Dear all,

On behalf of the GFCE Working Group on Cyber Security Culture & Skills and the Cyber Security Standards Members, it is my pleasure to send to you their suggestions regarding the update of the NICE Workforce Framework.

If you have any questions or comments, please let the GFCE Secretariat know.

Kind regards,
Manon

Manon van Tienhoven
Global Forum on Cyber Expertise

SUBMISSION

2020 NICE FRAMEWORK REQUEST FOR COMMENTS

NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY

January 2020

Introduction

About the GFCE

The Global Forum on Cyber Expertise (GFCE) is a global platform for countries, international organisations and private companies to exchange best practices and expertise on cyber capacity building. Its aim is to identify successful policies, practices and ideas and multiply these on a global level. Together with partners from NGOs, the tech community and academia GFCE members develop practical initiatives to build cyber capacity.

A critical component of the GFCE are its Working Groups. The Working Groups bring together the GFCE community (both members and partners) on themes of interest to encourage the dialogue on implementation of cyber capacity building. In addition, the Working Groups strengthen international cooperation by developing a common focus, enabling efficient use of available resources and avoiding duplication of efforts.

The Working Groups encompass existing and planned efforts of the GFCE community in building global cyber capacity along the line of the five prioritised themes of the Delhi Communiqué.

The five Working Groups related to the themes are:

- GFCE Working Group A: Cybersecurity Policy and Strategy;
- GFCE Working Group B: Cyber Incident Management and Critical Infrastructure Protection;
- GFCE Working Group C: Cybercrime;
- GFCE Working Group D: Cybersecurity Culture and Skills;
- GFCE Working Group E: Cybersecurity Standards.

This submission provides views and recommendations of contributing Working Group D and E members in relation to the request for comments by NIST for the update to the NICE Cybersecurity Workforce Framework, NIST Special Publication 800-181. We would particularly like to thank AustCyber, National Informatics Centre of India and Palo Alto Networks for their contributions.

An Overview

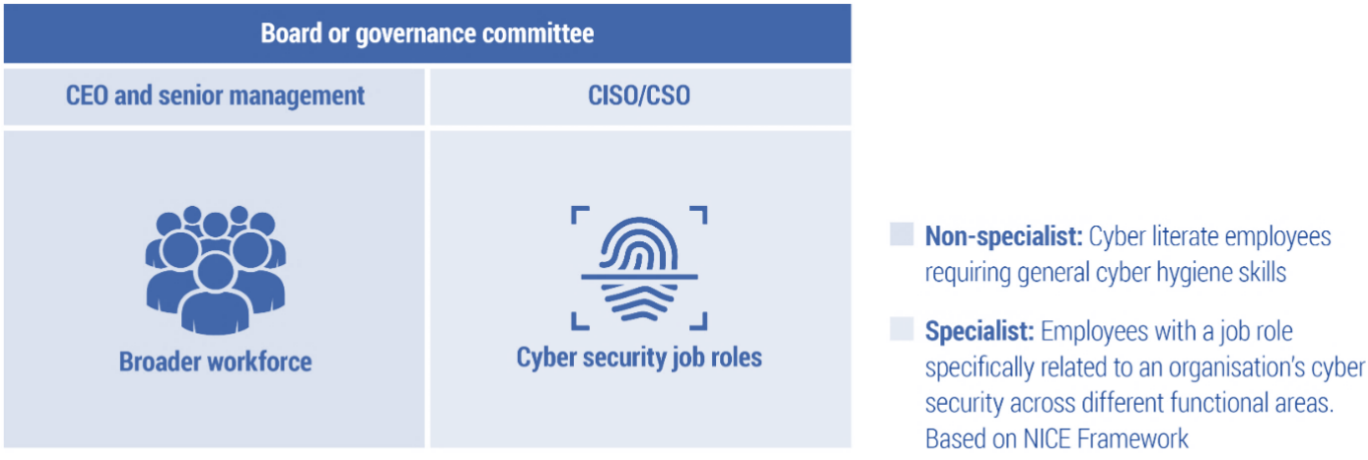
"The foundation of a cyber resilient economy is a cyber secure workforce."

Strong cybersecurity skills and capabilities are a key driver of economic activity and are critical for national prosperity.

'Cyber literacy', or knowing how to effectively protect digital assets, is not only relevant for professionals working in the cybersecurity sector, it is also becoming a must-have skill for every worker in the digital age, regardless of occupation. All organisations that rely on the internet to conduct business today need a 'cyber-literate' workforce that can secure it against routine cyber risks. This is true for large and small employers, the private and public sector, the developed and developing economies. In sum cyber literacy is the foundation for workplace security, which at scale enables better national cyber resilience.

A Cyber-literate workforce is complementary to the cybersecurity workforce. The cybersecurity workforce is comprised of professionals whose overarching role is to 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 cyber space or indeed any other work role that makes up a nation's core cybersecurity workforce. Indeed, a job in cybersecurity is as diverse as the people we need to work in the sector.

