Forwarded for consideration.

Please note that I have retired and this is my current email.

V/R

Chris Kelsall

Chris Kelsall
June 19, 2019

The following is my personal opinion. It does not reflect the opinion of any organization or person other than myself.

We Have a Cyber Workforce Problem!

It's 2019 and we, as a nation, are still trying to define the cyber workforce. What started out in 1996 as Information Technology, Information Management and Information Resources Management which then added Information Assurance got knocked way off balance around 2008 with the beginning of the widespread use of "cyber" and "cybersecurity". The Comprehensive National Cybersecurity Initiative (CNCI) of 2008 established goals for protecting the nation's information technology and information and we've never looked back.

We can't go a day without seeing at least one article, paper or report on the state of the nation's cybersecurity workforce and critical shortages and needs. The good news is that there are so many good people involved that the wealth of useful information expands almost at the rate of Moore's law. The problem is we've yet to bring it all together.

The development on a National Cybersecurity Workforce Framework began in 2010 and the first version was published in 2013. The published framework identified what it called cybersecurity categories and specialty areas. But if you look closely at the definitions you'll see that the categories and specialty areas go beyond that normally associated with securing and protecting networks and systems. Common use of the term "Cybersecurity" from the Comprehensive National Cybersecurity Initiative (CNCI) began leading to an identity crisis - who's cyber, who's cybersecurity, who's in and who's out. Meanwhile much of what was being addressed related directly to Information Assurance as detailed in Federal Information Security Management Act.

Regardless, through hard work, discussions, and disagreements the NICE Framework was developed and published in 2013. It's a framework, not a mandated structure, it's provides top level categories and, most importantly, allows organizations and people to identify with an area and specialty and then take it from there. It can be configured as needed by organizations, private and public, large and small depending on their needs.

However, the NICE workforce framework was deemed incomplete and has been replaced by the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework published in the National Institute of Standards and Technology (NIST) Special Publication 800-181. That publication states that the framework remains a “reference” and that “when used at the organizational level the user should customize what is pulled from the NICE framework.” This framework expands the previous categories and specialty areas structure to now include cybersecurity work roles within each specialty area. In response to the direction in the Federal Cybersecurity Workforce Assessment Act (FCWAA) of 2015, the Office of Personnel

Management (OPM) converted the framework into the Federal Cybersecurity Coding Structure that all Federal Agencies must use to code Federal Agency cybersecurity positions. The framework is no longer a reference, it's a mandate. OPM issued "Interpretive Guidance for Cybersecurity Positions" in October of 2018. That guidance further mandates the use of the NICE framework in the development of position descriptions, applying grading criteria to positions with cybersecurity work, and associated recruitment actions including ranking of qualified applicants. The FCWAA also required that Federal Agencies identify work roles of critical need and plans to mitigate those shortfalls. These plans were to have been submitted in April of 2019.

The Department of Defense Office of the Chief Information Officer (DoD CIO) played a major role in development of the framework detailed in the NIST 800-181 and is mandating it's use throughout DoD. Currently, DoD organizations must use the Department of Defense Cyber Workforce Framework (DCWF) (DoD does not use Cybersecurity at the highest level to describe the workforce and, instead, uses the term "cyber"). Currently the framework is being used to code DoD civilian and military positions to meet the FCWAA requirements. Unlike other Federal Agencies, DoD will soon mandate that all DoD organizations use the framework to determine the qualification requirements for all personnel assigned to positions with an assigned DoD Cyber Work Role Code (same coding structure as the OPM guidance).

We've come a long way from the reference that the original NICE framework and the framework in the NIST 800-181 established. It's now mandatory. But is it up to the level of being able to be used for recruitment and qualification (either for hiring or for on the job qualification? The draft DoD guidance is establishing foundational requirements and standards for the use of academic degree programs, training, and commercial cybersecurity certifications as the means of establishing that a person has the foundation knowledge, skills and abilities to be able to perform in designated work roles. Additionally, the proposed qualification program will implement the use of formalized on the job training and qualification that must address the tasks, knowledge and skills and abilities associated with the cybersecurity work role(s) assigned to the position.

