**Mr. Petersen:** Welcome to the NICE Framework in Focus. This is Rodney Petersen, the Director of the National Initiative of Cybersecurity Education, or NICE. I am joined today by Julie Chua, who is the manager of the risk management program in the Office of Information Security for the U.S. Department of Health and Human Services. Julie, thanks for joining us.

**Julie Chua:** Yes, thank you and I appreciate this opportunity to provide some insight to the NICE Framework and how it effects and impacts my work.

**Mr. Petersen:** Thank you, first Julie, why don’t you explain your role and responsibilities as a manager of the Risk Management Program in your organization.

**Julie Chua:** As a manager for the Enterprise Risk Management Program, I am directly underneath the Deputy CISO and the CISO, the Chief Information Security Officer. I am responsible for the overall strategic mission and the vision of a department-wide security risk management program. I make sure that information security and privacy, as well as our healthcare industry cybersecurity, are integrated within a successive enterprise risk management program. I make sure that it is aligned with all strategic plans as well as our mission, of course, within HHS. There’s two things that I’d like to highlight in terms of, I would say the vastness of my role at HHS. There are the sector engagement and critical infrastructure risk management efforts as well as HHS federal systems and environment efforts that speaks to more of our HHS systems, protecting them and making sure they are resilient.

**Mr. Petersen:** That’s great and I suspect my next question about the size of your team, is probably pretty large, if you take into account all of those sectors that are a part of HHS that are working independently in the private sector. But, let’s just focus on what you are doing within HHS. What is actually the size of your risk team and what types of roles do they fill?

**Julie Chua:** A combination of federal employees and contractors make up my team, and give or take, there are about thirteen to fifteen team members within the risk team and it runs the gamut from auditors and assessors, to cybersecurity entities including policy strategy focused individuals, risk management experts, and then I also have technical analysts and vulnerability analysts on the team as well as research development and analysis individuals as well.

**Mr. Petersen:** Julie, describe your career path to becoming a risk manager.

**Julie Chua:** It’s quite interesting actually. I was first and foremost a project manager/program manager right out of college. Into my five years working outside of, after graduating I should say, I decided that I wanted to become a business owner and that business was focused a lot on risk assessment, risk management, projects, and programs that involved software development and the clients were within the federal environment, non-profit and healthcare provider practices. I would like to note that the healthcare provider practices is because I come from a physician family, so most of my siblings, my parents they are physicians and I just found myself in the healthcare industry pretty naturally. Within that small business it was dealing with a combination of federal requirements as well as HIFA requirements and meaningful use more of an industry and sector-critical infrastructure cybersecurity. After owning a business, I decided to venture into the federal government and within 2013 I started within HHS at the Office of the National Coordinator for Health IT. Within that office, is what the policy and strategy focus office, we reviewed and analyzed proposed legislation, requirements, and we also advised the National Coordinator on Privacy Security, and data stewardship of electronic health information, health IT and we also served as the coordinator across the federal and private sector. One of our main goals was to educate our stakeholders on privacy and security issues and that our stakeholders group was small and medium sized providers and organizations within the sector. Within my stint at ONC we really looked at the impact of technological advances or proposed requirements on privacy and security. We looked at implications of health IT and the interconnectedness of our healthcare industry ecosystem and making sure that privacy and security was addressed or it did not impact it in a negative way. After that I was still in ONC, I became the security branch chief of the security branch within that division. My role evolved again into more of critical infrastructure cyber so a lot of the executive orders that called for security and resilience within our sector. I would lead on a lot of those initiatives and as I came into my current role within the office of information and security officer I already had a mixture of federal and sector work. It was kind of a good foundation for me to start within ONC, I had the broad prospective of our diverse regulatory authorities within HHS and how that interacted with the sector as well as how that interacted with our FISMA requirements and our federal requirements within HHS. That puts us to today so I hope that answers the question.

**Mr. Petersen:** That’s really fascinating and it’s fun to hear how your family influenced your career.

**Julie Chua:** Yes definitely.

**Mr. Petersen:** How could you envision using the NICE Cybersecurity Workforce Framework to guide your own career as well as your role as a hiring manager for your risk management team?

**Julie Chua:** In terms of my team’s involvement with the NICE Framework we were lucky to have been invited to do some updates to the risk management professional category itself to ensure that we had a way to kind of guide the career path towards a risk management professional. Right now it’s non-existent where you have a cybersecurity person who is interested in risk management but would just like to be policy focused or a risk management professional who would like to be technically focused. One of the things that I think we have tried to carve out is a path for someone who wants to do both, like myself. Or someone who is really just wanting to do a technical focus or a strategic focus and giving a person like myself, who are willing and able to cross that line a path towards a career choice as well.

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

**Julie Chua:** All of the above. Policy and strategy focus people, technical analysts, and the combination of both especially as we are seeing the culture shift to enterprise risk management which is broader than security risk management within cybersecurity. We are really having a hard time finding people who can step out of their technically focused cybersecurity role. And looking at the bigger picture and making sure that what they do in the operational technical side does not affect negatively what policy, what regulation, and what strategically we are trying to do.

