THE COMMONWEALTH CYBER SECURITY POSTURE IN 2020

REPORT TO PARLIAMENT

May 2021

CONTACT DETAILS

Phone
Media enquiries: asd.assist@defence.gov.au
Cyber Security Hotline: 1300 CYBER1 (1300 292 371)

Website
www.cyber.gov.au
Location of this report www.cyber.gov.au

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

ASD Assist
Email: asd.assist@defence.gov.au
Postal: Australian Signals Directorate
Brindabella Park
PO Box 5076
KINGSTON ACT 2604

Executive Summary

The Commonwealth Cyber Security Posture in 2020 (the Report) informs the Parliament of the status of the Commonwealth's cyber security posture. Overall, the Report finds that Commonwealth entities continued to improve their cyber security in 2020. Commonwealth entities have responded efficiently to cyber security advice and assistance and have increased their cyber security posture through improved alignment with the Essential Eight *Strategies to Mitigate Cyber Security Incidents*, basic cyber hygiene and business practices, and responses to cyber security incidents.

The cyber threat environment has deteriorated in 2020. The Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC) has noted an increase in the number of cybercrime reports and cyber security incidents. In addition, the ACSC has noted an increase in frequency and sophistication of operations by a range of state-based actors and cybercriminal syndicates. The ACSC has also noted an increase in the speed in which malicious actors have researched and then pivoted to exploit publicly-released vulnerabilities.

Levels of cyber security maturity continue to vary across the Australian government and sustained effort is required for Commonwealth entities to meet the challenges of the evolving cyber threat environment.

Results from the *ACSC Cyber Security Survey* showed improvement in Commonwealth entity implementation of the Essential Eight strategies relating to user application hardening, application control, restricting administrative privileges and adopting daily backups. However, the baseline adoption of the Essential Eight across the Australian government still requires further improvement to meet the rapidly evolving cyber threat environment.

Australia's Cyber Security Strategy 2020 positions the Australian government to better meet these evolving cyber threats, investing $1.67 billion over ten years to strengthen Australia's cyber security, including $1.35 billion for the Cyber Enhanced Situational Awareness and Response (CESAR) package.

The CESAR package will maintain and enhance the cyber security capabilities of the ACSC and the assistance provided to Australians over the next decade. The CESAR package will enable the ACSC to identify more cyber threats, disrupt more foreign cybercriminals, build new partnerships with industry and government, and protect more Australians. The ACSC's enhanced capability and situational awareness will assist Commonwealth entities to improve and maintain their cyber security posture and resilience.

The Australian government continues to grow capability, delivering positive cyber security outcomes for Commonwealth entities. In particular during 2020:

- the Cyber Hygiene Improvement Programs increased coverage of active Commonwealth government domains by about 320%
- over 150,000 threat events were prevented through a pilot Protective Domain Name System (PDNS) program
- the pool of independent assessors under the Information Security Registered Assessors Program (IRAP) grew by approximately 9%.

The Australian government will also continue to strengthen its cyber security capabilities through the Harden Government IT Initiative, established as part of *Australia's Cyber Security Strategy 2020*. Centralising the management and operations of information and communications technology (ICT) systems run by Commonwealth entities will help strengthen the government's cyber security posture and improve cyber resilience across those entities.

The next report will be delivered in November 2022. The change in timing is to align with financial years, enabling clearer reporting, particularly in relation to significant Commonwealth funding commitments. Instead of crossing two financial years, each new report, from 2023 onwards, will focus on the cyber security posture for a single financial year. The report delivered in November 2022 will be a hybrid report, covering 1 January 2021 to 30 June 2022.

Introduction

Throughout 2020, Australia was targeted by a range of adversaries who conducted persistent cyber operations that posed significant threats to Australia's security, stability and prosperity. As publicly announced by the Prime Minister and Minister for Defence on 19 June 2020, the ACSC assisted a number of entities during the sustained targeting of all levels of government, industry, political organisations, academic institutions, health and essential service providers and operators of other critical infrastructure by a sophisticated state-based actor.

Access to government networks remained a top priority for malicious cyber actors. Cyber operations deliberately targeted Commonwealth entities with an intent to obtain information of strategic value to undermine our advantage and strengthen theirs. Targeting of personal information of Australian residents and government staff was evident.

COVID-19 shaped Commonwealth entities' cyber security postures in unprecedented ways in 2020. With the urgent need to enable continuity of government through remote working, new cyber threats from state actors and criminals emerged that required new vigilance as a considerable surge in government work was conducted online and often remotely, away from the added security of corporate firewalls and virtual private networks (VPNs).

To support the Australian Government's awareness of the overall cyber threat environment – and the continual recalibration of cyber security measures – Commonwealth entities are required to self-assess their implementation of the Essential Eight and report annually to both ASD and the Attorney-General's Department (AGD). In addition, working with ASD and AGD, the Department of Home Affairs coordinates Australia's cyber security policy settings, driving improvements across government and industry.

The ACSC within ASD leads the Australian Government's operational cyber security capability. The ACSC brings together cyber security capabilities from across the Australian government to provide cyber security advice and assistance to Commonwealth entities, state and territory and local governments, businesses, academia, and individuals.

The ACSC monitors cyber threats targeting Australian interests and, when a serious cyber security incident occurs, leads the Australian Government's response: providing advice and assistance to remediate and mitigate the threat and strengthen our nation's defences.

