UNITED STATES MARKET INSIGHTS REPORT

Australian Government
Department of Industry, Science, Energy and Resources
Industry Growth Centres

AustCyber
Australian Cyber Security Growth Network

CONTENTS

INTRODUCTION 3

STATE OF PLAY 5

Australia/United States Free Trade Agreement (AUSFTA) 5

US NATIONAL CYBER STRATEGY 7

Critical Infrastructure Cybersecurity Policy 7

US DEPARTMENT OF DEFENSE EXPENDITURE 9

ACCELERATORS AND INNOVATION 11

Federally Funded Research and Development Centers (FFRDC) 11

Federal Risk and Authorization Management Program (FedRAMP) 11

CYBER SECURITY STANDARDS AND REGULATION 13

National Institute of Standards and Technology (NIST) 13

National Initiative for Cybersecurity Education (NICE) Framework 13

International Traffic in Arms Regulations (ITAR) 13

Cyber Maturity Matrix Certification (CMMC) 14

Health Insurance Portability and Accountability Act (HIPAA) 14

Other US State laws 14

New York Cybersecurity Regulation (23 NYCRR 500) – Financial Services 15

CYBER SECURITY OPPORTUNITIES 17

Data and privacy 17

Security awareness and training 18

Detection and response 19

INVESTMENT OVERVIEW 21

Who are the major industry players? 21

CONSIDERATIONS FOR ENTERING THE US 23

REFERENCES 24

INTRODUCTION

Cyber security continues to be one of the largest growth markets globally; driven by the increased need for secure data solutions, privacy and transactional data, and the introduction of emerging technology that relies on the security of data transmission. The global cyber security market is currently worth around US$145 billion and is set to increase by 86 per cent to US$248 billion by 2026.[i]

This report is the first in a series that AustCyber is producing as part of its global engagement strategy to assist Australian cyber security companies looking to scale and expand into international markets.

These reports will provide insight into selected priority markets and detail areas of growth, opportunities and risks for Australian cyber security product and service exports. The reports will align closely with AustCyber's initiatives and activities in each region over the next two years, providing clear direction for Australian cyber companies looking to scale.

The priority regions and markets are:

1. **The Americas** – United States, Canada and Latin America
2. **United Kingdom** – EU, Ireland and Germany
3. **Indo-Pacific** – Singapore, Indonesia and Malaysia (includes reference to Thailand, Vietnam, Philippines and India)

STATE OF PLAY

The decentralised provision of cyber security in the US (and global) markets means that demand is large, diverse and constantly changing. In 2019, the global cyber security market size was valued at US$145 billion and it is projected to expand at a CAGR of 15.6 per cent to US$270 billion by 2026. The United States will generate much of this demand, both for its domestic market, but also because many global organisations locate cyber security decision-making in the US.

The sectors of focus driven by broader federal government requirements and current expenditure include:

- transport;
- critical infrastructure;
- healthcare;
- financial services;
- government – federal and state;
- retail; and
- energy and utilities.

Investment and spending trends within these sectors across the US and global markets include:

- security and resilience of supply chains;
- data and privacy;
- detection and response;
- security awareness and training;
- cyber policy and compliance;
- managed security services; and
- cyber insurance.

According to the *Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac,* legacy systems particularly in the health, energy and utility sectors pose challenges in outdated processes and technology.[ii] This provides an opportunity in the managed security services solutions area to reduce overheads and allow cyber security functions to manage systems more effectively and efficiently.

Australia/United States Free Trade Agreement (AUSFTA)

A free trade agreement was established between the US and Australia in 2005. The US is the largest and most significant investor in Australia, accounting for 27 per cent (AU$939 billion) of Australia's total foreign investment stock as of December 2018.[iii] The US is also by far Australia's largest foreign investment destination, accounting for 28 per cent (or AU$719 billion) of Australia's total overseas investment stock as of December 2018. Two-way investment has almost tripled since the agreement came into force.

In 2018, the US was Australia's third-largest two-way trading partner in goods and services, worth AU$73.9 billion. Australia's goods and services exports to the United States were AU$23.1 billion.[iv]

Under AUSFTA, Australian companies have a competitive advantage as the agreement states that Australian companies pay no tariffs/import duties and have no quota restrictions on several product/sector areas. Additionally, Australian companies have access to streamlined customs procedures and a number of market access opportunities only open to Australian companies. The AUSFTA provides access to the federal government procurement market in the United States (valued at over US$535 billion) and the government procurement markets of 31 US states.

US NATIONAL CYBER STRATEGY

The US released its first cyber strategy in over 15 years in September 2018. The strategy aligns with its National Security Strategy and is built around four key pillars:

- defend the homeland by protecting networks, systems, functions, and data;
- promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;
- preserve peace and security by strengthening the United States' ability – in concert with allies and partners – to deter and if necessary, punish those who use cyber tools for malicious purposes; and
- expand American influence abroad to extend the key tenets of an open, interoperable, reliable and secure Internet.

There is a particular focus on enhancing and protecting critical infrastructure, also covering supply chain, information sharing and data storage.

President Biden has highlighted cyber security as a continuing top priority for his Administration. This renewed focus follows the recent SolarWinds incident, among many other malicious intrusions. The Biden Administration is preparing an Executive Order on cyber security that will likely focus on companies seeking to do business with the federal government. This will focus on procurement of cyber tools from industry and encourage greater collaboration between the private sector and government to build a safe and secure online environment for all Americans. These changes to the federal procurement process will be to achieve 'trickle-down' reforms to the private sector. It is also likely to impact the policies of other nations.

