Mr. Petersen: Welcome to our Framework in Focus interview. The NICE Cybersecurity Workforce Framework or NIST special publication 800-181, establishes a taxonomy and common lexicon used to describe cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE framework is intended to be applied in the public, private and academic sectors. Today we're interviewing Carol Schmidt who works at the National Institute of Standards and Technology which is part of the U.S. Department of Commerce. Carol thank you for joining us today.

Ms. Schmidt: Thank you Rodney for having me.

Mr. Petersen: Carol could you please explain your role and responsibilities as a program manager at the office of information systems management at NIST?

Ms. Schmidt: My role as a program manager encompasses a lot of different areas. I did previously have individual responsibility for IT security and privacy awareness training and education for NIST staff operationally and they expanded that to include supervisory skill-set.

Ms. Schmidt: So now my team, that's comprised of five individuals, their responsibilities that I oversee, encompass IT security and privacy directus management, supporting the NIST Chief Privacy Officer and representing NIST with our headquarters department and conducting privacy assessments, continuing to oversee and manage IT security and privacy awareness training and education. And then I have some team members that are IT security officers for organizations internally that support such functions as human resources, finance, acquisitions, facilities, etc.

Mr. Petersen: Describe your career path to becoming a Program Manager at NIST?

Ms. Schmidt: I have been within the government, specifically with NIST, for close to thirty-three years. I actually started my career on a high-school co-op program thirty-three years ago and at that time I came on-board as a clerk typist. That was when the clerk typists were first introduced within the government. Through the years my career evolved from clerk-typist to computer specialist to IT specialist, managing a BAA program on PKI technology. Then becoming a computer scientist supporting activities of the information infrastructure task force, if you can remember, was several years ago. Thereafter I worked on the research side of our NIST organization where I was a system administrator and I conducted research on digital libraries. From the research organization I transitioned over to what is now our Chief Information Officer (CIO) Organization supporting security and privacy internal to NIST. So, I do report to our Chief Information Security Officer, and I also, in a matrix fashion, report to our Chief Privacy Officer, and now have the managerial responsibilities for the team.

Mr. Petersen: Thank you that's fascinating. How can you envision using the NICE Cybersecurity Workforce Framework to either guide your own career or in your role of the hiring manager for your organization?

Ms. Schmidt: At this point I won't be using the framework for my own career but I do see great value for our community as a whole. In the short-term the NICE framework is really assisting us in the identification of our critical needs operationally. Having employee positions and expanding to our Associate positions within NIST, those workforce codes provide us insight into like positions across the enterprise and that contributes to ensuring growth and sustainment of our workforce. Applying those codes allows for matching work requirements and skills with curricula develops through academic and industry work experience. NIST operationally is in the process of expanding our use of the NICE framework within our HR and associate processes. While we're using the codes for more strategic planning, I see us using the codes for enforcement as well. What I mean by that is using the coding structure and applying that down to specific roles and what they have access to. We have an upward view from strategy then a downward view into actual operations.

Mr. Petersen: So, the potential use of the NICE framework for authorization or access control is kind of a by-production of the identification of work roles in the framework.

Ms. Schmidt: Absolutely and also helping us normalize statements of work and position descriptions across the roles identified in the framework whereas before they may not have been present.

Mr. Petersen: What type of cybersecurity jobs are the most difficult for you to fill in your organization?

Ms. Schmidt: With my small team I recently had to fill two positions. One was a directus position and the other a privacy position. While they each has their own unique challenges, it was most difficult to find incumbents for the privacy position. I had many folks that applied for the privacy position and had experience and education in security but not necessarily privacy. Now that we're seeing this convergence of security and privacy I think that's the greatest challenge, finding the expertise that really encompasses both of those areas.

Mr. Petersen: Another really good point and I think in the process of the draft comments for the NICE framework we received a lot of input about how to be more inclusive of privacy knowledge, skills, and abilities and tasks, as part of the different work roles that people perform.

Mr. Petersen: How do you decide if an academic degree or a cybersecurity certification is required for a job announcement for your organization?

Ms. Schmidt: Several years ago, I was on a Department of Commerce task force and at that time we identified and documented roles which required a professional certification. Those roles married up to DODs efforts where we had to define in policy what those roles were that were significant in terms of IT security. We do have a requirement for several security roles to have cybersecurity certifications and that policy identifies what certifications should be. That being said, if we have a candidate for an open position that meets all other criteria we're not so rigid with our policy that we would not hire them without a certification. We would create a development plan to get them where they would need to be with the professional certification. Of course, being in the NIST environment academic degrees are the preference. If you have an academic degree and you have a professional certification those are both highly sought after in our environment.

