO PARLIAMENT
NOVEMBER 2023

Use of the Coat of Arms

The Commonwealth Coat of Arms is used in accordance with the April 2014 *Commonwealth Coat of Arms: Information and Guidelines*, published by the Department of the Prime Minister and Cabinet and available online (http://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Website

www.cyber.gov.au

Contact us

Feedback about this report is welcome and should be directed to:

Phone

1300 CYBER1 (1300 292 371)

Email

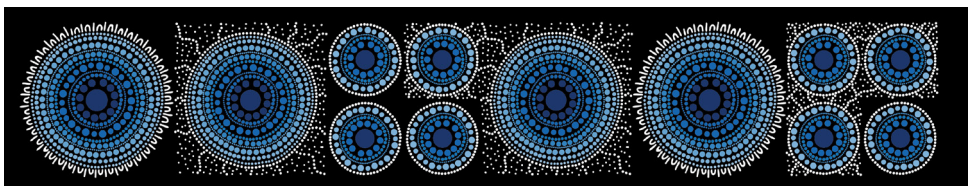
asd.assist@defence.gov.au

Post

PO Box 5076, Kingston ACT 2604

Acknowledgement of Country

We acknowledge the Traditional Owners and Custodians of Country throughout Australia and their continuing connections to land, sea and communities.
We pay our respects to them, their cultures and their Elders; past, present and emerging. We also recognise Australia's First Peoples' enduring contribution to Australia's national security.



Contents

Executive summary 1
1. Introduction 4
2. Cyber security hardening 7
3. Incident preparedness and response 14
4. Leadership and planning 16
5. Building Australian Government cyber security 18
6. Conclusion 23

List of Figures

Figure 1: Percentage of entities with *Essential Eight* Maturity Level 2 or higher (*Essential Eight* plus compensating controls) 10
Figure 2: Percentage of entities with *Essential Eight* Maturity Level 2 or higher (*Essential Eight* strategies only) 10
Figure 3: Implementation of email domain security 13
Figure 4: Implementation of email encryption 13
Figure 5: Implementation of website encryption 13
Figure 6: Dormant websites 13
Figure 7: Indicators to entities' cyber security incident preparedness and response 15
Figure 8: Indicators or entities' leadership and planning 17

Executive summary

The *Commonwealth Cyber Security Posture in 2023* (hereafter 'the report') informs Parliament on the implementation of cyber security measures across the Australian Government for the 2022–23 financial year. According to the *Flipchart of PGPA Act*[1] *Commonwealth entities and companies*,[2] as of 30 June 2023 the Australian Government comprised 100[3] non-corporate Commonwealth entities (NCEs), 72 corporate Commonwealth entities (CCEs) and 17 Commonwealth companies (CCs); totalling 189 Australian government entities.[4]

The information included in this report is primarily derived from the annual *Australian Signals Directorate (ASD) Cyber Security Survey for Commonwealth Entities* (hereafter 'the ASD survey'). In 2023, 87 per cent of government entities responded to the ASD survey, a decrease from 92 per cent of entities who responded in 2022. Data collected by ASD in the performance of its cyber security function supplements the survey information.

This report also references findings of the *Protective Security Policy Framework Assessment Report 2021–22*[5] (hereafter 'the PSPF Assessment Report') published by the Attorney-General's Department (AGD). *PSPF Policy 10: Safeguarding data from cyber threats* (Policy 10) addresses strategies to mitigate common and emerging cyber threats. As of 1 July 2022, Policy 10 requires that entities implement all of the ASD's *Essential Eight* cyber security strategies to Maturity Level 2. The 2023 report is the first to assess Commonwealth cyber security since this requirement was updated.

For the purposes of this report, an entity's cyber security posture is considered against the following criteria:

- Cyber security hardening: An entity's implementation of cyber security technical mitigations, primarily the *Essential Eight* [6] mitigation strategies, to reduce the likelihood of an information and communications technology (ICT) system being compromised.
- Incident preparedness and response: An entity's readiness to respond to a cyber security incident, and actions when a cyber security incident occurs.
- Leadership and planning: An entity's leadership engagement with cyber security and broader cyber security culture.

1. 'PGPA Act' refers to the *Public Governance, Performance and Accountability Act 2013.*
2. *Flipchart of the PGPA Act entities and companies*, PGPA Act Flipchart and List | https://www.finance.gov.au/government/managing-commonwealth-resources/structure-australian-government-public-sector/pgpa-act-flipchart-and-list.
3. The number of NCEs quoted includes the Australian National Preventive Health Agency. This agency is listed on the PGPA Flipchart; however it ceased operations in 30 June 2014, and is therefore excluded from all assessment described in this report.
4. The total number of Australian government entities increased from 185 at the end of the 2021-22 financial year.
5. *PSPF Assessment Report 2021–22*, Protective Security Policy Framework (PSPF) Assessment Report 2021–22 | Protective Security Policy Framework.
6. *Essential Eight*, Essential Eight | Cyber.gov.au.

New information has been included in this year's report, to supplement information provided in preceding reports.

- Cyber Hygiene Improvement Programs (CHIPs) results have been reported at the entity level, in addition to being reported at the server or domain level. This provides insight into the proportion of entities that have effectively implemented a security measure, as well as the measure's implementation across federal government networks, overall.
- This report includes statistics relating to the use of legacy systems, generated from new questions incorporated in the ASD survey. These questions were added in response to work conducted across the Australian Government to better define and quantify the use of legacy systems in government networks.
- This report includes a statistic on the existence of funded cyber security improvement programs across Australian government entities, generated from new questions incorporated in the ASD survey. This information provides an insight into entities' efforts to improve their cyber security.

Findings presented in this report indicate that the cyber security posture across federal government entities is well-established in some areas, and requires improvement in others.

a. The proportion of government entities that reached Overall Maturity Level 2 across the *Essential Eight* mitigation strategies has improved. In 2023, 25 per cent of entities reached Overall Maturity Level 2 when compensating controls are taken into account, increasing from 19 per cent in 2022.

b. Between 2022 and 2023, the proportion of government entities applying effective email domain security and website encryption increased, as measured by ASD's CHIPs. However, the proportion of government entities applying effective email encryption decreased, as did the proportion of entities hosting only valid websites on their web servers.

c. The majority of entities had planned for a cyber security incident, and were ready to respond if needed. In 2023, 82 per cent of entities reported having an incident response plan, an increase from 79 per cent in 2022; of those 90 per cent had updated it within the past two years, and 69 per cent exercised it at least every two years.

d. The percentage of entities reporting cyber security incidents to ASD declined over the 2022–23 financial year. In 2023, 42 per cent of entities indicated that they report at least half of the cyber security incidents observed on their networks to ASD, compared with 51 per cent of entities in 2022.

e. Indicators of cyber security leadership and planning remained high, and showed improvement across entities. In 2023, 73 per cent of entities had a cyber security strategy, an increase from 72 per cent in 2022; and 83 per cent addressed cyber security disruptions in their business continuity and disaster recovery planning, an increase from 82 per cent in 2022.

f. The proportion of entities that provided annual cyber security training to their workforce increased over the 2022–23 financial year, with 78 per cent of entities providing this training in 2023, compared with 68 per cent in 2022. However, the proportion of entities providing privileged user training (PUT)[7] at least annually remains low at 39 per cent.