President Biden has nominated the first National Cyber Director; a demonstration of the Biden Administration's commitment to lean forward in cyber security and harden government and industry computer systems against hacks and other online intrusions. The National Cyber Director is a position created by Congress and recommended by the Cyberspace Solarium Commission.

The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to *"develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences."*

The recently released Cyberspace Solarium Commission report 2020[v] delivers a strategy of layered cyber deterrence and contains 80 recommendations organised into six pillars. The report recommends a joint collaborative environment that will allow the fusion of threat information, data and insights from across government, state and industry. There are also recommendations to increase the powers and budget of the CISA to address gaps within critical infrastructure, and the ability to respond to and the resilience against a cyber event.

Critical Infrastructure Cybersecurity Policy

Executive Order 13800, May 2019 – updated;[vi] signed by President Trump has allocated specific outcomes to focus on cyber security across critical infrastructure networks. The order builds on Executive Order 13636, Feb 2013[vii] President Obama – Improving Critical Infrastructure Cybersecurity and Executive Order 13800, May 2017.[viii]

The Executive Order 13800 focuses on three specific areas:

- cyber security of federal networks;
- cyber security of critical infrastructure; and
- cyber security for the nation.

The application of EO13800 includes the development of new cyber security approaches that use emerging technologies, improving information-sharing and risk management related to cross-sector interdependencies, and building resilience to large-scale or long-duration disruptions. This will be applied across all federal agencies, and consequently, wider adoption through the DIB and larger organisations providing services to government agencies.[ix]

Recent events linked to the US election, data collection and the influence of tech companies over wider social issues have raised a number of issues in the minds of US citizens.

The Biden Administration released the US$9B American Rescue Plan in January 2020. There were 77 recommendations to assist US federal cyber security challenges, including assistance to the US Cybersecurity and Insfrastructure Security Agency (CISA) and the General Serice Administration (GSA) to complete cyber security and IT modernisation projects. This included re-establishing security expert positions to work in the Office of the US CISO and White House positions. There was also funding for a CISA project designed to improve monitoring and incident response across US Federal agencies.

This new spending is in direct response to the SolarWinds supply chain hack which affected federal agencies including Treasury, Commerce, Homeland Security, Justice and Energy Departments, as well as a number of other private firms.

The 2021 National Defense Authorization Act (NDAA) includes 77 security provisions, including restoring the position of National Cyber Director at the White House, a position made defunct under the previous Administration.

27 of the 77 cybersecurity recommendations contained within the NDAA are based on recommendations from the Cyberspace Solarium Commission report released in 2020.

US DEPARTMENT OF DEFENSE EXPENDITURE

As an indication of the scale of these opportunities, the US Federal Government will spend an estimated US$17.4 billion on cyber security in FY2020 – up $790 million from 2019. The largest portion of this, more than 50 per cent, is cyber spending by the US Department of Defense for a total of US$9.6 billion in FY2020. The Administration requested US$9.8 billion for FY2021.[x]

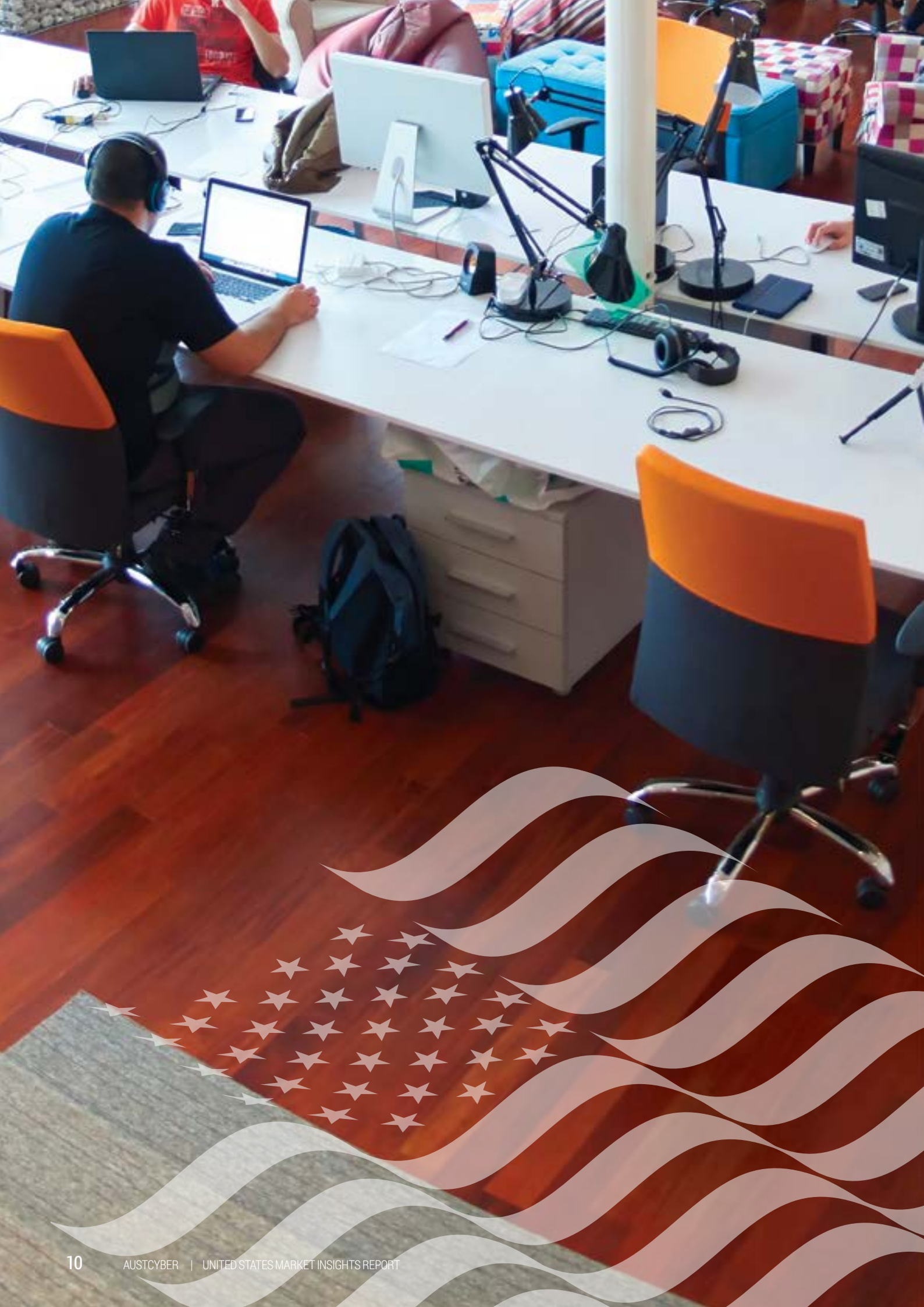
Agency	Funding FY2020 (USD)
Department of Defense	9643M
Department of Homeland Security	1919M
Department of Justice	881M
Department of the Treasury	522M
Department of Energy	557M
Department of Veteran Affairs	513M
Department of Health & Human Services	460M
Department of State	400M
Department of Commerce	392M
Department of Agriculture	311M
Total USD	**$15,598M**