Figure 1. Cyber skills needed in a typical workplace



The GFCE Working Group D: Skills and Culture acknowledges the NIST Publication 800-181 - National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework - as an important publicly available resource to describe the diversity of cybersecurity work roles as well as the knowledge, skills, abilities and tasks that underpins each.

In its current form the NICE Framework does a good job of describing the depth and breadth of cybersecurity work roles that make up the core of the cybersecurity workforce. Though the NICE Framework was developed to suit the purposes of the United States' cybersecurity workforce, the GFCE believes that it has wider applicability internationally and can act as a powerful tool in support of its capacity building mission.

At the GFCE Annual Meeting in Addis Ababa, Ethiopia in October 2019, the Working Groups convened to provide insights on their work to the wider GFCE member base and African Community. Working Group D: Skills and Culture provided a showcase of the NICE Framework to attendees who got to explore the Framework and discover its potential use cases in their national and organisational contexts.

The overarching consensus of the aggregated feedback is that the NICE Framework provides a better than average starting point for international cybersecurity workforce development purposes. Feedback commonly referenced the similar nature of cybersecurity work across international borders and the growing need for countries to collaborate in cyberspace. The global skills shortage is a theme that unites all countries though skills shortages are particularly acute in developing countries owing to the allure of skilled migration. Therefore, a resource like the NICE Framework not only provides a common international language to refer to cybersecurity work it also provides the necessary building blocks for all countries to skill new and transitioning workers for a job in cybersecurity.

Other NIST and international cybersecurity standards are critical tools that provide guidance on appropriate risk controls to improve a user's cybersecurity posture. The NICE Framework is complementary to these as it provides the architecture for creating the workforce that can implement the risk controls of recommended in other cybersecurity standards. Together these tools can help an organisation and country achieve better resilience to the threats they face on-line.

Moving forward the cyber resilience of our economies is paramount, and the foundation of cyber resilience must be a highly capable, cyber secure workforce.

This submission provides the GFCE Working Group D and E response to the National Institute for Standards and Technology request for comments on the NICE Cybersecurity Workforce Framework, NIST Special Publication 800-181.

The structure of the submission answers the discussion questions relating to improvements to the NICE Framework under the following themes:

1. Making the NICE Framework more relevant for global adoption
2. Taking the NICE Framework to the next level
3. Managing cybersecurity risk through a single pane of glass

The discussion questions under the section on Awareness, Applications, and Uses of the NICE Framework have been completed to the best of the Working Group's ability noting that some questions are not applicable and some answers to questions reflect more of an organisational response from GFCE Working Group members. Where this is the case it has been indicated.

This submission also reflects the views and experiences of representatives from multiple developed and developing countries that attended the GFCE Annual Meeting in Addis Ababa in October 2019. In particular, the GFCE wishes to highlight the endorsement of the recommendations in this submission by the Africa Cyber Security and Digital Rights Organisation (ACDRO).

Summary of Recommendations

1. Making the NICE Framework more relevant for global adoption

1.1 Develop implementation guidelines and toolkits for user groups that wish to adopt or refer to the NICE framework. This could leverage the model used for other NIST Cybersecurity practice guides.
1.2 Partner with the Global Forum on Cyber Expertise to adapt implementation guidelines and toolkits for countries seeking capacity building support.
1.3 Partner with the Global Forum on Cyber Expertise to develop official translations of the NICE Framework in key languages
1.4 Consider a British English spelling version of the NICE Framework to facilitate greater adoption across English speaking countries
1.5 Partner with the Global Forum on Cyber Expertise to develop tailored communication materials for key international audiences that sell the benefits of adopting the NICE Framework as a cyber capacity building measure.
1.6 Remove references in the NICE Framework to specific United States legislation and Presidential Directives so that they can be read as country agnostic. Reference to specific national legislation etc can be moved to country specific practice or implementation guides.

2. Taking the NICE Framework to the next level

2.1 Change the “Speciality Area” level of the NICE Framework to focus on security teams instead.
2.2 Identify new work roles, such as Security Awareness Professionals and Cloud Security Engineers for potential inclusion in the update to the Framework.
2.3 Undertake international labour market analysis to cross check the relevance of existing NICE Framework work role titles against those used by most employers.
2.4 Undertake a full audit of KSATs to synthesise potential duplicates and to simplify language where possible.
2.5 Develop user guidelines to better enable measurement of knowledge areas.
2.6 Consider adding a select range of ‘soft skills’ to all work roles e.g. critical thinking, communication skills, teamwork etc
2.7 Implement more regular reviews and updates to KSAs that reflect the evolving technology and threat landscape.
2.8 Develop guidelines for assessing work role proficiency levels that provide NICE Framework users with expectations of proficiency at entry level, intermediate and expert.
2.9 Create career profile templates for cybersecurity professionals to use to describe their career pathway. These could be aligned to NICE work roles and used internationally.
2.10 Create career profiles of real-world cybersecurity professionals that align to work roles in the NICE Framework. Add interactive links between select career profiles and NICE Framework work role in existing and future tools.