The ACSC's cyber security advice on how to prevent and respond to cyber security incidents can be found on cyber.gov.au. At the centre of the ACSC's advice is the *Strategies to Mitigate Cyber Security Incidents*[1]. While no single mitigation strategy can comprehensively prevent cyber security incidents, the eight mitigation strategies with an effectiveness rating of 'essential' are considered the cyber security baseline for all organisations to help protect their systems against a range of cyber threats. These eight strategies are known collectively as the Essential Eight[2].

[1] Further information on the *Strategies to Mitigate Cyber Security Incidents* can be found at Strategies to Mitigate Cyber Security Incidents.
[2] Further information on the Essential Eight can be found at: Essential Eight.

Individual Commonwealth entities retain responsibility for maintaining the confidentiality, integrity and availability of their information. Cyber security maturity is a risk management issue for each accountable authority to balance in the context of their unique risk environments and the complexities of their operations.

About this Report

The Joint Committee of Public Accounts and Audit recommended that ASD and AGD report to Parliament annually on the Commonwealth's cyber security posture. The Australian Government agreed to this recommendation in April 2019, in order to support increased transparency in cyber security reporting. This is the second such annual report.

Identifying the cyber security posture, or security vulnerabilities, of individual Commonwealth entities may increase their risk of being targeted by adversaries. This Report, therefore, does not identify specific Commonwealth entities – all data has been anonymised and provided in aggregate.

This Report is based on information held by ASD and AGD from 2020. The information indicates the maturity of a Commonwealth entity's cyber security posture at the time it was provided and is specific to the unique circumstances of that entity, at that time.

The findings in this Report are limited to information obtained through the *ACSC Cyber Security Survey* and the AGD's *Protective Security Policy Framework* (PSPF) maturity reporting – both of which cover financial year 2019–20 – combined with the results of Cyber Hygiene Improvement Programs undertaken throughout 2020. Some of the information is self-reported and has not been independently verified. It is important to note that no one Commonwealth entity – including ASD and AGD – has full oversight or visibility of the cyber security posture of all entities, due to the fact that, under the *Public Governance, Performance and Accountability Act 2013*, each entity is responsible for the security of its own ICT systems.

Australian Government cyber security initiatives in 2020

Throughout 2020, the Australian Government continued its work to establish effective cyber security behaviours and increase the overall cyber security posture of Commonwealth entities and the services they deliver.

The evolution of the whole-of-government Cyber Uplift

In mid-2019, the Australian Government expanded ACSC assistance to Commonwealth entities through the *Whole-of-Government Cyber Uplift for Federal Government Systems and the 2019 Federal Election* budget measure (Cyber Uplift). Throughout 2020, the ACSC has evolved the original Cyber Uplift program to further strengthen the cyber security posture of Australian government ICT systems through enhanced technical guidance, improved verification, and increased transparency and accountability. Cyber security uplift for Commonwealth entities has continued through the following key activities:

- **The Cyber Maturity Measurement Program (CMMP)** enables specialist ACSC teams – working with Commonwealth entities – to review ICT systems against the Essential Eight mitigation strategies. Each Commonwealth entity benefits from tailored advice on how to improve their cyber security posture. In some instances, where the Commonwealth entity does not have the capability internally, the ACSC provides additional funding for the entity to employ specialist commercial vendors to help them implement the ACSC's recommendations. Since the CMMP was established in mid-2020, five assessments have been undertaken.
- **The ACSC Cyber Security Uplift Services for Government (ACSUSG)**, funded as part of the CESAR package, provides support to Commonwealth entities who require additional assistance in implementing the ACSC's advice.
- **The Cyber Security Aftercare Program (CSAP)** enables the ACSC to maintain contact with Commonwealth entities it has assessed in order to continue to assist them to develop, adapt and maintain their cyber security posture. This program provides entities with the opportunity to receive additional ACSC services and assistance, including through the ACSUSG.

Cyber Hygiene Improvement Programs

The ACSC continues to actively monitor and assess the risks impacting Commonwealth ICT systems through increased monitoring of technical security controls and identifying known security vulnerabilities.

The Cyber Hygiene Improvement Programs (CHIPs) involve a series of cyber hygiene campaigns to improve the cyber security posture of Commonwealth, state, and territory government entities. CHIPs has visibility of, and is tracking, cyber hygiene indicators across 71,315 active Commonwealth government domains. This represents an increase in visibility of 54,297 active domains since February 2020 – an increase of approximately 320%. This provides the ACSC with visibility of internet-facing websites across 187 Commonwealth entities.

Through CHIPs, the ACSC provides Commonwealth entities with data-driven and actionable information to guide their cyber security efforts, supporting the adoption of common cyber hygiene practices, including the targeted management of ICT system improvements and maintenance.

In 2020, four major capabilities were added to CHIPs:

- email encryption scanning – detecting whether government email servers were configured to encrypt email
- dormant website scanning – assessing whether government websites were running up-to-date software, displaying default websites or using expired certificates
- critical security vulnerability[3] scanning – detecting high-impact security vulnerabilities in government internet-facing endpoints
- service visibility – providing Commonwealth, state, and territory entities with insight on the services they have open to the internet.

CHIPs also conducts high priority operational tasking activities in response to identified and potential cyber threats or significant events. Through these activities, CHIPs can quickly build visibility of, and develop insights on, security vulnerabilities across Commonwealth, state and territory, and local governments, and guide urgent remediation work. In 2020, 14 high-priority operational tasking activities were undertaken. This included scans of:

- the remote access and working-from-home arrangements implemented by Commonwealth entities in response to COVID-19
- all Australian-attributed IP addresses to identify vulnerable F5 devices, compromised Microsoft exchange servers and Microsoft Windows Domain Controller Zerologon vulnerabilities
- all Commonwealth entities in response to the release of the MobileIron proof-of-concept exploit code (see Case Study 1).

