**NICE Framework in Focus – Gregory Bird**

**Mr. Petersen**: The NICE Cybersecurity Workforce Framework published as NIST Special Publication 800-181 establishes a taxonomy and common lexicon that is used to describe cybersecurity work. The NICE Framework is intended to be applied in the public, private, and academic sectors. In this edition of the NICE eNewsletter we’re profiling Gregory Bird who is the missions systems branch chief at the cybersecurity infrastructure agency or CISA at the U.S. Department of Homeland Security. Greg, thank you for letting us learn more about your career pathway and how to better understand or apply the NICE Framework from the lens of someone who’s performing cybersecurity work.

**Gregory Bird**: Thank you Rodney.

**Mr. Petersen**: Can you explain your roles and responsibilities as the Mission Systems Branch Chief at CISA?

**Gregory Bird**: My role as Branch Chief traverses a broad range of different areas and responsibilities. The core of my duties entails overseeing the personnel supporting the planning, development, operations and maintenance of the IT systems, supporting CISA’s role in the protection of the Nations critical infrastructure.

**Mr. Petersen**: Can you explain a bit more about the size of your group and what type work roles that the people that report to you fill?

**Gregory Bird**: I currently have a team that is a mix of both government civilians and contractors. I currently have twenty-five different government civilians that actually fall under me and approximately sixty different contractors. They perform a large gambit, anything from IT systems and security engineering, program and project management, service management, IT systems and operations maintenance, which includes anything from logistics enterprise architecture, testing validation, cybersecurity, 508 compliancy, and all of that.

**Mr. Petersen**: If you could say a little bit more about your own career path and how you became that Mission Systems Branch Chief.

**Gregory Bird**: In total I’ve been working in the IT field for nearly thirty years. I started originally as a programmer and then shortly afterwards joined the United States Marine Corp. While in the Marine Corp, I worked as a programmer, mainframe operator, web administrator, server operator, network tech, and firewall administrator. After that time, I worked in commercial contracting for a number of years primarily supporting the Department of Defense clients working extensively with the Marine Corp as a Senior Network Security Engineer. After my time doing that, I transitioned back to government service where I took over as the Deputy for Integrated Network Support which oversaw all the network and security operations for the Marine Corp’s enterprise network. A few years after that I had taken another position still with the Marine Corp’s cyberspace operations group leading the network and security engineering for the entire mixed end. That role fell under the Marin Corps cyber space command. Just over two years ago I switched over to DHS taking over the IT operations and then shortly later I became the Branch Chief of what’s now Mission Systems. I’ve also worked providing instruction for various IT certifications and also work in the community as a technology mentor and teach cybersecurity to local school districts as well as various civic and community organizations.

**Mr. Petersen**: Sounds like a great history and career path as well as providing and giving back to the community. Focusing on the NICE Cybersecurity Workforce Framework how do you use it both to guide your own career or how could you envision using it as a hiring manager in your organization?

**Gregory Bird**: I regularly utilize it as a supplement that lays out all of the specialty areas, work roles as aligning knowledge, skills, abilities, and tasks for working with my cyber agencies retention program as well as creating, updating position descriptions and hiring justifications and when I’m crafting employee’s performance plans. I also regularly leverage the Framework outright when planning the capability requirements for not only the recruitment of employees but for general mentorship and guidance of my employees and mentees. The NICE Cybersecurity Workforce Framework not only lays out the various job areas, roles, tasks, ksa’s required for the jobs but a lot of recent work we’ve done has really expanded to provide waiting and prioritizing various tasks, knowledge, ksa’s, certifications, recommended industry membership and partnership, conferences, trainings, along with how the roles can likely feed each other and be fed by one another. It’s become my one-stop shop for anything dealing with the cybersecurity workforce. It’s also lent to a better understanding of duties and responsibilities of my cybersecurity workforce when I’m actually talking to non-workforce members such as human resource or human capital personnel and upper management. The simple coding that it provides also gives a fantastic querying within the organization to identify personnel shortfalls and target education and growth opportunities. In the future I really hope to be able to use it more and leverage it with other organizations with their various identity access management to help create more role-based permission models as an initial form of validation of need to know.

**Mr. Petersen**: That’s terrific. You’re perhaps the first person I’ve heard talk about how you use it for performance management with your personnel to both guide and develop their career. Many people talk about how they use it to craft position descriptions or use in recruitment and hiring. To transition to that topic what type of cybersecurity jobs are the most difficult for you to fill in your organization?