3. Managing cybersecurity risk through a single pane of glass

3.1 Integrate the NICE Framework with other NIST cybersecurity standards where practical.
3.2 Engage with other standards bodies e.g. ISO and US DoD (CMMC) to assess the feasibility of aligning NICE work roles within other cybersecurity standards.
3.3 Develop a NIST practice guide that demonstrates a single pane of glass approach to using the NICE Framework with other standards.
3.4 Develop public case studies of organisations using multiple NIST standards (including NICE) to manage their cybersecurity risk
3.5 Develop clear guidelines for organisations with the need to develop customised work roles at the classified level to do so within the overarching structure of the NICE Framework as described by NIST.
3.6 Develop a process for organisations with customised work roles at the classified level to voluntarily report metadata to NIST for tracking purposes.

Making the NICE Framework more relevant for global adoption

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

The NICE Framework is a useful tool for cyber capacity building

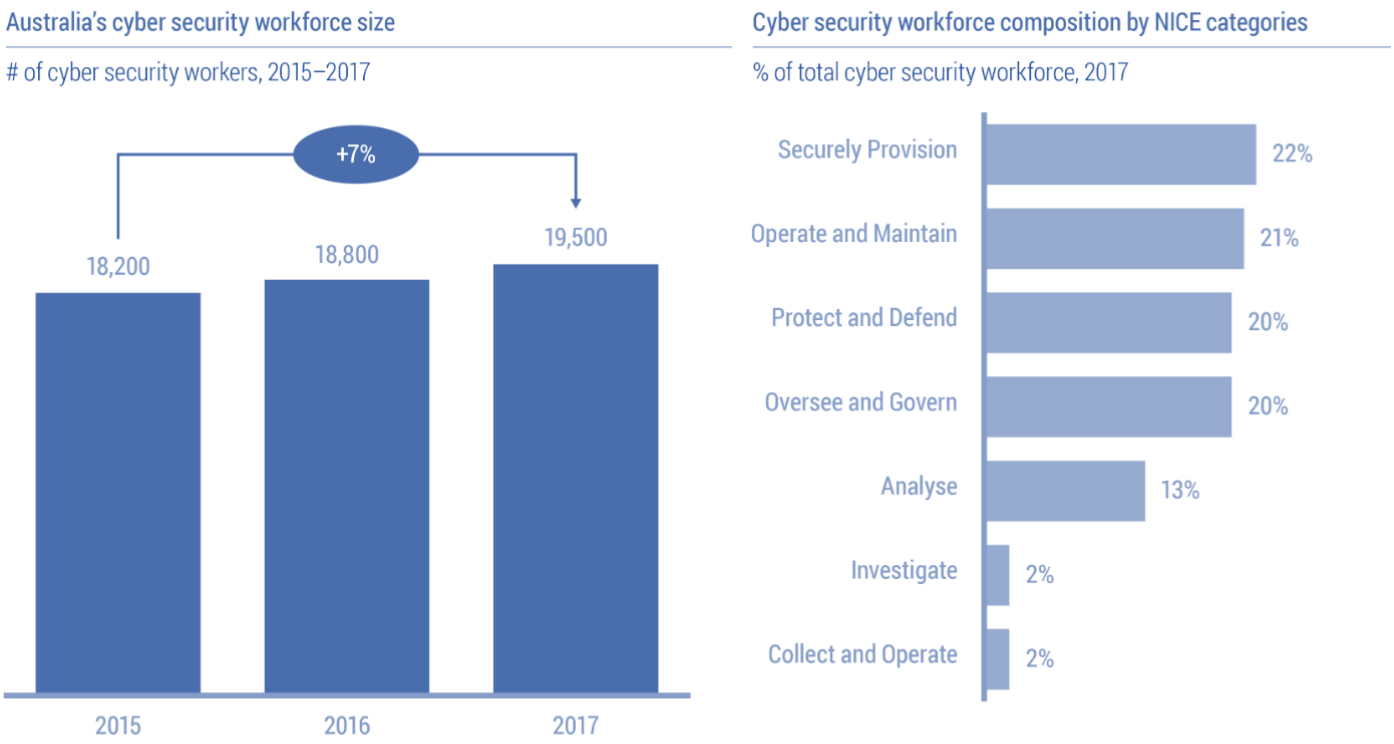
The NICE Framework has been recognized by the GFCE Working Group D: Skills and Culture as one of its best practice resources for use in its cyber capacity building mission. With the current global cybersecurity skills shortage estimated at close to 3 million job vacancies worldwide, developed and developing countries are calling out for potential solutions to this challenge. Developing countries however have a particularly acute need for creating more skilled cybersecurity professionals given that many countries struggle to keep existing cybersecurity professionals from migrating to better paid jobs in developed countries.

