Review team

It is with great pleasure that I attach our submission to the NICE Framework Request for Comments. I have copied Rodney Petersen, who graciously provided us with an extension to the deadline for this consultation process to enable us to broaden our engagement with Australian organisations.

Please do not hesitate to contact me or Prerana Mehta, our Chief of Ecosystem Development, should you wish to discuss any part of our submission. We understand the document will be made public and has been shared with Australian Government colleagues for reference.

Best regards

Michelle Price
Chief Executive Officer
AustCyber - the Australian Cyber Security Growth Network Ltd
@AustCyber | @Cyber_Roo
www.austcyber.com

AustCyber
Australian Cyber Security Growth Network

SUBMISSION

2020 NICE FRAMEWORK REQUEST FOR COMMENT

UNITED STATES NATIONAL INSTITUTE
OF STANDARDS AND TECHNOLOGY

JANUARY 2020

Introduction

The foundation of a resilient economy is a cyber enabled workforce.

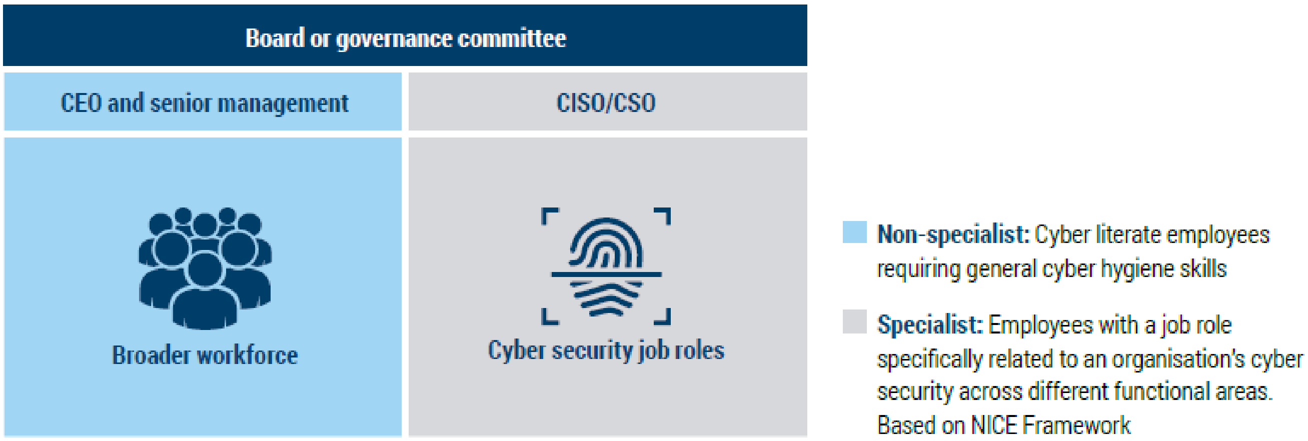
Strong cyber security skills and capabilities are a key driver of economic activity and are critical for national and international growth.

’Cyber literacy’—knowing how to effectively protect digital assets—is not only relevant for professionals working in the cyber security sector, it is also becoming a must-have skill for every worker, regardless of occupation, stage of career or geographic location. All organisations that rely on or intend to use digtal infrastructure to conduct business need a cyber literate workforce that can contribute to managing cyber risks. This is true for large and small employers, the private and public sectors, the developed and developing economies. In sum, cyber literacy assures the efficacy of organisational efforts to leverage data and digital infrastructure to grow as well as defend against malicious cyber risk.

The same applies to individuals and groups including families in the community. At scale, cyber literacy in the workplace and in our everyday lives enables the achievement of cyber resilience – at the local, national and international levels.

An economy’s cyber literate workforce is complementary to the cyber security workforce, comprised of professionals whose overarching role is to support and often ensure the confidentiality, integrity and availability of digital assets. This is true, albeit at different levels, whether you are an Incident Responder a Governance, Risk and Compliance Specialist, a Diplomat working on international norms in cyberspace or any other work role that makes up a nation’s core cyber security workforce. Indeed, a job in cyber security is as diverse as the people we need to work in and around the sector.

Figure 1. Cyber skills needed in a typical, larger workplace[i]


Board or governance committee
CEO and senior management
CISO/CSO
Broader workforce
Cyber security job roles
Non-specialist: Cyber literate employees requiring general cyber hygiene skills
Specialist: Employees with a job role specifically related to an organisation's cyber security across different functional areas.
Based on NICE Framework

Australia’s cyber security industry growth centre, known as AustCyber, has been providing national level advocacy across Australian governments, industry and academia for the adoption of the United States (US) National Institute of Standards and Technology (NIST) Publication 800-181 *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (the NICE Framework) as the best publicly available resource to describe the diversity of cyber security work roles as well as the knowledge, skills, abilities and tasks that underpins each role.

Though the NICE Framework was developed to suit the purposes of the US's cyber security workforce, AustCyber believes it has wider applicability and can act as a highly effective tool in support of a coordinated approach to developing Australia's national cyber security workforce. This has been successfully demonstrated by increased use of the NICE Framework by Australia's current and aspiring cyber security professionals, cyber security education and training providers and Australian employers.