Case Study 1 – MobileIron

In mid-2020, MobileIron was notified by security researchers of a vulnerability in its product and promptly released a patch. In September 2020 more details, including proof-of-concept code, became public. Based on the additional information, the ACSC assessed that the vulnerability was highly likely to be used by adversaries to target and compromise government systems. In response, the ACSC used CHIPs to undertake a high priority operational tasking activity to quickly identify internet-exposed and vulnerable MobileIron systems across Commonwealth, state and territory, and local governments. The ACSC notified all government entities operating vulnerable devices of the device details, the critical vulnerability and the urgent need to patch or otherwise mitigate the risk. This timely and actionable information from the ACSC allowed some government entities to pre-empt adversary exploitation of their MobileIron devices, in one case by hours.

Over 2020, the ACSC has observed increased speed in exploitation of publicly reported vulnerabilities. Both Citrix and MobileIron vulnerabilities had some of the fastest turnarounds for exploitation attempts by malicious actors in 2020. Reporting showed adversaries attempting to exploit these vulnerabilities within

[3] Critical security vulnerabilities refers to serious, internet exposed, 'copy paste' style software security vulnerabilities. If left unpatched these critical security vulnerabilities may lead to complete ICT system compromise.

days of proof-of-concept codes being publicly released. Organisations that cannot patch their internet-facing services in a very timely manner, especially legacy VPNs and websites, must improve their patching capability. Adopting Software-as-a-Service (SaaS) or Platform-as-a-Service (PaaS) cloud approaches to internet-facing services may assist.

Host-based sensor program

The ACSC's host-based sensor program aims to provide improved visibility of Australian government ICT systems to assist with identifying weaknesses, detecting intrusions and reducing consequences related to ICT system compromise. The program collects telemetry from government devices and is available to Commonwealth entities to assist in protecting their networks and data holdings.

In 2020, the host-based sensor program was expanded from a pilot covering approximately 10,000 devices to a program covering approximately 40,000 devices across a larger number of Commonwealth entities[4].

This expansion has provided the ACSC with improved visibility of Commonwealth entities' ICT systems, enabling the ACSC to provide threat surface reports to participating Commonwealth entities on a regular basis. These reports provide entities with insight into their cyber security posture, as well as targeted uplift advice, for those ICT systems enrolled in the program. In 2020, the ACSC produced 20 of these reports for participating Commonwealth entities.

Protective Domain Name System

In 2020, the ACSC established a scalable cyber defence capability, the Protective Domain Name System (PDNS). The Domain Name System (DNS) is critical to the successful operation of the internet, as it is essentially the 'phone book' of the internet. The PDNS capability seeks to prevent access to domains identified as malicious by blocking access to sites that host malware, ransomware, phishing attacks and other malicious content. The capability also provides situational awareness on system vulnerabilities within Commonwealth entities (see Case Study 2).

Case Study 2 – Protective DNS

In late 2020, a significant increase in a specific type of DNS traffic associated with a Commonwealth entity was detected by the ACSC's PDNS. This anomalous traffic – which was a possible indicator of intrusion activity – was brought to the attention of the Commonwealth entity and resolved via the entity's incident response processes. This incident highlighted the value of identifying and analysing abnormal DNS traffic flows to detect possible malicious activity and through this either mitigate or reduce the harm of an intrusion.

Under the pilot, the ACSC processed approximately 2 billion queries from eight Commonwealth entities over the period from April to December 2020 – and blocked 4683 unique malicious cyber threats, preventing over 150,000 threat events. In 2021–22, the capability will be offered to all Commonwealth entities.

[4] These numbers reflect program scope as at 31 December 2019 and 31 December 2020 respectively.

Australian Internet Security Initiative

Over 2020, the ACSC worked with public and private sector organisations to strengthen cyber security arrangements and build resilience through the Australian Internet Security Initiative. The Initiative provided daily information on malware-infected or vulnerable ICT systems via 2.6 million Active Compromise Reports and 472.8 million Vulnerable/Open Service Reports on vulnerable ICT systems to over 300 member organisations including Commonwealth entities, state and territory government entities, Internet Service Providers, medium-to-large private organisations and critical infrastructure.

Information Security Registered Assessors Program

The Information Security Registered Assessors Program (IRAP) is a key ACSC initiative that provides assurance that ICT systems are measured against the security controls set out in the *Australian Government Information Security Manual.* The IRAP provides a framework for ACSC endorsement of assessors. Endorsed IRAP assessors are engaged by Commonwealth entities and industry to provide an independent assessment of cyber security, suggest mitigations and highlight associated residual risks. In 2020, the ACSC initiated enhancements to IRAP to meet increasing demand for assurance services by government, growing the pool of IRAP assessors from 128 to 140. The ACSC is now piloting the expansion of IRAP training by partnering with public vocational establishments.

Privileged user training

In 2020, the ACSC introduced tailored training for privileged users within Commonwealth entities. Privileged users are technical staff with duties and system access that enable them to adjust and maintain the configurations of ICT systems.

The ACSC's privileged user training is a tailored two day course that uses theory and practical exercises to provide privileged users with an in-depth look at how they can apply strategies to mitigate cyber security incidents in their day-to-day work. In 2020, the ACSC delivered privileged user training to over 1000 staff from 84 Commonwealth entities.

Cyber security forums

Throughout 2020, the ACSC helped inform policy makers of key trends and the continuously evolving nature of the cyber threat environment, including by leading two Commonwealth Chief Information Security Officer Forums and four Information Technology Security Adviser Forums. First established by the ACSC in 2019 as part of the whole-of-government Cyber Uplift, these forums bring together senior government officials with responsibility for cyber security, providing an opportunity to share the collective knowledge and experience of all members. This helps to improve the cyber resilience of individual Commonwealth entities and the overall Commonwealth cyber security posture.