The GFCE recognises the importance of the NICE Framework, not a silver bullet, but as a common lexicon for the consistent understanding of the depth and breadth of the cybersecurity workforce. A common understanding of cybersecurity work roles as well as the knowledge, skills, abilities and tasks that relate to each is a necessary first step for all countries that wish to establish workforce development models and better education and training pipelines for a sustainable cybersecurity workforce. It is also an essential ingredient for creating positive impact on a country's level of cybersecurity maturity, particularly when cyber workforce development strategies are developed in tandem with holistic national cybersecurity strategies.

Although the NICE Framework was conceived to guide the development of the United States cybersecurity workforce, it is evident that the nature of cybersecurity work and the skills required to perform the work are similar if not the same across developed and developing countries. Even in its current form this makes the NICE Framework a powerful tool in the right hands.

In the 2018 update to Australia's Cybersecurity Sector Competitiveness Plan the NICE Framework was used to measure the current status of its national cybersecurity workforce. By adopting the NICE Framework, Australia was able to draw true insight into the make-up of its national cybersecurity workforce. It was also able to measure projected skills shortages, (18,000 by 2026) and the cost of current cyber skills shortages to the national economy estimated at $400 million per year. Given that cybersecurity work roles are rarely captured by official government labour market data collection mechanisms, Australia's application of the NICE Framework provides a useful example of a methodology to put parameter around a national cybersecurity workforce that is transferable to other countries.

Figure 2. Australia's Cybersecurity Workforce



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

Key use cases for user groups of the NICE Framework that are common to all countries

At the 2019 GFCE Annual Meeting held in Addis Ababa, Ethiopia members of Working Group D (including NIST) provided a detailed showcase of the NICE Framework to a global audience of people keen to understand its different use cases. The showcase focused on four key user groups common to all countries:

1. The current and future cybersecurity workforce
2. Education and training Providers
3. Employers (Public & Private)
4. Policy makers

The intention of the showcase was to test the applicability of NICE Framework use cases for each of the user groups from various countries, focusing on its benefits. The level of familiarity with the NICE framework amongst audience members was low.

Table 1. Use Cases and Benefits of the NICE Framework

User Group	Key Use Case	Benefits
1. The current and future cyber workforce	The NICE Framework is a resource to explore the diverse array of work roles in the cybersecurity sector as well as the knowledge, skills, abilities and tasks that relate to each.	• Dispels a common misconception that cybersecurity is only one job. • Explains the diverse nature of cybersecurity work and work roles. • Demonstrates that cybersecurity work roles are not only IT focused. There are also work roles that require people with policy, strategy, risk management and legal 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.
2. Education and training providers	The NICE Framework is a resource for mapping cybersecurity course and degree programme content to cybersecurity work roles.	• Provides a standard to develop **new** and ensure **current** course content teaches skills aligned to real cybersecurity work roles. • Enables education and training providers to develop cybersecurity 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 overgeneralising course content or teaching antiquated content • Dissuades education and training providers from rebadging IT qualifications as cyber qualifications • Enables national benchmarking of institutions, curriculum and graduate outcomes to better identify true 'centres of excellence'
3. Employers (Public & Private)	The NICE Framework is a resource to assess the skills and skills gaps of current and prospective cybersecurity professionals employed in a workplace.	• Provides a catalogue of cybersecurity work roles that may be required to secure an organisation's digital and human assets • Assists human resource teams and hiring managers in recruiting cybersecurity work roles by providing a template of content to include in job advertisements and position descriptions. • Provides a check box 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 team. • Provides a standard to ensure partnerships with education and training providers produce a pipeline of job-ready graduates aligned to work roles.
4. 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 cybersecurity workforce.	• Enables the development of measurement tools for greater visibility of cybersecurity skills and skills gaps across an economy. • Provides an evidence base to better target government funding towards cybersecurity 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 global audiences

At the end of the NICE Framework showcase at the GFCE Annual Meeting, stakeholders were asked to provide feedback on the proposed use cases and how they might apply to user groups in their national contexts. The feedback was overwhelmingly positive with several representatives from African countries expressing interest in adopting the NICE Framework as a specific capacity building measure.

Some points of feedback that were provided by participants were however focused on how to make the NICE Framework more appealing for international adoption. Key points are as follows:

- NIST Special Publication 800-181 is too long (135 pages) for most audiences to engage with. Creating more user-friendly tools to explore and use the Framework would facilitate greater adoption.
- 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 Framework would be helpful.
- The benefits of the NICE Framework for different user groups needs to be explained. Development of communication strategies and tools in a variety of languages would be useful. These could provide a consistent narrative that links cyber workforce development to greater cyber resilience.
- References to specific US Government Departments and legislation reduce the Framework's relevance in international contexts (E.g. K0168 Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.). These references could be removed from the NICE Framework and placed into country specific practice or implementation guides.