Defense expenditure on cyber security is predicted to increase as the US is still in the early stages of understanding how to apply cyber security to weapon systems under development. According to the US Department of Defense (DoD), the next largest recipients of federal cyber security funding are the Department of Homeland Security (DHS – US$1.9 billion), Department of Justice (US$881 million), Department of Energy (US$557 million) and the Department of Treasury (US$522 million).

Australian companies can apply for US Federal Government procurement program, but must meet foreign ownership requirements. This can be also be achieved by partnering with US companies.

The US Federal Government publishes many opportunities to sell cyber security solutions to governments, defence and intelligence communities regularly on the System for Award Management website SAM.gov– formerly known as FedBizOpps or FBO.gov. Many of these opportunities are also open to contractors from outside the US, although all successful bidders (US and non-US) must conform to multiple US regulations (for example, the US Federal Acquisition Regulation (FAR)).

US Federal Government regularly publish procurement tenders. These programs are advertised publicly and are available to view and apply online.



ACCELERATORS AND INNOVATION

US Federal agencies, including the recently established US Space Force,[xii] vary in terms of the types of companies and solutions that they target, although most seek cyber security solutions of one form or another. Some examples are:

- US Air Force's AFWERX
- Department of Homeland Security's Silicon Valley Innovation Program
- Defense Innovation Unit (DIU)
- Similar agencies are also emerging around the US Army (Army Futures Command/Army Applications Lab), the US Navy (NavalX), the Special Operations Command (SOFWERX) and the National Geospatial-Intelligence Organization (Silicon Valley Outpost)
- The Rapid Innovation Fund (RIF) provides a collaborative vehicle for small businesses to provide the US DoD with innovative technologies that can be rapidly inserted into acquisition programs that meet specific Defense needs. RIF is administered by the Under Secretary of Defense for Research and Engineering (USD(R&E)) Small Business and Technology Partnerships (SBTP).

In-Q-Tel (IQT) I[xiii] was established in 1999 to ensure that the United States' intelligence agencies had access to innovative technologies from the startup community to help protect and preserve US national security. CIA leaders recognised that technological innovation had largely shifted from the purview of government, R&D and large organisations to entrepreneurs and the startup community who were developing much-needed technologies in a quicker, less expensive way.

IQT provides a technical vetting capability where new deep tech innovative capabilities are matched with partner mission capability needs. IQT established an Australian subsidiary located in Sydney, in an effort to boost Australian national security posture and innovation – leveraging the five eyes relationship. Through their investment capital arm, they have invested in two Australian cyber security companies.

Federally Funded Research and Development Centers (FFRDC)

Federally funded research and development centers are not-for-profit organisations that contribute to solving large-scale problems. They work closely with US Government and operate under the Federal Acquisition Requirements (FAR). FFRDC's do not compete with industry, but provide impartial advice to government on large technical problem sets, as well as creative and cost-effective solutions to national problems. FFRDC's work in the fields of aviation, defense, energy, health and human services, space, federal agency modernisation and homeland security.

MITRE[xiv] is one such example of an FFRDC. MITRE operates NIST's National Cybersecurity FFRDC (NCF) – which is dedicated to cyber security and the advancement of secure technologies. The NCF advises NIST and the National Cybersecurity Center for Excellence (NCCoE). The NCCoE is a private public partnership and collaborative hub where government, industry and academia work together on national cyber security challenges for business infrastructure. One example of the work developed by MITRE as a FFRDC is the MITRE ATT&CK Framework.