Mr. Petersen: How do you keep your skills and those of your team members sharp and current?

Ms. Schmidt: In the operational environment we're fortunate to be involved in projects that are NIST wide and are varied in terms of what they are trying to do. I do encourage training and back up of one another in their respective areas which broadens their knowledge of those other areas. For example, a security officer that might oversee finance have their own challenges within that area as opposed to a security officer who oversees securities within the facilities organization. I encourage them to back up one another and share information about how their doing their job, what tools their using, etc. I also encourage my team to attend talks internal to our organization so that they can understand the business of NIST and how then security is applied to that business. I encourage them to get involved in other projects outside of cybersecurity where it might be automation or automating research area for example.

Mr. Petersen: NIST is certainly a great organization to learn from because of our research mission and the applied cybersecurity division and the computer security division I'm sure you will find no shortage of internal resources for some of that professional development.

Ms. Schmidt: Absolutely. In addition, we have our folk's frequent security conferences and trainings that are provided by the public. My team, each member has an academic degree that is related to their position but I certainly encourage institutional training as well.

Mr. Petersen: How are you attempting, or maybe the larger office of information systems management, to make that workforce more diverse?

Ms. Schmidt: NIST appreciates diversity in both its culture and perspective and embraces workforce talents of many different forms. One way I support that is by supporting ways for people to connect with one another particularly with my role in IT security awareness training and education. I think it's important to have this diversity, about celebrating and leveraging our differences, but I think it's equally as important to celebrate communities in which people can share ideas, tools, and experiences. We do that through a number of different forums. We've got mail lists, quarterly meetings that all of our security officers attend, etc. That is one way. Another way is through the establishment of development plans or means to diversify ones' knowledge, skills, and abilities. I really believe that diversity doesn't begin and end with the hiring process. We not only need to keep and appreciate our diversity within ourselves and that's done through the various communities and so forth. Another means is merely through the work that is being done. In IT security and privacy, we have an opportunity to touch various business areas across our NIST research environment and we have opportunities to work collaboratively to apply security and privacy and of course that increases the knowledge that we have. That is another way we are supporting our diversity and our knowledge.

Mr. Petersen: As a NIST employee myself I remember participating in orientation where somebody from the office of information and system management or OISM as we think of it internally referred to themselves as 'part of awesome'. In fact, that could have been you who gave me the orientation.

Ms. Schmidt: It was me!

Mr. Petersen: What is it that you enjoy about working for awesome and as a part of NIST?

Ms. Schmidt: I appreciate that you still call us "awesome" [OISM pronounced as AWESOME] from a customer support standpoint we really appreciate that. For myself I most enjoy working with the people across NIST. We are an academic environment which means we work with really smart people. Smart people tend to challenge us and that's a good thing. That continues with our own thoughts and ideas; it presses us to be better. We do a lot of different work here at NIST. The very diverse nature of our work I so appreciate because we're constantly learning and growing. In terms of operations and what I do in my day to day job I appreciate having a voice and implementing and promoting change. I particularly like promoting change with automation. I would have to say the people, the mere fact of what we do here within our organization, and automating and changing things. That's what I enjoy.

Mr. Petersen: It has been an awesome experience working with your team. It's almost as good as an acronym as NICE! My final question is if you could give advice to a young person who is considering a career in cybersecurity, what would you tell them?

Ms. Schmidt: I'd say great. Go for it! I've had the opportunity to council many young people through the years and for those who were or are considering a career in cybersecurity I'd highlight that cybersecurity crosses many varied disciplines. For example, you can find within health care if you are a nurse and wanted to transition to cyber, it should be an easy segue in terms of applying it to the health care environment. I would encourage folks to find the discipline that they know most about and then segue this knowledge into how cyber and privacy can then be applied. We'll always have a need for domain area specialists. I would also encourage folks to read the detailed work role listing found in the NICE framework. That would really expose folks to common roles and what those roles mean and what are the ksa's associated with those roles. That's just another data point for folks trying to decide what type of role in cybersecurity to pursue.

Mr. Petersen: Thank you so much Carol. Thank you for your leadership of the security and engagement awareness team at NIST. Thank you for sharing your insights with us today.

Ms. Schmidt: Great, thank you Rodney.