The Australian Government continues to improve its cyber security posture. The government has committed $9.9 billion over a decade to fund the Resilience, Effects, Defence, Space, Intelligence, Cyber Enablers (REDSPICE) program; this funding commenced 1 July 2022. Through this program, ASD will deliver forward-looking capabilities essential to maintaining Australia's strategic advantage and capability edge. This builds on existing investment under the Cyber Enhanced Situational Awareness and Response (CESAR) Plus Program, which funds the delivery of ASD defensive cyber capability from July 2020 to June 2030.

In order to improve their overall cyber security posture, it is recommended that entities:

- continue to implement the *Essential Eight* mitigation strategies across their networks to at least Maturity Level 2
- implement effective email domain security, email encryption, and website encryption, as recommended by the *Information Security Manual* (ISM), and decommission dormant websites hosted on their web servers
- maintain an incident response plan, and exercise it at least every two years
- increase cyber security incident reporting to ASD
- provide PUT to their privileged users on an annual basis.

7. PUT is training tailored to personnel with responsibilities beyond that of a normal user, Guidelines for Personnel Security | Cyber.gov.au.

1. Introduction

The threat of malicious cyber activity to Australia's national security and prosperity is very real. Improving the cyber security of Australia's public, private and civil sectors is a priority of the Australian Government. The implementation of preventative cyber security measures is by far the best way to help secure Australian networks.

The report focuses on the cyber security posture of Australian Government entities. Government networks provide essential services to the Australian public, while holding the sensitive personal identifiable information (PPI) of a large proportion of the population. The Australian Government is committed to uplifting the cyber security of its ICT networks.

The Australian Government plays an important role in monitoring, shaping and enabling cyber security across the economy. In particular:

- ASD's Australian Cyber Security Centre (ACSC) provides cyber security advice and assistance to Australian governments at the federal, state, territory and local levels; business and critical infrastructure; as well as communities and individuals.
- The Department of Home Affairs leads Australia's national cyber security policy and strategy, driving improvement to cyber security policy across government and industry.
    - On 23 June 2023, the Government appointed the first National Cyber Security Coordinator, to lead national cyber security policy, the coordination of responses to major cyber incidents, whole of government cyber incident preparedness efforts and the strengthening of Commonwealth cyber security capability.
- During the reporting period, AGD managed the Protective Security Policy Framework (PSPF), which sets out government protective security policy and supports entities' implementation of that policy. This function has since moved to the Department of Home Affairs.
- The Digital Transformation Agency (DTA) drives digital transformation across government by providing strategic and policy leadership, and investment advice and oversight.

Within this context, entities are responsible for maintaining the cyber security of their data and networks. Specifically, each entity is responsible for the security of its own ICT systems pursuant to the *Public Governance, Performance and Accountability Act 2013* (Cth) (PGPA Act).

This report provides an assessment of the cyber security posture of entities as at 30 June 2023. It is the fourth such report to be tabled before the Parliament.

1.1 Key findings of this report

The key findings of this report indicate that most government entities have well-developed processes relating to cyber security incident preparedness and response, as well as strong cyber security leadership and planning. However, further work is required with regards to hardening ICT networks against malicious cyber activity. A lower proportion of entities are reporting the majority of their cyber security incidents to ASD than in 2022, potentially diminishing ASD's visibility of the cyber security threat environment.

1.1.1 Cyber security hardening

According to the ASD survey, the proportion of government entities that had reached the recommended maturity across the *Essential Eight* mitigation strategies is increasing, but remains low.

- 25 per cent of entities reported reaching *Essential Eight* Maturity Level 2 when compensating controls were taken into account, an increase from 19 per cent in 2022.
- 17 per cent of entities reported reaching *Essential Eight* Maturity Level 2 without considering compensating controls, an increase from 11 per cent in 2022.

This improvement in the overall *Essential Eight* maturity occurred in the context of updates to the *Essential Eight Maturity Model*, which strengthened the requirements to meet Maturity Level 2 and made it more difficult to achieve.

The proportion of government entities applying effective email domain security and website encryption, as measured by ASD's CHIPs, increased over the year. As of May 2023:

- 39 per cent of entities used effective email security, an increase from 33 per cent in 2022
- 10 per cent of entities used effective website encryption, an increase from 4 per cent in 2022.

However, as of May 2023:

- 18 per cent of entities used effective email encryption, a decline from 20 per cent in 2022
- 33 per cent of entities hosted only valid websites on their servers, and had removed any dormant websites, a decline from 40 per cent in 2022.

1.1.2 Incident preparedness and response

Responses to the ASD survey indicated that the majority of entities had planned for a cyber security incident, and were ready to respond if needed.

a. 96 per cent of entities had identified the systems and data most essential to their business, an increase from 94 per cent in 2022.
b. 82 per cent of entities had an incident response plan, an increase from 79 per cent in 2022.
c. 83 per cent of entities had a security information and event management (SIEM) program or similar, an increase from 60 per cent in 2022.

However, the percentage of entities reporting cyber security incidents to their senior executive and ASD declined.

a. 72 per cent of entities indicated they had reported at least 80 per cent of incidents to their senior executive, a decrease from 80 per cent in 2022.
b. 42 per cent of entities reported at least 50 per cent of incidents to ASD, a decrease from 51 per cent in 2022.

1.1.3 Leadership and planning

Indicators of cyber security leadership and planning remained high.

a. 73 per cent of entities reported having a cyber security strategy, an increase from 72 per cent in 2022.

b. 83 per cent of entities reported that they had addressed cyber security incident disruptions in business continuity and disaster recovery planning, an increase from 82 per cent in 2022.

c. 80 per cent of entities were participating in ASD's Cyber Security Partnership Program, an increase from 75 per cent in 2022.

d. 82 per cent of entities reported having a funded body of work planned to improve their cyber security.[8]

A greater proportion of entities are providing annual cyber security training: however, the annual provision of privileged user training remains low. According to the ASD survey:

a. 78 per cent of entities provided cyber security training to their workforce at least annually, an increase from 68 per cent in 2022

b. 39 per cent of entities provided privileged user training at least annually, an increase from 34 per cent in 2022.

1.2 About this report

This report is prepared in response to a 2017 recommendation from the Joint Committee of Public Accounts and Audit (JCPAA),[9] that ASD and AGD report annually on the Commonwealth's cyber security posture to Parliament.