The GFCE is potentially well placed to be a partner of choice for NIST by making use of the GFCE network to facilitate greater international adoption of the NICE Framework as a specific capacity building measure. Doing so would deliver on key elements of the NICE strategic plan and be of net benefit to other international cyber capacity building efforts by giving countries the foundational tools and guidance for better national cybersecurity workforce planning.

Recommendations

1.1. Develop implementation guidelines and toolkits for user groups that wish to adopt or refer to the NICE framework. This could leverage the model used for other NIST Cybersecurity practice guides.
1.2. Partner with the Global Forum on Cyber Expertise to adapt implementation guidelines and toolkits for countries seeking capacity building support.
1.3. Partner with the Global Forum on Cyber Expertise to develop official translations of the NICE Framework in key languages
1.4. Consider a British English spelling version of the NICE Framework to facilitate greater adoption across English speaking countries
1.5. Partner with the Global Forum on Cyber Expertise to develop tailored communication materials for key international audiences that sell the benefits of adopting the NICE Framework as a cyber capacity building measure.
1.6. Remove references in the NICE Framework to specific United States legislation and Presidential Directives so that they can be read as country agnostic. Reference to specific national legislation etc can be moved to country specific 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

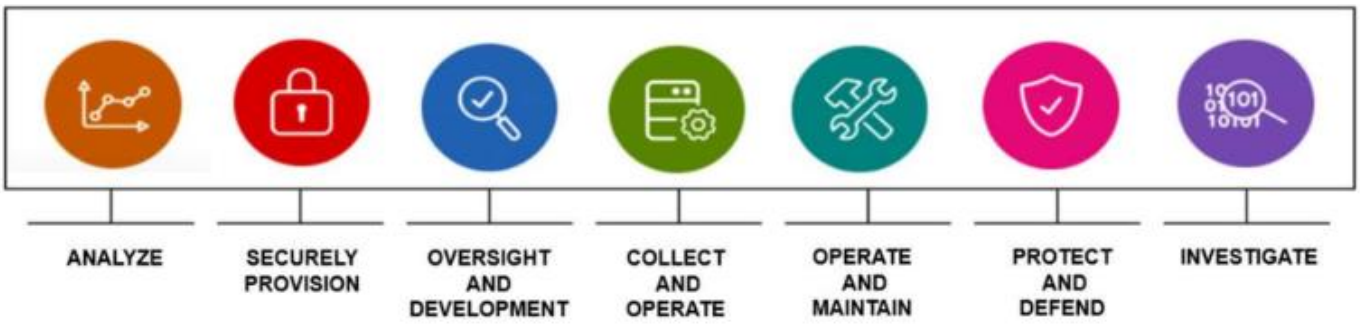
Improving the scope of the NICE Framework

The current version of the NICE Framework described in NIST Special Publication 800-181 is comprehensive. At 7 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 cybersecurity workforce. While the scope of the Framework is wide-ranging a review of each of the elements should still be considered.

The 7 NICE Framework Categories

The organising categories for the NICE Framework are appropriately broad to encompass the depth and breadth of cybersecurity work roles both current and emerging. It is the view of the GFCE Working Group D that these categories do not require any alterations at this time and should remain static. That said providing a mapping of categories to the core functions defined in the NIST Cyber Security Framework, namely, Identify, Protect, Detect, Respond, and Recover would be helpful.

Figure 3. NICE Framework Categories



The 33 Speciality Areas

The usefulness of the Speciality Areas in the NICE Framework requires review. Although the intended purpose of this layer of the NICE Framework is clear in the title, it is unclear how users of the NICE Framework are supposed to engage with it differently to 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 e.g. Executive Cyber Leadership (EXL). It is also however because the Speciality Areas have little meaning from an operational perspective in a workplace.