AustCyber has also been active in supporting wide Australian adoption of the NICE Framework though its annual Cyber Security Sector Competitiveness Plan, a globally unique publication on the economic aspects of cyber security as an industry. Through the 2018 Update to the Plan, Australia was for the first time able to measure its cyber security skills gap and subsequent cost to the national economy by using the NICE Framework as the taxonomy for cyber security jobs and skills. AustCyber has also developed an interactive dashboard for users to explore the NICE Framework and assess its applicability to their own context.

The nature of cyber security work undertaken in economies around the world is similar; this supports the notion that Australia's experience in applying the NICE Framework can provide a benchmark of sorts on the NICE Framework providing common language for any economy and its employers and workforces to better describe cyber security work. The NICE Framework also provides the necessary building blocks for baselining the skills required by new and transitioning workers for a job in cyber security. In this sense, it is a key mechanism for international collaboration in cyber security and workforce mobility.

Other NIST and international cyber security standards are also critical tools that provide guidance on appropriate risk controls to improve cyber security posture. The NICE Framework is complementary to these as it provides the architecture for creating the workforce that can implement risk controls that will ultimately help an organisation and nation achieve better resilience to cyber-physical threats.

This submission provides AustCyber's response to NIST's Request for Comments on its Special Publication 800-181. In takes account of the views and experiences of our partners and stakeholders engaged in growing Australia's cyber security sector, across industry, government and the research community in Australia and abroad. The structure of the submission answers the discussion questions relating to improvements to the NICE Framework under the following themes:

- Making the NICE Framework more suitable for Australia
- Taking the NICE Framework to the next level
- Managing cyber security risk through a cyber security standards.

Summary of recommendations

Making the NICE Framework more suitable for Australia

1. Develop implementation guidelines and toolkits for NICE Framework target at distinct user groups. This could leverage the model used for other NIST cyber security practice guides.
2. Consider a British English spelling version of the NICE Framework to facilitate greater adoption in Australia and other English-speaking countries
3. Generalise references to specific United States legislation and Presidential Directives in the NICE Framework so that they are country agnostic. Country specific references can be moved to practice or implementation guides.

Taking the NICE Framework to the next level

4. Change the "Speciality Area" level of the NICE Framework to focus on security teams instead.

5. Identify new work roles, such as Security Awareness Professionals and Cloud Security Engineers for potential inclusion in the update to the NICE Framework.
6. Undertake international labour market analysis to cross check the relevance of existing NICE Framework work role titles against those used by most employers.
7. Undertake a full audit of KSATs to synthesise potential duplicates and to simplify language where possible.
8. Develop a guidelines to better enable measurement of knowledge areas within the KSATs.
9. Consider adding a select range of ‘soft skills’ to all work roles.
10. Implement more regular reviews and updates to KSATs that reflect the evolving technology and threat landscape.
11. Develop guidelines for assessing work role proficiency levels that provide NICE Framework users with expectations of proficiency at entry level, intermediate and expert.
12. Create a career profile template for cyber security professionals that identify with a work role in the framework to use to describe their career pathway. This could be used internationally.
13. Create career profiles of real-world cyber security professionals who are employed in work roles described in the NICE Framework. Add interactive links between career profile work role titles in relevant NICE Framework tools.

Managing risk through cyber security standards

14. Integrate the NICE Framework with other NIST cyber security standards where practical.
15. Engage with other standards bodies to assess the feasibility of aligning NICE Framework work roles within other national and international cyber security standards.
16. Develop a NIST practice guide that demonstrates a single pane of glass approach to using the NICE Framework with other standards.
17. Develop public case studies of organisations using multiple NIST standards (including NICE) to manage their cyber security risk.