The data in this report is primarily derived from the *ASD Cyber Security Survey for Commonwealth Entities* (ASD survey). ASD conducts annual surveys of federal government entities regarding their cyber security practices. NCEs are required to respond to the survey under *PSPF Policy 5: Reporting on Security*,[10] while CEs and CCs are encouraged to participate. In 2023, 87 per cent of all federal government entities participated in the survey. This report focuses on the 2023 survey, while drawing on the 2021 and 2022 surveys for context.

This report also references findings from the PSPF Assessment Report for the 2021-22 financial year. Each financial year, NCEs must report on their security posture, with particular reference to the implementation of government policies under the PSPF; the PSPF Assessment Report is an aggregated assessment of that data.

Any insight into the cyber security posture of individual entities made available to malicious cyber actors may increase the risk of those entities being targeted. As such, this report does not identify entities by name. All results have been anonymised and aggregated.

8. Questions on this topic were introduced to the ASD survey in 2023; as such, data is not available for prior years.
9. *JCPAA Report 467: Cybersecurity Compliance*, Report 467: Cybersecurity Compliance – Parliament of Australia (aph.gov.au).
10. *PSPF Policy 5: Reporting on security*, Policy 5: Reporting on security | Protective Security Policy Framework.

2. Cyber security hardening

The implementation of technical cyber security controls helps entities defend their ICT environments against cyber security threats, thereby avoiding costly remediation, system downtime, lost productivity, and loss of public confidence. This report assesses the cyber security posture of entities using two data sets:

- Responses to the ASD survey: Entities report on their progress implementing the controls recommended by the *Essential Eight*. Based on the responses, ASD calculates the entities' maturity levels.
- CHIPs results: CHIPs performs quarterly scans to detect key cyber hygiene indicators on entities' internet-facing systems and services.

2.1 The Essential Eight

The *Essential Eight* outlines a set of eight mitigation strategies designed to help entities reduce their likelihood of experiencing a cyber security incident, and the impact of an incident if it does occur.

The *Essential Eight* comprises the following eight mitigation strategies:

1. Application control
2. Patch applications
3. Configure Microsoft Office macro settings
4. User application hardening
5. Restrict administrative privilege
6. Patch operating systems
7. Multi-factor authentication
8. Regular backups.

The *Essential Eight Maturity Model*[11] describes four maturity levels (0 to 3). Maturity levels are calculated against each of the eight mitigation strategies, based on the implementation of the recommended controls. A network's Overall Maturity Level is equal to its least-mature strategy.

Higher levels of maturity are designed to defend against moderate-to-high degrees of sophistication in adversary tradecraft and targeting. As of July 2022, the PSPF mandates that NCEs implement the *Essential Eight* strategies to at least Maturity Level 2.

The *Essential Eight* recommends that entities implement the eight mitigation strategies using a risk based approach. Where strategies cannot be fully implemented, compensating controls may be used to manage the residual risk. As such, this report provides entities' maturity levels when compensating controls have been taken into account (Figure 1), as well as their maturity levels based on their implementation of the *Essential Eight* mitigation strategies alone (Figure 2).

11. *Essential Eight Maturity Model*, Essential Eight Maturity Model | Cyber.gov.au

2.1.1 Updates to the *Essential Eight*

In November 2022, ASD updated the *Essential Eight Maturity Model*, with relation to the 'Patch applications' and the 'Patch operating systems' mitigation strategies. The new recommendations were that:

- entities use an automated method of asset discovery at least fortnightly, to detect assets residing on their networks
- vulnerabilities scanners used by entities are to use up-to-date vulnerability databases.

These new recommendations were introduced to address entities' lack of visibility of assets on their networks. This lack of visibility, coupled with out-of-date vulnerability scanners, could result in assets remaining unpatched and prime targets for exploitation by malicious actors.

These changes may cause entities' *Essential Eight* maturity levels to decline if they did not have good visibility of their assets, or were not conducting regular asset discovery scanning.

2.1.2 Implementation of the *Essential Eight*

According to findings of the ASD survey, the proportion of entities that have reached Maturity Level 2 across all eight mitigation strategies has increased, but the proportion remains low.

a. 25 per cent of entities reached Overall Maturity Level 2 when compensating controls were taken into account;[12] an increase of 6 percentage points from 19 per cent in 2022.

b. 17 per cent of entities reached Overall Maturity Level 2 when relying on the implementation of Essential Eight controls alone; an increase of 6 percentage points from 11 per cent in 2022.

As shown in Figure 1 and Figure 2:

a. 'Regular backups' had been implemented to Maturity Level 2 by the highest proportion of entities (71 per cent with compensating controls, and 65 per cent without compensating controls).

b. 'Restrict administrative privileges' had been implemented to Maturity Level 2 by the lowest proportion of entities (40 per cent with compensating controls, and 28 per cent without compensating controls).

c. 'Configure Microsoft Office macro settings' had the greatest improvement in entities' implementation to Maturity Level 2. This level was reached by:

   - 64 per cent of entities when accounting for compensating controls, an increase of 20 percentage points since 2022 when 44 per cent of entities reached Maturity Level 2
   - 57 per cent of entities without accounting for compensation controls, an increase of 22 per centage points since 2022 when 35 per cent of entities reached Maturity Level 2.

12. In 2023, the ASD survey used updated questions regarding the use of compensating controls, seeking additional information on their application and how they were managed. This increases the level of rigour applied to the collection of this data, and the reliability of the results.

d. 'Patch operating systems' had the least improvement in entities' implementation to Maturity Level 2, when compensating controls were taken into account.
    - In 2023, 46 per cent of entities reached this maturity level, a decline of 1 percentage point since 2022 when 47 per cent of entities reached Maturity Level 2.
e. 'Patch applications' had the least improvement in entities' implementation to Maturity Level 2, when compensating controls were not taken into account.
    - In 2023, 37 per cent of entities reached this maturity level, a decline of 3 percentage points since 2022 when 40 per cent of entities reached Maturity Level 2.

Entities should assess their cyber security technical controls, to ensure they are achieving the desired effect. In 2023, 79 per cent of entities reported having mechanisms in place to assess the effectiveness of their technical controls.[13]

The use of legacy technologies[14] within a system can inhibit the implementation of the *Essential Eight*. In 2023, 76 per cent of entities reported the use of legacy technologies in their networks. Of these, 69 per cent indicated that the use of those technologies had impacted their ability to fully implement the *Essential Eight*.[15]

13. Questions on this topic were introduced to the ASD survey in 2023; as such, data is not available for prior years.
14. *PSPF Policy 11: Robust ICT systems*, (PSPF Policy 11), Policy 11: Robust ICT systems | Protective Security Policy Framework.
15. Questions on this topic were introduced to the ASD survey in 2023; as such, data is not available for prior years.

