

# gov tech review

**GOVERNMENT CIOs**  
FACING DISRUPTION PRESSURES

**AGENCIES BEING CHALLENGED**  
IN UX MATURITY

**AI PROJECT**  
AIMS TO DELIVER ARCHIVE REFORM

## COMMUNICATIONS

AUSTRALIA HELPS SET THE  
AGENDA FOR THE ALWAYS-  
CONNECTED WORLD

Q1 2020  
PP100021607

 **ROADS**  
**& TRAFFIC** EXPO  
INFRASTRUCTURE • TECHNOLOGY • INNOVATION

Australia's National Trade Show for the Roads  
and Transport Ecosystem 1-2 September 2020 ICC, Sydney  
FREE registration [www.terrapinn.com/exhibition/road-traffic-expo](http://www.terrapinn.com/exhibition/road-traffic-expo)



# Make The Autonomous Network A Reality Today

Creating a secure, self-healing network to support IoT devices requires the latest technological advancements. Talk to Extreme Networks, a leader in network automation, security, analytics and cloud networking to help you drive your digital transformation journey forward.

## Are You Ready for Wi-Fi 6?

If your network needs to support a high density of users, with a variety of mobile devices, IoT, both downstream and upstream, then 802.11ax (Wi-Fi 6) may be in your future.

Powered by **Smart OmniEdge**



## Elevate Your Automated Campus Deployment

Build an automated, secure, intelligent end-to-end campus network.

Powered by **Automated Campus**



## Network Agility Drives Digital Transformation

Leverage cross-domain automation, network visibility and adaptable platforms for quicker competitive response and better business outcomes.

Powered by **Agile Data Center**



Extreme Networks is a recognised Leader in the 2019 Gartner Magic Quadrant for Wired and Wireless LAN Access Infrastructure.

To learn more, visit <https://au.extremenetworks.com/> or call 61 (02) 9060 6438 to speak to a networking solutions expert today.

## FEATURES

**6 | Australia and the WRC — seeking spectrum harmony**

Australia's WRC-19 delegation focused on advancing the nation's legitimate interests in spectrum policy and technology matters.

**29 | Fighting fire with comms firepower**

The NSW Telco Authority found itself in the thick of battle during the recent bushfires.

**14 | What government CIOs should know about digital IDs**

Government CIOs must find a way to create digital IDs for citizens that are secure yet convenient.

**33 | Programming an artificial future**

Australia has an opportunity to potentially lead the way in the AI and greater digital transformation sectors.

**24 | AI project aims to deliver archive reform**

Understanding the context of government records will be key to automating the archiving of petabytes of data.

**36 | Australian agencies lagging in UX maturity**

Government agencies are lagging well behind the private sector in delivering products with a superior user experience.

- 16 | Switching partner pays off for IX Australia
- 18 | AI, analytics boost icare's claims capabilities
- 20 | Meeting citizens' expectations in the digital age
- 28 | Government CIOs facing disruption pressures
- 38 | Improving cyber resilience is a nationwide effort
- 39 | Ethical AI for defence forces
- 40 | Open government and digitising the customer experience
- 42 | AusCERT at the forefront of cybersecurity



# Insider



## Coronavirus and communications

**As I write this, the chaos caused by the coronavirus that causes COVID-19 is hitting the nation, and the wider world, hard. Coming on top of the summer bushfires, this new crisis is throwing many workplaces, activities, conferences and so on into disarray. While some workers and organisations will be affected for a period of probably some months, I guess one silver lining is that, for many, technology will come to the rescue. The ability for a large number of employees to do their work from home is all thanks to our wonderful, modern, connected world.**

That connectedness depends upon communications, of course, and it is a need that will continue to grow seemingly indefinitely... particularly mobile communications such as the forthcoming 5G revolution. Communications of all kinds, and especially 5G, were the subject of discussions at the recent World Radio Conference, at which Australia was well represented. 5G promises to revolutionise whole sectors of the economy, with ubiquitous super-high-speed connectivity across most of inhabited areas of our continent.

Such capabilities will no doubt be welcomed by our brave firefighters, disaster response crews and emergency workers, who sometimes struggled with communications issues during the awful summer bushfires. We should all be thankful for the efforts of the personnel of the NSW Telco Authority and its equivalents in the other states and territories, who worked tirelessly and in conjunction with other agencies and private companies to tackle problems as they arose, and restored communications links as soon as possible after they had been damaged.

The theme of digital transformation just won't go away. Governments at every level are steadily pushing forward with plans to make dealing with departments and agencies much easier for citizens. In order to achieve this, careful attention must be paid to customer experience and usability issues... topics at that are covered in some detail in this issue of *GTR*.

Finally, artificial intelligence is the new black when it comes to future digital technologies. In this issue we look at an innovative program that aims to use AI to help government archivists tackle the ever-growing volume of data and publications that must be sorted, classified and either archived or safely deleted. And we also look at the work Standards Australia is doing to prepare the nation for the future. Its latest report, *Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard*, is well worth a read.

**Jonathan Nally, Editor**  
[editor@govtechreview.com.au](mailto:editor@govtechreview.com.au)

**Wfmedia**  
connecting industry

A.B.N. 22 152 305 336  
[www.wfmedia.com.au](http://www.wfmedia.com.au)

Head Office:  
Locked Bag 2226  
North Ryde BC NSW 1670  
Ph +61 2 9487 2700

EDITOR  
Jonathan Nally  
[jnally@wfmedia.com.au](mailto:jnally@wfmedia.com.au)

EDITORIAL ASSISTANT  
Natasha Doyle

PUBLISHING DIRECTOR/MD  
Geoff Hird

ART DIRECTOR/PRODUCTION MANAGER  
Julie Wright

ART/PRODUCTION  
Colleen Sam, Veronica King

CIRCULATION  
Dianna Alberry, Sue Lavery  
[circulation@wfmedia.com.au](mailto:circulation@wfmedia.com.au)

COPY CONTROL  
Mitchie Mullins  
[copy@wfmedia.com.au](mailto:copy@wfmedia.com.au)

ADVERTISING SALES  
Liz Wilson Ph 0403 528 558  
[lwilson@wfmedia.com.au](mailto:lwilson@wfmedia.com.au)

Caroline Oliveti Ph 0478 008 609  
[coliveti@wfmedia.com.au](mailto:coliveti@wfmedia.com.au)

 **PUBLIC  
SECTOR  
NETWORK**  
OFFICIAL EVENT PARTNER  
[publicsectornetwork.co/events](http://publicsectornetwork.co/events)

**FREE SUBSCRIPTION**  
for industry and business professionals  
Visit [www.GovTechReview.com.au/subscribe](http://www.GovTechReview.com.au/subscribe)

*If you have any queries regarding our privacy policy please  
[email\\_privacy@wfmedia.com.au](mailto:email_privacy@wfmedia.com.au)*

*All material published in this magazine is published in good faith and every care is taken to accurately relay information provided to us. Readers are advised by the publishers to ensure that all necessary safety devices and precautions are installed and safe working procedures adopted before the use of any equipment found or purchased through the information we provide. Further, all performance criteria was provided by the representative company concerned and any dispute should be referred to them. Information indicating that products are made in Australia or New Zealand is supplied by the source company. Westwick-Farrow Pty Ltd does not quantify the amount of local content or the accuracy of the statement made by the source.*





# Protect and empower the digital identities of your modern workforce.

From single sign-on and password management to adaptive multifactor authentication, LastPass is the comprehensive access platform for securing every entry point to your business.

[www.lastpass.com](https://www.lastpass.com)



# AUSTRALIA AND THE WRC — SEEKING SPECTRUM HARMONY

## AUSTRALIA'S DELEGATION TO THE WRC-19 FOCUSED ON ADVANCING THE NATION'S LEGITIMATE INTERESTS IN SPECTRUM POLICY AND TECHNOLOGY MATTERS.

**E**very three or four years, the International Telecommunication Union (ITU) holds the World Radiocommunication Conference (WRC), where changes to the Radio Regulations are considered. The Radio Regulations is the global treaty governing the use of RF spectrum and satellite orbits.

WRC-19 was held from 28 October to 22 November 2019 in Sharm el-Sheikh, Egypt. More than 3000 state and industry delegates from 163 countries and 424 representatives of 130 organisations participated. Australia sent a delegation of 31 government and industry representatives, led by the then Department of Communications and the Arts.

Historically, Australian engagement in WRCs had been led by the Australian Communications and Media Authority (ACMA) as the WRC was considered to

be a technical forum. While the WRC continues to be a technical forum, agendas are increasingly also covering policy matters. So in 2017, the federal government transferred responsibility for Australian engagement in the WRC to the Department, recognising that departments of state are better placed to respond to policy matters. The Department and ACMA still work closely together in preparing for WRCs, with the ACMA continuing to lead on technical matters.

The WRC-19 agenda spanned the mobile phone, satellite, aeronautical, maritime, scientific, defence and transport sectors. Agenda items typically consider whether particular RF spectrum can be shared without causing harmful interference. Each WRC also sets the agenda for the next WRC. The global telecommunications industry is closely engaged in the meeting, including mobile and satellite companies.

The head of Australia's delegation to WRC-19 was departmental Assistant Secretary Cathy Rainsford.

"Australian radiocommunication experts from government and industry engage in international study groups of the ITU throughout the 3- to 4-year World Radiocommunication Conference cycle," Rainsford said. "Experts also meet domestically to contribute to studies and prepare to represent Australia at international and Asia-Pacific preparatory meetings."

### PREPARATORY WORK

The Australian Preparatory Group for WRC-19 comprised about 50 experts and provided advice to government to inform decisions on Australia's positions on each agenda item. The group included representatives from:

- the mobile industry (AMTA, Telstra and Optus)
- the satellite industry (NBN Co, Optus, Myriota, Intelsat, Inmarsat, Globalstar, Pivotal, Iridium, Boeing, Airbus, Omnispace, O3b, Telesat, Viasat)
- the broadcasting industry (Free TV, Commercial Radio Australia, Prime, SBS)



- the amateur radio community
- the Communications Alliance
- government agencies that rely on spectrum (Department of Defence, Airservices Australia, Australian Maritime Safety Authority, Australian Space Agency, Bureau of Meteorology and Commonwealth Scientific and Industrial Research Organisation).

Membership of the Preparatory Group can change over time, with membership open to any interested party who agrees to guidelines for participation.

“Over the four-year preparatory period before WRC-19, Australian delegates participated in 41 ITU Radiocommunication Sector meetings,” Rainsford said.

“These meetings review studies into issues on the WRC agenda to examine whether interference is likely to occur between radiocommunication services, and what technical and regulatory measures could be adopted to prevent or minimise harmful interference.

Based on the results of studies, the ITU Radiocommunication Sector develops a technical report (the Conference Preparatory Meeting report) providing options for possible adoption at WRC.

There was regional preparatory work, too, conducted by the Asia-Pacific Telecommunity (APT), the regional intergovernmental telecommunication organisation. The APT’s member countries include Australia, China, India, Iran, Japan, Korea, Mongolia, New Zealand, Pakistan, Pacific and South-East Asian countries. A series of five meetings preceding the WRC enabled APT member states to negotiate views for the APT region to present at international meetings.

#### AUSTRALIA'S WRC AIMS

According to Rainsford, the “overarching objective for Australia at WRC-19 was to ensure that international arrangements through the Radio Regulations treaty continue to be consistent with the rational and efficient use of Australia’s sovereign assets in the radio frequency spectrum”.

Other Australian objectives were to:

1. Establish new globally or regionally harmonised radiofrequency spectrum allocations, identifications and coordination arrangements (including technical or operational requirements) that:
  - are technically feasible (ie, will not cause unacceptable interference to

existing radiocommunication users, particularly safety and emergency services);

- respond appropriately to changing technology and industry practice;
- promote regulatory certainty to enable investment;
- promote economies of scale to reduce equipment costs;
- promote global interoperability of new and evolving technologies and services across all sectors, including to support Australia’s international capabilities;
- align with Australia’s domestic spectrum policies and priorities.

2. Ensure continued protections for, and strengthening of international cooperation on, scientific uses of the spectrum including radioastronomy, meteorology, earth exploration and space weather monitoring.

3. Ensure continued protections for, and strengthening of international cooperation on, navigation and safety services, including aeronautical and maritime radiocommunications.

4. Strengthen international cooperation on shared global radiofrequency spectrum and satellite orbit resources.





"Australia's primary interests in the WRC-19 agenda were the evolution of 5G mobile broadband, connectivity on planes and ships, deployment of large satellite constellations, and scientific and transport safety uses of spectrum," Rainsford said.

## SPECTRUM FOR 5G

The conference agreed new global identification of spectrum for future use by 5G mobile broadband in the 24.25–27.5 GHz, 37–43.5 GHz and 66–71 GHz bands. Other bands between 45.5 and 48.2 GHz were also identified for mobile broadband use in some countries.

These identifications will provide large contiguous blocks of spectrum for deployment of 5G, promote economies of scale in 5G equipment development and manufacture, and enable service interoperability for international roaming.

Underpinning the agreement to identify spectrum for 5G were regulatory limits to protect meteorological satellite sensors from mobile broadband operating in the 24.25–27.5 GHz band. Going into WRC-19, there was consensus that protection was required, but significant contention on the level of protection.