Making the NICE Framework more suitable for Australia

Reflections on questions 1, 2 and 4: Improvements to the NICE Framework

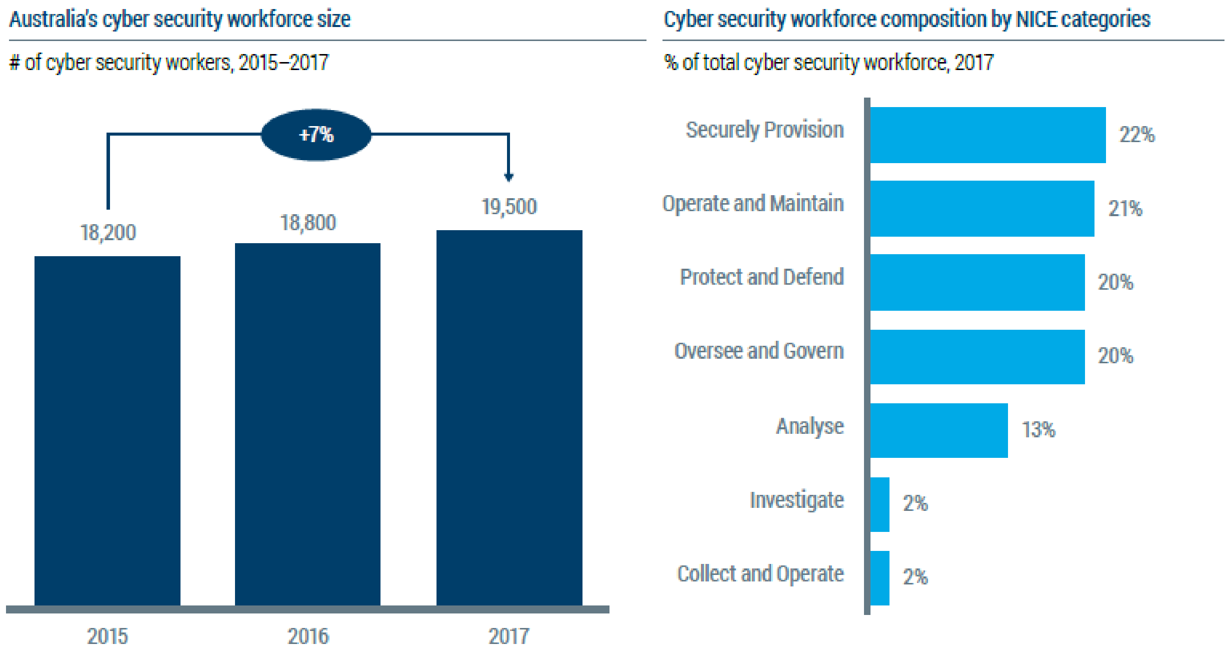
The NICE Framework is a useful tool for measuring a nation's cyber security workforce as well as cyber skills and skills gaps.

AustCyber considers the adoption of the NICE Framework is the first step to developing a common understanding of cyber security work roles as well as the knowledge, skills, abilities and tasks that relate to each role. This is a practical measure for the establishment of better education and training pipelines and high quality workforce development programs, required for a sustainable, globally competitive national cyber security workforce. It is also an essential ingredient for creating positive impact on a country's level of cyber security maturity, particularly when cyber workforce development strategies are developed in tandem with holistic strategies for cyber defences and developing innovative cyber security products and services.

AustCyber has been leading national advocacy for the wide adoption of the NICE Framework by Australian cyber security professionals, education and training providers, employers and policy makers since 2017. With the current level of cyber security job vacancies worldwide estimated to be close to three million, countries including Australia urgently need to start referring to the cyber workforce through a common lens.

By leveraging the NICE Framework, through the Australia's Cyber Security Sector Competitiveness Plan, we have been able to draw true insight in to the make-up of Australia's national cyber security workforce, measure projected skills shortages (18,000 by 2026) and the cost of current cyber skills shortages to the national economy (estimated at A$400 million per year)[ii].

Figure 2. Australia's Cyber Security Workforce[iii]



Australia's cyber security workforce size

# of cyber security workers, 2015–2017

Cyber security workforce composition by NICE categories

% of total cyber security workforce, 2017

Note: Distribution of cyber security workers across NICE categories derived using the distribution of job ads across NICE categories for 2017

Source: Gartner; TalentNeuron; AlphaBeta Analysis

We note that given that cyber security work roles are rarely captured by official government labour market data collection mechanisms, Australia's application of the NICE Framework for workforce analysis provides a methodology that is transferable to other countries. In could also, with some adaptation, be made suitable for workforce analysis at the organisational level.

Key use cases for Australian user groups of the NICE Framework

In Australia, AustCyber has distilled users of the NICE Framework into four distinct groups. In our experience as a member of several international bodies, these groups are similar if not the same across numerous other countries:

- The current and future cyber security workforce
- Education and training providers
- Employers, across public and privae sectors
- Policy makers.

Each of these user groups have a slightly different use case and benefits for adopting the NICE Framework.

Table 1. Use Cases and Benefits of the NICE Framework

User Group	Key Use Case	Benefits
The current and future cyber workforce	The NICE Framework is a resource to explore the diverse array of work roles in the cyber security sector as well as the knowledge, skills, abilities and tasks that relate to each role	• Dispels a common misconception that cyber security is only one job • Explains the diverse nature of cyber security work and roles • Demonstrates that cyber security work roles are not only IT/ ICT focused. There are also work roles that require people with policy, strategy, risk management, legal and other skills • Provides a reference tool for individuals to self-audit the skills they think they possess versus those required to perform a chosen work role
Education and training providers	The NICE Framework is a resource for mapping cyber security course and degree programme content to cyber security work roles	• Provides a standard to develop **new** and ensure **current** course content teaches skills aligned to real cyber security work roles • Enables education and training providers to develop cyber security course curriculum aligned to teaching expertise • Provides a framework to produce job-ready graduates aligned to the needs of local employers • Enables the development of practical exercises that test learner competency against common tasks performed in a work role • Dissuades education and training providers from over-generalising course content or teaching antiquated content • Dissuades education and training providers from re-badging IT/ ICT qualifications as cyber qualifications • Enables national benchmarking of institutions, curriculum and graduate outcomes to better identify true 'centres of excellence'