FIGURE 1: Percentage of entities with *Essential Eight* Maturity Level 2 or higher (*Essential Eight* plus compensating controls)

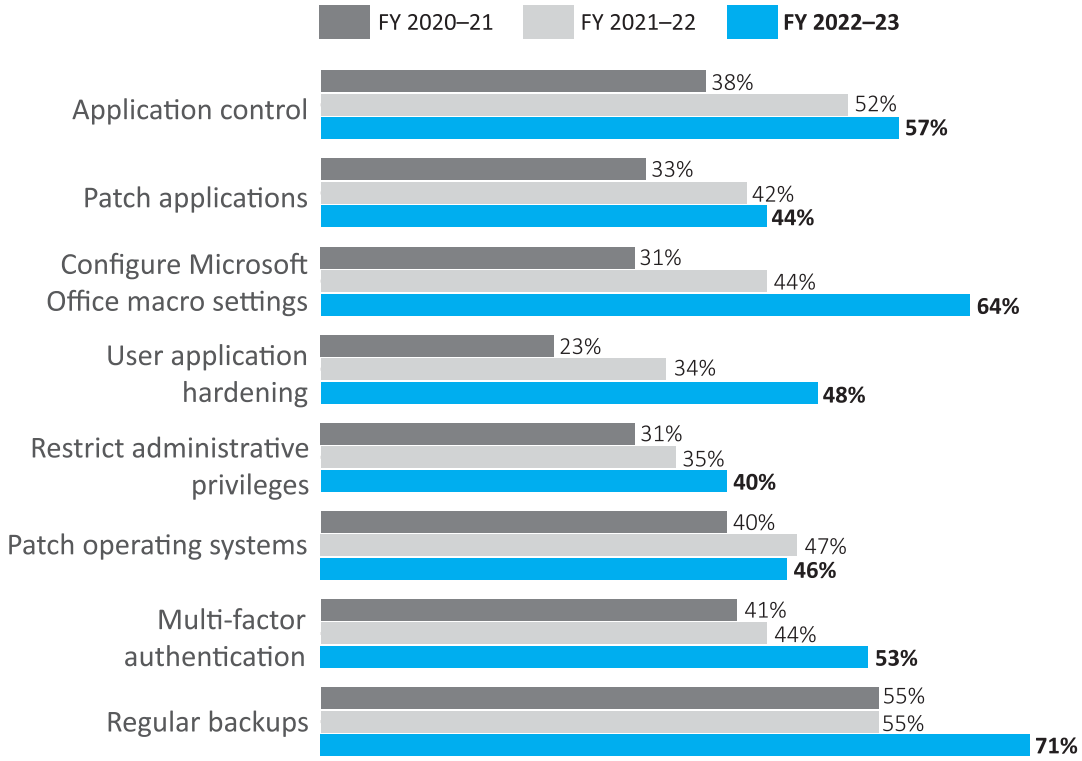
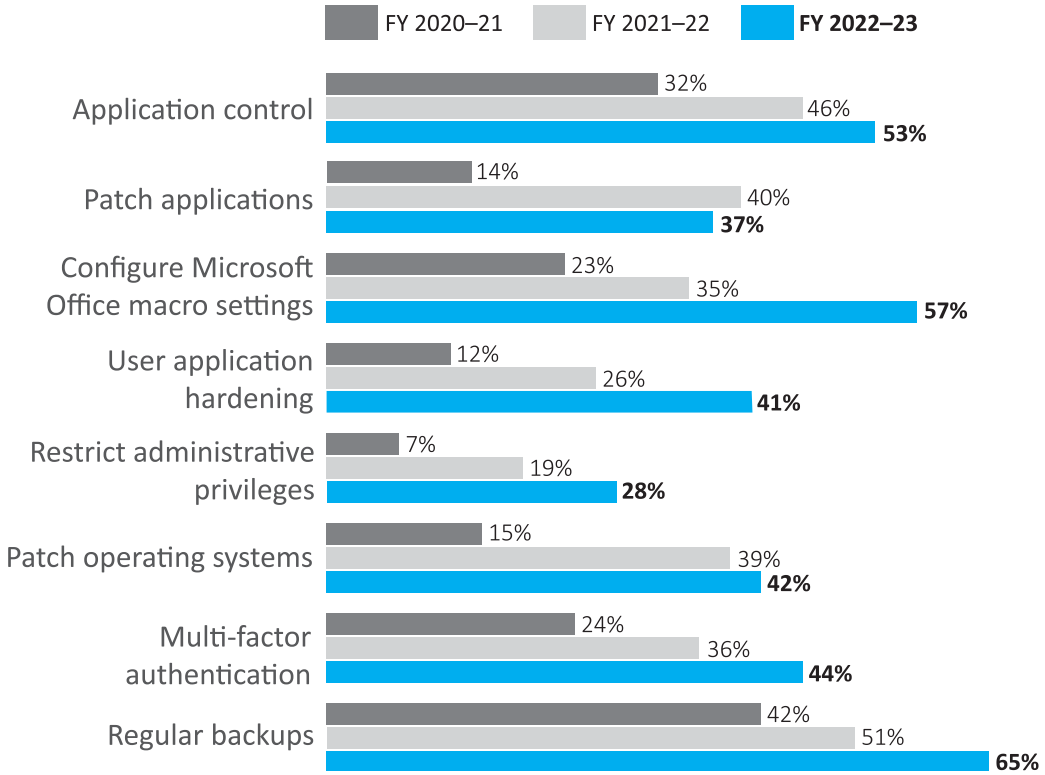


FIGURE 2: Percentage of entities with *Essential Eight* Maturity Level 2 or higher (*Essential Eight* strategies only)



2.1.3 *Protective Security Policy Framework Assessment Report 2021–22*

The PSPF, which is mandatory for all NCEs, includes two policies which specifically address cyber security posture.

- *PSPF Policy 10: Safeguarding data from cyber threats* (Policy 10)[16] addresses strategies to mitigate common and emerging cyber threats. Until 1 July 2022, the policy required entities to implement the ASD Top Four strategies to mitigate cyber security incidents; the Top Four is a subset of the *Essential Eight*. Since 1 July 2022, Policy 10 has required entities to implement the *Essential Eight* to Maturity Level 2.
- *PSPF Policy 11: Robust ICT systems* (Policy 11) focuses on safeguarding ICT systems to support the secure and continual delivery of government business. This includes safeguarding ICT systems from cyber threats by effectively implementing principles outlined in the ISM.[17]

Each financial year, NCEs must report on their security posture, with particular reference to the implementation of government policies under the PSPF; the PSPF Assessment Report is an aggregated assessment of that data. The 2021-22 PSPF Assessment Report indicated that:

- 25 per cent of entities had implemented Policy 10 to at least a 'managing'[18] level of maturity
- 44 per cent of entities had implemented Policy 11 to at least a 'managing' level of maturity.

The rate of Policy 10 implementation reported in the PSPF Assessment Report is higher than ASD's findings for the same financial year. The ASD survey found that 19 per cent of entities had implemented the *Essential Eight* to at least Maturity Level 2, taking into account compensating controls.