The compromise outcome provides a staged approach. Between now and 2027, temporary interference limits will be applied to mobile broadband, becoming more stringent in 2027 when 5G rollouts reach maturity.

## LARGE SATELLITE CONSTELLATIONS

The need to address spectrum 'warehousing' in light of filings for new very large satellite constellations was addressed at WRC-19 by a new regulatory framework for the staged deployment of these constellations over a seven-year period.

The new rules provide a set of milestones for deployment to avoid large non-geostationary (NGSO) satellite systems (some up to 75,000 orbital slots) being filed with the ITU but never deployed, tying up these scarce resources indefinitely.

The outcome reflects Australia's objectives and should promote a competitive global NGSO satellite industry and provide broadband around the world.

## BROADBAND ON AIRCRAFT AND SHIPS

WRC-19 agreed international conditions for operation of 'Earth stations in motion' (ESIM) in the frequency bands 17 GHz and 28 GHz. ESIM commonly provide satellite Wi-Fi on aircraft and cruise ships.

The outcome includes regulatory limits to protect satellite and terrestrial radiocommunication systems, including 5G mobile broadband networks in 28 GHz being deployed in Korea, Japan and the US.

It is expected that the aviation and maritime industries will benefit from expanded service provision by satellite networks.

## TRANSPORT SAFETY COMMUNICATIONS

Australia successfully negotiated a result that supported ongoing studies on rail spectrum but avoided restrictions on any particular bands in the Radio Regulations. This outcome supports Australia's rail industry to be able to continue using the specialised rail hardware that operates within current national mobile allocations.

Australia successfully opposed international regulation for Intelligent Transport Systems (ITS). Any regulation specifying particular technologies or frequencies would restrict fast-evolving development of ITS technologies that connect vehicles, improve traffic management and assist safe driving.

The WRC outcome also aligns with the class licensing arrangements put in place by ACMA in the 5850–5925 MHz band in January 2018.

## IMPROVED MARITIME SAFETY

WRC-19 successfully paved the way for addition of the Iridium satellite system to the Global Maritime Distress and Safety System (GMDSS) as a second service provider, opening a monopoly previously held by Inmarsat. Iridium's system will expand GMDSS capacity and coverage, especially in polar regions.

Regulatory changes took into account radioastronomy and aeronautical services operating in frequency bands adjacent to the Iridium system.





DID YOU KNOW?

# **SAS<sup>®</sup> BRINGS ARTIFICIAL INTELLIGENCE AND ANALYTICS TO THE CLOUD.**

You can run SAS on private, public or hybrid cloud infrastructures to better manage how AI work is done. SAS works with all major cloud providers to give you the power and freedom to innovate and be agile in the cloud.

[sas.com/discover](https://sas.com/discover)



**POWERFUL ANALYTICS.  
REAL RESULTS.**

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. © 2019 SAS Institute Inc. All rights reserved.

## GENDER DECLARATION

Early in the conference, agreement coalesced to develop a declaration Promoting Gender Equality, Equity and Parity in the ITU Radiocommunication Sector. At WRC-19, only 18% of participants were women — an increase of just 1% from WRC-15.

The declaration is a statement that ITU member states recognise that more is needed to facilitate the full participation of women in this space.

## AUSTRALIA'S INTERESTS

While Australia doesn't have any particularly special domestic requirements that differ greatly from those of other countries, there are aspects for which we need to lobby at WRCs.

"International spectrum allocations can affect the availability and cost of communications equipment for Australian consumers and industry; for example, mobile phones and base station equipment. Australian WRC positioning takes this into account and generally supports harmonisation where economies of scale would lower costs for Australian consumers and industry," Rainsford said.

"Australia is lucky to enjoy a relatively low-interference environment, as we are an island nation with few neighbours close by. Our geography also means we rely on both terrestrial and satellite technology for communications, whereas some administrations are more reliant on one or the other," she added.

"A key goal is to avoid international regulations that would constrain

Australia's ability to manage spectrum domestically, including to take advantage of our geographic isolation.

"We also support international cooperation as the best way to safeguard and improve important aeronautical and maritime communications, and to ensure scientific uses of spectrum can continue to supply important information (eg, meteorological sensor data) to Australia."

## SPECTRUM SQUEEZE

Spectrum and satellite orbits are scarce resources, naturally limited in availability, and there is inevitable competition among major manufacturers and technologies vying for access to spectrum.

"With the rise of mobile phones over the last three decades, more and more spectrum has been sought to underpin high-speed mobile broadband and communications. At the same time, consumers and industry are demanding connectivity everywhere, which drives demand for spectrum from the satellite industry," Rainsford said.

"The international radiocommunication community continues to recognise that cooperation and compromise delivers better outcomes (more spectrum and less interference) for everyone," she added.

"Australia encourages cooperation and compromise on the international radiocommunications stage. While demand is increasing, improvements in technology mean that spectrum can be used more efficiently, and makes viable the use of spectrum at higher frequencies."

What are some of the next big challenges for international spectrum regulation?

"Australia will continue to work towards international arrangements that provide certainty for interference management and flexibility to allocate spectrum efficiently, to its highest value use," Rainsford said.

"Technologies using wireless connectivity, and spectrum that underpins it, continue to evolve. Spectrum needs to be managed for both new entrants and existing users.

"Increasing the efficiency of spectrum use, including through spectrum sharing, is likely to require continued international cooperation."

## LOOKING AHEAD TO WRC-23

The conference agreed an agenda for the next WRC in 2023, comprising 19 agenda items and two areas for study.

One band, 7025–7125 MHz, will be considered for potential global identification for mobile broadband. Significant spectrum will be considered for identification for mobile broadband in Region 2 (Americas), including 3300–3400 MHz, 3600–3800 MHz and 10–10.5 GHz, while 6425–7025 MHz will be considered for mobile broadband identification for Region 1 (Europe, Africa and post-Soviet states).

The satellite industry is seeking regulatory arrangements for operation of ESIM with non-geostationary-orbit satellite constellations in several bands between 17 and 30 GHz, and for operation of ESIM with geostationary-orbit satellites using 12.75–13.25 GHz.

The scientific community will explore use of extremely high frequencies to support Earth exploration satellite services in 231.5–252 GHz, and an upgrade of the status of the space research service in 14.8–15.35 GHz.

Other agenda items include several potential adjustments for satellite, aeronautical and radio navigation spectrum.



Cathy Rainsford and members of the Australian Delegation to WRC-19, signing the final acts at the conclusion of the conference.

Conference images courtesy ITU; photographers D. Woldu, M. Mousa and H. Essawy.



# SECURE YOUR DATA & EQUIPMENT

**A data enclosure is your last line of defence, so it needs to be strong enough to stop unauthorised access.**

**The MFB range of Class B and Class C enclosures are purpose built frames fitted with key locks and boltwork approved by the Australian Government Security Construction and Equipment Committee (SCEC)**

All enclosures are fitted with tamper evident cable entry systems, high impact clear polycarbonate panels on doors, secure venting systems and certified combination locks.

An alternative product, the MFB range of High Security enclosures provides a lower level of security and is not SCEC approved. Effectively construction methods mirror the Class B and Class C series, however the doors are fitted with a cheaper bilock keying system. Also additional flexibility with the design regarding cable entry encourages effective quick installation and high volume data cable installations.

With over 50 years in the business, and backed by the SCEC approval for manufacture, these Australian built 19" rack mount enclosures provide peace of mind in relation to the security your data needs.



DESIGNERS & MANUFACTURERS  
OF 19" RACK SYSTEMS



PROUDLY  
MANUFACTURING  
IN AUSTRALIA



AUSTRALIAN MADE  
MAKES AUSTRALIA



[www.mfb.com.au](http://www.mfb.com.au) VIC (03) 9801 1044 / [sales@mfb.com.au](mailto:sales@mfb.com.au) NSW (02) 9749 1922 / [sydney@mfb.com.au](mailto:sydney@mfb.com.au)

# Headlines



## City of Adelaide to switch to 100% renewable energy

The City of Adelaide is set to use 100% renewable energy to power its assets from 1 July 2020 as part of its plan to go carbon neutral.

A new deal with Flow Power will see wind and solar energy power the city's "corporate and community buildings, council event infrastructure, electric vehicle chargers, barbecues in the Park Lands, water pumps, street lighting and traffic lights — everything that council operates" and reduce the city's emissions by 50%, according to Adelaide Lord Mayor Sandy Verschoor.

"The electricity to be provided by renewable generation each year is equivalent to powering over 3800 homes. The switch will reduce emissions by over 11,000 tonnes or the equivalent of taking 3500 cars off the road. Electricity cost savings are anticipated to be in the order of 20% compared to the City of Adelaide's most recent contract.

"This partnership will not only save our ratepayers money; it helps cement Adelaide's international clean and green reputation," Verschoor said.

The electricity will be delivered from Clements Gap wind farm in mid-north South Australia and new solar farms on the Eyre Peninsula and in the south east. The Streaky Bay and Coonalpyn solar farms, which Flow Power has acquired from Tetris Energy, are expected to help generate local employment opportunities in construction and operational stages, the council said.

Sydney and Newcastle have also engaged Flow Power for renewable energy, with Newcastle starting its new contract on 1 January this year. As a result, electricity from the Sapphire Wind Farm should now be powering "every sportsground floodlight, local library, park-BBQ and any other facility Council operates", according to Newcastle Lord Mayor Nuatali Nelmes.

Sydney is expected to make the switch on 1 July, with its pools, sports fields, depots and buildings, including the Sydney Town Hall, to be powered by the Sapphire Wind Farm, as well as Bomen Solar Farm and a non-profit community-owned solar scheme on the NSW south-east coast. The move is projected to reduce the city's emissions by around 20,000 tonnes per year — equivalent to powering 8000 households.

## Finance to trial a common whole-of-government ERP platform

The federal Department of Finance has announced that it is working with the Shared Services Provider Hubs to co-design a new GovERP initiative.

The initiative is part of the Australian Government's Shared Services Program, which aims to "consolidate, standardise and automate the delivery of core transactional corporate services across non-corporate Commonwealth entities", according to an approach-to-market announcement on the AusTender website.

"The GovERP initiative comprises the design, development and trial of a common whole-of-government platform, which will deliver a range of standardised corporate and financial services," the announcement said.

"The first tranche of the initiative will prototype a foundation enterprise resource management (ERP) platform for trialling across the Provider Hubs that already operate an SAP-based ERP.

"As such it will use SAP/4 HANA as the core technology solution, along with a range of complementary cloud-based products sourced from the open market, to test the delivery of common HR and Financial Services via a Provider Hub model.

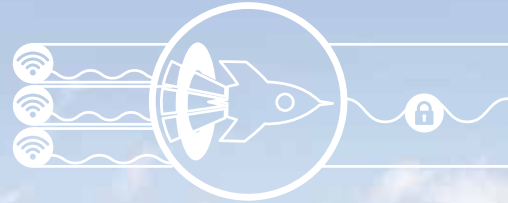
"The GovERP initiative will soon be entering a new project delivery phase and this will involve multiple approaches to market (ATM) to procure appropriate cloud-based complimentary products and services to integrate with a Core SAP/4 HANA platform."







# Extend MPLS Over Multiple 4G/5G



Build secure VPN connections to remote sites without wired links. Use stateful firewalls at the network edge, or forward traffic to the UTM at headquarters. For additional security, use **SpeedFusion™** SD-WAN to disassemble your sessions and send them across multiple WAN.



## Unbreakable VPN to Remote Locations



### SDX

Modular Enterprise Grade Router

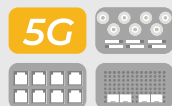


### SpeedFusion Engine

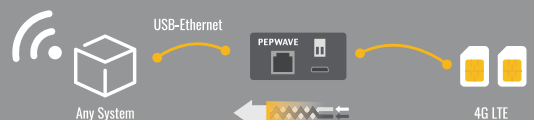
Integrate SpeedFusion SD-WAN Into Any System



Futureproof and Scalable



Multiple Module Types



Fuse multiple WANs for unbreakable connectivity

# WHAT GOVERNMENT CIOs SHOULD KNOW ABOUT DIGITAL IDS

Sarah Hippold, Gartner

## GOVERNMENT CIOs MUST FIND A WAY TO CREATE DIGITAL IDS FOR CITIZENS THAT ARE SECURE YET CONVENIENT.

**N**oémi lives in France. She needs to file her income tax return and — since she's already doing 'admin stuff' — she also checks the status of her healthcare reimbursements and signs up on the local electoral list. FranceConnect enables Noémi to access the public services needed to complete these tasks using a single login.

Noémi's story is a clear example of how digital identities can make citizens' lives and interactions with government agencies easier.

According to Arthur Mickoleit, Senior Principal Analyst at Gartner, governments have long been investing in digital identity and authentication methods to make sure citizens can easily, securely and legitimately access public services.

But Mickoleit says success has so far been very patchy. In some Nordic countries like Norway or Sweden, almost the entire population uses digital citizen IDs. Other countries, such as Australia, Germany or the US, have long tried to establish a system but have not succeeded for reasons that often revolve around an overly bureaucratic culture, which leads to an underperforming customer experience.

To create working and successful digital citizen IDs, government CIOs

must focus on three things: governance, technology and user experience.