Employers	The NICE Framework is a resource to assess the skills and skills gaps of current and prospective cyber security professionals employed in a workplace	• Provides a catalogue of cyber security work roles that may be required to secure an organisation's digital and human assets • Assists human resource teams and hiring managers in recruiting cyber security work roles by providing a template of content to include in job advertisements and position descriptions • Provides a checklist of knowledge, skills and abilities that can be tested at interview in order to gauge proficiency in a work role • Enables more targeted spend of professional development budgets by providing a framework to test current employee skills gaps against work roles. This is particularly relevant for upskilling an organisations IT/ ICT team. • Provides a standard to ensure partnerships with education and training providers produce a pipeline of job-ready graduates aligned to work roles
Policy makers	The NICE Framework is a resource to benchmark and continually measure population level cyber skills and skills gaps required for a sustainable national cyber security workforce	• Enables the development of measurement tools for greater visibility of cyber security skills and skills gaps across an economy • Provides an evidence base to better target government funding towards cyber security education and skills • Provides an evidence base for targeted policy interventions when required or desired, e.g. awarding centre of excellence badges to education and training providers based on job outcomes for learners

Making the NICE Framework more relevant for Australian users

AustCyber has gone to considerable effort to demonstrate the NICE Framework for Australian user groups. This includes demonstrating its use for cyber workforce measurement and skills analysis to policy makers, through the Australian Cyber Security Sector Competitiveness Plan, and the subsequent development of an interactive dashboard of the NICE Framework allowing all user group to easily visualise and explore work roles.

These efforts have gone a long way to demonstrate the NICE Framework use cases to key audiences, though much more could be done.

An updated version of the NICE Framework should evolve to encourage greater adoption by countries and organisations outside the United States. Some points of feedback that may assist in this are as follows:

- NIST Special Publication 800-181 as a singular interface with the Framework is not user friendly (135 pages) for most audiences. Creating supporting tools to explore and use the NICE Framework would facilitate greater adoption. This could include promulgation of a white labelled version of AustCyber's material.
- It is unclear how the NICE Framework can or should be implemented at a national or organisational level. Practice and implementation guides, case studies and other general advice on how different user groups should implement the NICE Framework would be helpful and support broader adoption.

- The benefits of the NICE Framework for different user groups need to better communicated. Development of generic communication strategies and tools that could be adopted by different organisations and countries would be useful. These should provide a consistent narrative that links cyber workforce development to greater national and organisational cyber resilience.
- References to specific US Government agencies and legislation reduce the NICE Framework's relevance in international contexts, for example K0168 Knowledge of applicable laws and statutes (e.g., in Titles 10, 18, 32, 50 in US Code). These references could be removed from the NICE Framework and placed in to country specific practice or implementation guides.

AustCyber is well placed to be the coordinating partner of choice for NIST to facilitate greater Australian adoption of the NICE Framework. Doing so would deliver on key elements of the NICE strategic plan and be of net benefit to the national interests of both countries by providing common guidance for better national cyber security workforce planning.

Recommendations

1. Develop implementation guidelines and toolkits for NICE Framework target at distinct user groups. This could leverage the model used for other NIST cyber security practice guides.
2. Consider a British English spelling version of the NICE Framework to facilitate greater adoption in Australia and other English speaking countries.
3. Generalise references to specific United States legislation and Presidential Directives in the NICE Framework so that they are country agnostic. Country specific references can be moved to practice or implementation guides.

Taking the NICE Framework to the next level

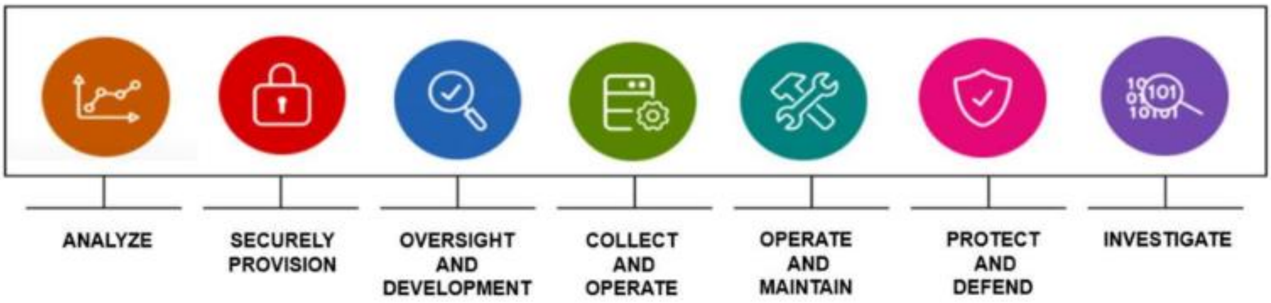
Reflections on questions 3, 6, 7, 8, 9 and 11: Improvements to the NICE Framework

The current version of the NICE Framework is comprehensive. With seven categories, 33 speciality areas and 52 work roles, the Framework provides users with a detailed understanding of the typical technical and non-technical job types that make up the cyber security workforce. While the scope of the Framework is wide-ranging a review of each of the elements should still be considered.