Some discrepancy between these results may be expected as the PSPF Report and the ASD survey use different assessment models to determine cyber security maturity. Additionally, the PSPF reporting only addressed the Top Four strategies, while ASD reporting assessed the implementation of the full *Essential Eight*.

2.2 Cyber Hygiene Improvement Programs (CHIPs)

Under the CHIPs program, ASD systematically scans domains and servers, including those associated with federal government entities, to find indicators that effective cyber security standards and protocols have been implemented.

16. *PSPF Policy 10: Safeguarding data from cyber threats*, Policy 10: Safeguarding data from cyber threats | Protective Security Policy Framework.
17. *Information Security Manual* (ISM), Information Security Manual (ISM) | Cyber.gov.au.
18. Under the PSPF self-assessment maturity model, a 'managing' level of maturity indicates a 'Complete and effective implementation of the PSPF'.

CHIPs scans for a range of indicators of cyber security, including the use of effective:

- security protocols on email domains[19]
- encryption on email servers[20]
- encryption on web servers.[21]

CHIPs scanning also determines whether web servers are hosting valid websites, as opposed to dormant websites which may be used to host malicious activity.[22]

This report addresses the proportion of:

- domains or servers that have implemented recommended minimum security measures, and
- federal government entities that have implemented those measures across at least 90 per cent of their servers or domains.

This is the first year this report has addressed CHIPs scanning at the entity level. The new analysis provides insight into entities' individual implementation of security measures, as well as the implementation of measures across federal government networks, overall. While this data was not available for the 2022 report, it has been generated retrospectively for this report using historical data.

The number of domains and servers managed by a given entity varies significantly. As such, an increase or decrease in the number of domains or servers implementing a given security measure is often not reflected at the entity level.

The following compares the CHIPs results from May 2022 and May 2023:

a. The implementation of effective email domain security (Figure 3):
   - by domain, decreased from 62 per cent in 2022 to 59 per cent in 2023
   - by entity, increased from 33 per cent in 2022 to 39 per cent in 2023.
b. The implementation of effective email server encryption (Figure 4):
   - by server, increased from 34 per cent in 2022 to 39 per cent in 2023
   - by entity, decreased from 20 per cent in 2022 to 18 per cent in 2023.
c. The implementation of effective website encryption (Figure 5):
   - by server, increased from 29 per cent in 2022 to 37 per cent in 2023
   - by entity, increased from 4 per cent in 2022 to 10 per cent in 2023.
d. The proportion of web servers hosting only valid websites, i.e. not hosting dormant websites (Figure 6):
   - by server, increased from 80 per cent in 2022 to 83 in 2023
   - by entity, decreased from 40 per cent in 2022 to 33 per cent in 2023.

19. Minimum recommended email domain security: The domain has a valid DMARC record, or has a valid DMARC record on its base domain, with an effective policy of 'reject' or 'quarantine'.
20. Minimum recommended email encryption: The website sends an HSTS header when accessed AND HTTPS is enabled AND no weak or insecure cipher suites are used AND users are redirected to an HTTPS connection AND the oldest supported version of TLS is 1.2 or higher AND client – initiated.
21. Minimum recommended web server encryption: The mail server supports Opportunistic TLS (STARTTLS) AND supports at least TLS 1.2 (but may also allow TLS 1.1 and TLS 1.0 for backwards compatibility) AND has a valid certificate AND offers at least one strong cipher AND offers no insecure ciphers.
22. Minimum recommended valid websites posture: According to existing indicators the website appears to be current and up to date.