### GOVERNANCE

Government CIOs whose agency provides a digital service have to choose between two models:

- Manage the entire identification and authentication process in-house
- Turn to a growing list of digital identity service providers (IDSPs)

It's become clear that the better option, in most cases, is to use one or more third-party IDSPs. This allows government agencies to focus their limited capacities on their core business: providing citizen services. And it reduces the 'clutter' citizens perceive when having to deal with multiple logins for different institutions.

By 2023, at least 80% of government services that require authentication will support access through multiple digital ID providers, according to Mickoleit. Citizens can then use the digital identity of their preference to interact with government agencies instead of having to manage single-purpose identities for each agency.

However, governments must keep in mind that there are different options for outsourcing digital identity provisioning — from government-issued digital IDs over those issued by companies to combined approaches like FranceConnect. Each option has its pros and cons.

©stock.adobe.com/au/Minerva Studio

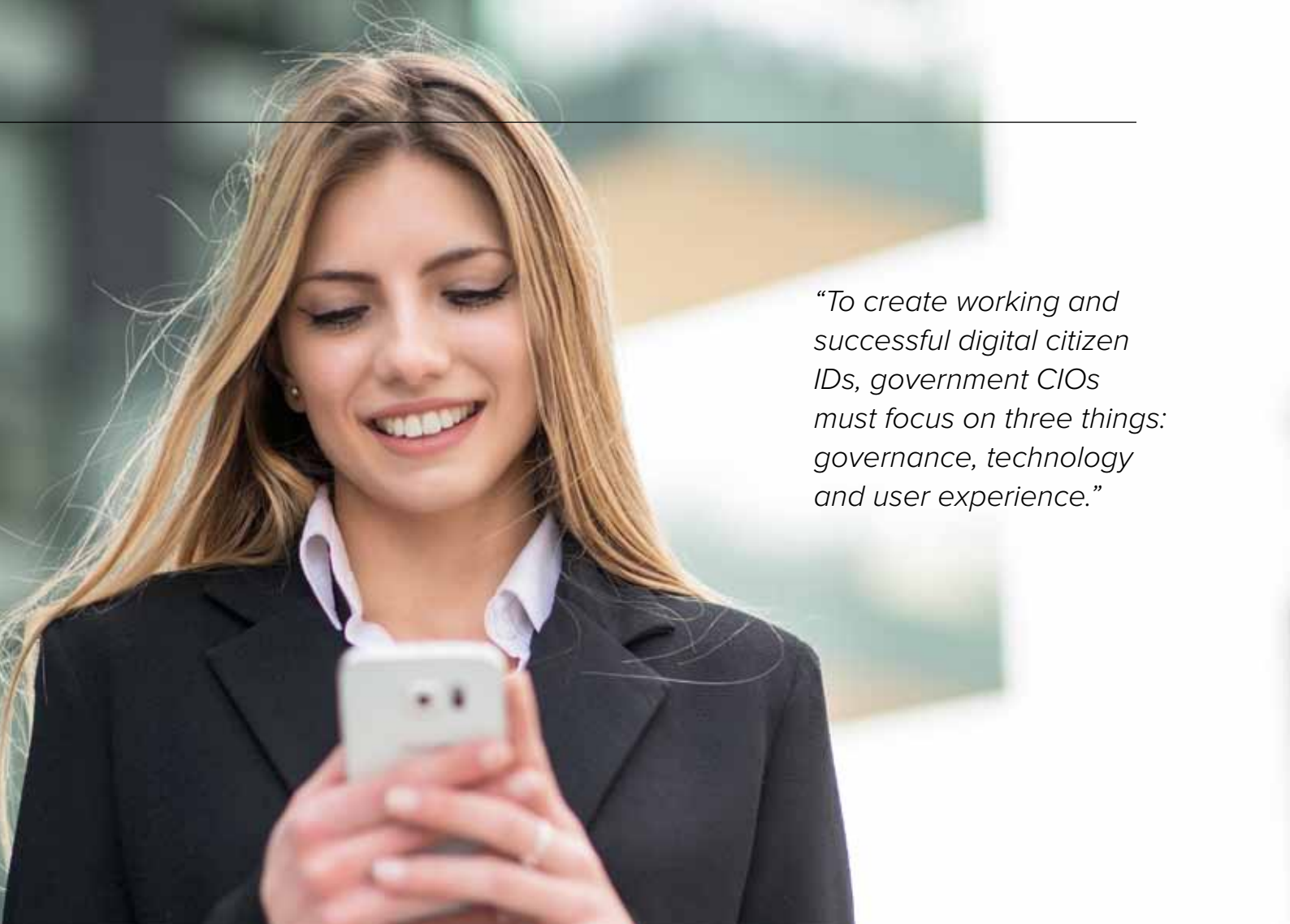
For example, when commercial IDSPs gain greater control over citizen identities and potential insights into their use, privacy concerns will arise. Government CIOs must find a balance between the benefits of faster take-up when partnering with the private sector and potential clashes between the interests of different stakeholders.

### IDENTITY DESIGN

Government and citizen expectations around digital identity can be difficult to balance. Government CIOs prioritise a high level of security to ensure citizens are who they claim to be when they access a service. Citizens, on the other hand, mostly want easy and convenient access.

In the past many governments favoured caution over convenience,





*“To create working and successful digital citizen IDs, government CIOs must focus on three things: governance, technology and user experience.”*

which often resulted in very secure systems that were difficult to use. Only the most tech-savvy citizens took on the challenge, while everyone else stuck with the traditional, analog points of access.

To balance security and convenience, government CIOs should take a more flexible approach and ensure levels of security are specific to the service offered. For example, booking an appointment should require less rigid security measures than declaring your taxes, let alone casting an online vote in national elections, as you can do in Estonia.

Governments need to understand that secure design of identities is not only a technology matter. The recent incidents of digital ID misuse in Estonia

were mostly a mix of phishing and social engineering, which needs to be anticipated. Government agencies should run campaigns that sensitise people to the fact that digital identities are becoming as valuable and important to protect as analog identities.

#### TECHNOLOGY

Technologies for digital identity are evolving at a rapid pace. This means that government CIOs must factor change into their technology choices, but also provide a form of continuity for their users.

Mickoleit says the three canonical authentication factors — knowledge, token and biometric trait — will continue to be a part of identification and authentication processes. They are established, they are secure and they

constantly evolve in their availability, as you can currently see with biometric sensors.

Nonetheless, it's critical that government CIOs stay on top of how security and user convenience profiles evolve over time. For example, the standard two-factor authentication methods with SMS-based transaction codes are now being replaced by dedicated code generator apps for more secure and convenient access.

In the future, blockchain approaches might provide even better privacy and user control over identity. And as ID technologies become more widespread and affordable, they can accelerate social inclusion of the estimated 1 billion people worldwide that currently have no formal means of identification.



# SWITCHING TECHNOLOGY PAYS OFF FOR IX AUSTRALIA

**I**X Australia is Australia's only not-for-profit, carrier-neutral internet exchange point. It's owned and operated by the Internet Association of Australian (IAA) and is currently the largest peering service provider in Australia with more than 70% market share. IX Australia is also the longest-running and lowest-cost internet exchange in Australia, providing peering, virtual leased line (VLL) and cloud interconnection services for approximately 400 corporate members of the IAA.

Building on the success of WA-IX, a multi-lateral peering exchange established in Perth in 1997, IX Australia has also established multiple peering exchanges in ACT, NSW, Queensland, South Australia and Victoria with plans to establish a point of presence in Tasmania in 2020.

"We are always striving for best practice, and we have a diversified offering for members, as well as providing access to major content delivery networks including Amazon, Microsoft, Google and Netflix," said Terry Sweetser, IX Australia's General Manager.

With the diversification and nationalisation of the business and an exponential growth in data traffic, and only a small engineering and development team to manage its infrastructure, IX Australia selected Extreme Networks as its switching partner in the mid-2000s. The partnership has enabled IX Australia to maintain cost-effective, reliable and market-leading internet exchange services to IAA members. IX Australia required a complex, scalable and secure MPLS network, providing capabilities such as:

- virtual private LAN and virtual private wire services;
- tighter levels of security control and management;
- hosting and running embedded configuration, deployment, and orchestration code;
- automated proactive incident detection, trend analysis, alerting and reporting;
- support for a full stack development environment.

"Extreme Networks is the 'killer app': it does everything we need. No-one

else can do it. Without Extreme, we would have to have solutions from multiple vendors, making it much more expensive to implement and difficult to manage," Sweetser said.

IX Australia has built its own tools to manage the Extreme environment, and currently uses templates to configure and provision new users and services. The Extreme operating system (EXOS) running on the switching infrastructure detects and reports on any outages across the network, with notifications automatically updated to IX Australia's status pages, and engineers alerted to troubleshoot and restore or escalate.

"EXOS is really good at identifying trends and pre-empting any issues before they become noticeable, particularly with our optics," Sweetser said.

Utilising ExtremeSwitching X870 Series switches, IX Australia was able to launch 100 Gbps peering services in late 2018, with the ISP Aussie Broadband the first to sign up in early 2019.

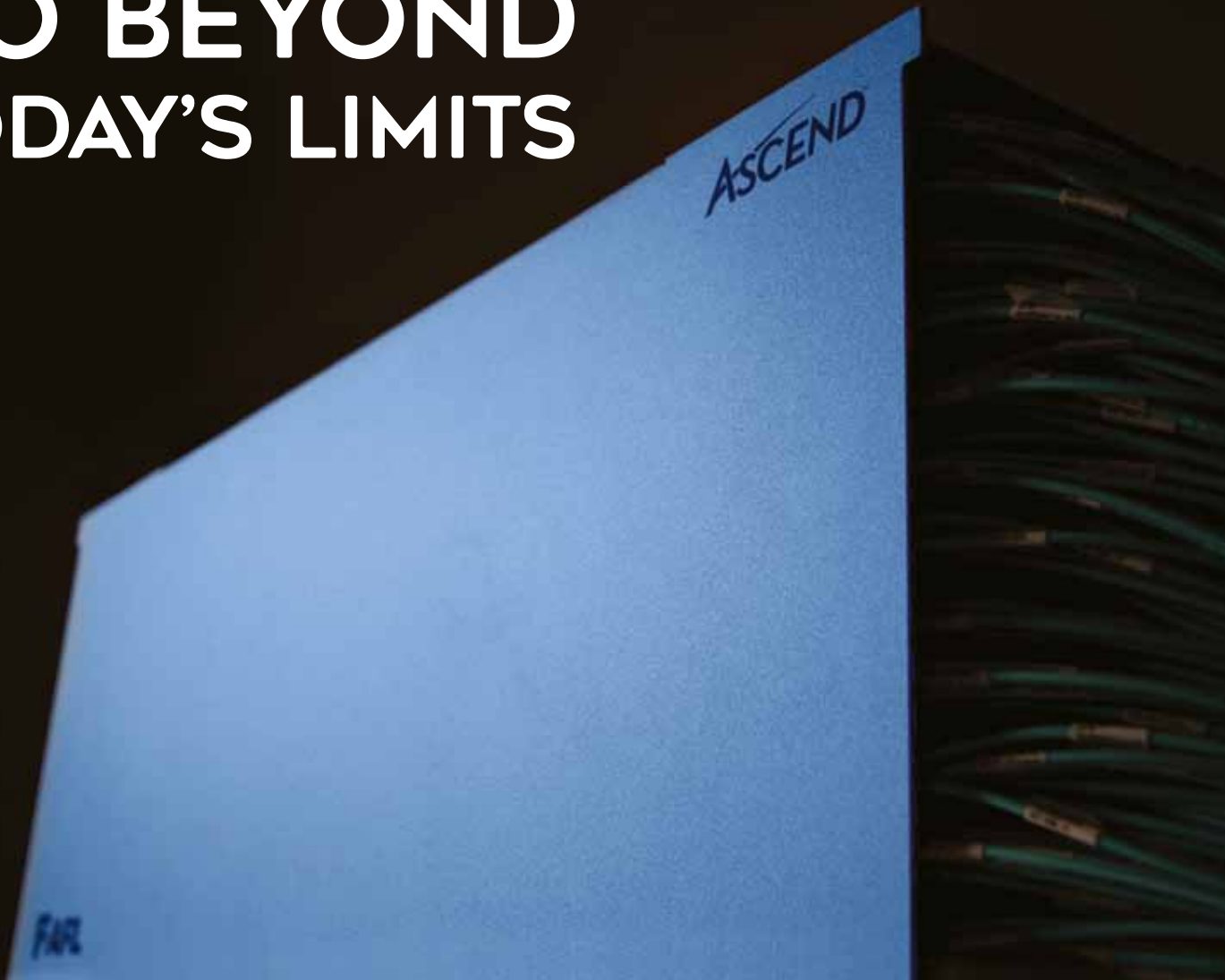
"With data use increasing exponentially each year, services such as these become more and more critical to enable ISPs to keep prices to their customers low," said Phillip Britt, Managing Director at Aussie Broadband.

"Content is driving everything," Sweetser added. "For businesses it's cloud services, and for consumers it's video on demand."

IX Australia plans to upgrade its infrastructure and roll out 400 Gbps peering services for its members. In the future Sweetser predicts that requirement will quickly climb to 1 Tbps.

In 2020, IX Australia has plans to fully automate the provisioning of all new services and ports from the point of demarcation on the network. This will speed up the organisation's responsiveness to orders and efficiencies in the delivery of services for customers, enabling IX Australia to maintain its competitive market advantage and free up its small administration team to focus on more strategic activities.