Categories

The organising categories for the NICE Framework are appropriately broad to encompass the depth and breadth of cyber security work roles, both current and emerging. It is the view of AustCyber and our partners that these categories do not require any alterations at this time and should remain static.

Figure 3. NICE Framework Categories[iv]



Speciality Areas

AustCyber considers the usefulness of the Speciality Areas in the NICE Framework requires review. Although the intended purposes of this layer of the NICE Framework is clear in the title, it is unclear how users of the NICE Framework should engage with it differently to the work roles. This is in part because 87 per cent of Speciality Areas relate to two or less work roles, while 51 per cent relate to only one work role, often with the same name as the work role itself, for example ‘Executive Cyber Leadership’ (EXL). It is also likely because the Speciality Areas have little meaning from an operational perspective in a workplace.

Another way of structuring this layer of the NICE Framework is to consider reframing Speciality Areas as team structures. Employers often use the seven Categories of the NICE Framework to distinguish security functions within their organisation, but will often at the next layer down refer to security teams that support that function. An example of this might be a ‘Protect and Defend’ function (so, Category) that is supported by a red and blue team as well as a security awareness team.

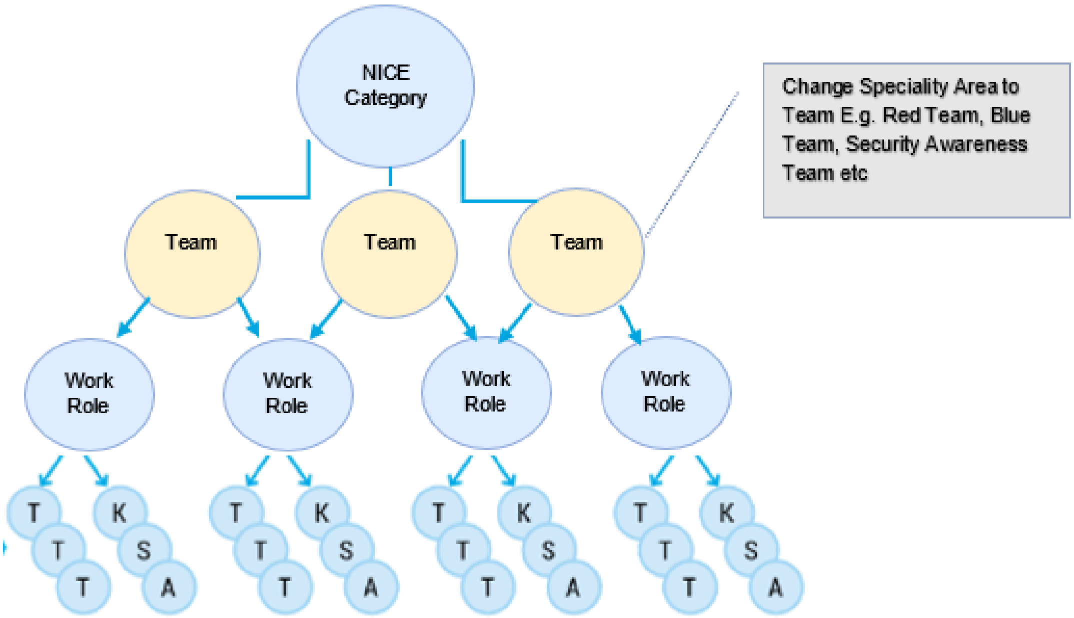
Redefining the Speciality Areas aspect in this way would facilitate a more intuitive understanding of the NICE Framework from an organisational implementation perspective by:

- enabling the Human Resources function of an organisation to undertake strategic workforce planning;
- providing the framework to ensure each security function has the right composition of teams and team members with the required skills; and

- showing which work roles employers should be recruiting for when standing up new security teams or expanding existing teams.

This approach would also facilitate NIST's ability to undertake a mapping exercise that ensures that the 52 work roles, and any potential additions, do actually sit within common team structures used by private and public sector employers. It is important to note here that certain work roles may relate to multiple teams depending on the context.

Figure 4. Structure of the NICE Framework: Changing Speciality Areas to Teams


NICE Category
Team
Team
Team
Change Speciality Area to Team E.g. Red Team, Blue Team, Security Awareness Team etc
Work Role
Work Role
Work Role
Work Role
T
T
T
K
S
A

Work Roles

The 52 work roles in the NICE Framework provide good coverage of the various technical and, importantly, non technical work roles that make up a cyber security workforce. That said, the fast pace at which emerging technology and the threat landscape is evolving means that new security focused work roles warrant consideration for inclusion in an updated NICE Framework. Two arguably uncontentious examples of new work roles that warrant inclusion in the update are Security Awareness Professionals and Cloud Security Engineers.