Federal Risk and Authorization Management Program (FedRAMP)

The Federal Risk and Authorization Management Program[xv] is a government-wide program that provides a standardised approach to security assessment, authorisation, and continuous monitoring for cloud products and services for government. Currently, there are 190 FedRAMP authorised cloud providers and 37 authorised assessors in the program. Work is underway for the cyber maturity matrix certification to give reciprocity for any vendor that has the authority to operate with the federal government through FedRAMP or through a third-party certification system.

CYBER SECURITY STANDARDS AND REGULATION

The US Department of Commerce sets standards for cyber security in defence, government and commercial sectors that often have global impact. Companies selling into defence supply chains must comply with the US DoD's Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

In cyber security governance outside of defense and intelligence communities (although often working closely with them), the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) often takes a leading role, although many other federal, state and municipal agencies are active in the sector.

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology[xvi] cyber security program supports its overall mission to promote US innovation and industrial competitiveness by advancing measurement science, standards and related technology through research and development. The NIST cyber security framework integrates industry standards and best practices to help organisations manage their cyber security risks. It provides a common language that allows staff at all levels within an organisation – and at all points in a supply chain – to develop a shared understanding of their cyber security risks. The NIST cybersecurity framework is used by 30 per cent of US organisations and is projected to grow to 50 per cent by 2020. This framework is supported by AustCyber through the National Initiative for Cyber Education (NICE).

National Initiative for Cybersecurity Education (NICE) Framework

National Institute of Technical Standards (NIST) has developed the National Initiative for Cybersecurity Education (NICE), which is a partnership between government, academia and the private sector focused on cyber security education, training, and workforce development. The mission of NICE is to energise and promote a robust network and an ecosystem of cyber security education, training and workforce development. The NICE skills framework has been endorsed by US Government and is a key factor in selecting and identifying skills for current and prospective employees. DoD, Department of Homeland Security and the Department of Labor are all currently implementing the framework.

International Traffic in Arms Regulations (ITAR)

International Traffic in Arms Regulations is the US regulation that controls the manufacture, sale and distribution of defense and space-related articles and services as defined in the United States Munitions List (USML). ITAR is interpreted and enforced by the US Department of State. Foreign organisations, including Australian cyber security companies, must be compliant with requirements if they are utilising and storing controlled unclassified information (CUI) and ITAR information. Further, this information must be stored in a cloud resource that resides on a FedRAMP approved cloud provider.

Cyber Maturity Matrix Certification (CMMC)

The Cyber Maturity Matrix Certification (CMMC) from the Office of the Under Secretary of Defense for Acquisition and Sustainment[xvii] was introduced in March 2020. This program will become the standard requirement to operate within the US Government acquisition and procurement process. All businesses must become certified and it will be a 'go, no go' process. Any company within the DoD supply chain must be certified before commencing work with the DoD. This is a direct change from the previous DFAR's requirements.

The US DoD has introduced an interim rule to DFARS that will see the CMMC rolled out in phases over the fiscal years 2021–2025. This will include a pilot to implement CMMC Level 3 requirements and below on new acquisitions. The interim rule will allow the US DoD to verify the protection of Federal Contract Information (FCI) and Controlled Unclassified Information (FCI) with the unclassified networks of the Defense Industrial Base (DIB).

The CMMC is a unified cyber security standard for contractors that are part of the Defence Industry Base (DIB). The standard is assessed across one to five levels of maturity. This will include at the highest maturity level 171 embedded practices and processes to ensure security and compliance with suppliers who hold Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The matrix covers basic cyber hygiene to advanced/progressive capability – these are commensurate with the level of information/capability that the supplier provides and manages. The CMMC requires compliance with the FAR/NIST requirements and has also referenced the Australian Cyber Security Centre's Essential 8 and the United Kingdom's Cyber Essentials.

The adoption of the CMMC across the DIB will create both opportunities and risks for Australian companies looking to enter the market to work with US Government agencies. This includes, but is not limited to reporting, capability tools, skilling and education, data management and encryption. Australian companies should also consider the level of CMMC that may be required in order to operate with US Government agencies. All companies within the US acquisition and procurement cycle will be required to be fully compliant by 2025.

Companies compliant in the Cyber Maturity Matrix Certification (CMMC) will be well positioned to apply for work within the US Federal Government and critical infrastructure.

Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA Privacy Rule was established in 1996 and introduced by the US Department of Health and Human Services (HHS). HIPAA established national standards to protect individuals' medical records and other personal health information, and applies to health plans, healthcare clearing houses and healthcare providers who conduct certain transactions electronically.

HHS reported that $6.2 billion was lost in 2016 by the US healthcare system due to data breaches.[xviii] HIPAA applies to all healthcare providers, health plans, and healthcare clearing houses if those organisations transmit health data electronically in connection with transactions for which the HHS has adopted standards.

Opportunities exist in detection and response, data and privacy compliance and auditing.