# GO BEYOND TODAY'S LIMITS



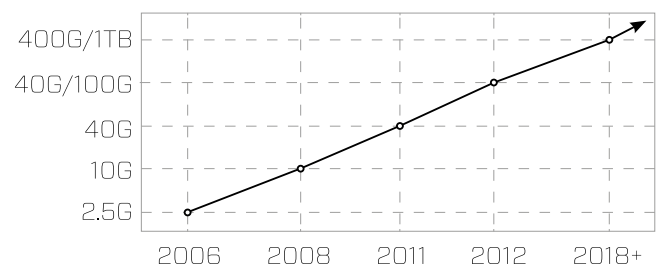
**With increasing bandwidth demands,  
you must rise above today's standards.**

Every year we see exponential growth in bandwidth consumption. AFL's new **ASCEND™** platform is not built for what you need today, but what you will need tomorrow. To be ready for tomorrow's networks, you need to be flexible. Get to 800Gb and beyond with **ASCEND**.

**Learn more at [AFLglobal.com/ASCEND](http://AFLglobal.com/ASCEND)**

Australia: 1300 232 476  
New Zealand: 09 927 7140

**Optical Network Progression**







# AI, ANALYTICS BOOST ICARE'S CLAIMS CAPABILITIES

A NEW CLAIMS TRIAGE MODEL BASED ON ANALYTICS HAS TRANSFORMED THE WAY ICARE ADDRESSES WORKERS COMPENSATION IN NSW.

**I**care (Insurance and Care NSW) is responsible for delivering insurance and care services to businesses, people and communities in NSW. A key part of this is supporting public and private sector workers and employers, understanding the appropriate level of care required to help people return to work. This covers 326,000 employers and 3.6 million employees, paying out \$800 million in weekly benefits and

\$650 million in medical payments to support recovery.

Melanie Wind, General Manager, Data and Analytics for icare, has been with the organisation since it formed in 2015. With 20 years' experience in data and analytics, she has a wealth of expertise in deriving value from complex data architectures. In 2019, she was tasked with implementing a new claims triage model, designed to transform the way icare addressed workers compensation.



©stockadobe.com/au/LIGHTFIELD STUDIOS

There are two ways for claims to be initiated with icare: either the injured worker submits an incident claim or an employer submits a claim on the worker's behalf. In this field, claims have been processed using a standard, one-size-fits-all approach for 30 years.

Support can involve medical treatment, rehabilitation services, education and vocational training and a series of other care services. Two

people with the same injury may not need the same level or type of support.

icare's executive leadership had higher ambitions centred on a new service model, so in 2016 as part of an overhaul of the personal injury claims service model, icare prioritised matching the needs of each claim with services to accelerate each injured worker's return to full health and work.

Wind was tasked with building a new claims triage engine, looking at identifying key information about each claim, the type of injury and history of the worker to pinpoint the level of support and case worker required. While there is a raft of experts with a wealth of experience in claims management, icare recognised the potential for analytics, AI and machine learning to augment human expertise and more accurately predict support levels in an automated fashion.

Tasked with a time frame of six months to implement an analytically driven approach to claims triage, icare turned to SAS to support the implementation of its vision for automated decisioning. This was complemented by the formation of a new internal team of data scientists.

A project of this nature is not without its challenges, with Wind highlighting the importance of aligning expectations upfront and planning integration with front-end systems. Equally critical is preparing data for both modelling and effective triage.

Beginning with a rule-driven approach, icare worked with SAS consultants to build an increasingly sophisticated set of models to enhance the claims management process. Using structured data including 96 different data points and 61 biopsychosocial variables per claim, icare shifted from a regression model to a random forest model from SAS Enterprise Miner, increasing accuracy by 15%.

As the claims triage engine matured, the use of machine learning and AI capabilities has grown increasingly

sophisticated. icare can now call on over a year's worth of de-identified claims data to increase the accuracy of the models which are processing claims in near real time.

"This level of performance is critical as icare are now able to respond to 10 triage requests per second during peak time, which ensures the team can service the needs of customers as quickly and efficiently as possible," Wind said.

Key aspects of icare's success have been having an analytics champion in Wind and strong executive sponsorship, particularly the vision created by Elizabeth Uehling (Group Executive, Personal Injury). C-suite direction of the project has been central to icare's success, as its data science team has brought key executives on the analytics journey, demonstrating key wins and showing the value-add that analytics can bring to traditional approaches to claims processing.

This facilitated a shift from a rules-first approach to demonstrating the predictive power of the models and continuous improvement achievable as machine learning models are trained further.

icare is now looking at more dynamic claims management approaches as well as using unstructured data which can be leveraged to dynamically triage claims processing.

"The important thing for icare was that we started small and simple and were able to build trust in the capability. From starting small, we then matured to building out a fully integrated machine learning solution that became increasingly sophisticated over time," Wind said.

The enhanced ability, driven by analytics, AI and machine learning, is driving better outcomes for icare, helping to triage claims more accurately and resolve claims faster. By starting simple and building on incremental wins along the journey, icare is changing the way it offers insurance and care for the people of NSW.

# MEETING CITIZENS' EXPECTATIONS IN THE DIGITAL AGE

Dan Gray

AUTOMATION CAN DELIVER INSTANTANEOUS, INDIVIDUALISED AND 100% ACCURATE SERVICE AND ADVICE FOR BOTH CITIZENS AND GOVERNMENT EMPLOYEES.

**P**ublic trust in government is underpinned by different 'rules' that often cascade from legislation (high-level, aspirational) to policy (interpretations of the operational intent of legislation) to regulation (operational, specific and transactional).

These rules are the basis for all government decision making. They are complicated, generally not user-friendly and require expertise to understand. Often they are overlapping and contradictory, and sometimes downright inaccurate and unfair.

This makes it very difficult for the average citizen to understand them — how to stay on the right side of them, and how to take legitimate advantage of rules and programs — ultimately requiring expert assistance.

Most governments struggle with this complexity too, relying on a very high level of employee knowledge and experience, a high level of patience from citizens, and tactical attempts to support better decision-making through the use of IT-heavy, code-based systems that

focus on IT efficiency rather than customer experience.

And all decisions that government makes need to be auditable in order to underpin public trust.

Against this backdrop, governments around the world are facing an unprecedented challenge through disruption such as the 'Experience Economy'. The expectations of citizens are escalating at a rate that government cannot keep up with — and worse, they are not funded adequately to meet the challenge, yet alone get ahead of it!

The rise of large and powerful cohorts such as the 'millennials,' who will soon be a major part of the global workforce, is adding to this challenge. They are 'digital natives,' born with the Internet and mobility, and driving a wave of change in non-government sectors that is reshaping entire industries.

There is a natural flow-on from this disruption into their engagement with government — they are 'digitally impatient,' and have been conditioned to expect government to be as easy to deal with as their favourite online shopping site.

Most government agencies also lack the 'competitive tension' that drives innovation and funding in non-government sectors — in most cases they have relative or absolute monopolies that can lead to institutional resistance to real, customer-focused change.

The rules are also becoming more complicated as governments struggle to keep pace with disruptive change in industries such as banking, insurance, transport and travel.

This all sounds pretty dire, but there is a way of meeting all these challenges simultaneously! Through the use of capabilities such as Oracle Policy Automation (OPA), government agencies can:

- Enable the 'legislation, policy or regulation' owner to capture the rules in natural language. No specialist IT skills are needed apart from knowing how to use Microsoft Word and Excel.
- Test that the rules provide the outcomes intended, and refine them in real time without needing specialist IT skills.





- Update the rules as they change without needing a large and expensive IT team.
- Enable citizens to engage with the rules through a 'guided digital interview' — just like a one-on-one, face-to-face interview with a subject matter expert — except through a variety of UIs (web, mobile, chatbot, smart-speaker etc).
- Provide a complete and comprehensive decision report in natural language for every guided digital interview — essentially an audit trail of the engagement with the virtual SME, and one that is 100% accurate and aligned to the source rules.
- Enable government employees of all experience levels to become 'instant experts' through the use of the same guided digital interview approach, while safeguarding

against the loss of valuable knowledge when experienced employees leave or retire.

- Use the guided digital interview to reduce the number of employees needed to handle many citizen enquiries, instead redeploying those employees to higher-value tasks that focus on a better citizen experience.
- Use the same rules that drive the guided digital interview to drive complex calculations for government benefits, payments, entitlements and so on, reducing the potential for error and the time to distribute.
- Inject the rules and associated logic into existing internal/external online systems, enabling government to leverage existing investments.

In summary, OPA enables

government to deliver instantaneous, individualised service and advice to employees and citizens that is 100% accurate, and always explains the interaction in language that the user can understand. When you consider the demands of the Experience Economy and cohorts such as millennials, OPA is the ideal capability to help government meet its unenviable challenge.

One final point: imagine if you migrated all legislation, policy and regulation to OPA — you could dramatically streamline the operation of government, dramatically reduce costs and dramatically increase public trust through the delivery of more accurate and understandable decisions.

*Canberra-based Dan Gray is Account Director, Customer Experience, Strategic Accounts for Oracle.*

## Featured products

### A3 multifunction printers

Epson's A3 multifunction WorkForce printers with PrecisionCore technology are designed to print heat-free and enable users to produce more with up to 87% less energy than a comparable laser-based device.

The WorkForce Pro WFC878R, WF-C878RTC, WF-C879R and WF-C879RTC models can deliver up to 86,000 pages in black ink or 50,000 in colour. The WF-878R desktop printer can be used as the main print device in smaller businesses or a workgroup device in larger ones.

WorkForce Enterprise models C20600, WF-C20750 and WF-C21000 are suitable for higher-intensity work and can

print 60, 75 or 100 pages/min, respectively. They also come with finishing options, including offset finishing and stapling, booklet-making and automatic hole-punching.

*Epson Australia Pty Ltd*  
[www.epson.com.au](http://www.epson.com.au)



### Micro data centre

Schneider Electric's EcoStruxure Micro Data Centre is designed to support distributed IT network deployment in environments ranging from small edge applications to hyperscale data centres.

The self-contained unit includes a single-rack enclosure, remote monitoring and management services, physical security, UPS, power distribution and cooling devices.

Users can install a 6U wall mount to keep the unit's edge servers, networking equipment and UPS off the floor. The mount is designed to be less intrusive than other enclosures and comes with an integrated dust filter and fan ventilation, making it suitable for light industrial environments.

*Schneider Electric*  
[www.schneider-electric.com](http://www.schneider-electric.com)





# A Titanic Lesson – Changing the Fate of Government Through the Essential 8

**D**escribed by Mark Toomey of Australia's Digital Leadership Institute, being the leader of a large and established organisation is like being the Captain of the Titanic and trying to change direction. A metaphorical comparison to a journey that was fraught with a series of errors that led to the demise of over 1500 souls. The Titanic and its doomed fate have become important lessons in leadership — of unknown risks and misplaced confidence, poor communication and failures to act, and inadequate crisis management.

So, what is it we have learnt from our past mistakes; about weak links in human behaviours, lack of visibility to what's ahead of us, and loose processes which under threat, can sink us?

Evidence suggests we haven't learnt a whole lot. Collisions of magnitude continue to mark the reputation of government, as agencies try to navigate at full speed through the murky waters of transformation and change, simultaneously opening themselves up to increased cyber-attacks.

Through the hard lessons, it seems governments have become experts in humility. One can't forget the noble admission by Australian National

University Vice-Chancellor, Professor Brian Schmidt, who published a report following its June 2019 cyber-attack in which he said, "we could have done more".

## Why AREN'T we doing more?

For one, organisations and particularly government departments, continue to be resource stretched. The majority of whom are still allocating skeleton staff to cyber security, and worse yet, do not have the skills, capacity, experience or playbooks to address cyber security incidents.

Dominic Scislo, ASG Group's Cyber Security Delivery Lead, has worked extensively across security for government organisations over his 30-year ICT career.



©stockadobe.com/au/nyragongo & jjomathai

Scislo described a culture within government that still treats cyber security as a ‘checkbox’ exercise.

“Many (organisations) go through the motions to become administratively compliant, but this doesn’t equate to cyber resilience and neither does it scream the hallmarks of a truly secure entity,” Scislo said.

“The expectation that any organisation can achieve a suitable level of security by pressing a few buttons is simply unrealistic.”

Non-mandatory strategies for security compliance were published in 2019 by the Australian Signals Directorate (ASD) to advise businesses and government on ways to mitigate cyber security incidents.

There are 37 mitigation strategies in total, with the ‘top four’ and ‘Essential Eight’ being a prioritised set of strategies that are likely to mitigate up to 85 percent of targeted cyber security attacks, according to the Australian Cyber Security Centre. Referencing the latest government Protective Security Policy Framework (PSPF) compliance report released in November 2019, Scislo said, “The Essential Eight are an absolute baseline for organisations. They are a starting point. Yet there are still 40 percent of agencies that don’t even meet the ASD’s top four.”

### Essential Eight — just the tip of the iceberg

When the Titanic took its maiden voyage in 1912, it was manned by 893 crew. Of those crew members, only six were watch officers and 39 were seamen. Most of whom were unfamiliar with the ship.

As the ship sailed at nearly full speed through the North Atlantic Ocean during a winter that had produced large crops of icebergs, the lookouts failed (despite six warnings) to spot the looming “dark mass” hidden by a haze on the horizon.