Election support

In the lead up to, and during, the May 2020 Eden-Monaro by-election the ACSC provided cyber security support to the Australian Electoral Commission, including threat briefings, vulnerability assessments, and advice and assistance. The ACSC also provided support to a range of state and territory elections during 2020.

National Exercises

The National Exercise Program helps validate and strengthen Australia's nation-wide cyber security arrangements by helping Commonwealth entities review and test their incident response plans. This helps ensure Commonwealth entities can respond effectively to – and recover quickly from – a cyber security incident.

In 2020, the ACSC assisted with nine cyber security exercises, involving nine Commonwealth entities. These exercises improved command, control and coordination of cyber security incident response activities within Commonwealth entities; helped broaden the understanding of roles and responsibilities within and across governments and industry; and increased cyber security resilience across the Australian government.

Cyber security incident investigations

ACSC responses to, and investigations of, cyber security incidents help increase the cyber security posture of Commonwealth entities. As the ACSC investigates a cyber security incident, staff advise the affected Commonwealth entity of the security vulnerabilities they identify and give advice on the necessary remediation measures to put in place. The ACSC then uses this information to confirm – or update where necessary – the general cyber security advice it provides to other Commonwealth entities, industry, and the public, through alerts and advisories on cyber.gov.au or to ACSC partners through the Partner Portal. The ACSC also provides proactive notifications of cyber security incidents and offers advice and assistance to other impacted and vulnerable Commonwealth, state, and territory entities and private organisations.

In 2020, the ACSC responded to 434 cyber security incidents affecting Commonwealth entities – 46% of which were self-reported to the ACSC. The remaining 54% were identified through ACSC investigations, reporting from international partners and third parties, and analysis of a variety of classified and open-source material. Figure 1 shows the number of Commonwealth entity cyber security incidents responded to by the ACSC during 2019 and 2020. Observed spikes in February 2019 and April 2020 aligned with the beginnings of two major cyber campaigns which the ACSC responded to.

Commonwealth entity cyber security incidents

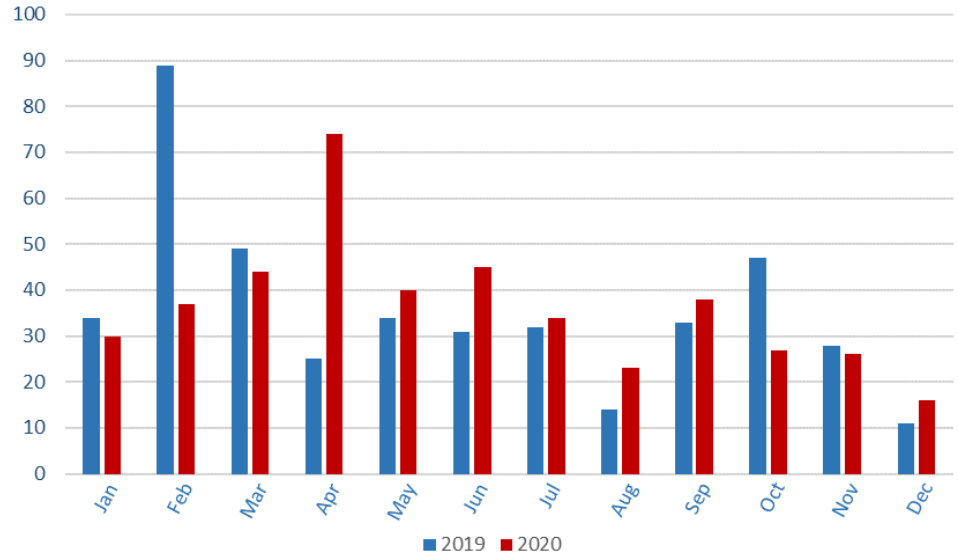

Figure 1: Commonwealth entity cyber security incidents per month, responded to by the ACSC in 2019 and 2020.

Case Study 3 – Advisory 2020-008: Copy-paste compromises

Some of the cyber security incidents involving Commonwealth entities were high-profile and complex. On 19 June 2020, the Prime Minister and the Minister for Defence publicly announced that the Australian Government was aware of, and responding to, a cyber security incident involving the sustained targeting of Australian governments and entities by a sophisticated state-based actor.

The ACSC published an advisory titled *Advisory 2020-008: Copy-paste compromises – tactics, techniques and procedures used to target multiple Australian networks* which was derived from the adversaries' heavy use of tools copied almost identically from open source. The advisory details the tactics, techniques and procedures (TTPs) identified during the ACSC's investigation of the cyber campaign, as well as advice on the mitigations to reduce the risk of compromise. The ACSC regularly updates the advisory with additional information to ensure Commonwealth entities and other organisations are able to protect their networks. The advisory has been updated four times since initial release and the public advisory was last updated on 16 September 2020.

Commonwealth entities have responded efficiently to ACSC's cyber security advice and assistance, and have been quicker to undertake measures to remediate the impacts of this activity. The ACSC has observed less extensive compromise of networks as a result of the 2020 activity in comparison to the 2019 activity. The positive response by affected Commonwealth entities in taking action has assisted in averting sustained disruption to essential services, and has increased cyber security resilience across Commonwealth entities.