**Mr. Petersen: G**iven the challenges you just described how do you decide if an academic degree or a cybersecurity certification is required for a job announcement in your organization?

**Julie Chua:** I’ll do the certification first. I use certification as a floor if you have it, it means you speak the universal language of information security, cybersecurity, risk management, and it also shows that you are dedicated to the field that you’ve chosen. For the announcements that I’ve done for my risk team a bachelor’s degree is always good. These days you always could come from a totally different background and nothing cybersecurity so I don’t necessarily scope that degree to, for example, computer science or information management, I think it does lend itself to a broader spectrum of degrees when it comes to specifically the risk management career path. And I would have to add, though, the experience would have to speak to those things if you don’t have a degree or your certification does speak for that.

**Mr. Petersen:** That’s a great point as we often forget that experience is as important as academic degrees and certifications when it comes to credentials somebody might bring to the job. How do you keep your skills and those of your team sharp and current?

**Julie Chua:** Training is a big thing for me. I always try to provide training opportunities for team members. I point them out if I see some. I, myself, try to keep abreast with new training every year. It’s never a good time. We always say we don’t have time for training, but I’ve taken it upon myself to just make sure once a year I do some sort of training. HHS provides opportunities to do that and I would say that it’s a good thing that it is emphasized within HHS. Other things are making sure we are keeping up with current events. Speaking engagements is another thing that I try to encourage team members. Most of them are adverse to speaking engagements, but I let them know it is something to broaden their prospective. Either hearing other speakers, or preparing for one, would actually help with keeping with current trends and what’s in articles and what’s trending. Another thing is, I try to challenge them to think strategically and critically. Especially when a new requirement or strategy comes out, I emphasize with them where, if they point something out in an article, not to just point it out, but to say how it impacts our work or how it could potentially impact our work.

**Mr. Petersen:** That’s a really excellent point about the presentation and the outreach. You take for granted the type of learning that occurs and the preparation as well as the actual speaking to an audience and engaging with them through Q&A.

**Julie Chua:** Yes, absolutely.

**Mr. Petersen:** How do you work to make your workforce diverse?

**Julie Chua:** I would say I would go back to the speaking engagements and attending conferences and training. You meet a lot of different people. And I emphasize that because, as I said prior to another question we had in terms of academic degree, when it comes to a risk management profession within cyber you would be surprised where people come from. I think that’s why there is such a diversity right now within the cybersecurity world, is because people are finding themselves in this career path from a business degree or an English degree, where they bring to them a different kind of thinking that is outside the box of just being a technically focused person.

**Mr. Petersen:** That’s a really great point. The diversity of thought or experiences that people bring to a position that really requires a team to solve problems from different perspectives. It sounds like you enjoy your work, but what is it that you most enjoy about your role as an enterprise risk manager for HHS?

**Julie Chua:** I truly believe in our mission. I came to HHS because I advocate for the small, medium-sized providers or the small, medium-sized operating divisions within HHS because I know that they are the ones who need the most help, the most guidance in terms of cybersecurity practices. I also know that my work and my teams work within the department makes a difference to each and every individual across our industry and our sector. Even if it takes a while, for example, to see a policy or a strategy come to fruition and get implemented you know that you are making a difference with all of these engagements that you do, the outreach that we conduct. Working with the private sector on a lot of these cybersecurity issues that are just too huge for just federal government alone to tackle. That’s another thing that I enjoy a lot with HHS, we engage with the sector, with our private industry partners with a lot of the things that we do and I think that gives us a lot of the successes that we’ve seen so far.

**Mr. Petersen: I**f you could give advice to a young person considering a career in cybersecurity or maybe doesn’t even know about cybersecurity, what would you tell them?

**Julie Chua:** On the tactical side, I would say intern a lot or try to do volunteer work within an area that you think interests you. On a more introspective prospective, as with any career decision, I would say know the why. Because the how will always come. When you know why you are interested in something or trying to get into a certain field or area, specific to risk management within cyber, hopefully there will be more defined paths towards more policy and strategy. Technical emergency response is another one I think people don’t think is related to cyber, but we are closely partnering with a lot of emergency response and first responders in our sector because cybersecurity has become a big, major threat for the healthcare industry. Another thing is, considering a career in cyber, there are so many different areas and I would say take some certifications because you want to learn, not because of what they are. The acronyms, they are just bonuses and it actually shows that you are invested in that career path. But I wouldn’t say that it should solely be to have that acronym after your name. Another thing to consider is, are you looking at cybersecurity because you are tech savvy and you can help develop and identify innovative technology and solutions? Or are you more of a policy and strategy focused person where you can affect legislation, policy, and strategy that would effect the entire industry?

**Mr. Petersen:** Thank you, this is Julie Chua. Julie is the manager of the risk management program in the Office of Information Security in the U.S. Department of Health and Human Services. Julie, thank you so much for being featured in this newsletters NICE Framework in Focus.

**Julie Chua:** Thank you again for the opportunity.