Unable to turn quickly enough due to its size, the Titanic suffered a glancing blow that buckled its side and opened six of sixteen compartments to the sea.

We all know what happened next. A ship that “not even God himself could sink”, disappeared beneath the water’s surface less than three hours later.

Metaphorically, the factors that contributed to the sinking are not all too dissimilar to the cyber security challenges our government organisations face today. Lack of experienced resources, lack of visibility, and due to size — an extremely complex change process.

Lloyd Lush, Chief Information Security Officer and General Manager, Infrastructure Managed Services at ASG Group, is responsible for security across the enterprise and oversees ASG’s delivery platform to its clients.

Following the 2019-20 Australian Government Budget review and a commitment to support a whole-of-

government cyber uplift, Lush says there has been a number of ASG government clients that have acknowledged their compromising security position and are taking action to remediate.

“We (ASG) created ASG’s Essential Eight services to help government organisations determine what level of maturity they are at with regards to the implementation of the Essential Eight.

“It’s worrying how many organisations there are out there that still lack visibility into their own cyber security posture,” said Lush.

From here, a maturity level is determined, and a strategy and roadmap is developed to create a clear vision for achieving the desired security posture.

ASG’s approach to remediation involves leveraging the ecosystem of people, processes and emerging technologies to gain compliance, confidence and resilience.

Security needs to be intertwined into the fabric of an entire organisation to create what Lush described as “defence in depth” — the only way to safeguard assets and critical systems — *the real heart of the ocean*. “The Essential Eight are only the tip of the iceberg. They’re intended to provide the first line of defence for a rapidly changing and increasingly complex cyber security environment.

“This means fusing security into the entire business operating model. There’s no shortcut, no silver bullet.

“Our message is to act with intent now. Security does come with a cost, granted. But the cost of continuing to make excuses could hurt you more,” said Lush.

ASG Group is an established provider of digital solutions and services for government. Leveraging automation, innovation and sovereign capabilities, ASG’s Essential Eight Services deliver a real-time view of a client’s security posture to drive smarter remediation, faster.



ASG Group  
[www.asggroup.com.au](http://www.asggroup.com.au)



GETTING MACHINES TO UNDERSTAND THE CONTEXT OF GOVERNMENT RECORDS WILL BE KEY TO AUTOMATING THE ARCHIVING OF PETABYTES OF DATA.

**T**he federal government has announced millions of dollars in grants to Australian tech companies, to help spur innovation that will solve some of the trickiest technology challenges it currently faces.

Under the Business Research and Innovation Initiative (BRII), six businesses have been granted \$1 million each to develop their proposed solutions. That \$6 million is in addition to \$1,465,597 allocated in feasibility study funding.

“Some businesses are working to use intelligent data to keep our tourism industry at the leading edge, while others are ensuring we manage risks of hitchhiking pests on shipping containers,” said the federal Minister for Industry, Science and Technology, Karen Andrews.

“This funding will help businesses which have completed feasibility studies further develop their innovative solutions.”

The BRII program challenged tech companies to solve specific problems within the following topic areas:

1. Providing fast and secure digital identity verification for people experiencing family and domestic violence.
2. Using intelligent data to transform tourism service delivery.
3. Upgrading government’s capability to help deliver world-leading digital services.
4. Managing the biosecurity of hitchhiking pests and contaminants on shipping containers.
5. Automating complex determinations for Australian Government information.

# AI PROJECT AIMS TO DELIVER ARCHIVE REFORM

Jonathan Nally

Amongst the \$1 million recipients working to protect Australia’s flora and fauna from pests, diseases and contaminants that can arrive on sea containers is Industry Spec Drones, which proposes to use unmanned flight technology to manage biosecurity risks, and Trellis Data, which will use detection technologies such as microwave and infrared to manage potential biosecurity threats.

Another firm, WEJUGO, will use its \$1 million grant to “develop a visitation and tourism analytics platform that combines data from transactional, telecommunications, social media and other digitally sourced data into a 360° view of tourism impacts across economic, environmental and cultural performance metrics”, according to BRII program documents.

And Surround Australia will leverage existing tech platforms to build a solution that “identifies the cultural and heritage dimensions of records”.

## AUTOMATING DATA DETERMINATIONS

The overall aim of the BRII’s ‘Automating complex determinations for Australian Government information’ theme is to “develop an accurate and scalable way to decide the value of government digital information and data and to determine whether it should be preserved or destroyed” using “artificial intelligence, machine learning, automation, data management and analytics, data science, archiving, business process management” technologies, according to the BRII program.

This challenge is not just a theoretical construct. The National Archives of



Australia (NAA) has a real problem on its hands with dealing with the volume of data generated by government, and deciding which records need to be kept and for how long, or whether they can be destroyed.

At the moment, this process is done largely manually, which imposes a huge cost burden on the NAA and government in general.

According to BRll program guidance, “The National Archives is looking for an automated, innovative, accurate and reliable solution to create and manage complex decisions about the value of information and data. Humans can then redirect their efforts towards exceptional and complex decision points. This product would be attractive to governments at all levels, as well as any private sector or not-for-profit

organisation that manages information and data.”

One company aiming to tackle this challenge is Canberra-based Lenticular, one of the \$1 million grant recipients. Lenticular aims to “develop a system that aims to help government make informed decisions about record keeping by developing and crafting contextual knowledge, and accessing this knowledge through user-configurable rules”.

Lenticular was co-founded by Trevor Christie-Taylor and Luan Nguyen, two members of the team behind the Parliamentary Document Management System (PDMS). The PDMS connects Australian Government agencies and parliament under the whole-of-government Parliamentary Workflow Solution system. It is used by more than

50 agencies, has 26,500 registered users and processes an average of 302,000 records every year.

Lenticular’s NAA-challenge inspired BRll project is partly a response to its experience in developing the PDMS, and will rely heavily on artificial intelligence.

“Currently, AI is like a butler, which comes with a timely suggestion and helps answer a question that’s quite narrowly defined. And were trying to open that up a bit. We’re trying to create a more personal relationship between the AI and the users of the organisation,” Christie-Taylor said.

“We’re working on a system where the user is in charge of what is being learned... so the user’s actually steering it like a car. They know they’re steering it. They know they’re guiding the AI towards what needs to be done.

“So instead of asking a narrow question like, ‘What is the weather like in Canberra?’ we’re asking a potentially very difficult question, like ‘Is this document important?’”.

Christie-Taylor points out that it’s hard enough for people to answer such questions, because nobody knows everything. It’s even more difficult for machines to do it, because the question becomes ‘Important to whom and why?’

“But if we put those two in combination, the people and the machine, the people continuously teaching the machine ‘this sort of thing is important to us’ and continually prodding that ‘this particular controversy means a lot to us,’” it will teach the AI which documents are important and why, Christie-Taylor said.

“We’re developing petabytes of data in the form of text every year, and what are we going to do with that stuff?” he asks. “Because some of it is going to be really important to tell the story of Australia. And some of it is just text; it cannot possibly be important to anybody.

“The machine cannot possibly know, just by looking at the words, that ‘this is important’. It has to understand the context, and that’s really where we’re coming from.”





## Password protection when it matters most

When IT solutions provider MOQdigital needed an enterprise password management solution, LastPass ticked all the boxes.

**F**ounded in 2005 and with 350 staff across offices in Brisbane, Sydney and Sri Lanka, solutions provider MOQdigital is a Microsoft and Citrix Gold Partner and Cisco Premier Certified Partner that helps businesses transform to the digital world. Its client activities range from server migrations to on-premise and cloud-based solutions, business integration, consulting, implementation and managed services.





As an end-to-end service provider, maintaining the security and sovereignty of MOQdigital clients' data is paramount. "Password security is a big concern of ours, as being a managed services provider, we have requirements to keep credentials for clients and their systems, so we needed a secure repository to do that," said the company's IT Operations Manager, Jason Muir. To that end, MOQdigital began the search for an enterprise password management solution, and settled on LogMeIn's LastPass.

## Solution

Members of the MOQdigital team had used LastPass individually prior to the company selecting LastPass Enterprise, so Muir said they were already aware of some of its capabilities and benefits.

"We were using the personal version of LastPass and now we've moved on to the complete enterprise solution to cover all our password management requirements," he said.

When seeking out an enterprise password management solution, MOQdigital was looking for two main benefits: improved security of credentials and increased productivity. LastPass remembers all of the passwords that staff need so there are fewer password resets, and — with the capability of LastPass Admin console — when employees leave the company, it is easy to remove their permissions so they can no longer access any company or client systems.

"The staff love it, and from my perspective, it gives me a level of comfort knowing that people aren't storing passwords on little bits of paper or within their own personal repositories," said Jason.

## Results

LastPass has delivered a range of benefits to MOQdigital that have enhanced security and improved workflows.

"Password sharing has been a big bonus for us in terms of business continuity," said Muir. "Now, when we start a project, a password folder for that client is created and populated with credentials for the various systems.

"When it then comes time to transition it to our Managed Service team, we then can easily transfer the access rights, so that only the relevant group of engineers have the necessary access.

"This level of security compartmentalisation allows us to provide a level of comfort to our clients knowing that we treat access to their systems in this way."

LastPass has also helped MOQdigital maintain the security of its systems when it brings in outside contractors to assist with projects on a temporary basis. Being able to control the visibility of the credentials

required for access is a key benefit for the company.

"We can control it right down to a single account and a single password for a single system, or indeed scale it right up to an entire site if needed," said Muir. "Being able to control that at a granular level is really critical for us because all staff only receive the amount of access they require."

MOQdigital also utilises the Secure Notes feature within LastPass to great effect. "In addition to using LastPass for passwords, we've been able to record some security information that we don't want to hold in other knowledge-based systems, and we can actually store it alongside the specific systems credentials so that all the relevant info is in the one place," said Muir.

Another significant benefit of LastPass Enterprise is its reporting capabilities, which enables MOQdigital to determine who accessed which systems and when, and generate reports on the findings, ensuring that enterprises can identify whether everyone who has used the system has the appropriate level of access.

"Some of our clients have data sovereignty requirements and need to ensure that all data remains within Australia," said Muir. "LastPass built their tenancy within Australia allowing us to ensure we were compliant and maintain our current contracts.

"This shows a real level of agility and commitment by LastPass to their clients that we recognise and highly value."

Overall, Muir sees LastPass as integral to security and productivity at MOQdigital.

"We have an ISO27001 information security certification and we are currently going through another auditing process," he said.

"Password security is a question that always comes up, so with LastPass, that's a big tick in that box and we move on.

"Essentially, it is our product of choice for password management and I can't see another solution out there that comes close."

**LastPass**... |  
by LogMeIn

**LastPass**  
[www.lastpass.com](http://www.lastpass.com)

# GOVERNMENT CIOs FACING DISRUPTION PRESSURES

Dylan Bushell-Embling

GOVERNMENT IT LEADERS WORLDWIDE ARE MORE LIKELY THAN THEIR PRIVATE SECTOR COUNTERPARTS TO REPORT THAT THEIR ORGANISATION FACES DISRUPTION AND FUNDING SHORTFALLS.

**G**overnment IT leaders worldwide are facing major organisational disruption and funding shortfalls, research from Gartner shows. The survey of government and non-government CIOs in 64 countries found that these pressures are higher in the public sector than across all other industries.

The report found that 58% of government CIOs have faced organisational disruption and 52% have faced a funding shortfall during the past four years.

These pressures are expected to continue heading into 2020, with government respondents only expecting an average budget increase of 0.1% from 2019. The majority of government respondents meanwhile expect their IT

budgets to either stay the same (28%) or decrease (28%) for the year.

Other significant challenges being faced by government IT leaders include labour disruption (41%), IT service failures (35%), severe operating cost pressure (35%), cybersecurity issues (24%), shifting consumer demand (24%) and adverse regulatory intervention (23%).

The report also found that government respondents are more likely to be behind rather than ahead of the curve in terms of recovering from a disruption. Some 39% of respondents are behind the curve in terms of finding the right talent to fill the organisation's needs, with just 13% ahead of the curve.

This pattern is repeated across other metrics such as the speed at which new business initiatives are launched (35% to 26%), the ability to fund new business initiatives (34% to 26%), the speed at which business initiatives are successfully completed (33% to 16%) and the ability to fund new budget initiatives (26%).

Gartner Senior Research Director Alia Mendonsa said the results demonstrate that CIOs of government organisations are still developing their digital leadership skills and strategy.

"Governments are struggling in many areas, following disruptions including changes in leadership, reorganisations and funding shortfalls. For many

government CIOs, disruption will affect their IT budget growth, and the funding and launch of new business initiatives will suffer," she said.

"The government sector is [also] lagging behind other industries in all aspects of strategy, particularly in its ability to communicate a clear and consistent business strategy that articulates how the organisation will achieve its vision."

Mendonsa said less than half of government CIOs (48%) reported that their organisation had a clear and consistent overall business strategy.

In the absence of such a strategy, she said government CIOs need to incorporate strategic business outcomes into their digital government strategy.

On the bright side, government CIOs are ahead of their private sector peers in terms of developing and delivering customer-centric digital services.

The survey also found that government IT leaders expect data and analytics (34%), artificial intelligence (28%) and cloud technologies (19%) to be the main game-changing technologies for the year ahead. Other areas of priority include conversational platforms, edge computing and digital twin technology.