Other US State laws

US Congress has also recently introduced cyber security legislation that seeks to help states by providing grants to improve cyber security at state and local levels. S. 1065 and its companion bill, H.R. 2130, the State Cyber Resiliency Act, would assist states and local governments in coordinating resources, better responding to cyber threats and enhancing cyber resiliency through a series of state grants administered by DHS. Similarly, S. 1846, the State and Local Government Cybersecurity Act, provides funding to states for improved security measures and opportunities to collaborate with federal officials on cyber risks, defensive measure and threat indicators.[xix]

State legislatures' biggest priority in recent years – outside of election security – has been focused on improving cyber security practices within state government and increasing resources and training to combat cyber threats.

In 2019 at least 43 states and Puerto Rico introduced or considered close to 300 bills or resolutions that deal significantly with cyber security, including appropriations for cyber security. The top 10 categories of cyber security issues, other than appropriations, range from elections to connected devices.

New York Cybersecurity Regulation (23 NYCRR 500) – Financial Services

In March 2017, the New York State Department of Financial Services (DFS) implemented 23 NYCRR 500, generally referred to as the New York Cybersecurity Regulation. Its aim is to encourage financial services firms doing business in the state to minimise their security risks.

23 NYCRR 500 requires financial institutions to meet certain regulatory minimum standards to assist organisations in preventing data breaches, including:

- Risk-based minimum standards for information technology systems, including data protection and encryption, access controls, and penetration testing.
- Requirements that a program is adequately funded, overseen by a chief information security officer (which can include a third-party service provider), and implemented by qualified cyber security personnel.
- Effective incident response plans that include preserving data in order to respond to data breaches including notice within 72 hours.
- Accountability provided by identification and documentation of deficiencies, remediation plans, and certifications of compliance on an annual basis.
- Audit trails designed to detect and respond to cyber security events.
- Annual reports covering the risks faced, all material events, and the impact on protected data.

Opportunity exists for capabilities in cyber policy and compliance, audit, risk assessment and incident response planning for application in the financial services sector as a result of new cyber regulation 23 NYCRR 500.

A summary of key regulations and frameworks in place in the US are below (note: this list is not exhaustive):

NIST – National Institute of Standards and Technology

ISO – International Organization for Standardization

PCI-DSS – The Payment Card Industry Data Security Standard

CCPA – California Consumer Privacy Act

SOC – Sarbanes-Oxley Act

GLBA – Gramm-Leach-Billy Act

FedRAMP – Federal Risk and Authorization Management Program

ITAR – International Traffic in Arm Regualtions

NERC CIP Standards – NERC Critical Infrastructure Protection Standards

CIS Controls – Center for Internet Security Controls

HIPAA – Health Insurance Portability and Accountability Act

GDPR – General Data Protection Act

AICPA – American Institute of Certified Public Accountants

COBIT – Control Objectives for Information Related Technologies

FISMA – Federal Information Security Modernization Act

FERPA – Family Educational Rights and Privacy Act

COPPA – Childrens Online Privacy Protection Rule

CYBER SECURITY OPPORTUNITIES

Data and privacy

Data continues to grow increasingly important as it is the building block of a digital economy. It is expected that globally there will be over 96 zetabytes of data by the end of 2020.[xx] The continued growth of IoT and subsequent data demand will bring opportunities in secure cloud, privacy, data management and orchestration, machine learning and evolving AI.

The *Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac* sites that the digital attack surface is increasing exponentially, with the number of IOT devices predicted to rise globally to up to one trillion devices by 2022.

This will provide opportunities in the areas of data and privacy, cyber policy and compliance requirements, detection and response, security awareness and training, password management and cyber insurance. Importantly, whilst large organisations often have budget and resources to manage these requirements, this is not always the case. Small to medium businesses will struggle to manage these services with internal resources, therefore driving a need for comprehensive managed services.

There is an opportunity for solutions targeted to small and medium businesses in data management and orchestration, privacy solutions, cyber policy and compliance, detection and response, security awareness and training, password management and cyber insurance.

The recent US 2020 election events and the growing amount of private data online will continue to raise opportunities for data security solutions that translate easily and effectively to the broader public and SMBs. There is a continuing focus on data privacy as the general US population grows more informed about security, their rights and impacts of identity theft.

Consumers are becoming more aware of cyber security and will, over time, make the decision not to work with companies with a poor track record or with companies who they deem they cannot trust when it comes to privacy and data-management. This presents an opportunity for companies that offer solutions in data and privacy protection, as well as solutions that enhance and provide consumer protection and awareness.

The US does not have a comprehensive data privacy law, but has several sectoral laws, many of which contain data and information privacy regulations. Many companies who operate internationally adhere to the requirements under the UK General Data Protection Regulations (GDPR) and the recently passed California Consumer Privacy Act (CCPA). There is continued support to enact a comprehensive law, however, this is unlikely anytime soon. Currently, the states of California, Massachusetts, New York, Hawaii, Maryland and North Dakota are the only jurisdictions with data privacy laws in place. As more businesses move towards cloud in on-prem and remote, there will be greater requirement to understand the data and the where, what, who has access and how to monitor for compliance.

Companies who hold large volumes of private and personal data are under continued scrutiny. This provides an opportunity for Australian cyber companies that offer solutions in enhanced reporting or data and privacy protection. The health, retail and financial sectors in particular are looking for solutions.

The increased adoption and availability of machine learning technologies, Artificial Intelligence and 5G, together with the ongoing and growing requirement for data orchestration and resilience will also be key trends for 2021–2022. These elements combined with the 'ever increasing speed to market' of threats will continue to give rise to opportunities for Australian cyber businesses with technology solutions in these spaces.