FIGURE 3: Implementation of email domain security

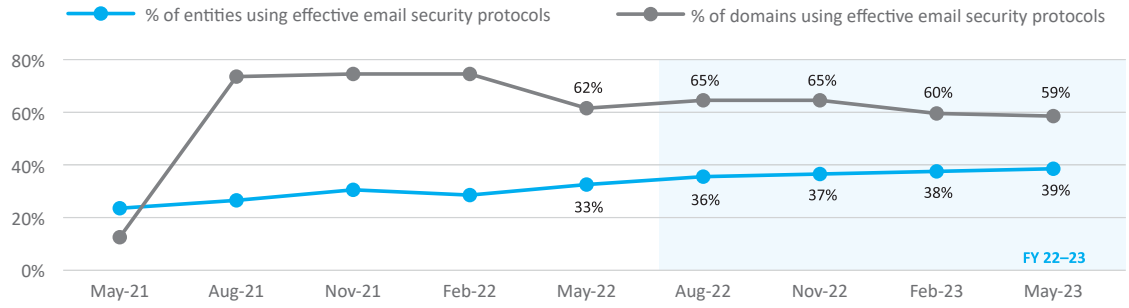


FIGURE 4: Implementation of email encryption

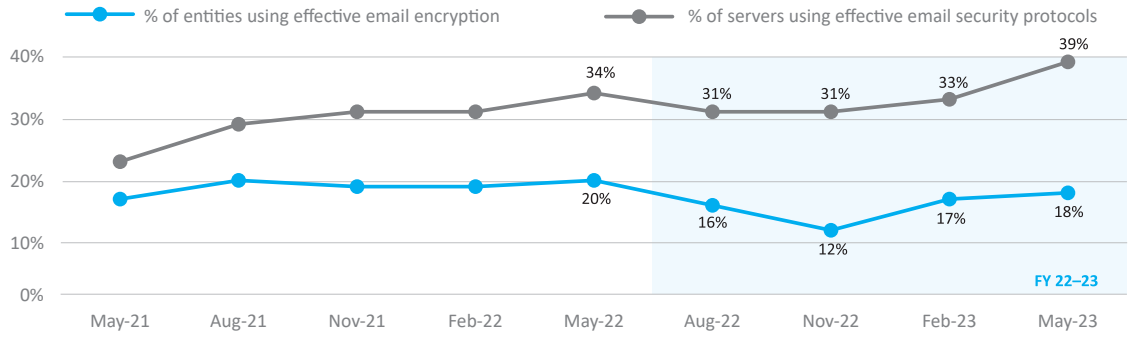


FIGURE 5: Implementation of website encryption

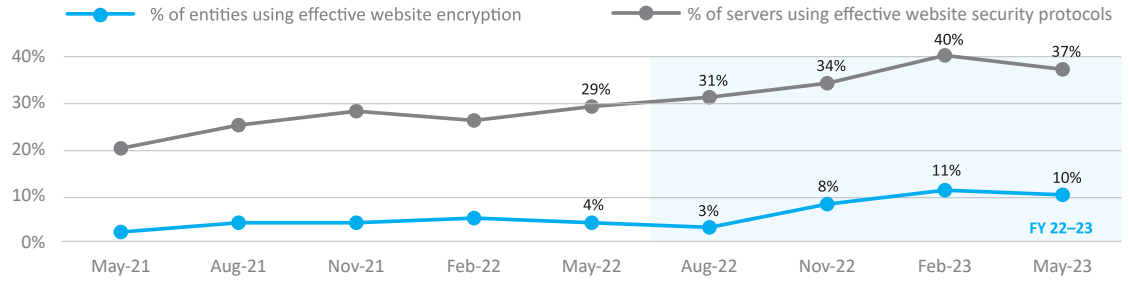
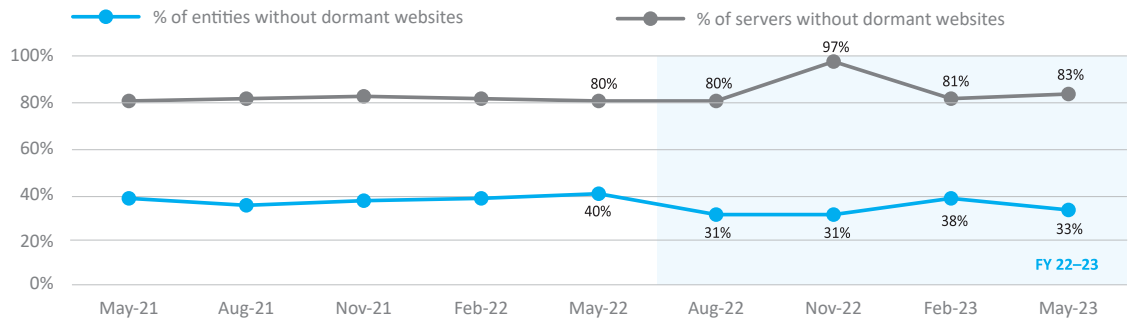


FIGURE 6: Dormant websites



3. Incident preparedness and response

Cyber security events and cyber security incidents are defined in the ISM, as follows:

- A cyber security event occurs when a system, service or network flags a possible breach of security policy, a failure of safeguards, or a previously unknown situation that may be relevant to security.
- A cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.

Cyber security incidents may result in the denial of access to, the theft of, or the destruction of systems and data. If not effectively managed, a cyber security incident may undermine public confidence in an entity, and the incident's remediation may consume significant resources.

Entities should plan for, and prepare to respond to, cyber security incidents. This includes identifying the data and systems essential to their business, accounting for cyber security incidents in business continuity planning, and developing and exercising an incident response plan.

It is essential that entities report cyber security incidents to ASD, to ensure those incidents are dealt with appropriately and that any impact is considered in full. According to *Policy 5: Reporting on security*, entities are required to report 'significant or reportable' cyber security incidents to ASD.

The Australian Government is a common target for malicious cyber activity. In the 2022–23 financial year, ASD received 348 cyber security reports from federal government entities; of these 52 related to confirmed cyber security incidents. Federal government reporting represents 31 per cent of all cyber security reporting, and 9 per cent of cyber security incident reporting, recorded by ASD.

3.1 Implementation of incident preparedness and reporting

In relation to incident preparedness and response, the cyber security posture of entities is assessed using responses from the ASD survey. The survey included questions designed to assess entities' levels of preparedness to respond to a cyber security incident, and their incident reporting behaviours.

Responses to the survey indicate that the majority of entities had planned for a cyber security incident, and were ready to respond if needed. As shown in Figure 7:

a. 96 per cent of entities had identified the systems and data most essential to their business, an increase from 94 per cent in 2022

b. 82 per cent of entities had an incident response plan, an increase from 79 per cent in 2022. Of these:
   - 90 per cent of entities had updated their plan within the last two years
   - 69 per cent of entities exercised their plan at least every two years.

c. 83 per cent of entities reported using a security information and event management (SIEM) program or similar, an increase from 60 per cent in 2022.

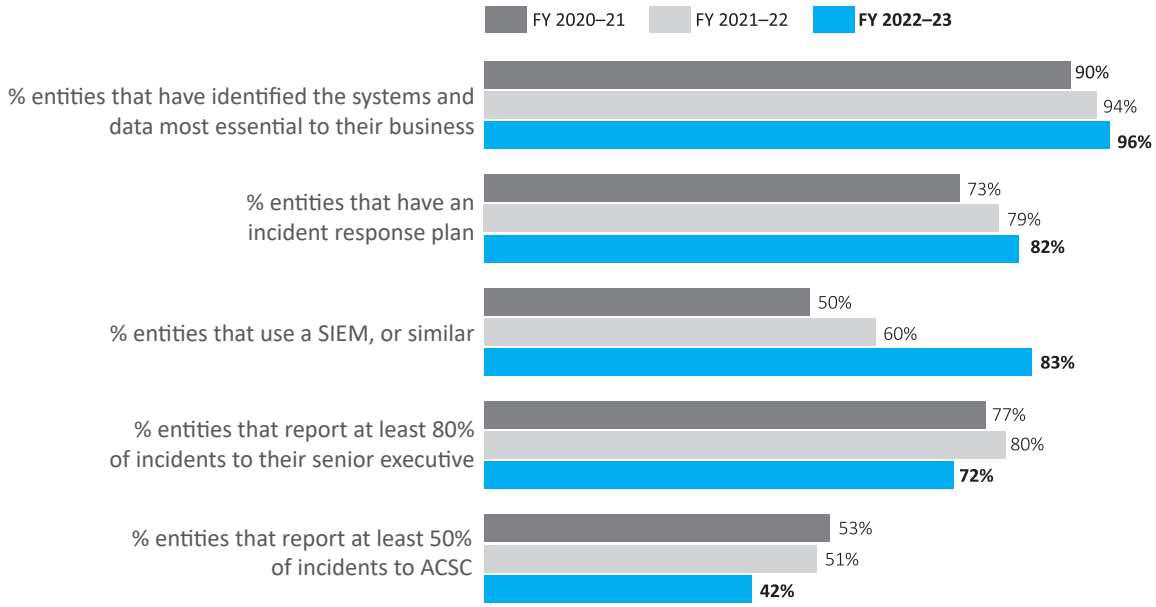
However, according to the survey, entities' reporting of cyber security incidents had declined:

a. 72 per cent of entities reported at least 80 per cent of cyber security incidents to their senior executive, a decline from 80 per cent in 2022

b. 42 per cent of entities reported at least 50 per cent of cyber security incidents to ASD, a decline from 51 per cent in 2022.

Under PSPF Policy 5, entities are required to report 'significant or reportable' cyber security incidents to ASD. The low rate may be due to a proportion of entities experiencing a high number of low-impact incidents that they do not consider to meet the PSPF reporting threshold.

FIGURE 7: Indicators to entities' cyber security incident preparedness and response



4. Leadership and planning

Strong leadership is essential in setting and maintaining a positive cyber security culture, and ensuring that cyber security remains part of an entity's planning and everyday business. In particular, the Chief Information Security Officer (CISO) plays a key role in setting the strategy and direction of an entity's cyber security program. CISOs are typically responsible for providing strategic guidance to their entity's cyber security program and ensuring compliance with cyber security policy, standards, regulations and legislation.

The broader workforce also plays a key part in maintaining cyber security, and entities should provide ongoing cyber security awareness training to all personnel to help them to best understand their cyber security responsibilities.