Australian Government Information Security Manual

Adversaries continually evolve their tradecraft to defeat preventative measures that organisations, including Commonwealth entities, put in place. Throughout 2020, the ACSC continued to make regular updates to the *Australian Government Information Security Manual*, and other cyber security publications, to ensure the advice it contained was contemporary, contestable and actionable. These updates were based on information the ACSC gathered from its cyber intelligence and incident response functions about adaptation in adversary TTPs and from its assessment and uplift activities with Commonwealth entities.

COVID-19 support

The COVID-19 pandemic saw an increase in the operational tempo for the ACSC in 2020, with an increase in government and public need for cyber security advice and support tailored to meet the challenges of the cyber threat environment. Key support provided in 2020 included:

- providing technical cyber security advice to the Digital Transformation Agency (DTA) for the development and implementation of the COVIDSafe app
- conducting covert disruption and offensive cyber operations to combat COVID-19 themed malicious cyber activity
- providing hospitals and health service providers across the country with cyber security advice, and sharing threat information and technical support to help mitigate risks
- producing a suite of tailored cyber security advice products
- working with Services Australia and Telstra on Telstra's Malicious SMS Blocking Pilot Program[5].

[5] The pilot program boosts Australia's cyber resilience by blocking illegitimate phishing text messages that are impersonating myGov and Centrelink communications before they reach Telstra customers, thereby protecting Services Australia customers who may not be able to recognise a genuine communication from a scam. The ACSC's unique insights into the tradecraft and motivations of cybercriminals has been a key contribution to this pilot.

The Commonwealth's cyber security posture

Levels of cyber security maturity vary across the Australian government. While the cyber security posture of Commonwealth entities continues to improve, progress could be faster and entities remain vulnerable to cyber threats. Sustained effort will be required for Commonwealth entities to mature and ensure their cyber security postures remain resilient to the evolving threat environment.

Essential Eight implementation is improving.

The ACSC's cyber security advice on how to prevent and respond to cyber security incidents can be found on cyber.gov.au. At the centre of the ACSC's advice is the *Strategies to Mitigate Cyber Security Incidents*[6]. While no single mitigation strategy can comprehensively prevent cyber security incidents, the eight mitigation strategies with an effectiveness rating of 'essential' are considered the cyber security baseline for all organisations to help protect their systems against a range of cyber threats. These eight strategies are known collectively as the Essential Eight[7].

In 2020, implementation of the Essential Eight across Commonwealth entities improved slightly in comparison to previous years. More Commonwealth entities are taking steps to apply the baseline strategies and increase the maturity of their implementation. Commonwealth entities are concurrently assessing their threat environment and implementing further recommended mitigation strategies drawn from the *Strategies to Mitigate Cyber Security Incidents*. Overall, individual Commonwealth entities retain responsibility for maintaining the confidentiality, integrity and availability of their information. Cyber security maturity is a risk management issue for each accountable authority to balance in the context of their entity's unique threat environments and the complexities of their operations.

Some Commonwealth entities excel, integrating the *Strategies to Mitigate Cyber Security Incidents* guidance into their cyber security practices, with sophisticated and highly effective security controls in place to mitigate cyber threats. Although other Commonwealth entities are still working to implement the baseline controls, with the support of the ACSC they are actively taking important steps to maintain and further strengthen their cyber security posture.

The Essential Eight strategies, and the associated maturity model, evolves year-on-year in response to the changing cyber threat environment. As such, comparative data between years is not always available.

[6] Further information on the *Strategies to Mitigate Cyber Security Incidents* can be found at Strategies to Mitigate Cyber Security Incidents.

[7] Further information on the Essential Eight can be found at: Essential Eight.

Particular improvements noted through the *ACSC Cyber Security Survey* between 2019 and 2020 include:

- 12% more Commonwealth entities are achieving a higher maturity level with the 'user application hardening' mitigation strategy. In addition, 12% more entities are fully aligned[8] with the intent of the mitigation strategy compared with 2019, which is the biggest percentage shift in Commonwealth entities achieving Maturity Level 3 for any mitigation strategy. This mitigation strategy helps reduce the potential attack surface of workstations, as well as limiting adversaries' ability to bypass other security controls.
- 10.5% more Commonwealth entities have progressed from mostly to fully aligned[9] with the 'application control' mitigation strategy. This mitigation strategy assists in the prevention of the initial execution of malicious code on servers and workstations.
- 9.5% more Commonwealth entities have progressed from mostly to fully aligned with the 'restrict administrative privileges' mitigation strategy. This mitigation strategy assists in preventing the exploitation of highly privileged user accounts by adversaries.
- 11.4% more Commonwealth entities have progressed from partly to mostly aligned[10] with adopting the 'daily backups' mitigation strategy. This strategy assists Commonwealth entities to recover from ransomware attacks and avoid the need to pay ransoms to cybercriminals.

While additional work is required in order for all Commonwealth entities to improve their cyber security maturity, the impact of the increasing implementation of the Essential Eight – along with other mitigation strategies – is improving the Commonwealth's overall cyber security posture.

Adoption of the Essential Eight across the Australian government still requires further improvement to meet the rapidly evolving cyber threat environment.

Results of the *ACSC Cyber Security Survey* indicate that current implementation of the Essential Eight will need to continue to improve to meet the rapid changes taking place in the broader cyber security threat landscape. This finding is supported by AGD's analysis of entities' PSPF maturity reporting in 2019–20, which indicated that cyber security remains an important priority for Commonwealth entities, with considerable work to be done to raise the maturity of their mitigations of common and emerging cyber threats.

[8] Maturity Level Three under the Essential Eight Maturity Model means an entity is 'fully aligned with the intent of the mitigation strategy'. Further information is available at: Essential Eight Maturity Model.