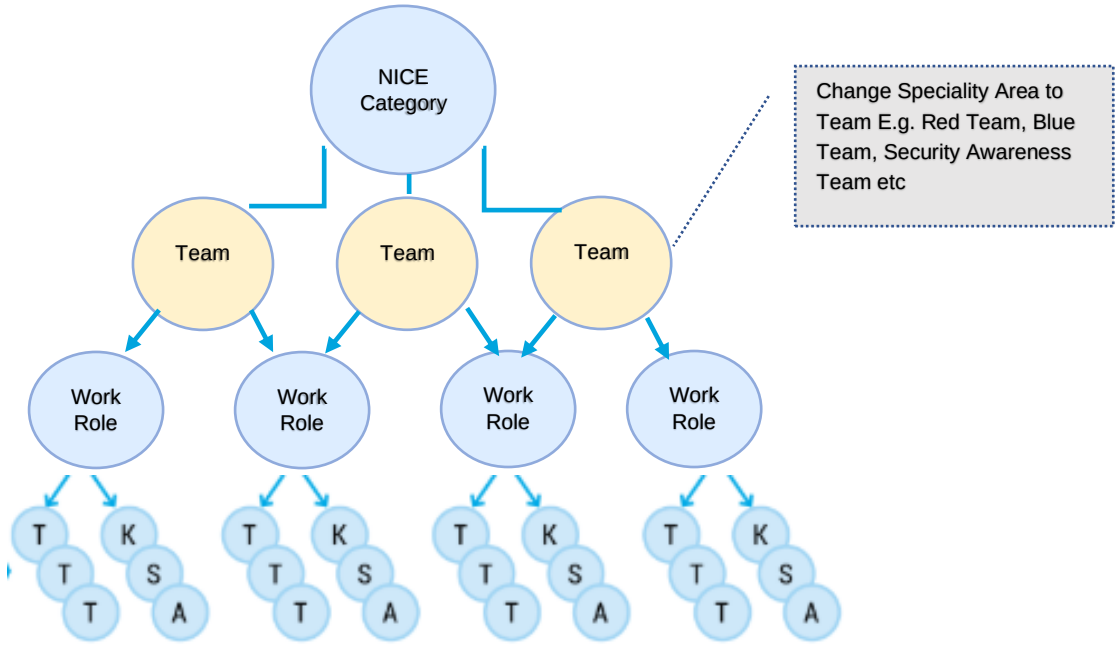
Another way of structuring this layer of the NICE Framework is to consider reframing Speciality Areas as team structures. Employers often use the 7 categories of the NICE Framework (or 5 categories of the NIST cybersecurity framework) to distinguish security functions within their organisation. However, at the layer down they will often refer to security teams that support that function. An example of this might be a Protect and Defend function (category) that is supported by a red and blue team as well as a security awareness team.

Redefining Speciality Areas 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 better strategic workforce planning
- providing the framework to ensure each security function has the right composition of teams and team members with the required skills.
- showing what 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 NICE work roles, and any potential additions, realistically do 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 organisation or context.

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



The 52 Work Roles

The 52 work roles in the NICE Framework provide good cover of the various technical and non-technical work roles that make up the cybersecurity 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 non-controversial examples of potential new work roles that warrant inclusion in the update are Security Awareness Professionals and Cloud Security Engineers.

In addition to this all security professionals need to be able to find themselves in the Framework. 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 as closely as possible the work roles used by real-world employers. Reflecting these in the NICE Framework is essential for increasing voluntary adoption of the NICE Framework.

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 Framework is the inclusion of a Cybersecurity Generalist work role to satisfy the needs of Small to Medium Enterprises (SMEs). Over 90 percent of businesses worldwide are SMEs accounting for 50 per cent of employment worldwide and 40 per cent of national income (GDP) in emerging economies. SMEs are also the most vulnerable to a cyber-attack or data breach which can have a devastating effect on a small business resulting in loss of income, reputational damage or in many cases loss of the business itself.

While all businesses into the future will require a cyber-literate workforce, certain SME’s may also require a Cybersecurity Generalist on staff. Depending on the business this may be a standalone work-role or the job of the Office Manager, the Receptionist or the Business Owner. This is because the ways and means to manage cybersecurity risks is different dependent on the size and type 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 5 staff, an SME in retail versus a local council, a publicly listed company or private entity, an exporting organisation or a start-up.

Just as all 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 properly secure its digital assets. The skills required to perform as a Cybersecurity Generalist 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 Cybersecurity Generalist work role is provided in the table below.

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

Theme	Unit Title	Description
Cybersecurity Awareness	Foundations of cybersecurity	What Cybersecurity 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 lifecycles
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 -e-mail/phone attacks to get information; Shoulder surfing - unobscured screens, watching typed passwords, listening to discussions; Persuasion - face-to-face and conversation.
Business Practices	Promote Cybersecurity awareness in an SME/business	How to engage and promote cybersecurity 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.

Developing Work Role Case Studies

The diversity of cybersecurity professionals, the industries they work in, their career paths and their outlook are a story that could be better told through the NICE Framework. It would be good to see the development of NICE work role case studies that could be accessed interactively by users exploring the 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.

Knowledge, Skills, Abilities and Tasks (KSATs)

The knowledge, skills, abilities and task layer of the NICE Framework provides the level of detail necessary for the overall usefulness of the NICE Framework. For learners it provides a reference tool to self-audit skills they think they possess versus those required to perform a work role; for cybersecurity education and training providers it serves as a reference tool to ensure curriculum and training products are teaching skills that align to work roles; and for employers it provides a baseline for what cybersecurity professionals on staff need to know and do in specific work roles. There are however improvements that can be made to this layer of the NICE Framework to increase the useability and assist users with its implementation.