4.1 Implementation of leadership and planning

In relation to leadership and planning, the cyber security posture of entities was assessed through a series of ASD survey questions designed to provide indications of their cyber security leadership, planning and overall culture.

Over this financial year, survey responses indicated improvement in cyber security leadership and planning, as shown in Figure 8. Specifically:

a. 73 per cent of entities reported having a cyber security strategy, an increase from 72 per cent in 2022.

b. 83 per cent of entities addressed disruptions due to cyber security incidents in business continuity and disaster recovery planning, an increase from 82 per cent in 2022.

c. 80 per cent of entities participated in the ASD's Cyber Security Partnership Program,[23] an increase from 75 per cent in 2022.

Entities indicated they had undertaken forward planning with regards to cyber security. In the 2023 ASD survey, 82 per cent of entities reported having a funded body of work to improve their cyber security posture.[24]

The percentage of entities providing annual cyber security training has also increased.

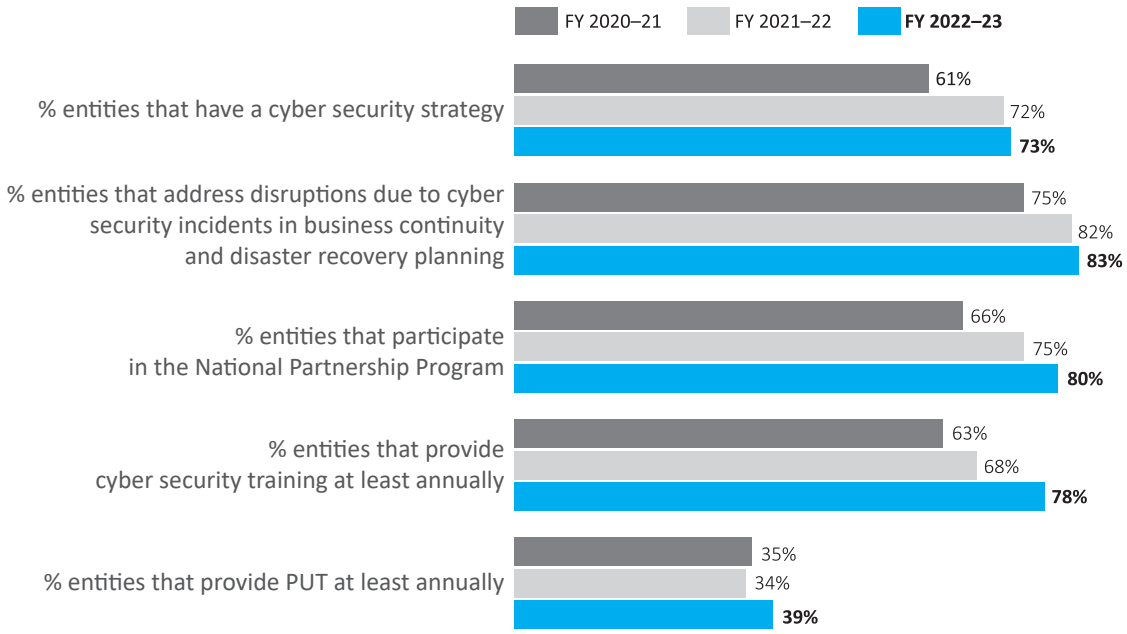
a. 78 per cent of entities provided cyber security training for their workforce at least annually, an increase from 68 per cent in 2022.

b. 39 per cent of entities provided privileged user training (PUT) at least annually, an increase from 34 per cent in 2022.

23. The National Partnership Program enables Australian organisations and individuals to engage with the ACSC and fellow partners to lift cyber resilience across Australia, ASD's Cyber Security Partnership Program | Cyber.gov.au.

24. Questions on this topic were introduced to the ASD survey in 2023; as such, data is not available for prior years.

FIGURE 8: Indicators or entities' leadership and planning



5. Building Australian Government cyber security

The Australian Government continues to build and improve its cyber security posture. The government has committed $9.9 billion over a decade to fund the Resilience, Effects, Defence, Space, Intelligence, Cyber Enablers (REDSPICE) program; this funding commenced 1 July 2022. REDSPICE responds to the deteriorating strategic circumstances in Australia's region, characterised by rapid military expansion, growing coercive behaviour and increased cyber attacks. Through this program, ASD will deliver forward-looking capabilities essential to maintaining Australia's strategic advantage and capability edge.

A key pillar of this program is Enhanced National Cyber Defence, which delivers improved critical infrastructure resilience against sophisticated cyber attacks; increased visibility of threats to Australia's critical systems; improved machine-time threat intelligence sharing across government and industry; and doubled persistent hunt and nation-wide cyber-incident response.

REDSPICE builds on existing investment under the Cyber Enhanced Situational Awareness and Response (CESAR) Plus Program, which funds the delivery of ASD defensive cyber capability from July 2020 to June 2030. This program was designed to boost protection and cyber resilience for all Australians.

This chapter outlines key systems and services delivered by ASD to support federal government entities to build their cyber security through the REDSPICE and CESAR Plus programs.

CASE STUDY: Effective prevention of cyber security risk: detection and mitigation of software vulnerabilities

In January 2023, a federal government entity engaged a cyber security company to conduct penetration testing on its systems. The company identified serious vulnerabilities in a software product used by the entity. The software was installed on the entity's network and was part of its Software-as-a-Service (SaaS) offerings.

Once informed of the vulnerabilities, the entity contacted other known users of the software, including other government entities. The entity also authorised the cyber security company to report the identified vulnerabilities to both the software vendor and ASD. ASD, using the CHIPs scanning capability, identified and informed other impacted entities that were operating the same software. ASD also warned international partners of the vulnerabilities.

The identification of the vulnerable software and the subsequent notification to impacted parties gave users the opportunity to mitigate the threat of potential exploitation, while the software vendor developed and released patches. As a result of these actions, no instances of compromise were detected.

5.1 ASD services supporting Australian Government cyber security

The following ASD services have been funded under the REDSPICE or CESAR Plus programs.

Cyber security hardening

Cyber security maturity assessment and uplift

ASD's Cyber Maturity Measurement Program (CMMP) assessments involve teams of technical subject-matter experts working with government entities to assess their cyber security maturity against the *Essential Eight* mitigation strategies, as well as assessing their broader cyber security posture. Entities are provided with a detailed report containing tailored advice and recommendations to improve their cyber security maturity.

ASD also assists government entities – through the provision of ASD ICT professionals – to implement cyber security controls, and provide advice and recommendations aligned with ASD's findings.

In the 2022–23 financial year, ASD undertook:

- 5 CMMP assessments with federal government entities, an increase from 3 assessments in the previous financial year.
- 13 uplift services for government entities to improve their cyber security hygiene, awareness, and implementation of a security roadmap, an increase from 5 in the previous financial year.