[9] Moving from Maturity Level Two to Three under the Essential Eight Maturity Model means an entity has moved from 'mostly' to 'fully aligned with the intent of the mitigation strategy'.

[10] Moving from Maturity Level One to Two under the Essential Eight Maturity Model means an entity has moved from 'partially' to 'mostly aligned with the intent of the mitigation strategy'.

The following key findings highlight the issues which were impacting the ability of some Commonwealth entities to achieve a more mature and resilient cyber security posture:

- Commonwealth entities continue to have a number of obsolete and unsupported operating systems and applications.
- Commonwealth entities not using cloud-based services struggle to patch their internet-facing services in a timely manner.
- Many Commonwealth entities do not have a fast or flexible ICT modernisation cycle, noting the Essential Eight is significantly easier to implement on modern ICT systems that are designed using security-by-design principles (this would allow them to immediately benefit from modern security features, and then more efficiently apply best practice cyber security).
- Commonwealth entities misunderstand, misinterpret and inconsistently apply the Essential Eight.
- The effects of the cyber skills shortage intensified in 2020, with more entities identifying the lack of cyber skills in their workforce as a barrier to adopting the Essential Eight. As with 2019, insufficient budget and staffing were also reported as notable barriers for adopting the Essential Eight.

Implementation of the mandatory mitigation strategies outlined in PSPF 'Policy 10: Safeguarding information from cyber threats' is incomplete.

The *Protective Security Policy Framework* (PSPF), administered by AGD, mandates that all non-corporate Commonwealth entities[11] implement four specific Essential Eight mitigation strategies (known as the Top Four)[12] and strongly recommends the adoption of the entire Essential Eight. Commonwealth entities must also consider other strategies included in the ACSC's *Strategies to Mitigate Cyber Security Incidents*. Initial analysis from AGD's 2019–20 PSPF maturity reporting shows that entities' self-assessed implementation of the mandatory Top Four mitigation strategies remains at low levels across the Australian Government, with:

- 11% of non-corporate Commonwealth entities reporting an *ad hoc*[13] level of maturity (see Figure 2)
- 55% of non-corporate Commonwealth entities reporting a *developing*[14] level of maturity (see Figure 2)
- overall, *Policy 10: Safeguarding information from cyber threats* having the highest reported levels of *ad hoc* maturity.

[11] As defined in the *Public Governance, Performance and Accountability Act 2013*, section 11(b).

[12] ASD's Essential Eight incorporates the four mitigation strategies (application control, patch applications, restrict administrative privileges, and patch operating systems) mandated by the PSPF's *Policy 10: Safeguarding information from cyber threats.*

[13] The *ad hoc* maturity rating is defined as partial or basic implementation and management of PSPF core and supporting requirements.

[14] The *developing* maturity rating is defined as substantial, but not fully effective, implementation and management of PSPF core and supporting requirements. Entities may have this rating due to a single issue rather than a low level of maturity across all PSPF requirements.

2018–19 and 2019–20 PSPF maturity reporting

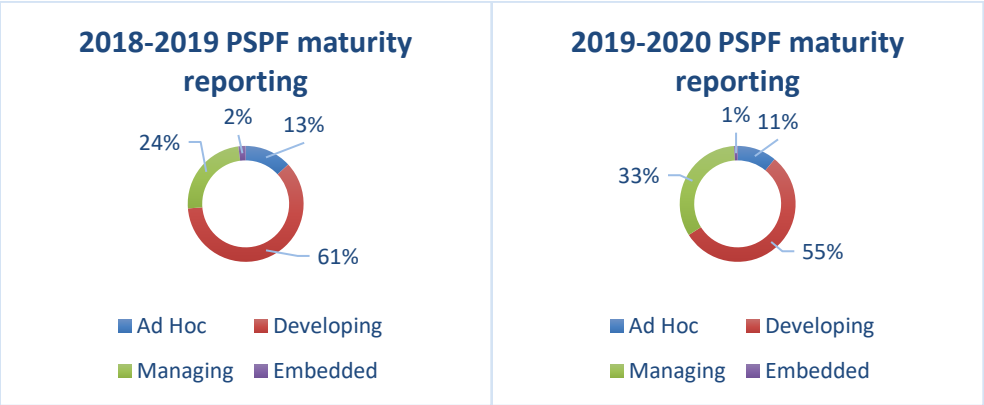

Figure 2: 2018–19 and 2019–20 PSPF maturity reporting by non-corporate Commonwealth entities – self-assessment responses to PSPF Policy 10 Safeguarding information from cyber threats.

Commonwealth entities are improving their internal cyber security culture.

Commonwealth entities are still making positive progress in improving their cyber security culture. It is critical that good cyber security practices are part of core business. Data from 2020 demonstrated that Commonwealth entities are maturing their risk management approach with positive improvements in governance, training, leadership engagement and community of interest engagement. In particular:

- Approximately 75% of Commonwealth entities include cyber resilience in their business continuity plans and have developed incident response plans, an increase from the 51% reported in 2019.
- 36% more Commonwealth entities are delivering cyber security training to staff as part of their induction programs. 70% of Commonwealth entities implement annual cyber security training requirements, which is equivalent to the percentage reported for 2019.
- 21% more Commonwealth entities are participating in sharing and collaboration forums, such as the ACSC's Chief Information Security Officer Forum. These forums enable Commonwealth entities to leverage existing government resources and knowledge, and reduce duplication.
- Cyber security is discussed quarterly or more frequently at the most senior management levels in 82% of Commonwealth entities.

Despite the increased cyber threats, greater attention to bolster cyber security practices across Commonwealth entities has improved the Australian government's cyber security posture.