Providing guidelines to measure knowledge areas

The current version of NIST Special Publication 800-181 makes it 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.

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

Knowledge areas are however difficult to measure. For an education or training provider that maps their cybersecurity curriculum to the NICE Framework, stating that a student will develop "Knowledge of cyber threats and vulnerabilities" could mean different things to different people. One lecturer could say they meet this knowledge area by providing one slide on this topic in one class. Conversely another lecturer could teach an entire unit on cyber threats and vulnerabilities across an academic semester. Without guidelines on how to assess knowledge areas both cases are arguably valid. Though It is understood that the level of knowledge obtained is likely commensurate with the level of study i.e. an undergraduate student would not be expected to possess the same level of knowledge as a master's student, more guidance on how knowledge areas should be measured is critical for consistent implementation.

Skills, Skills, Skills

Of the 52 work roles in the current version of the NICE Framework there are no skills that are common across all work roles. This point is interesting because of the common cry from employers for greater 'soft skills' in cyber security professionals generally. A review of the skills used in the NICE Framework also suggests that some of the language used to describe different skills could be synthesised so that those that skills that are largely the same can be synthesised. This is a point which can also be applied to all other knowledge, ability and task statements.

Ensuring KSATs keep pace with the evolving technology and threat landscape

The way in which technology and the threat landscape has evolved over the years 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 users and enterprises to stay ahead.

In the context of the evolving technology and threat landscape, 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 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 so that updates flow down to vendor products and the education and training providers that direct them to learners. More regular updates will also provide an incentive for education and training providers to invest more in teacher professional development as each jostle for better skilled teachers in a competitive training market.

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

A common observation from employers seeking to implement the NICE Framework is that there is no guidance on proficiency levels within a work role. Though not the fault of the NICE Framework, a potential consequence of this is that many employers develop misaligned expectations of what a new cybersecurity graduate is expected to know and do versus someone that has 2, 5 or 10 years of experience. It is also possible that this 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 don't need, can't afford or that isn't available in the market – resulting in job advertisements staying open for much longer than they otherwise would.

While larger more sophisticated 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 at entry level versus an expert would make the NICE Framework more useful for all user groups by:

- Establishing a career development continuum for individual work roles
- Managing employer as well as new cyber security professional expectations
- Providing better guidelines to education and training providers on skill proficiency levels required by their graduates

Recommendations

2.1 Change the "Speciality Area" level of the NICE Framework to focus on security teams instead.
2.2 Identify new work roles, such as Security Awareness Professionals and Cloud Security Engineers for potential inclusion in the update to the Framework.
2.3 Undertake international labour market analysis to cross check the relevance of existing NICE Framework work role titles against those used by most employers.
2.4 Undertake a full audit of KSATs to synthesise potential duplicates and to simplify language where possible.
2.5 Develop user guidelines to better enable measurement of knowledge areas.
2.6 Consider adding a select range of 'soft skills' to all work roles e.g. critical thinking, communication skills, teamwork etc
2.7 Implement more regular reviews and updates to KSAs that reflect the evolving technology and threat landscape.
2.8 Develop guidelines for assessing work role proficiency levels that provide NICE Framework users with expectations of proficiency at entry level, intermediate and expert.
2.9 Create career profile templates for cybersecurity professionals to use to describe their career pathway. These could be aligned to NICE work roles and used internationally.
2.10 Create career profiles of real-world cybersecurity professionals that align to work roles in the NICE Framework. Add interactive links between select career profiles and NICE Framework work role in existing and future tools.

Managing cybersecurity risk through a single pane of glass

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

A 'single pane of glass' approach to cybersecurity standards

The goal of cybersecurity standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. A cybersecurity standard defines both functional and assurance requirements within a product, system, process, or technology environment. Fundamentally, they are designed to assist any entity, regardless of size to keep information systems and data secure.

Implementing any standard requires the assignment of risk. This seems obvious but organisations often get it wrong believing a technology once installed will manage the risk itself or that risk 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 cybersecurity the risk never truly leaves an organisation. Therefore, employers need to assign cybersecurity risk within an organisation to an appropriate employee with the right knowledge, skills and abilities to be the responsible risk owner.

By aligning the NICE framework with other NIST cybersecurity standards 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 2. 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 NICE into other cybersecurity standards such as ISO 2700. Lessons could also be learnt from the Cybersecurity Maturity Model Certification. 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.

The classified versus the unclassified cybersecurity workforce

A strong cybersecurity sector backed by a highly capable workforce will ultimately underpin the future success of every industry in developed and developing economies. This is because a cyber resilient economy fosters greater trust in a country's ability to promote itself as a safe and desirable place for businesses to pursue digitally driven growth. It is therefore incumbent on government, industry and academia to work together in pursuit of this.