To put this in context, in the private sector, cybersecurity personnel are sought out to meet the needs of the organization. That may, or may not, map to specific NICE Framework cybersecurity work roles, but there may be some basis for use of the framework as a reference. But, when you look at employment advertisements you'll see that companies look at what they value and what the person they are looking for should be able to do to be a part of their team. Accomplishments are recognized, whether it be education, certification, training and even more importantly experience. Also, they seek out people they feel would be of value to their organization and spend the time not only discussing the needs of the company, but why they want the person to work for them and why it would be good for the person.

We are doing the opposite from what private industry is doing by the way we are going to use the framework. We are looking to place every obstacle possible, and a large number of hoops for people to jump through, just to qualify to be possibly interviewed. It has been said multiple times during the period of the requirements identified for the DoD Information Assurance workforce certification program that the emphasis of that program was a check in the box (certification obtained) instead of real determination of the abilities of the person. Current proposal for the new DoD program just adds more boxes and additional means of checking some of those boxes (approved training and/or academic degrees in addition to approved commercial cybersecurity certifications). Additionally, it adds all sorts of qualifiers to the use of those options and standards. It's going to not only be hard for the applicant to determine what they have to do to even apply for a job or even what the job is about, but also for the hiring manager to get all the pieces together and accurately detailed in recruitment and position description documentation. One unanswered question is what to do if there is no approved education, training or certification for a work role? Current proposed DoD policy says that the organization that is responsible for the specific work role requirements "should evaluate alternatives". Once assigned to a position the person will also need to complete on the job qualification based on the cyber work role tasks and KSAs. Failure to do so will result in removal from the position.

The crucial element of the programs at the national, Federal and DoD levels is the framework. But what if the framework is flawed? The Navy has been conducting research and analysis across all areas from position coding, to determination of which academic degrees, DoD training, commercial certification, and experience can be used to meet foundational qualification requirements. Navy has also been analyzing what will be required in on the job qualification programs to be mandated requirements and is beginning to look at the implications on recruitment and position classification.

Within DoD the DCWF is mandated as the standard for six areas: position coding; education, training; certification; on-the-job training; and (proposed) experience. Four of those areas have a requirement that 70% of the learning objectives; examination areas/questions or on-the-job tasks must map to the tasks and KSAs of a cyber work role in order to be approved to meet qualification requirements for that work role. Two areas: position coding and education have no minimum mapping mandated. Finally, four of the areas are content based: position coding (what is in the position description); training, certification; and education. Two are what is actually being done (the actual on the job work): experience and on-the-job training.

The consequences of these mandates is coming to light as Navy continues to determine what can be used to meet qualification requirements.

The first basic flaw is that there is no minimum mapping requirement required to be met before a position can be assigned a cyber work role code. The determination could even be made even because the title of the cyber work role and/or the description seem to apply or, worst case, a single knowledge, task, skill, or ability is needed/performed as a part of the work assigned to a

position. Federal and DoD coding issues are demonstrating some of the issues surrounding this approach. As DoD has said that civilian personnel in specific OPM job series (2210, 1550, 0391) are considered core cyber they must have at least one primary cyber work role code assigned. Besides the fact that positions classified with these job series, 0391 in particular, can't find a work role that matches to their position, other relationships are very tenuous. In some cases, a person may only complete one or two tasks in the area.

Since the work role code determines the qualification requirements, that person will now need an academic degree, approved training, or an approved certification that matches 70% of the tasks and KSAs – things that they don't know, won't ever do, and have no idea what is entailed in completing those tasks.

The other side of the picture is that the 70% minimum will exclude multiple certifications already approved for use within DoD today because of the more restrictive structure and implementation of new proficiency levels. Since DoD CIO has mandated that all tasks and KSAs associated with a cyber work role apply at every proficiency level, determination of mapping will be difficult at best. Formal review has not begun. A large issue exists in that most of the current cybersecurity certifications are cybersecurity, and not Information Technology, focuses. Certifications may not exist for use in much of the IT arena.

This same issue also applies to approval and mapping of training. After a recent data call, DoD CIO briefed that of the 509 DoD Component submitted training courses submitted as mapping to the DCWF, they determined that only 4 actually mapped. They did also say that some of the Army courses submitted were a partial map.

The determination by DoD CIO not to impose the 70% minimum on academic degree programs is puzzling. A formal review of their curriculum would seem to present the largest opportunity for work roles, or multiple work role mapping. Since there is no minimum, it would appear that if the degree program title and description appear to align with work role and s description, a match is assumed.