Implementation of website encryption has improved across Commonwealth entities.

Website encryption supports public confidence in engaging with government systems online and is a highly visible indicator of basic cyber hygiene. Hypertext Transfer Protocol Secure (HTTPS) is a common protocol that provides website encryption and authentication, helping to assure users of the World Wide Web that they are connecting to the website they intended to, and that their interactions cannot be viewed or modified while in transit. Since 2019, the ACSC's CHIPs has

focused one of its campaigns on improving encryption on Australian government websites. During this reporting period, HTTPS encryption use has improved across Commonwealth entities (see Figure 3).

HTTPS Implementation

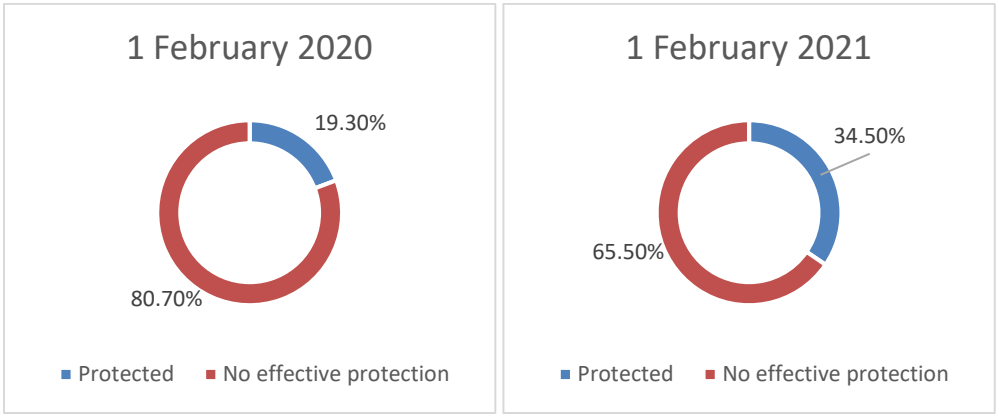

Figure 3: Commonwealth entity implementation of effective website encryption (HTTPS) in February 2020 and February 2021.

Implementation of malicious email mitigation strategies has marginally improved across the Commonwealth.

Socially engineered emails containing malicious attachments and embedded links are routinely used in targeted cyber intrusions against organisations. In 2020, the ACSC's CHIPs continued its campaign on combatting fake emails. The ACSC advises that Commonwealth entities can reduce the likelihood of their domains being used to support fake emails by implementing Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting and Conformance (DMARC) records in their DNS configuration. The CHIPs campaign continued to increase the number of Australian government domains implementing these strongly recommended fake email mitigation strategies (see Figures 4 and 5), but the overall number of Australian government domains with appropriate configurations remains low – further work is needed.

Sender Policy Framework (SPF) Implementation

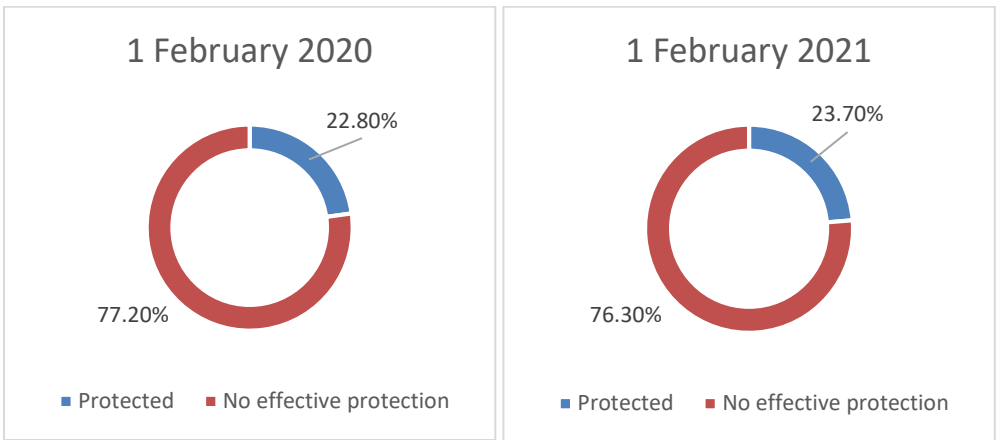

Figure 4: Commonwealth entity implementation of SPF in February 2020 and February 2021.

Domain-based Message Authentication, Reporting and Conformance (DMARC) Implementation

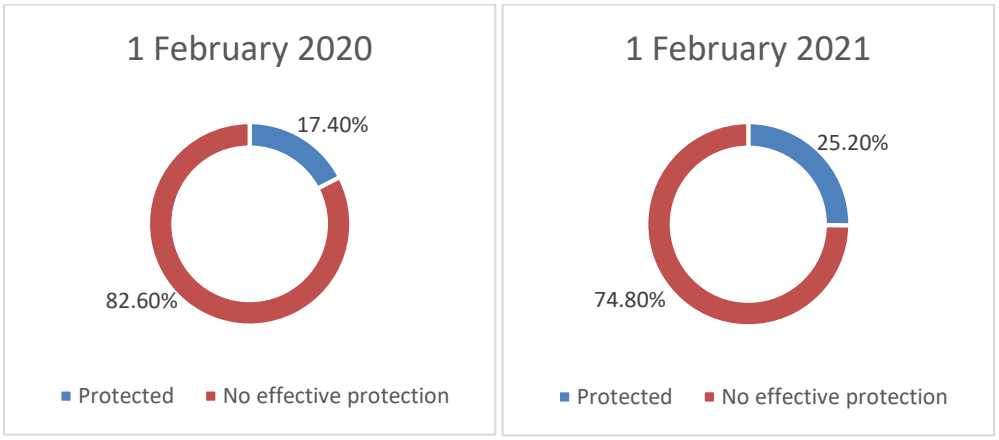

Figure 5: Commonwealth entity implementation of DMARC in February 2020 and February 2021.