With the advent of AML, AI and 5G, opportunity for solutions in data orchestration and resilience are key trends forecasted out to 2022.

Security awareness and training

Cyber security skills continue to be a major challenge for US Government and companies. The implementation of new and emerging technologies will continue to drive strong demand for skilled talent and capability to generate new solutions and support cyber security technologies from implementation to operation. There is also increasing need for cyber security skills in non-traditional, but aligned sectors of health, retail and supply chains.

There are a number of initiatives underway across the US Federal Government to partner with academic institutions to develop a cyber security workforce. There is a continued focus for online training for cyber security professionals that is aligned with federal government requirements outlined under 8570[xxi] and 8140 Department of Defense Approved Baseline Certifications. These certifications are the reference used for hiring cyber security professionals into the federal government workforce. Whilst not mandatory for state government, many Defense Primes and providers to government adhere to these recommendations.

The US Department of Labor, Department of Homeland Security and the Department of Defense are all currently utilising the NICE Cybersecurity Workforce Framework. Australian training providers should note these requirements and apply as needed to their approaches.

Detection and response

The curve-ball that is COVID-19 has identified a number of areas of opportunity in supply chain resilience. The emergence of non-state adversaries and e-criminals trying to take advantage of the virus is another indicator that any future events like this will drive risk across the market. It will be imperative that businesses position themselves to deal with this now and for future events. The lack of skilled cyber security professionals will only exacerbate this challenge.

In addition, the self-isolation requirements of COVID-19 for personnel has driven many to online services that were not previously well utilised, such as banking services and online facilities. There has been a significant rise in online services such as virtual medical appointments, groceries and medications. Opportunities exist to assist businesses to understand their customers and shopping needs, particularly around big data analytics and supporting the customer online experience.

The growing introduction of smart warehouses and IOT solutions will give rise to increased attention from online hacking and phishing attempts.

Healthcare and hospitals are emerging as a valuable target for cybercriminals looking to gain access to personal and patient information. Hospitals are vulnerable as they often have legacy systems and a lack of experienced cyber personnel.

The increasing need for data for businesses to operate effectively will see an increased need in interoperability between current and new solutions and the ability to continue to operate in times of crisis. Security solutions that meet the needs for an enterprise solution, particularly for a distributed workforce, e-commerce platforms, manufacturing, defence and healthcare will grow in need and complexity.

A continuing risk in this space will be the budgetary constraints that are levied on existing security budgets and the ability of CISO's and CIO's to allocate and redirect this budget to new solutions or emerging technologies that provide solutions within enterprise security options and data management.

INVESTMENT OVERVIEW

Investment in cyber security startups continues to be a hot point in the private venture capital market.[xxii] The top ten US based VC investors (Accel, Sequoia Capital, Redpoint Ventures, Bessemer Venture Partners, New Enterprise Associates, ClearSky, Bain Capital, Paladin Capital Group, GGV Capital and M12) participated in 90 funding rounds with total proportionate investment value of $825 million in 2018.

In 2019, the capital investment in cyber security[xxiii] hit an all-time high – the average deal size was $17.3 million, with a median of $7 million. A number of US VCs have already invested in Australian cyber companies including ForgePoint Capital and Paladin Capital Group. The outlook continues to be positive with interest intensifying in the last 12 months.

According to Gartner, cyber security spending is forecast to grow 9% a year from 2021–2024. This is across all industries and businesses of all sizes as they look to build capabilities and defenses needed to retain security in the new COVID-19 virtual backdrop.

Venture Capital firms may also take a hedge towards late-stage over early-stage deals. Areas of significant capital investment have included e-commerce, Artificial Intelligence, education technology, health technology, cloud migration and blockchain. Investment has been linked to technologies with a direct link to the pandemic economy.

COVID-19 has accelerated investment into cloud and remote-working budgets by organisations. However, there still remains some reluctance to proposed investments due to a low perceived risk or technology that has a lack of demonstrable ROI. There exists the opportunity to educate boards to comprehend the scale of threats when making investment decisions.

Examples like the SolarWinds hack will influence this ongoing education and interest by boards investing in technology solutions.

Who are the major industry players?

The US market is highly segmented. In 2018, the top three suppliers accounted for less than 6 per cent of global (as opposed to US) military cyber security sales and the top ten accounted for just over 11 per cent. The top ten contractors in US military cyber security in 2017 were: General Dynamics-CSRA, Raytheon, SAIC-Engility; Lockheed Martin, CACI International; Harris-L3, Northrop Grumman, Booz Allen Hamilton, ViaSat and Leidos.