Further to the above, it is important to review the titles of existing work roles in the NICE Framework so they reflect industry terminology (which may be contextual by country or region such as North America or Europe). Popular job titles like “Penetration Tester” or “Security Researcher” are not adequately covered in the current NICE Framework. This does not necessarily mean adding new work roles to the NICE Framework but rather ensuring that those currently included reflect the job market, perhaps by using language such as ‘also known as’ against each work role. All security professionals need to be able to find themselves in the Framework. Reflecting these in the NICE Framework is essential for increasing voluntary adoption.

Consideration should also be given to how best reflect particular adaptations for roles performed in classified and sensitive environments, noting of course the sensitivities around doing so. Governments and other organisations engaging in sensitive environments around the world are experiencing skills shortages the same as their unclassified cousins—their use of appropriately adjusted work roles in an outward facing capacity would assist with recruitment efforts as well as support the education system to provide job ready graduates; internally it could assist with retention and employee career progression.

Creating a work role in the NICE Framework to cater for Small to Medium Enterprises (SMEs)

Another area which warrants consideration in an updated version of the NICE Framework is the inclusion of a ‘Cyber Security Generalist’ work role to meet the needs of Small to Medium Enterprises (SMEs).

For Australia, small businesses account for 97 per cent of registered businesses, 35 per cent of gross domestic profit and employ 44 per cent of the nation’s workforce[v]. SMEs are also the most vulnerable to a malicious breach or compromise, which can have a devastating effect on their ability to recover and grow. In fact, in a study done by KPMG and one of Australia’s national news providers in 2018, it was found that around 60 per cent of Australian mid sized companies that suffered a compromise were going out of business within six months[vi].

While all organisations into the future will require a cyber literate workforce, certain SMEs may also require a Cyber Security Generalist on staff, noting the person occupying the work role may also be the Office Manager, the Receptionist or the Business Owner. This is because the ways and means to manage cyber security risks is different dependent on the size, type and operating context of organisation. Management of the same or similar set of cyber risks will be different for an SME with 80 staff versus an SME with five staff, an SME in retail versus defence industry, a publicly listed company or private entity, an exporting organisation or a startup, and so on.

Just as all cyber security professionals should be able to find themselves in the NICE Framework, every business should be able to refer the Framework for guidance on what skills a staff member might need to help the business obtain a basic level of cyber security and ongoing cyber resilience. The skills required to perform this suggested new work role likely go beyond that of Security Awareness and are more likely akin to Occupational Health and Safety for the digital age.

A proposed skillset based on key competency areas that could be considered for a Cyber Security Generalist work role is provided in the table below.

Table 2. Sample Skillset (Units of Competency) for a Cyber Security Generalist

Theme	Unit Title	Description
Cyber Security Awareness	Foundations of cyber security	What cyber security means to me and why it matters. Identifying my risks and creating a 'threat profile'
Data protection	Securely manage customer data and other Personally Identifiable Information (PII)	What encryption is and why it is used, general awareness of security when storing and sharing data, risks and benefits of cloud storage, use of regular backups
Hardware protection	Understand and mitigate security risks from bad actors	Strategies for improving security on personal computers, phones, USB and external devices, and network-related protection strategies, including virus protection, safe use of public WIFI and VPN use
	Patch software across multiple devices	Regular updating of software on computers and mobile devices, security patch life-cycles
Identity verification and protection	Best practices for securing your identity online and practices to avoid identity and data theft	Best practices for maintaining data security and secure identities e.g. develop and secure strong passwords, fundamentals of 2FA, account splitting etc
Social Engineering	Protecting yourself from online and physical threats	Explore different ways that individuals may be exposed to risk via: Phishing - email/phone attacks to get information; Shoulder surfing - unobscured screens, watching typed passwords, listening to discussions; Persuasion - face-to-face and conversation

Business Practices	Promote cyber security awareness in an SME/business	How to engage and promote cyber security awareness in a business including through security awareness of and use of trusted online resources
	General data protection strategies for securing your business	Develop an understanding of a business's online risk profile and strategies to improve security e.g. data protection frameworks, disaster recovery plans.

A similar skillset to the one described above has been adopted by the Australian Vocational Education and Training (VET) sector for national implementation[vii].

Developing proficiency levels to describe a career development continuum within work roles

A common observation from employers seeking to implement the NICE Framework is there is no guidance on proficiency levels within a work role. Though not because of the NICE Framework, a potential consequence of this is that many employers develop misaligned expectations of what a new cyber security graduate would know and be able to do versus someone that has two, five or 10 years of experience.

It is also possible that misalignment of employer expectations is a key driver of the global skills shortage as employers go through costly and lengthy recruitment processes for talent that they either do not need, cannot afford or that is not available in the market—resulting in job advertisements staying open for much longer than they otherwise would.

While larger, more cyber mature employers may have the time and resources to tailor proficiency levels for their own purposes, most employers do not. Though this submission recognises that standardising proficiency levels is difficult, given the different needs of individual organisations, providing some guidance on what baseline proficiency looks like for a work role, versus an expert for example, would make the NICE Framework more useful for all user groups by establishing a career development continuum for individual work roles.