But the top emerging technologies already being adopted in government include cybersecurity (84%), AI (33%) and robotic process automation (33%).

Mendonsa said government CIOs have their priorities right. "Government CIOs need to prioritise investment in emerging technologies according to potential value for their institution," she said.

"More mature technologies such as cloud, and data and analytics, offer immediate benefits in terms of capability and scalability for delivering digital government services, and therefore may be prioritised. Experiments with AI and robotic process automation may start small initially, and once their value can be demonstrated, initiatives involving these emerging technologies may be scaled up over time."

# FIGHTING FIRE WITH COMMS FIREPOWER

Jonathan Nally

THE NSW TELCO AUTHORITY FOUND ITSELF IN THE THICK OF BATTLE DURING THE RECENT BUSHFIRES.

**D**uring this summer's awful bushfires, firefighters — both volunteer and professional — along with numerous other emergency personnel, utilities crews, council employees and many others, have worked tirelessly over many

months to tackle the crisis. And many of those personnel have worked almost continuously during that period.

Unseen in the background, others too have been working to provide and maintain essential services to those frontline crews and, by extension, the wider public.

That dedication is exemplified by the NSW Telco Authority, whose Network Operations team and Telecommunications Emergency Management Unit had provided 150 continuous days (as of early February) of 24-hour emergency coordination of telecommunications support for the bushfire operations, including having liaison officers based at Rural Fire Service headquarters when required.







*The tower at Mt Wandera. Burnt cables can be seen running all the way up the tower.*



*The CCEP site at Mt Ganghat on the NSW north coast. A satellite solution was installed to enhance communications.*

The support has been vital in assisting the NSW Rural Fire Service, Fire and Rescue NSW, NSW Ambulance, NSW Police and the State Emergency Service perform their roles.

The Authority is responsible for managing the Government Radio Network (GRN), the primary network for NSW government agencies and emergency services organisations that use mobile radio communications.

The GRN provides the essential link between headquarters and firefighters on the ground, in all corners of NSW, supporting everything from firefighting to air operations, ambulance response and other emergency services tasking.

Almost 10 million calls were made across the GRN between 1 November 2019 and 1 February 2020.

“Next to Triple Zero, this is the most important emergency communications network in NSW,” said the Authority’s Managing Director, Kylie De Courteney.

The Authority has worked closely with agencies to protect radio communications towers throughout the

crisis, some of which were damaged by the fires.

“Bushfires put a huge strain on our telecommunications infrastructure, limiting radio coverage and mobile phone coverage,” said De Courteney.

“It was vital to get the Government Radio Network communications back up for firefighters so fleets on the ground and in the air can continue to coordinate operations, response and recovery,” she said.

Where network infrastructure was damaged by the fires, the Authority rapidly deployed a series of ‘cell on wheels’ (COWs) portable base stations.

“After two Government Radio Network sites at Mt Wanderer and Batemans Bay were destroyed in the fires, we immediately deployed COWs to provide temporary radio communications at these sites, including working with the Australian Defence Force to airlift equipment from Coffs Harbour to Cooma,” De Courteney said.

The Authority’s bushfire support efforts also included restoring or

expanded critical communications where existing infrastructure had been destroyed or where mains power supply was not available.

More than 20 portable generators were pressed into service to ensure electricity could be maintained where mains power had been affected, and many were put on standby for deployment into areas identified as being at risk from the fires.

As well as restoring communications, the Authority proactively put portable generators on standby, readied capacity expansion kits to manage radio congestion, and stationed four COWs at sites identified as being at risk of being affected by the fires.

## NEW AND ENHANCED SITES BROUGHT ON EARLY

“More than 20 new and enhanced GRN sites being delivered under the Critical Communications Enhancement Program were fast-tracked and brought online early to support firefighting efforts,” De Courteney said.

“The sites were made operational using temporary satellite infrastructure, to provide essential and enhanced radio communications coverage for emergency services.”

During the firefighting operations, more than 10 Optus Satellite Services very-small-aperture terminals (VSATs) were used in affected areas to supplement radio communications.

NSW Telco backhaul architects also designed a satellite solution and installed it into portable pelican-style cases. The system used Kymeta satellite panels, which — unlike a typical dish that must be physically aligned to a satellite — are electronically steered and enable rapid deployments.

The Authority also worked with carriers to fix damaged infrastructure to restore essential services such as internet access, mobile phone coverage and electricity for hospitals, businesses, volunteer organisations and other services.

# Cyber criminals dangle coronavirus-themed lures

Cyber criminals have expanded their coronavirus-themed attacks and are now preying on victims by playing on various conspiracy theories.

**A**s Australia continues to work to contain the COVID-19 pandemic, threat actors are also working overtime using coronavirus-themed lures to convince people to click. To date, the cumulative global volume of coronavirus-related email lures represents the greatest collection of attack types — united by a single theme — that has been seen in years, if not ever. Currently, attackers are using coronavirus themes for nearly all types of attacks, including (but not limited to) business email compromise (BEC), credential phishing, malware, and spam email campaigns. Threat actors are also actively abusing the names and logos of many companies and organisations within these campaigns in an attempt to manipulate recipients. Of particular note is the spoofing and brand abuse of national and international

health organisations around the world, including the World Health Organization (WHO), the United States Centers for Disease Control (CDC), and Canadian and Australian national health organisations. The targeting of these attacks has ranged from extremely broad to narrowly focused and campaign volumes have fluctuated between small and large. Attribution includes both well-known and unknown threat actors. Some of the well-known threat actors include TA505 and TA542. And while all industries have been targeted, Proofpoint has seen specific targeting of healthcare, education, manufacturing, media, advertising and hospitality organisations in certain campaigns. Proofpoint expects attackers will continue to leverage coronavirus themes in their attacks for some time to come.

## Campaign examples

At left is an example showing how threat actors are using coronavirus fears, and impersonating brands, to convince users to click. The message claims to be from Australia HealthCare, a fake but plausible name for a national healthcare organisation and promises Coronavirus prevention tips. If a user were to click the link, they would be taken to a fake Adobe website to enter credentials. Threat actors also launched a campaign using an email lure that stokes conspiracy theory fears, that there is a cure for coronavirus, that isn't being shared. One email claimed there is a cure being hidden

by government entities because the virus is being used as a bioweapon. It then urges the recipient to receive further information on the 'cure' by clicking on the link provided in the email.

If the recipient clicks on the link, they are taken to a fake DocuSign website where they're told they need to enter credentials to get the information.

Attackers are also subverting internal businesses' credibility in their attacks. Proofpoint has seen a campaign that uses a coronavirus-themed email that is designed to look like an internal email from the company's president to all employees.

This email is extremely well-crafted and lists the business' president's correct name.

The messages contained a Microsoft Word attachment with an embedded URL that leads to a fake Microsoft Office website to enter credentials. Once the credentials are entered, the user is then redirected to the legitimate World Health Organization coronavirus information site, making the phishing transaction seem legitimate.

Overall, Proofpoint anticipates attackers will continue to leverage COVID-19 as it develops further worldwide and will also likely pursue potential targets who are now being asked to work from home. Its threat research team recommends users stay vigilant for malicious emails regarding remote access and fake corporate websites, all aimed at ensnaring teleworkers. When working remotely, be sure to use a secure Wi-Fi connection, protect your VPN log-in, use strong passwords, think twice about clicking on links and confirm all transactions are authentic.

## Sources:

<https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update>  
<https://www.proofpoint.com/us/corporate-blog/post/ta505-and-others-launch-new-coronavirus-campaigns-now-largest-collection-attack>  
<https://www.proofpoint.com/us/corporate-blog/post/attackers-expand-coronavirus-themed-attacks-and-prey-conspiracy-theories>

**proofpoint.**

**Proofpoint Inc.**  
[www.proofpoint.com/au](http://www.proofpoint.com/au)





# Public Sector Network

Join our network of Public Sector professionals.

Connect with your peers today!

## Connecting Government

**Public Sector Network** is a social enterprise that exists to help government around the globe to break down silos, collaborate, and work together for better outcomes for citizens.

Our growing community spans all tiers of government and public services, and allows members to network, benchmark and share best practice on a secure and closed-door platform.

Sign up today to start connecting and learning with your peers!



### Network

Identify and connect with relevant peers across all levels of government



### Benchmark

Share your stories and compare notes with other public servants

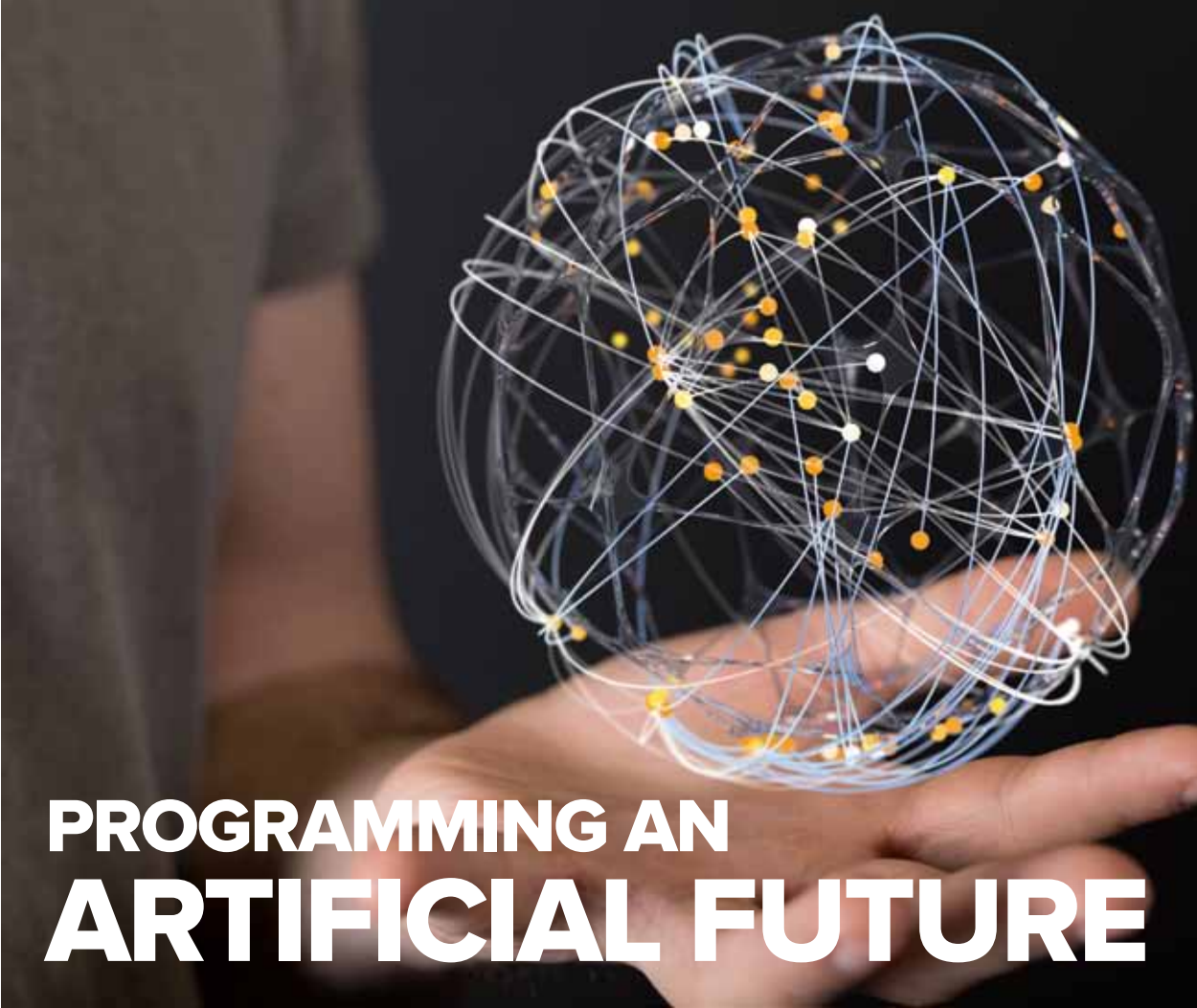


### Best Practice

Read, watch and listen to leading government experts around the globe

Visit [www.publicsectornetwork.co](http://www.publicsectornetwork.co)





# PROGRAMMING AN ARTIFICIAL FUTURE

AUSTRALIA HAS A SIGNIFICANT OPPORTUNITY TO NOT JUST GET INVOLVED BUT POTENTIALLY LEAD THE WAY IN THE AI AND DIGITAL TRANSFORMATION SECTORS.

Daniel Chidgey

**W**hen we think artificial intelligence, Arnold Schwarzenegger's Terminator leaping off buildings and clinging to helicopters comes to mind. Or more recently, Iron Man's many AI sidekicks like Jarvis and FRIDAY.

It's all science fiction and storytelling but how far away are we really from this reality? Automated machines haven't become part of our everyday life, but AI is slowly seeping into every facet of our lives, from Siri to self-driving cars, Netflix recommendations and predictive text. The infancy of AI is well and truly becoming indented in our day-to-day practices.

## LEADING THE CHARGE

While the future of fully-blown, or autonomous, AI seems a time away, the reality is we are already on our way, and Standards Australia intends to be a leading voice in supporting the ongoing development and use of AI. The technology is undoubtedly the future, underpinning the success of initiatives like smart cities, from simple pattern-recognition programs through to self-driving cars and beyond. Standards are the key to the safe and reliable use of this new technology as it continues to emerge as a life-changing innovation.