Next Steps

Commonwealth entities continue to improve their cyber security; however, ongoing effort is required to maintain the currency and effectiveness of cyber security measures. The ACSC will continue to help Commonwealth entities improve their cyber security posture and resilience – including by implementing the Essential Eight, tailored to the threat level they face – and continue to help entities maintain their cyber security once they reach the right cyber security posture.

In 2021, the Australian government will focus on a range of additional areas of effort to continue to increase the cyber security posture of Commonwealth entities. Through various programs and initiatives, this will include increasing the ACSC's visibility of Commonwealth entities' ICT systems, enhancing their protection and keeping pace with new and emerging technology and evolving cyber threats. To achieve this, it will be critical for Commonwealth entities to cooperate closely with the ACSC to provide access and assistance.

Cyber Enhanced Situational Awareness and Response package

As part of *Australia's Cyber Security Strategy 2020*, the new CESAR package of $1.35 billion will maintain and enhance the cyber security capabilities of the ACSC and the assistance provided to Australians over the next decade. The CESAR package will mean that the ACSC can identify more cyber threats, disrupt more foreign cybercriminals, build new partnerships with industry and government, and protect more Australians.

Since the announcement in June 2020, a number of initiatives have been implemented by the ACSC to support the CESAR investment including:

- increasing the number of Commonwealth entities with access to a PDNS which blocks 'bad' domains or malicious actors
- growing the ACSC Partnership Program
- enhancing and increasing the effectiveness of client facing systems, including cyber.gov.au.

CESAR is a significant 10-year investment. Throughout the next three financial years, a number of projects are subject to detailed scoping, design and pilot work. These projects will support the delivery of *Australia's Cyber Security Strategy 2020* which will keep Australia secure online by:

- balancing cyber security roles, responsibilities and partnerships across the government and industry — particularly in relation to the protection of critical infrastructure
- improving our information-sharing with partners, including through the further development of the Joint Cyber Security Centre (JCSC) program
- providing stronger defences for government ICT systems and data
- tackling the threat from cybercrime
- increasing the cyber awareness of Australians – helping them to make 'cyber-smart' decisions and be 'cyber hygienic'.

Harden Government IT

In August 2020, the Harden Government IT (HGIT) Initiative was established as part of *Australia's Cyber Security Strategy 2020* to implement consistent, whole-of-government cyber capabilities to strengthen government's cyber security posture and improve cyber resilience across Commonwealth entities.

The HGIT initiative aims to centralise the management and operations of the large number of ICT systems run by Commonwealth entities.

With the operation of centralised 'hubs', the Commonwealth seeks to reduce the number of targets available to adversaries, including nation states or state-sponsored adversaries. This would allow the Commonwealth to focus its cyber security investment on a smaller number of more secure ICT systems, strengthening the defences of government networks and improving cyber monitoring, detection and response capabilities.

Cyber Threat Intelligence Sharing

The ACSC will continue to evolve and improve its Cyber Threat Intelligence Sharing (CTIS) platform over the course of 2021, including through co-design of the next evolution with industry.

The CTIS platform provides structured cyber threat intelligence in a machine-readable format. Further investment will enhance the automation of CTIS information feeds and examine multi-directional flows. The CTIS platform reduces the effort it takes to share cyber threat intelligence and increases the Commonwealth's understanding of threats targeting its networks.

Host-based sensors program

The ACSC will aim to increase the number of Commonwealth ICT systems on which the host-based sensors program is deployed. Maximising host-based sensors coverage across the Australian government will allow the ACSC to form a pan-government view of the cyber threat landscape and leverage this knowledge to detect and reduce the consequences of system compromise.

By increasing the deployment of host-based sensors across more Commonwealth entities, the ACSC will continue to increase its visibility of the cyber threat posture of Commonwealth entities, enabling responses to new and emerging cyber threats.

Cyber Toolbox pilot program

The ACSC has developed several technical tools under the Cyber Toolbox pilot program that are intended to support Commonwealth entities in understanding and improving their cyber security posture. The Cyber Toolbox provides a scalable method of engagement with Commonwealth entities by providing tools similar to those that the ACSC uses in its sprint engagements. This provides the entities with an independent method of assessing their cyber security posture, without requiring direct engagement with ACSC. These tools have been recently released and, through the Cyber Toolbox pilot program, the ACSC will continue to explore the value of these tools in collaboration with Commonwealth entities.

Protection of the COVID-19 vaccine

The ACSC will increase its work with Commonwealth entities, researchers and manufacturers to support and protect Australian research into COVID-19 vaccines and secure the Australian delivery of the vaccines, including protecting the cyber security of the vaccine supply chain. The ACSC will share information with Australian and international partners to increase the common understanding of the threats, risks and adversary tactics, techniques, and procedures used.

Commonwealth cyber security posture reporting

The next Report to Parliament on the Commonwealth's cyber security posture will be delivered in November 2022. The change in timing is to align with financial years, which will allow for clearer reporting, particularly in relation to significant Commonwealth funding commitments, including CESAR and HGIT. Rather than crossing two financial years, each new report, from 2023 onwards, will focus on the cyber security posture for a single financial year. The Report to Parliament delivered in November 2022 will be a hybrid report, covering 1 January 2021 to 30 June 2022.