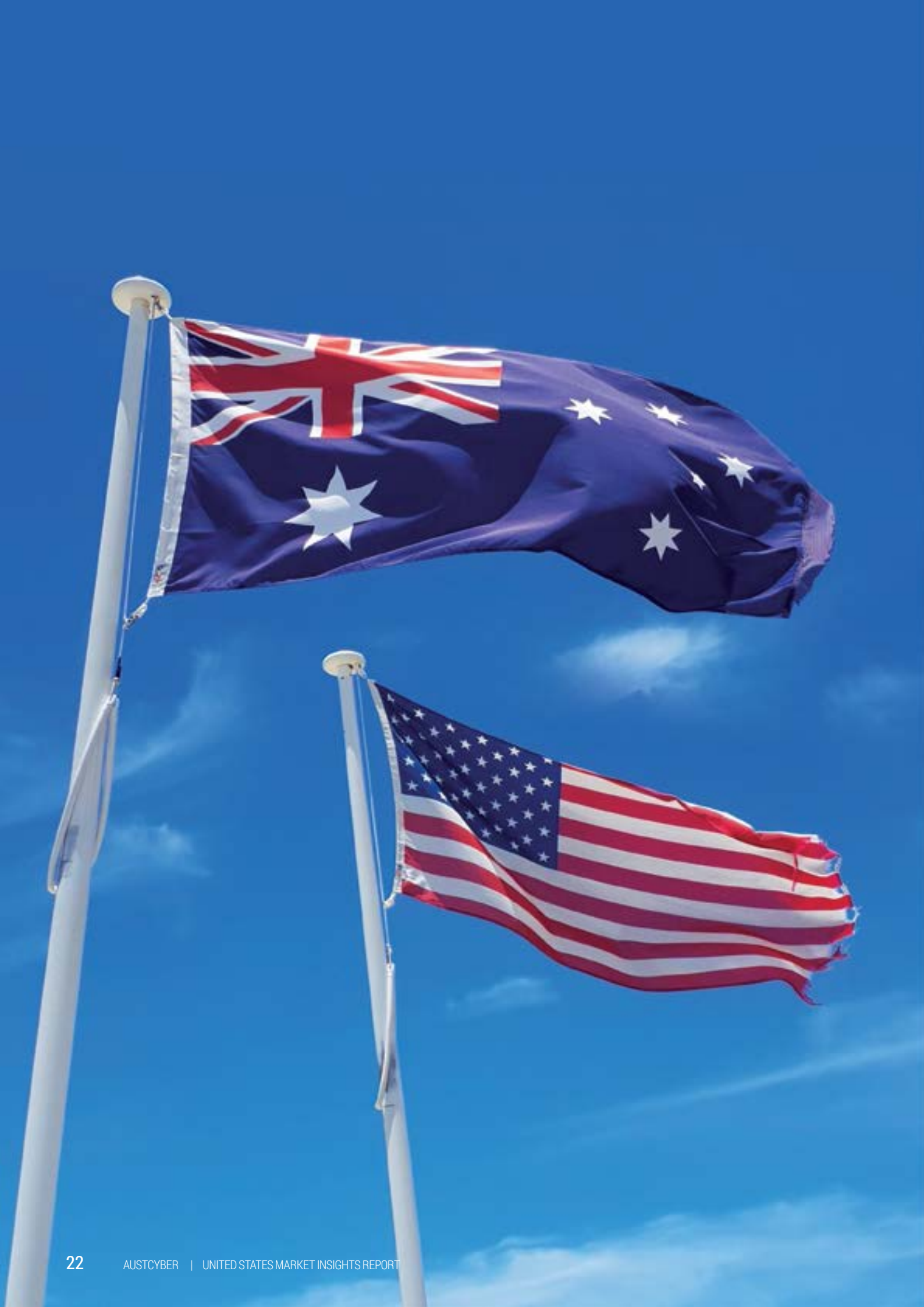
The top players active within the US cyber security market include Symantec, FireEye, Crowdstrike, Fortinet, Palo Alto, CyberArk, Synack, Carbon Black, Rapid7 and McAfee.

There are currently 2565 US cyber security companies currently active within the US market.[xxiv]

A guide range of businesses and their employee base is below:

- 1–100 employees = 1676 companies
- 101–1000 employees = 347 companies
- 1001–10 000 employees = 56 companies

Australian companies looking to enter the market need to have identified their niche area, researched available opportunities and contract vehicles. Another consideration to enter the market is under a partnership model, which may provide a unique offering. Particularly if this is with a US company to assist with access to contract vehicles or current programs/projects.



CONSIDERATIONS FOR ENTERING THE US

The close relationship between Australia and the US continues to see US companies willing to partner and engage with Australian companies for import and export opportunities. The AUSFTA and government to government relationships support this position.

Defence companies including Northrop Grumman, Boeing, Raytheon and Lockheed Martin all have global supply chain programs in place which could be effective vehicles to transfer Australian capability into the US ecosystem. There are a number of standing contract vehicles within each of these companies for capability that falls directly within the cyber security environment.

It is still important that companies considering doing business in the US take the time to understand the market and opportunities prior to launching within the US ecosystem.

Whilst opportunities do exist for Australian businesses to sell into the US Government market, consideration needs to be given to existing competition, as well as security and information requirements particularly focused on national security elements.