The NICE Framework should be representative of the entire cybersecurity workforce. While there may be a perception that classified work roles should not be publicly available, this submission maintains that they could at minimal to no risk to the originations and agencies that employ them unless of course they are being counted. No private business or government agency wants to publicly disclose that they have no Incident Responders for example.

As it stands the way the NICE Framework is currently structured provides ample room for organisations including in sectors of the economy undertaking classified work to develop customised work roles. What would be useful are NIST guidelines on how to develop custom work roles in a way that doesn't undermine the integrity of the NICE Framework.

Recommendation

3.1 Integrate the NICE Framework with other NIST cybersecurity standards where practical.
3.2 Engage with other standards bodies e.g. ISO and US DoD (CMMC) to assess the feasibility of aligning NICE work roles within other cybersecurity standards.
3.3 Develop a NIST practice guide that demonstrates a single pane of glass approach to using the NICE Framework with other standards.
3.4 Develop public case studies of organisations using multiple NIST standards (including NICE) to manage their cybersecurity risk
3.5 Develop clear guidelines for organisations with the need to develop customised work roles at the classified level to do so within the overarching structure of the NICE Framework.
3.6 Develop a process for organisations with customised work roles at the classified level to voluntarily report metadata to NIST for tracking purposes.

Awareness, Applications, and Uses of the NICE Framework

Describe the extent of current awareness of the NICE Cybersecurity Workforce Framework within your organization or sector or among individuals.

Awareness of the NICE Framework amongst the GFCE Community is low but increasing rapidly. Over the past 12 months a series of presentations on the NICE Framework and its use cases have been given to various GFCE audiences. This included presentations in Tel Aviv, during Israel Cyber Week 2019 and NICE Framework focused workshops at the 2019 GFCE Annual Meeting in Addis Ababa. It is important to acknowledge that NIST's active participation in the GFCE Working Group D has been critical to successfully communicating the Framework's usefulness to international audiences.

It is worth noting that during the GFCE Annual Meeting, Working Group D received expressions of interest for support from representatives from seven African countries relating to further explanation and/or adoption of the NICE Framework. The GFCE Secretariat is undertaking follow up on next steps to assist interested member states on how it can best assist them with their request.

Describe how you or your organization was introduced to the NICE Framework.

The GFCE Secretariat attended a pre-conference workshop on international cybersecurity workforce development initiatives at the 2018 NICE Conference in Miami, Florida. At the workshop a presentation was given to demonstrate use of the NICE Framework in Australia and the creation of an interactive dashboard to explore the NICE Framework. This presentation was subsequently given to other Working Group D members. The Working Group reached consensus on the usefulness of the Framework and dashboard tool for exploring cybersecurity work roles in different national contexts.

The NICE Framework has subsequently been recognized by the GFCE as a best practice tool for describing cybersecurity work roles and their relationship with knowledge, skills, abilities and tasks. The NICE Framework has also provided a mechanism to differentiate work plan packages aimed at education and skilling for the cybersecurity workforce and cybersecurity education and awareness aimed at the broader population.

Explain how you are currently referencing (i.e., applying or using) the NICE Framework and what plans, if any, you have for referencing it during the next year.

At the GFCE Annual Meeting in 2019, the Cyber Capacity Building (Cybil) portal was launched. Cybil is a publicly available portal where members of the international cyber capacity building community can find and share information to support the design and delivery of programs and projects. Cybil currently hosts the NIST Special Publication 800-181, the AustCyber NICE interactive dashboard as well select vendor training aligned to the NICE framework.

The Cybil portal will be updated over 2020 to include additional resources for use in international cyber capacity building.

If you are an education or training provider, describe how your organization uses the NICE Framework to develop or describe education and training content or associated credentials.

As an example of this GFCE Member Palo Alto Networks a custom 7 step ADDIE model to develop curriculum as listed below:

Step 1 – Define Academic Course Name(s) and Domains (ANALYSIS)

Step 2 – Design Course Objectives based on Domain Categories (DESIGN)

Step 3 - Select Work Role from the NIST/NICE Framework NIST 800-181 (DESIGN)

Step 4 – Align/MAP Work Role KSATS to Domains (DESIGN)

Step 5 – Develop lab environment based on Work Role Skills (DEVELOP)

Step 6 – Develop Syllabus, Content, Media, Labs, and Assessments (DEVELOP)

Step 7 – Implement on Moodle (LMS) Platform (IMPLEMENT/EVALUATE)

Describe any tools, resources, or publications that exist that reference or would benefit by referencing the NICE Framework.

Select examples include:

- Australia's Cybersecurity Sector Competitiveness Plan
- AustCyber NICE Dashboard and Video Tutorial

- The Italian Cyber Security Skills Shortage in the International Context
- MIND THE GAP: The Cyber Security Skills Shortage and Public Policy Interventions
- Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities

Describe any tools, resources, or technical support needed to increase the application and use of the NICE Framework.

A comprehensive list of recommendations regarding additional tools, resources and support is provided as part of this submission.