Developing Work Role Case Studies

The diversity of the cyber security professionals, the industries they work in, their career paths and their outlook are stories that could be better told through the NICE Framework. It would be useful to see the development of Work Role case studies that could be accessed interactively by users exploring the NICE Framework. This would help humanise the framework similar to New America's media platform, Humans of Cybersecurity, which is designed to elevate the stories of the people and ideas that are changing our digital lives. Another example of this can be found in an AustCyber project with the Australian Computing Academy at the University of Sydney to develop the Schools Cyber Security Challenges, targeted at all Australian high school students.

Knowledge, Skills, Abilities and Tasks (KSATs)

The knowledge, skills, abilities and task layer of the NICE Framework provides the level of detail that makes the overall Framework incredibly meaningful.

For learners, it provides a reference tool to self-audit skills they think they possess versus those required to perform a work role. For cyber security education and training providers, it serves as a reference tool to ensure curriculum and training products are teaching skills that align to work roles. For employers, it provides a baseline for what cyber security professionals employed in their organisation need to know and do in specific work roles.

There are, however, improvements that can be made to this layer of the Framework to improve is useability and assist users with its implementation.

Providing guidelines to measure knowledge areas

In the current version of Special Publication 800-181, it is difficult to discern which of the KSATs are common across all work roles. An analysis of KSATs using the NICE Framework pivot table tool shows that that there are only six knowledge areas that relate to all 52 work roles:

- Knowledge of cyber threats and vulnerabilities
- Knowledge of specific operational impacts of cybersecurity lapses
- Knowledge of computer networking concepts and protocols, and network security methodologies
- Knowledge of cybersecurity and privacy principles
- Knowledge of risk management processes (e.g., methods for assessing and mitigating risk)
- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.

However, knowledge areas are difficult to measure. For an education or training provider that maps their cyber security curriculum to the NICE Framework, stating that a student will develop "Knowledge of cyber threats and vulnerabilities" is not consistently measurable. One lecturer could say they meet this knowledge area by providing one slide on this topic in one class. Conversely, another could teach an entire unit across an academic semester on the same area. Without guidelines on how to assess knowledge areas, both cases are arguably valid. A baseline needs to be established, benefitting teachers, students and employers.

Though it is understood the level of knowledge obtained is likely commensurate with the level of study—an undergraduate student would not be expected to possess the same level of knowledge as a master's student, for example—more guidance on how knowledge areas should be measured is critical for consistent implementation and reliable quality in graduates across levels of formal education.

Skills!

Of the 52 work roles in the current version of the NICE Framework, there are no skills that are common across any of the roles. This point is interesting because the common frustration described by employers is for cyber security professionals to have greater 'soft skills' such as communication, judgement and leadership. An analysis of the skills within the NICE Framework also suggests that some of the language used to describe different skills could be synthesised. These are points which should be taken in to considerations during the update.

Ensuring KSATs keep pace with the evolving technology and threat landscape

The way in which technology and the threat landscape has evolved over the life of the NICE Framework and beyond proves that threat actors remain undeterred from compromising systems for their own gain. They exploit old and new technology to shift and adapt in their choice of attack vectors and tactics—prompting the need for professionals and organisations to have diversity of skills and experience in ther teams and/ or service providers.

In this context, it would be beneficial for the NICE Framework to take stock of new threats and counter measures at more regular intervals so that KSATs respond to the advent of new technology (and for that matter, iterations on existing technologies) as well as the evolving tactics, techniques and procedures (TTPs) used by malicious actors.

Providing regular reviews and updates to this layer of the Framework will need to be well communicated to ensure they flow into cyber security products and the education and training providers that apply them in the teaching environment. More regular updates will also provide an incentive for education and training providers to invest more in teacher professional development as each jostles for greater relevance in a competitive training market.

Recommendations

4. Change the Speciality Area level of the NICE Framework to focus on security teams instead.
5. Identify new work roles, such as Security Awareness Professionals and Cloud Security Engineers for potential inclusion in the update to the NICE Framework.
6. Undertake international labour market analysis to cross check the relevance of existing NICE Framework work role titles against those used by most employers.
7. Undertake a full audit of KSATs to synthesise potential duplicates and to simplify language where possible.
8. Develop a guidelines to better enable measurement of knowledge areas within the KSATs.
9. Consider adding a select range of ‘soft skills’ to all work roles.
10. Implement more regular reviews and updates to KSATs that reflect the evolving technology and threat landscape.
11. Develop guidelines for assessing work role proficiency levels that provide NICE Framework users with expectations of proficiency at entry level, intermediate and expert.
12. Create a career profile template for cyber security professionals that identify with a work role in the framework to use to describe their career pathway. This could be used internationally.
13. Create career profiles of real-world cyber security professionals who are employed in work roles described in the NICE Framework. Add interactive links between career profile work role titles in relevant NICE Framework tools.