REFERENCES

i. Australia's Cyber Security Sector Competitiveness Plan 2019 Update

ii. https://cybersecurityventures.com/cybersecurity-almanac-2019/

iii. https://www.census.gov/foreign-trade/balance/c6021.html

iv. https://www.dfat.gov.au/trade/agreements/in-force/ausfta/Pages/australia-united-states-fta

v. https://www.solarium.gov/

vi. https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/

vii. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

viii. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

ix. https://www.lawfareblog.com/summary-cybersecurity-executive-order

x. https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf

xi. https://ww2.frost.com/news/press-releases/next-gen-technology-adoption-pushes-global-military-cybersecurity-market-toward-16-billion-by-2023/

xii. https://www.spaceforce.mil/

xiii. https://www.iqt.org/

xiv. https://www.mitre.org/centers/national-cybersecurity-ffrdc/who-we-are

xv. https://www.fedramp.gov/about/

xvi. https://www.nist.gov/industry-impacts/cybersecurity-framework

xvii. https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf

xviii. https://compliancy-group.com/hhs-hipaa-cybersecurity-guidance-for-healthcare-organizations/

xix. https://www.ncsl.org/research/telecommunications-and-information-technology/state-and-federal-efforts-to-enhance-cybersecurity.aspx

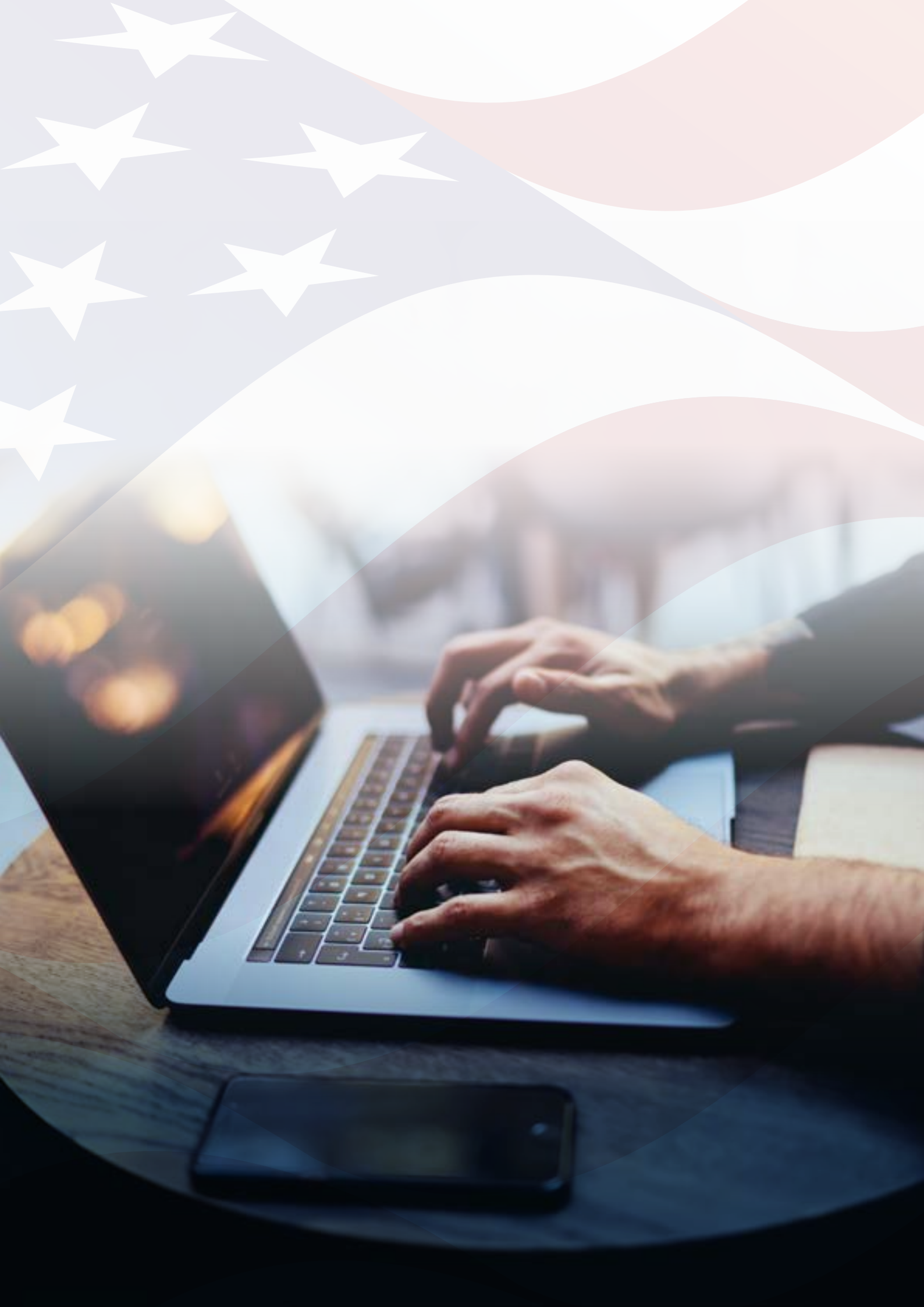
xx. https://cyber securityventures.com/cyber security-almanac-2019/

xxi. https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/

xxii. https://www.axios.com/cybersecurity-venture-capital-investment-2019-7cf466a8-a825-4ead-8aac-8520989ecbdc.html

xxiii. https://nvca.org/research/pitchbook-nvca-venture-monitor/

xxiv. https://www.crunchbase.com/search/organization.companies/field/hubs/org_num/united-states-cyber-security-companies



Contact

Email: info@austcyber.com

Phone: 0455 260 848

Website: www.austcyber.com

Twitter: @AustCyber

LinkedIn: AustCyber - The Australian Cyber Security Growth Network

Office: Unit 2, Level 4
1 Hobart Place
Canberra City ACT 2600

Australian Government
Department of Industry, Science, Energy and Resources
Industry Growth Centres

AustCyber
Australian Cyber Security Growth Network