This year has seen the launch of the Artificial Intelligence Standards Roadmap: Making Australia's Voice

Heard. The roadmap provides recommendations to ensure Australia can support AI and its future across the globe. A stable foundation is important to allow innovative projects and enhancements like this to grow and evolve. And at the rate these projects are expanding, standards will be essential.

Since 2017, 14 of the world's most advanced economies have announced over AU\$86 billion in focused AI programs and activities. In response to this, Australia, along with the United States, UK, China, Germany and others, has identified AI standards and policy frameworks as national priorities. Standards can establish common building blocks, and risk management frameworks, for companies, governments and other organisations.

This growth in AI and the investment underpinning it has the potential to transform the lives of Australians. Developing standards to support this growth is essential to shaping the responsible design, deployment and evaluation of these new technologies.

## DISCUSSIONS TRANSCEND BOARDERS

AI must be programmed to perform its intended function, to recognise patterns and make amendments to its programming to reflect the requirements these patterns recommend. The technology is essentially self-learning,

and the wrong programming can have dire implications.

For example, self-driving cars are designed to recognise infinite possibilities and work through situations, which can be life or death. Standards have the ability to help support the formation of these programs on an ethical basis: What should these outcomes be? How should cars weigh the implications? What is the value of a human life?

These standards could also work to set the guidelines for how to program this software to accurately reflect agreed upon regulations and allow for the safe use of AI in projects like self-driving cars. Without these standards, the vehicles programmed could vary greatly across manufacturers and countries with different cultural interpretations and values.

One of the more common concerns is security. With AI being used in potentially sensitive sectors like health care, banking or surveillance, it's essential the data is safe and secure. Standards will provide a path for limiting potential security breaches and the safe management of data. Programmers and developers of AI agree there is also the risk of potential bias in the system, after all the AI tech is programmed by humans and any potential bias could be passed

onto this self-learning system. It will also fall to standards to help mitigate these outcomes by providing guidelines to support consistency.

This is a global discussion; technology is increasingly blurring national borders and pays no mind to politics. Data is easily shifted from one device to another so it's essential AI is treated with this in mind. ISO and the International Electrotechnical Commission (IEC) established a subcommittee on artificial intelligence. It is the first standards activity to focus on the entire AI ecosystem. AI is not one technology, but a variety of software and hardware enabling technologies that can be applied in various ways in a potentially unlimited number of applications in almost every industry sector.

The roadmap itself outlines the steps necessary to ensure Australia is involved in the international discussion regarding AI as these developments become more frequent. This ranges from safety concerns and consumer demands to export and data sharing recommendations.

The launch follows a growing body of work on approaches to managing the impact of AI globally, which intersect with broader aspirations, such as those outlined in the United Nations Sustainable Development Goals. The opportunity, and challenge, for Australian stakeholders is to effectively use the standards process to promote, develop and realise the capabilities of responsible AI, delivering business growth, improving services and protecting consumers.

There is significant opportunity in the AI and greater digital transformation sector for Australia to not just get involved but potentially lead the way. The growth of AI is exponential and still a way from reality, but in order to one day reach an intended goal, there must be sound and proportionate regulatory and policy settings available to shape its evolution, and standards are essential to this.





# The mechanical cylinder: The missing link in an access control system?

On entry to most of the government or office buildings you are confronted with a host of access control initiatives to govern who is allowed and who is not allowed access. Be it the presentation of your card to a reader to open a turnstile, activate the lift or trigger an automatic door, access is controlled in an efficient and easily managed way, and our security programmed brains believe that all is good.

But this raises a question: How many of these doors/lifts/turnstiles have a mechanical key override?

The answer is many. Not all, but many.

This then raises further questions:

- Are the mechanical keys secure?
- Are they stored in a secure place and are not lost?
- Also, are they secure from attack and duplication (remembering that many keys can be visually read and even reproduced from a photograph)?

The problem is that as soon as they are in a person's hand, keys can be compromised by copying, duplication or even 3D printing. Our observation is that at many sites, extremely effective and costly access control systems are installed. These systems are hugely effective in monitoring and controlling access to the building, however, many of these systems have a very basic weak point that allows the whole system to be compromised. The chink in the armour is that **they are fitted with a conventional mechanical cylinder.**

This cylinder has no audit trail and can be in many cases mechanically manipulated (picked). Added to which any access to a key by an unscrupulous person can result in it being read, impressioned (in the way of an impression into a soft material) or photographed and 3D printed.

So now what? A solution is available. Install an electro-mechanical key system such as EKA CyberLock. The cylinders are opened with CyberKeys. Both are managed using software in the same way as an access control system.

The management software allows access to be granted when and where, or simply timed out or even revoked when required. CyberKeys are programmed through communicators such as a smart app and Bluetooth or a 20-key vault cabinet. The entire system can be audited and, to make it even simpler, can potentially be integrated with your existing access control system.

EKA CyberLock makes a range of cylinders to suit most common locks in the Australian market. For our latest case studies across major office buildings, communication towers, roads and traffic control boxes and much more, visit [www.ekacyberlock.com.au/case-studies](http://www.ekacyberlock.com.au/case-studies). To find out more or continue the discussion contact us at [sales@ekacyberlock.com.au](mailto:sales@ekacyberlock.com.au) or on 1300 722 311.



**EKA Cyberlock**  
[www.ekacyberlock.com.au](http://www.ekacyberlock.com.au)



# AUSTRALIAN AGENCIES LAGGING IN UX MATURITY

Dylan Bushell-Embling

**GOVERNMENT AGENCIES ARE STILL BEING OUTDONE BY THE PRIVATE SECTOR IN THE MATURITY OF THEIR USER EXPERIENCE DESIGN PROCESSES.**

**A**ustralian Government agencies are still lagging well behind the private sector in terms of delivering products with a superior user experience (UX), a new report finds.

The report from government-focused consultancy Intermedium and Esri Australia concludes that despite all the focus on user-centric thinking among Australian government agencies, UX maturity remains low.

The report estimates that state and federal government agencies will spend at least \$12 billion on digital initiatives in the current financial year, and some agencies are allocating up to 20% of their total project budgets to UX.

But for other agencies, spending on UX research requires redirecting funding traditionally set aside for the design component of a digital build.

Respondents also reported facing difficulty gaining support for the inclusion of UX-specific budget allocations across the lifespan of a project.

UX advocates also report being frustrated that the public servants responsible for controlling budgets are often too far removed from agency operations to understand the importance of and benefits of improving UX.

Agencies are also reluctant to outsource UX design even if they do not have the skillsets available in-house.

Departments are instead using materials and tools developed by their counterparts with larger UX budgets, such as the Digital Transformation Agency's Digital Services Standard.

According to the report, every dollar invested effectively in improving UX at the design phase has the potential to return either \$10 or \$100 compared to whether problems with the user experience need to be fixed during development or after a product's release, respectively.

Other respondents reported that it is not difficult securing budgets that frustrates UX activities, but the time that UX research and design consumes.

Australian federal and state governments are meanwhile at different stages of maturity in terms of the adoption of whole-of-government approaches to UX design and planning.

The report used a metric to calculate whole-of-government user maturity



scores based on the three pillars of intent, allocated resources and governance. It evaluated states and 16 individual agencies based on four stages of UX maturity — unrecognised, considered, committed and established.

It ranks the NSW (8.75) and federal (8.25) governments as being national leaders, followed by Queensland, Victoria and SA (8.00 each). WA (6.75) and the ACT (5.5) are less mature, with the NT and Tasmanian Governments having the lowest level of maturity among all jurisdictions (4.5).

Five of the nine jurisdictions reached the top of the maturity scale used for the calculation, and no jurisdiction fell below the “committed” level in their UX maturity score.

But UX maturity remains low across many agencies despite these whole-of-government efforts, the report found.

Maturity varies significantly across sectors. Departments with jurisdictions covering issues cutting across entire states — such as transport entities — are further along in UX adoption due to facing greater pressure to provide services that meet taxpayers’ expectations. But more niche departments with less citizen interaction are less mature.

In addition, only a few agencies have internal staff dedicated to ensuring user-centred thinking is a key consideration in their projects. A number of agencies also report being reluctant to invest in UX until there is evidence that KPIs can be implemented and adhered to while measuring usability performance.

Another common problem identified among respondents is an over-reliance on the traditional waterfall project management approaches rather than agile design approaches, which often leads to decision-makers cutting back on time-consuming UX activities as the launch date looms.

But other respondents reported that the relationship between agile design and UX is not necessarily complementary, with the inclusion of UX methodologies often slowing down agile design processes by enforcing regimented, purist UX work at every iteration.

All study participants agreed that widespread adoption of UX in an agency hinges on the existence of a change agent in a senior position.

But the study found that “the business case for UX activities can be difficult to communicate to senior executives who do not yet recognise the benefits of UX. As such, the inclusion of UX components as part of the budgeting process relies on the support of senior figures and strong business cases.”

Respondents also reported difficulty gaining the traction needed to “change the culture of an entire organisation with entrenched bureaucratic processes that limit deviation from the status quo”.

The report found that agencies are incorporating a number of approaches to exploring user insights to improve the UX design process, with the most popular methods involving directed and non-directed interviews with users, as well as usability testing.

But some agencies are exploring more sophisticated methods. These include eye movement tracking for users trying out beta products, tree

tests to determine whether a product has an appropriate information architecture and content hierarchy, and the development of user personas designed to act as a realistic representation of key audiences for a product.

Another technique becoming a go-to method for governments looking to design services around user needs rather than their internal structures is life journey mapping, the report found.

Life journey mapping involves developing government services based around a range of common life events, such as births and deaths in the family. The federal and NSW governments are leading in the adoption of this emerging technique.

The report recommends that agencies seeking to build UX capabilities start with analysing and scoring their existing UX maturity.

“UX maturity scoring allows organisations to analyse their current situation, providing a benchmark by which they can measure future changes in their approach to resourcing, policy and process,” the report states.

“As a starting point to address opposition to UX adoption, maturity scoring also helps to highlight the extent to which an organisation is already being guided by user-centred thinking.”

The report provides a template for agencies to conduct this UX maturity benchmarking. It recommends UX advocates ask five questions about their organisation:

- What level of awareness or support is there for UX among leadership at your organisation?
- To what extent is UX part of your organisational culture?
- What kind of UX resources are available to your organisation?
- How sophisticated are the UX methodologies used by your organisation?
- When in the project development cycle do you involve UX?



# IMPROVING CYBER RESILIENCE IS A NATIONWIDE EFFORT

Dylan Bushell-Embling

## DEPARTMENT OF HOME AFFAIRS SECRETARY MICHAEL PEZZULLO BELIEVES IMPROVING CYBER PREPAREDNESS, RESILIENCE AND RESPONSE REQUIRES A SOCIETY-WIDE APPROACH.

Improving Australia's cyber preparedness and resilience is a pressing issue that requires a whole-of-society response, according to Department of Home Affairs Secretary Michael Pezzullo.

The public sector veteran used a video address to the 2020 Edith Cowan and Home Affairs Cyber Security Forum to call for closer collaboration between government, industry and academia on managing Australia's cyber risks.

"Governments cannot do this on their own. Yes, in days past a lot of security threats were managed in great secrecy and by governments taking the lead," Pezzullo said in a video message.

"Government had all the information typically, and government had most of the response options and tools in their inventory. This is no longer the case, and especially so in cyber. Frankly, everyone is on the front line."

Pezzullo had been expected to deliver the keynote address for the Forum, which was convened to explore the key findings of last year's consultation on the 2020 Cyber Security Strategy, but was unable to attend in person because his department is dealing with a number of issues related to bushfires and biosecurity risks.

Developing a strong cybersecurity strategy will require improving cyber resilience, Pezzullo said. This will in turn require partnerships between governments and industry, between state

and federal agencies, and with "society at large".

One area where such partnerships can play a role is in cyber preparedness, he said. Such a vital area cannot be left to CIOs of organisations or to government agencies to manage alone.

"Preparedness is something that has to be thought about on that whole-of-society basis," Pezzullo said.

"Our universities play a great role in adding to our store of knowledge, research and thinking, as do cooperative bodies such as the CRCs, as do large corporations, as does the business sector at large, as do citizens themselves."

But at the same time, the government needs to lead these efforts, particularly in aspects to do with standards, trusted marketplaces and cyber awareness, Pezzullo said. Exploring the latest techniques and approaches is an important aspect of the preparatory work for designing the 2020 Cyber Security Strategy.

Other important considerations for the strategy involve incident management and response. Cybersecurity planning in the modern era requires considering a hack to be inevitable, which means a response will be required, Pezzullo said.

"If we accept the proposition that incidents are going to occur — no matter how we minimise their incidence or their severity — if incidents are going to occur, what are the best response strategies?" Pezzullo asked.

"What are the right protocols? How do we get emergency help particularly to those who are affected most egregiously? And indeed how do we as a nation and a people and a society respond, particularly to those most grievous hacks which are societal-wide and which have repercussions that spread beyond our IT usage?"

Finally, developing a fit-for-purpose security strategy will require answering important questions about recovery and resilience, Pezzullo said.