Managing cyber security risk through standards

Reflections on questions 5 and 12: Improvements to the NICE Framework

Implementing any standard requires the assignment of risk. This may seem obvious but organisations with low cyber maturity often get this wrong, believing onboarded technology will manage cyber risk or the risks can be outsourced to a third party. Though there are occasions where new technology or outsourcing risk may be a valid mitigation strategy, in the case of cyber security, the risks never truly leave an organisation. Employers need to assign cyber risk within their organisations to an appropriate employee(s) with the right knowledge, skills and abilities to be the responsible risk owner, manager and/ or responder.

By aligning the NICE Framework with other NIST cyber security standards (which map to international standards[viii]), a single pane of glass approach will emerge whereby risk controls will be aligned with the most appropriate NICE Framework work role to manage the risk. An example of how this might be reflected in the NIST Cybersecurity Framework is demonstrated in the table below.

Table 3. NIST Cybersecurity Framework

Function	Category	Subcategory	Informative References	Suggested Risk Owner
IDENTIFY (ID)	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	CIS CSC 4 COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 NIST SP 800-53 Rev. 4 PM-9	NIST SP 800-181 Oversee and Govern Executive Cyber Leadership (EXL) e.g. CSO or CISO
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 PM-9	
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	COBIT 5 APO12.02 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM11	

Integrating the NICE Framework with other NIST standards makes sense and could act as a precursor to integrating the NICE Framework into other international cyber security standards such as the ISO/IEC 27000 series for information security. Lessons could also be learnt from the US Office of the Under Secretary of Defense for Acquisition and Sustainment's Cybersecurity Maturity Model Certification (CMMC). It would also encourage greater voluntary adoption of the NICE framework, demonstrate the interoperability of technical and process controls with human resources and improve an organisation's ability to self-identify work role or skills gaps needed to implement controls and manage risk.

Recommendations

14. Integrate the NICE Framework with other NIST cyber security standards where practical.

15. Engage with other standards bodies to assess the feasibility of aligning NICE Framework work roles within other national and international cyber security standards.

16. Develop a NIST practice guide that demonstrates a single pane of glass approach to using the NICE Framework with other standards.

17. Develop public case studies of organisations using multiple NIST standards (including NICE) to manage their cyber security risk.

About AustCyber

AustCyber – the Australian Cyber Security Growth Network Limited – is a publicly funded, private entity which commenced on 1 January 2017. Our mission is to support the development of a vibrant and globally competitive Australian cyber security sector and in doing so, enhance Australia's future economic growth in a digitally enabled global economy as well as to improve the sovereign cyber capabilities available in defence of the nation.

We form a part of:

- the Australian Government's Industry Growth Centres Initiative established through the National Innovation and Science Agenda. AustCyber is one of six centres that have been set up in sectors of competitive strength and strategic priority to boost innovation and science in Australia; and
- the current Australia Government's Cyber Security Strategy, launched in 2016, as a coordination mechanism of cyber security R&D, innovation and industry growth innovation. It was through the industry consultation and development of the strategy that the concept for AustCyber was first conceived.

Our funding comes from majority Australian Government grants. We also receive funding under contracts with the governments of the Australian Capital Territory, New South Wales, Queensland, South Australia, Tasmania, Western Australia which we match to deliver in partnership AustCyber's national network of Cyber Security Innovation Nodes – with Victoria soon to join.

We work to align and scale Australian cyber security research and innovation related activities across the private sector, research communities, academia and within Australian governments. We are responsible for maintaining a strong supply of innovative Australian cyber security solutions and capability and have established ourselves as an independent advocate for the competitive and comparative advantages of Australian technical and non-technical cyber security capabilities. We are also responsible for ensuring Australia has the knowledge infrastructure and pipeline of talent needed to grow a globally competitive Australian cyber security sector.

Beyond our shores, we work with partners across many countries to develop export pathways for Australian solutions and capability. This helps the rapidly growing Australian cyber security sector tap into cyber security 'hot spots' around the world.

Further, with multinational companies that AustCyber engages with, we help to establish productive pathways into Australia's cyber security ecosystem through a range of mechanisms suited to the commercial interests and capability types provided by those companies (often in partnership with Austrade and State/Territory governments).

This has strengthened the breadth and depth of our networks that can be leveraged by Australian cyber security companies as part of their growth strategies and by other organisations in expanding Australia's impact on the global stage for cyber security and related fields.

[i] Australia’s Cyber Security Sector Competitiveness Plan, AustCyber, 2018 (subsequent update 2019), located at https://www.austcyber.com/tools-and-resources/sector-competitiveness-plan-2018 and https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019

[ii] As above

[iii] As above

[iv] An excerpt from AustCyber’s dashboard supporting the NICE Framework, located at https://www.austcyber.com/resources/dashboards/NICE-workforce-framework

[v] https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-small-business-counts2019.pdf

[vi] Report no longer available online, but quoted at https://www.mailguard.com.au/blog/mid-size-companies-cyber-attack

[vii] https://www.skillsforaustralia.com/cross-sector-projects/cyber-security/

[viii] MITRE Corporation has mapped NIST’s cyber security standards and guidance to international standards. An case study example can be found in work undertaken by AustCyber and MITRE Corporation in 2017-18, found at https://www.austcyber.com/resources/opportunities-to-harmonise