Another enterprise-wide issue is that not all of the tasks, skills and abilities listed in the NICE Framework and the DCWF are measureable through examinations or laboratory exercises. The first task listed in the NIST SP 800-181 states "Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk." To try to measure that would be unrealistic in other than in a real-world situation. There are others such as "Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders." Or "Identify organizational policy stakeholders." And "Serve on agency and interagency policy boards." This sets up the situation where training, education and certification programs will be unable to meet the 70% threshold because many of the core tasks and KSAs are measureable and are not a part of the programs.

Navy is working on both a pilot to determine the means of implementing the use of an Experience Credential for those who do not have a degree, certification, or approved DoD training. This is especially critical for civilian personnel. Many personnel have served for years after qualifying for their position in accordance with OPM guidance and they experience and accomplishments need to be recognized. Navy is finding, though, that in certain cases it is hard to watch the actual work being done by someone in the position to the tasks and KSAs associated with the designated work role code. So even if the person is doing what is required at a satisfactory or above level and qualified against OPM standards, they will not be able to obtain an experience credential and will be unable to qualify unless they complete approved education, training, or certification – at a cost to the Navy since this is a new requirement based on DoD guidance.

Just as concerning is that analysis conducted during the On-the-Job qualification program development found that since many of the jobs do not meet the 70% minimum threshold, the tasks, skills and abilities actually performed in the job do not require the tasks and KSAs mandated for the work role. To be required to address them in training and on-the-job programs would mean that the components and/or organizations would need to set up and evaluate personnel on tasks performed in a simulated environment – things that are not a part of their job and don't reflect how work is accomplished in the organization.

There are two ways to look at this. First, something is wrong with how Federal Agencies and DoD components describe their work, classify positions, and qualify personnel for hiring. This also means how they are accomplishing the work is wrong. This also means that the educational, training and certification programs in place today are wrong. The other way to view this is that all of those areas can't be wrong, the DCWF must be wrong. It, and the NICE Workforce Framework are not accurately, and adequately, portraying the actual work being done, and how the work is integrated/distributed across positions, teams and organizations.

If you are going to use a framework as a reference, that is one thing. The NICE Cybersecurity Workforce Framework and even the DCWF could serve as a reference, a starting point for further discussion based on a common understanding.

However, when you are going to use something for a standard, if must be fully documented with the valid and accurate – and complete – details needed to implement and manage against the standard. Our initial work in the position coding and qualification areas demonstrate that the frameworks do not yet have that level of accurate detail.

The framework can be seen in the same way we perceive national borders. For a national border to actually be a border three things must occur: (1) it must be documented and published; (2) the description must be understandable and done in relation to international norms; and, (3) it must be used and enforceable. A framework that is not accurately documented; that does not reflect the national and international landscape and current descriptions of skills, tasks and jobs; and is

not used is just a piece of paper at best. At worst, it will portray an environment that is inaccurate and unrealistic. Actions taken to meet the direction may well be inappropriate and detrimental.

Bottom line, if we are going to mandate the use of the frameworks as a standard for position classification, recruitment and qualification we will need to develop and provide a framework that accurately reflects the current cybersecurity workforce That framework must identify needs in terms of critical skills, provide a means of determining where to put emphasis on education, credentialing, certification, and training; and be viable enough to be able to be used to incorporate new workforce requirements as they evolve.

Maybe it's time for a cyber workforce deep breath, followed by formation of a team from private industry, academia, federal agencies and lone wolves to get together and actually describe what the workforce looks like in real life. This team should be able to address structure and needs from the smallest organization to multinational organizations. It needs to reflect the major sectors, and it needs to include both providers and customers. That group would also determine what the framework would/should be used for. Once you determine what it’s used for the structure and content can be developed and configured to support the need. Until we can accurately depict what exactly is out there along with what people need and institute a common language we will keep establishing silos that attempt to be a one size fits all, when actually there are a lot of sizes needed.

Once that is done you can detail the processes and guidance required to carry out a meaningful cyber workforce qualification program. Until a cybersecurity (cyber) workforce framework can accurately depict what exactly is out there along with what people need we will keep establishing

As DON, Navy and Marine Corps have found executing a program of this size and complexity is not an overnight activity. While the other DoD components may be able to leverage the work done by USN and USMC. All services will need time to develop plans, develop policy and have it approved, configure systems, inform personnel of their status, update personnel processes, establish training, and actually qualify personnel.