"How do we recover essential services quickly? And is this really just an issue in terms of our IT response? If data is being frozen, if essential services have gone offline, if other societal functions have been impaired, how do we respond societally? How do we respond with resilience, much in the same way as we do with disaster risk or climate risk or indeed biosecurity risk?" he said.

"It's these common society-wide risks that need to be mitigated and responded to that my department particularly is charged with thinking about society-wide impacts. That's why, as I've said already in this address, thinking about it on a whole-of-nation basis is absolutely imperative."

Findings from the conference will be used to help shape the advice the department is preparing for the government in terms of the 2020 Cyber Security Strategy, Pezzullo concluded.

He said the government is seeking to determine what parts of the existing strategy — which was developed in 2016 — remain fit for purpose and should be retained, and what parts should be replaced.





# ETHICAL AI FOR DEFENCE FORCES

Dylan Bushell-Embling

**A**s militaries the world over grapple with pros and cons of automating warfighting capabilities, the US Department of Defense has adopted a list of five ethical principles to govern the use of AI by US armed forces. The guidelines, which have been developed following 15 months' consultation with AI experts, aims to fulfil the department's purported objective of ensuring the US military lead the way in the development of AI ethics and the lawful use of AI systems.

According to the principles, the use of AI in warfare and national defence should be responsible, equitable, traceable, reliable and governable.

In practical terms, this will involve approaches including taking conscious steps to minimise unintended bias in AI capabilities, as well as setting explicit, well-defined uses for AI and engineering AI capabilities to avoid unintended consequences.

This includes "the ability to disengage or deactivate deployed systems that demonstrate unintended behaviour" —

meaning a hypothetical "Skynet" style AI could be shut off before going rogue and ushering in the apocalypse.

As part of the initiative, the department's Joint Artificial Intelligence Center will take the role of coordinating implementation of AI ethical principles within the defence forces. The centre is already hosting working groups to solicit input from services and AI and technology experts throughout the department.

The US Secretary of Defense, Dr Mark Esper, who drafted the recommendations the principles are based on, called on US allies — including Australia — to accelerate the adoption of AI in defence.

"The United States, together with our allies and partners, must accelerate the adoption of AI and lead in its national security applications to maintain our strategic position, prevail on future battlefields and safeguard the rules-based international order," he said.

"AI technology will change much about the battlefield of the future, but nothing will change America's steadfast commitment to responsible and lawful behaviour."

### AI AND AUSTRALIA

Australia's defence sector is accordingly grappling with similar issues surrounding the ethical use of AI. Last year in Canberra, the Defence Science and Technology Group jointly led an Ethical AI for Defence workshop to address ethics across a range of military applications for AI.

The workshop was also led by Plan Jericho and the Trusted Autonomous Systems Defence Cooperative Research Centre, and included representatives from the ADF, the Centre for Defence Leadership and Ethics, and industry, universities and institutes from Australia and overseas.

The workshop was one of the first steps towards the development of Defence's own ethical principles for the use of AI, as well as a roadmap for ethical AI use in the future.

In a recent blog post, Australian Army Major Daniel Lee said it will be important for the defence sector to build an interdisciplinary understanding of three aspects of the use of deployment and use of AI.

The first of these is understanding the technology, which will require developing a common lexicon about the nascent field. The second is strategy, which will involve understanding potential current and future uses of AI and autonomous systems. The final is ethics, and will require understanding whether individual strategies about the use of AI should be pursued.

"A broad understanding of the technological, strategic and ethical principles relevant to the potential employment of AI and autonomous systems will set the foundations for an informed discussion not only within Army, but also within the wider Australian Defence Force, society and parliament," Lee said.

"Only once Army understands what AI and autonomous systems are, and why and how they may be used, can we begin to discuss if they should be used in a military context at all."

# OPEN GOVERNMENT AND DIGITISING THE CUSTOMER EXPERIENCE

Christine Jones, Lyn Nicholson and Andrew Hynd

GOVERNMENTS ARE MAKING GREAT STRIDES ALONG THE ROAD TO DIGITISATION, BUT MANY PRIVACY AND ETHICS QUESTION MARKS REMAIN.

**G**overnments at all levels across Australia are continuing to push into digital transformation, with open government and digitising the customer experience being two of the overarching themes. Initiatives such as Service NSW's foray into digital driver's licences is a worthy example of this transition in service delivery.

With a massive take-up in the first 48 hours of being launched, the digital licence has been praised for streamlining and simplifying the customer experience, but data and privacy concerns have also been raised.

Service NSW — the single customer service division for the delivery of

government services — made great strides in 2019 in digitising forms and reducing the overall complexity of dealing with government.

But NSW is not alone in grappling with digital transformation — there are many initiatives underway across the states.

For example, the Queensland Government, as part of its DIGITAL1ST digital strategy for 2017 to 2021, is currently discussing projects such as digital hospitals, the use of drone technology to assist in turtle rehabilitation and new technology for emergency services.

At a Commonwealth level, a concerted approach is underway to develop a proposed national driver's licence facial recognition solution, with the Identity-

matching Services Bill 2019 the proposed statutory vehicle for implementing this.

Across the various states and at a national level, there are many legal angles to consider in bringing on these digital transformation initiatives, such as:

- Tortious liability — is there potential tortious liability associated with the initiative and how should governments seek to reduce liability?
- Copyright — are there copyright implications and how will they be treated?
- Permissible sub delegation of legislative authority — is there an express authorisation that enables the decision to be made by an electronic system?
- Personal information — is personal information involved and how will it be treated?
- Public accessibility and disclosure — will the information be accessible or can it be disclosed on application?

- Admissibility in court — will the data be admissible in a court or tribunal?
- Maintaining the digital record — what are the record-keeping obligations imposed?

## NSW: BALANCING DATA SHARING AND PRIVACY

The NSW digital strategy and the Open Data policy have allowed the sharing of government data on over 10,000 datasets and the development of many applications that have been useful to consumers, in particular concerning transport usage.

NSW has not been dogged by the problems that have persisted at a federal level, where de-identified or purportedly de-identified data sets have been released and subsequently been able to be re-identified.

NSW is set to remain at the forefront of digitisation, through the demonstration of a significant commitment to preserving privacy. This is led by the NSW Chief Data Scientist, Dr Ian Oppermann, one of the leaders in the field of de-identification and the editor of *Privacy-Preserving Data Sharing Frameworks – People, Projects, Data and Output*, published by the Australian Computer Society in December 2019. This publication has a forward written by the NSW Minister for Customer Service.

However, this has not always been the case and the introduction of the Opal card — which enabled individuals to be tracked — raised the ire of many... in particular, the then NSW Information and Privacy Commissioner. It resulted in a private action being taken by a privacy advocate who initially was successful in the NSW Civil and Administrative Appeals Tribunal (NCAT) in February 2018. It was claimed that Transport for NSW had breached the individual's privacy and the NSW Privacy and Personal Information Protection Act, but in August 2018 the NCAT Appeal Panel set aside the decision.

All of this change is occurring as the tide of trust in digital platforms appears

*“However, with the push to use digital technology comes a number of challenges to ensure that data is used properly and citizens’ privacy is protected.”*

to be slowly turning and individuals are moving to take back control of both their data and digital personas. NSW appears well placed to operate in that environment, balancing data sharing and privacy.

## QUEENSLAND: THE DIGITAL1ST STRATEGY

The Queensland Government is seeking to lead the way in digital government as part of its DIGITAL1ST digital strategy which, the government predicts, will save millions of dollars per year.

Queensland is also looking at projects such as digital driver's licences, with a trial of a digital app due to be released in the Fraser Coast region in the coming months.

However, with the push to use digital technology comes a number of challenges to ensure that data is used properly and citizens' privacy is protected. Already there have been challenges over the state government's digital hospital projects, with concerns that Queensland Health's integrated electronic medical record software was causing a spike in mislabelling of blood tests.

Following privacy concerns relating to the introduction of My Health Record nationally, the focus is on ensuring these new technologies are used in the right way, without jeopardising patient privacy.

In this light, Queensland's current privacy regime presents potential concerns. The *Information Privacy Act 2009* (Qld) provides a regime that is generally seen to be in need of review and updating, particularly in light of global privacy standards having been lifted to a much higher bar recently

through introduction of the European General Data Privacy Regulation (GDPR) and other similar regimes. Notably, the Commonwealth Government's intention is to amend the *Privacy Act 1988* (Cth) to bring in higher penalties more in line with GDPR, even though it was last updated more recently (in 2018) than the Queensland legislation.

However, it should be noted that there has been a potential increase in privacy protection for Queenslanders with the enactment of the *Human Rights Act 2019* (Qld), which provides protection from unlawful or arbitrary interference by government with a person's privacy.

Another key area for government to consider in relation to privacy relates to emerging technologies such as drones. Current regimes are not designed to apply to this type of technology, and leave citizens uncertain as to their rights and obligations in relation to potential invasions of privacy by drones.

A further key question for the government is the emerging area of data ethics, reflecting the increasing focus not on simply “can data be collected and used?” but on the question of “should data be collected and used?” In the light of a significant drop in trust by consumers generally, prompted by major data breaches on an almost daily basis, a strong approach on the ethical collection of data can be a significant step in restoring that trust.

*Christine Jones is Construction & Infrastructure Partner at law firm Holding Redlich, while Lyn Nicholson is Corporate & Commercial General Counsel and Andrew Hynd is Corporate & Commercial Partner.*



# AUSCERT AT THE FOREFRONT OF CYBERSECURITY

AUSCERT HELPS MEMBERS PREVENT, DETECT, RESPOND TO  
AND MITIGATE CYBER AND INTERNET-BASED ATTACKS.

**B**ased at The University of Queensland, AusCERT was formed over 26 years ago as a global pioneer of cybersecurity intelligence and a leading cyber emergency response team (CERT) in the Australian and Asian-Pacific region. As a not-for-profit security group, AusCERT helps members prevent, detect, respond to and mitigate cyber and internet-based attacks.

AusCERT Sensitive Information Alerts notify organisations about specific breaches and provide members with alert notifications by email and SMS when sensitive material specifically targeting their organisation is found online by the AusCERT analyst team.

"Data breaches, credential dumps and sensitive documents are uploaded to the public web every minute of every day," said AusCERT Senior Manager Mike Holm. "This can be done by malicious individuals, oblivious contractors and even well-meaning staff.

"Sensitive Information Alerts give analysts and IT managers the best

chance to quickly get on top of the issue and contain potential damage to their organisation."

The problem for most organisations is that the human resources, time and financial cost involved to keep track of possible data breaches is unaffordable. According to Holm, this is the main reason why organisations of all sizes use AusCERT's Sensitive Information Alerts service.

AusCERT offers a range of 24/7 services including SMS Alerts. Clients choose the services they require or AusCERT can customise a bespoke solution to suit specific security needs. Services available include:

**Incident Management** Use proactive or reactive services (or both) to help detect, interpret and respond to attacks from anywhere across the globe.

**Phishing Take-Down** AusCERT's strong international CERT relationships mean we have a high success rate in delivering phishing take-downs as soon as possible after they are detected.

**Security Bulletins** AusCERT members can get up-to-date and consistent

security bulletins from a wide range of vendors, making it much easier to streamline security patching.

**Security Incident Notifications** Daily Member Security Incident Notifications (MSINs) are customised to each member's network to keep members ahead of any potential security problems.

**Malicious URL Feed** When added to a member's firewall blacklist and SIEM, this Australian-based feed helps prevent local network compromises.

**Sensitive Information Alert** Alert notification is provided to members via email when sensitive material specifically targeting their organisation is found online by the AusCERT analyst team.

**Early Warnings** SMS notifications are available for the most critical security threats and vulnerabilities.

There are also a number of other add-ons and a range of countermeasures available. For more information, contact AusCERT via [membership@auscert.org.au](mailto:membership@auscert.org.au).

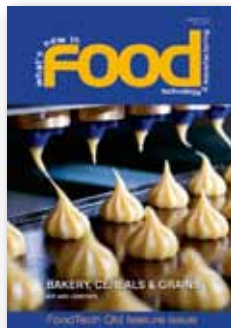
AusCERT  
[auscert.org.au](http://auscert.org.au)

# FREE

for government and industry professionals



The magazine you are reading is just one of **11** published by Westwick-Farrow Media. To receive your **free subscription** (print or digital plus eNewsletter), visit the link below.



[www.WFMedia.com.au/subscribe](http://www.WFMedia.com.au/subscribe)





TECH IN GOV

14<sup>th</sup> Annual Tech in Gov

4 - 5 August 2020

National Convention Centre, Canberra

Co-located with:



**Australia's largest ICT event for the government**

**2000+ attendees • 120+ speakers • 3 co-located events**

**BOOK YOUR CONFERENCE PASS TODAY**

## EXPLORE

the role of next-gen technologies  
in executing strategy and  
enhancing service delivery



**APPLY TO SPEAK**

### Exhibitor or Sponsor

techingov@terrapinn.com  
+61 2 8908 8515

## DISCOVER

how international governments are  
leveraging technology to better  
serve their citizens



**APPLY TO EXHIBIT**

### Apply to Speak

benton.ng@terrapinn.com  
+61 2 8908 8527

## NETWORK

with other government  
professionals, the private sector  
and entrepreneurial community



**REGISTER NOW**



Quote  
'GOVTECH20'  
**SAVE 20%**

**REGISTER ONLINE**

**www.techingov.com.au | +61 2 8908 8555**