Cyber Hygiene Improvement Programs (CHIPs)

CHIPs measures the cyber posture and hygiene of government internet-facing systems and assets, by scanning external indicators of cyber security vulnerabilities. CHIPs provides quarterly reports to government entities detailing their vulnerabilities. These reports provide network owners with actionable information to help them to understand their vulnerabilities and inform cyber security posture improvement activities.

High-Priority Operational Tasking Cyber Hygiene Improvement Programs (HOT CHIPs)

HOT CHIPs conducts targeted scans in response to particular cyber security-related events. These scans build ASD's visibility of particular cyber security vulnerabilities across the Australian economy and offer network owners highly targeted, timely and actionable threat intelligence.

In the 2022–23 financial year, ASD performed 103 HOT CHIPS scans.

Active Vulnerability Assessments (AVA)

ASD's AVA capability identifies security vulnerabilities that may be used by a sophisticated cyber security actor. An AVA is a long-term engagement with high priority customers to simulate the presence of a sophisticated cyber adversary while remaining undetected on the customer's network. The outcome of the AVA activity allows customers to understand their vulnerabilities, and test their response to detecting unusual activity.

Hunt

ASD proactively conducts cyber threat hunt operations on critical Australian networks to detect intrusions by sophisticated cyber actors. This service is offered to high priority entities, including in support of events of national significance.

In the 2022–23 financial year, ASD conducted 2 hunt activities on priority government networks.

Sensor programs

The Host Based Sensor (HBS) Program and the Gateway Sensor Program Network (GSPN) provide visibility of the cyber security posture of Australian Government ICT systems by collecting telemetry data from government devices. They allow ASD to help entities identify weaknesses in their cyber security and detect intrusions on their ICT infrastructure and mitigate the consequences of compromise.

In the 2022–23 financial year, ASD supported:

- 8 new federal government entities to join the HBS program, bringing the total number of entities to 39
- 1 new federal government entity to join the GSPN program, bringing the total number of entities to 62.

CASE STUDY: Disruption of fake Australian government website

Malicious actors had established a fake Australian government website in an effort to harvest personal information from the Australian public. In some instances, the actors were able to steal the victim's login credentials as well as personal identifiable information (PII), including their full name, date of birth, residential address and bank details.

Drawing on a combination of public reporting and analysis of related data, ASD was able to fully characterise the fake website and define technical 'indicators of compromise' to assist entities self-identify any instances of the malicious activity on their own networks. The indicators of compromise were also fed into the Australian Protective Domain Name System (AUPDNS), a system designed to block malicious internet domains, further extending protection for the over 500 entities using the service.

A domain takedown request was also issued by ASD, and the malicious infrastructure was taken down by the website administrator.

Incident preparedness and response

Alerts and advisories

ASD publishes alerts and advisories to cyber.gov.au to inform Australians on cyber security threats and mitigations. Individuals may subscribe to the ACSC Alert Service to receive alerts via email.

Cyber Security Hotline

The Australian Cyber Security Hotline '1300 CYBER1' (1300 292 371) provides advice and assistance to Australian individuals and entities impacted by cyber security incidents. The hotline is available 24 hours a day, seven days a week.

National Exercise Program (NEP)

The NEP works in partnership with Australian critical infrastructure and government to scope, plan, deliver and evaluate cyber security exercises to improve Australia's overall cyber resilience. The NEP also delivers exercise management training workshops for industry and government.

In the 2022–23 financial year, ASD delivered 23 exercises for government and critical infrastructure organisations.

Incident response

ASD provides incident response services to all entities that have been compromised by malicious cyber actors. ASD prioritises deployment of specialised digital forensics and incident response services in response to incidents causing significant impact to Australia and/or incidents involving high-harm actors.

Cyber Threat Intelligence Sharing (CTIS)

ASD operates the CTIS platform. CTIS allows participating entities to share observable indicators of compromise (IOCs) at machine speed. Participating entities can use these IOCs to identify activity on their own networks. The CTIS platform also allows participating entities to share with other CTIS partners the IOCs observed on their own networks.

In June 2023, 12 per cent of federal government entities had joined the CTIS platform, an increase from 2 per cent in 2022.

Australian Protective Domain Name System (AUPDNS)

The AUPDNS uses threat intelligence to build a block list of known and assessed malicious web domains. These domains are often used to distribute malware, as part of malicious command and control channels, or as part of a data-exfiltration channel. AUPDNS prevents devices on subscribed networks from accessing the malicious domains on the block list, thereby interrupting potential malicious activity.

In June 2023, 24 per cent of federal government entities were using AUPDNS, a decrease from 26 per cent in 2022. This decrease is due to an increase in the total number of federal government entities, rather than a decline in the number of participating entities.

Leadership and planning

ASD's Cyber Security Partnership Program

ASD's Cyber Security Partnership Program works with Australian critical infrastructure and government to scope, plan, deliver and evaluate cyber security exercises to improve Australia's overall cyber-resilience.

CASE STUDY: Effective cyber security hardening post compromise

In February 2022, following a system compromise of a small federal government entity, ASD conducted a Cyber Maturity Measurement Program (CMMP) assessment of all IT systems connected to the entity's corporate network.

ASD identified and verified eight critical findings relating to specific vulnerabilities and weaknesses. A further 69 uplift opportunities related to the *Essential Eight* and general cyber security hardening and best practice were recommended as part of the assessment.

Following the CMMP assessment, ASD supported the entity to uplift its cyber security posture. This engagement, which spanned the 2022–23 financial year, focused on both short-term and long-term uplift activities relating to the implementation of the *Essential Eight* mitigation strategies, in addition to broader cyber security uplift activities.

Throughout the engagement, the entity worked with ASD productively and proactively, building a cooperative relationship while taking steps to improve its cyber security posture. As a result of this engagement, the entity has significantly increased the number of *Essential Eight* controls in place, and continues to implement ASD recommendations to further improve its cyber security posture.

6. Conclusion

The findings presented in this report indicate that entities' cyber security postures were well-established in some areas, and required improvement in others. In particular:

a. The proportion of government entities that had reached Overall Maturity Level 2 across the *Essential Eight* mitigation strategies had improved.

b. Between 2022 and 2023, the proportion of government entities applying effective email domain security and website encryption increased, as measured by ASD's CHIPs. However, the proportion of government entities applying effective email encryption decreased, as did the proportion of entities hosting only valid websites on their web servers.

c. The majority of entities had planned for a cyber security incident, and were ready to respond if needed.

d. The percentage of entities reporting cyber security incidents to ASD had declined over the 2022–23 financial year.

e. Indicators of cyber security leadership and planning had remained high, and showed improvement across entities.

f. The proportion of entities that provided annual cyber security training to their workforce increased over the 2022–23 financial year; however, the proportion of entities providing PUT at least annually remains low.

6.1 Report to Parliament 2024

The *Commonwealth Cyber Security Posture in 2024* report to Parliament will be delivered by November 2024.