Chris Kelsall
July 20, 2017

Subject: Response to NIST RFI for Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development in Support of Executive Order 13800

1. Are you involved in cybersecurity workforce education or training (*e.g.*, curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)?

Yes. Private citizen with nearly 20 years' experience within the Department of Defense in determining and documenting military, government civilian and contractor Information Technology, Information Assurance, Cyber Information Technology and Cybersecurity workforce personnel, education, qualification, certification and qualification requirements. 15 years' experience in development and implementation of workforce policy and management.

2. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

Various "industry-wide" performance assessments and degrees and certifications may have a place, but the ultimate decision should rest with the cybersecurity workforce leadership in an organization. How the organization does business and structures their workforce and work must be an essential consideration for workforce metrics. A high level enterprise view, while a starting point, doesn't reflect how the work is distributed among workers in an organization. (e.g., on a large network there could be a large number of people doing focused work, while in other circumstances the work would need to be combined into one position).

3. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

No. as detailed in the Draft NIST SP 800-181 there's a lot missing and a lot of issues. The comments received during the open comment period for the publication reflect that. Additionally, there are multiple "roles" not captured in the framework but commonly used and detailed by both the public and private sector. Additionally roles identified in NIST cybersecurity publications should be clearly linked to the framework are not adequately addressed. A high level of risk exists as the Office of Personnel Management (OPM) is using the draft roles based framework to develop a coding structure that Federal Agencies are required to use to code Federal government cybersecurity positions in accordance with the Congressional Federal Cybersecurity Workforce Assessment Act. The picture that will be drawn using this approach will not present an accurate and comprehensive model needed to properly understand the work accomplished by the Federal cybersecurity workforce. The information provided by the NICE framework provides enough utility at the specialty level to provide some context, but delving down into the KSAs and Tasks and roles leaves gaps. The NIST direction that the framework serves as a reference is appropriate, but there is much more that needs to be addressed. Cybersecurity fundamentals along with technology changes, process changes and the business needs in the private and public sector more appropriately determine how the work is structured and what capabilities are needed by the cybersecurity workforce to grasp and conduct current, new and evolving cybersecurity work. Just as with the OPM Occupational Series definitions - it's a starting point and may be able to provide insight in areas that people aren't sure of. But the roles framework is not necessarily the cookie cutter standard that everyone should employ and qualify their people too. There is national-wide informal agreement on many positions, job titles and even roles as can be seen in certification types, academic degree programs and training programs - military training programs in particular. Many private organizations adjust the work based on how they do business and from lessons learned. This is especially relevant regarding which people, with which backgrounds and experience are best suited for taking on new and different work. The framework, as currently structured, does not address proficiency levels or experience - which is also a critical shortfall. Additionally, the concept of "competencies" isn't a part of the structure. Competencies help detail what is required to be able to perform the functions of the position in a successful manner. That's not something that the framework currently addresses. People and organizations look at job announcements or position descriptions and say - yes that's me or yes that's what I need. The framework does not rise to that level yet.

More work needs to be done - under NIST and NICE leadership - to establish a framework that more accurately reflects cybersecurity work. Rather than asking for a report on the Federal Cybersecurity workforce, Congress should amend their requirement to first require that an agreed upon and inclusive framework be developed and provided.

4. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

Organizations are continually working to review and revise policies as needed as technology and the work evolves - but normally they're way behind the time when they are first needed when published. The better question here is, are the resources needed in place to provide education and training for the cybersecurity workforce. Currently, resources are in place based upon what can be allocated in context of the overall missions of the organization and budgetary limitations. There is never enough money, time or approved instructional programs for the cybersecurity workforce, but that's true across almost all occupations. The key in the future is to not only look at the technology, but also at how the workforce must be educated, trained and gain the experience necessary for the technology to be utilized. This also needs to be considered when quick acquisitions and deployments of new technology occur. The analysis and work needed to determine who in the workforce would be the best candidates to take on the new work and what it will take to develop their skills and abilities to that level must start at the same time that the look for new technological solutions starts. One major consideration that isn't being fully addressed, and something like the NIST framework might support, is work integration. When something new is added to a system or network there's a need to see how that technology integrates and impacts everything else that is part of the system or network. That isn't currently done in a formal way with much of the workforce. How will this impact the cybersecurity team, who will do what and what will they need to know to be able to function as a team. Organizations look at what occupation is best suited for the work and what the workload impact is, but full integration of the processes and work required to operate the system or network isn't always considered. Even if we determine that someone must now take on new skills and their workload must go up, we don't normally look at how that affects the work of those around them. Additionally we don't normally factor in time for personnel development both to improve the ability of the person and also to integrate new processes across the team. Policy enforcement is an issue. What are the consequences of not adhering to the policy has to be a primary consideration. But even more critical is answering the question: is the policy actually executable based upon the resources made available? Within the Department of Defense the time to develop, review and approve new policy is extremely lengthy. Policy should be in place before something is expected to happen, not as an afterthought. Lastly, there's the need to answer the question: does the policy provide any value?

On a national level, resources and emphasis must be provided to NIST to support revision, development and publication of workforce standards.

5. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy vs financial sectors)?

Knowledge, skills and abilities vary based on the needs of the organization, but generally what's provided in academic degree programs, military training, technical training and measured through certification programs reflects a general consensus. The academic programs and the certification assessments along with technical training have been developed based on the actual technology involved, the key processes needed to utilize the technology and the business model developed through experience by those organizations that utilize the technology. As the business models evolve you see the developmental requirements evolve. Mostly in direct response to the technology itself or as an identified need to formalize the knowledge, skills and abilities required to utilize the new capabilities. Many studies say that what employers, and I would say employees also, value is experience. The ability to actually perform the work successfully to the level needed by the job. With military training, new recruits - who may have no cybersecurity background - are taken in based on aptitude and then provided the basics so that they can move into a position and eventually gain the experience and proficiency needed to perform the work and move on to positions of increased complexity and responsibility. Within the Federal Workforce there has been the perception that we hire cybersecurity professionals fully ready to accomplish the work. That is unrealistic. There are unique factors both in the technological configuration of the organization's network and in how the cybersecurity team does business that can only be gained from on the job experience. We must ask ourselves what the person must be capable of to enter into the job - but also what can only be learned while actually performing the work. I would ask the question - based on what people are equipped with coming from an academic degree program, demonstrated knowledge and ability in regard to a certification, or from training programs, what does the employer need to do to fully integrate the person into the cybersecurity team. If the answer is you can't get that just from the existing workforce, where does there need to be a bridge? At that point you can determine if you have the necessary foundational abilities that can be built upon, or if something new has to be brought into play to educate and train people. Finally, much of the work that seems to be in areas where employers are saying I can't get enough qualified people is highly specialized. The Cybersecurity Credentials

Collaborative (C3) has a great concept that should be considered: Foundational: This credential ensures a person has pre-requisite knowledge, skills, and abilities before attempting to work in this functional area. Related: This credential ensures an individual has knowledge, skills, and abilities that are generally aligned to this functional area. Individuals possessing these skills should have conceptional familiarity in this functional area. Specialist: This credential ensures that an individual has demonstrated knowledge, skill, and ability within this NICE functional area. I would add to this, that the Related category also indicates that a person has knowledge, skills and abilities that go beyond the foundational area providing the person with an increased ability to work with people in other functional areas. If organizations and employers truly wish to determine what their needs are they should consider applying this concept - is the work totally within this area, is it related to other area, or is it a specialized subset of the area.

6. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

The most effective developmental programs should be judged on usefulness and value - rather than say this is a really good program, look at the industry studies that show what certifications are most valued, which graduates from which institutions are most valued - and why? Military training is also highly successful and valued along with military experience. Almost all transitioning military members find good cybersecurity jobs upon transition from military service. But I would say it's subjective and until the academic community in particular establishes a more common lexicon of what academic degree programs should include there will be different perceptions from different groups. The discussion of establishing a good piece of the cybersecurity occupation as a vocation has merit. Successful programs must address what is needed for the person in their area to be successful after completion of programs. The program, regardless of what it is, should be recognized and its graduates sought after because they are known to provide abilities at a level valued by the employer.

7. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

Instead of saying we don't have enough qualified people, look at what we really can expect in terms of numbers and areas of expertise, then determine how to address the gap. There should be a blend of technology and the human workforce. What can the technology do that I really don't expect to be able to have enough people with the knowledge and abilities to do? What do I really need to have people doing? There needs to be a shift from the "this is what we want this" to "what is really needed". Measure expectations based on what you can truly expect to have for resources. The three best Cybersecurity scientists in the world can build the tool that answers every need, but if they are the only ones who can operate it, then it doesn't support widespread use. But there is opportunity here also. As the use of emerging gamifying and competitions within the cybersecurity workforce have shown, there are folks within the population, the cybersecurity workforce, and the general workforce that have aptitude, capabilities, and concepts that we have yet to identify and bring into the cybersecurity realm. Part of that problem is we aren't going far enough to entice folks to take a chance at cybersecurity - competition being the best vehicle. Just like people try baseball, chess or driving an Uber they don't know if they'll like it until they do. Not everyone will, not everyone will make the big leagues. However, some will if they are somehow convinced to try cybersecurity work to see what it's really all about. On top of that, within the Federal government we need to change our attitude and what people perceive the federal government employee as being. Look at private industry and how they do business and their best practices and adapt those to the Federal cybersecurity workforce. The biggest challenge is determining why people join the Federal government, why they stay and why they leave - and then encouraging the good and limiting the bad.

8. How will advances in technology (*e.g.*, artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

The more appropriate question is what will be the balance between human and technology going forward? Any technological advances must include an assessment of what the human/technology interface looks like and what should be done by technology and what must be accomplished by humans. Workforce has always been running behind technology with developers working hard to provide the required capabilities without regard to what it means to those who have to make the capability work.

Another issue with new technology, and AI, is that the technology is never "perfect". Even if integration is accomplished properly there can be consequences that were never expected. When we move further toward using technology - and AI - to evaluate great masses of data and provide an answer or evaluation, we will never be able to determine whether the conclusion presented and the underlying information isn't the product of inaccurate - or manipulated - data. The more we automate, the more we will need to determine what we need to do to trust the information.

The concept of the "Right Person, with the Right Abilities, in the Right Place, at the Right time and doing the Right Thing for the Right Reason" (paraphrasing from the Navy nuclear power program) has to be key in the future.

The Pentagon’s Department of Defense, Rapid Reaction Technology Office, which looks to develop prototypes and host technology demonstrations to counter emerging and anticipated threats, has issued a special notice to industry that includes the following as areas of interest:

> - Autonomous cyber defense; cyber situational awareness, planning and decision support; cybersecurity for infrastructure, endpoints and edge devices; control systems, internet of things security; and hardware and software assurance.
>
> - standoff detection/sensors, device neutralization, counter vehicle attached IEDs (VAIEDs), electronic countermeasures for advanced wireless signals and techniques, robotics, data analytics/predictive algorithms, counter tunnel and mapping technologies and biometric signature collection and exploitation.

That’s a very wide range of new capabilities. The question that needs to be asked is what do we need and expect our people to do when employing these new capabilities. Decision making obviously comes to the forefront along with oversight. But what are the "hands on" capabilities required to not only use the new technology - but to also ensure that it integrates with the overall enterprise and that the overall enterprise is properly configured, operated and monitored. We need to be able to answer the question - What happens when the check engine light comes on?

Just like the question of inherently governmental must be used in determining which Federal positions must be filled by military or government civilians because of the decisions being made or actions being taken, there must be a clear delineation of what is "inherently human". Decision-making, oversight, tasks required by law and complexity of operations all have to be taken into account.

Instead of asking what's the impact on the workforce (usually read as how must the workforce catch up) the question must be asked up front - what's the right role of the workforce here and what should be technology based and what is the required balance.

9. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

   i. At the Federal Level?

   First and foremost:

   Make a paradigm shift - rid the Federal government of the term "we only hire personnel who are fully qualified for the work described in their position description". Realize that government cybersecurity folks must continue to develop across all of their careers. But make it a tenet that there are specific things that a person must have in order to come into a position to be able to understand what they must learn on the job. Include the idea that the work will change and that the Federal agencies must be able to ensure that their workers are given the right developmental opportunities to grow and adjust as individuals and team members.

Also:

(1) Congress and the Executive Branch really need to look at what the legal roles of people are within the cybersecurity domain. Both operations within US networks and outside US networks. Then determine what is inherently human and inherently governmental.

(2) Take the actions necessary to accurately portray cybersecurity work and the cybersecurity workforce. DO NOT put in place an inaccurate picture that will serve as the starting point for making future decisions - get it right and get it right soon. Bring in private industry; identify best practices on how cybersecurity teams are structured.

(3) Take the Office of Personnel Management (OPM) out of the cybersecurity personnel arena. Ensure that appropriate laws and policies detailing legal requirements and personnel protections are in place - but then let the Federal Agencies develop and implement their plans. If, as we constantly say, we're in competition with private industry - then compete with private industry. Identify and implement the best practices that private industry uses to attract and retain and grow their workforces. We can't expect to develop a 21st century workforce with decades old classification standards being applied by Human Resource practitioners who many times do not have a key understanding of the issues and requirements related with cybersecurity workforce personnel.

(4) Take the actual structure identified by the framework developed under item 2 and then look at the work in two ways - inherently human and inherently governmental. Once you've done that then publish that information and ensure that

developers take that into account when they build new technology. It's been said for years, but mostly not listened to, that human factors must be a major consideration when developing new technology.

(5) Move beyond the individual in describing and addressing workforce needs - look at how the work can be spread out among teams of people and how to address the overall processes needed to support the technological capabilities required by the organization and maybe even the interoperability between multiple government and private organizations.

(6) The Federal Virtual Training Environment for cybersecurity is an extremely valuable resource. The Federal cybersecurity workforce needs more though. Much like military personnel receive training both to support their current work but also to enhance their abilities for positions of more complexity and responsibility, something similar - and equal in value - should be established for the Federal civilian workforce. A part of this enterprise would also include content associated with new technology coming into the enterprise. Creation of such an entity has been discussed for a while, now is the time to establish such a capability.

(7) The time has come to direct and implement cybersecurity workforce funding. Congress or the Executive branch needs to direct that all agencies include in their budget a line for cybersecurity workforce to address not only financial incentives such as recruitment and retention bonuses, but also - and even more importantly - dedicated funding for cybersecurity workforce development. As OPM would say the HR authorities are there and as the workforce itself would say, they know what developmental opportunities exist that are beneficial. There just is always the issue of finding available funding to do what needs to be done. The time has come to stop treating cybersecurity workforce funding as an un-funded mandate competing with all the other workforce funding requirements and to establish and provide dedicated funding for the workforce. Until the time that funding for the cybersecurity workforce becomes so ingrained in agency funding requests that its second nature, there must be direction and resources provided from the enterprise level.

(8) The "report" emphasis must be shifted. We have had enough calls for information and studies and reports that haven't resulted in any new positions or new funding. The time has come to actually ask the Federal cybersecurity workforce to truthfully answer three questions - Why did you take a cybersecurity job with the Federal government? Why are you staying in that job? What would make you leave that job? Based on the results from the workforce itself, then look at what is working, what isn't and what needs to be addressed.

a. At state or local level, including school systems?

b. By the private sector, including employers?

c. By education and training providers?

d. By technology providers?

As mentioned above, the human factor must be addressed to a greater level than is currently being done. Every new technology should include an impact statement and how the technology is expected to be configured, operated and maintained by the cybersecurity workforce out in the field. Cybersecurity workforce requirements must be part of the up front development, not an add on later down the line.