**Gregory Bird**: These days we’re never short of applicants for the cybersecurity positions but two I really find it difficult to fill within my particular organization are my IT project managers as well as my information systems security officers. For IT project managers, while finding individuals with general project management capabilities isn’t too daunting, finding ones with the IT specialization, I’ve found much more difficult. IT especially the developmental activity as additional nuances that are not always understood by your traditional project managers and it can be a stumbling block to a successful project if they are not properly addressed. Additionally, with the IT experience frequently the lack of ability to speak to the business side, translating experience, or translating the technical jargon into terms and phrases the business side will not only understand but will also resonate with them tends to be a problem with the IT focused personnel in this role. The next area I have a problem filling is my ISSO’s. Performing ISSO duties takes not only takes a vast array of experience but it’s also benefited greatly by an individual that is meticulous and inquisitive in nature. The individual must not only understand the security but that it doesn’t just entail denying or blocking everything but that it’s all about enabling the mission. The key to security is risk management and performing appropriate trade-offs or finding solutions to allow the required capability in an acceptable and secure manner. Those specialized nuances and skills sets for both those positions are probably the hardest ones I have finding trouble actually filling within my organization.

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

**Gregory Bird**: In my current organization, while academic degrees and certifications are very valuable and sought after, I’m very selective on when I actually require them in a job announcement, limiting them only to specific job roles that require them typically due to some type of regulatory or governance stipulation. Other than practical skills exams, both the degrees and certifications, it is one of my few litmus tests that I have to help pre-validate an individual’s knowledge, skills, and abilities. However, I’m very cognizant of the fact that those formalized and structured means are not the only way that my prospective employees can get those skills so there are plenty of non-structured means, on the job training, things like that that I don’t want to rule out of my value equation of trying to select somebody. Additionally, just because somebody possesses those credentials it doesn’t mean they necessarily move beyond that core book knowledge or maintain their knowledge, skills, and abilities with current technology and trends. While I’m very selective when I use it for job announcements, once I do have them onboard, I do actually work into their various developmental plans what ways to get them to those various things that will help add additional validation of the skill sets that they provide.

**Mr. Petersen**: Speaking of keeping up with those current trends and kind of evolving your expertise, how do you, yourself, and your team members keep your skills current and sharp?

**Gregory Bird**: That of course is very important one in this field because of the fast pace of change. I’ve tried to adopt more of a mantra of continual learning for myself and my staff. For myself and my team I mix it up as much as possible. When there is a specific subject matter that my team or I need to learn about I’ll turn to more of the formalized training. For the rest of it I highly encourage joining of various professional organizations that are aligned within our field, continuous constant reading of industry magazines and articles, getting myself and my personnel to conferences, seminars, and also establishing mentorships with others within their current skillset as well as one that they may want to get to eventually. I also provide my team with various resources and I hold internal informal training sessions on topics that relate and generally to the cybersecurity field rather than just a specific role within the cybersecurity field. I also regularly work with my team in helping them to see the larger picture instead of just their individual role; trying to get them thinking outside the box and how the different roles actually link up with each other and end up feeding each other. I work them to try to do a lot of cross-pollination in between my teams so they can get at least at a cursory level learn all of the different roles that are out there and I found it really helps to leverage the use of my team members much better to overall make a more secure product in the end.

**Mr. Petersen**: Given the focus on teams that you’re describing how are you or CISA attempting to make your workforce more diverse?

**Gregory Bird**: Diversity is definitely one of the defining strengths of America as a whole and the diversity of the workforce is essential to accomplishing the various missionaries of CISA. We interact with millions of people across the country and around the world in execution of our mission and given the complexity of our missionaries, it’s imperative to recruit and retain a workforce that directly reflects the diversity of the Nation we serve and protect. Moreover, the attributes, abilities and experiences of each team member contributes and fosters innovative solutions to some of our most challenging issues and it enhances decision making by providing a broader range of perspectives and experiences. Our efforts to increase diversity also includes a direct recruitment of individuals with varying backgrounds of experience, both looking at private and public sectors, small, large, medium businesses, and even varying agencies and departments within the federal government. Because each one faces different challenges, regulations, constraints and all that lead to different ways methods of tacking the exact same type of problem set. This vast diversity facilitates a much more comprehensive approach to our solution development and risk and threat analysis which in turn creates better solutions for our customers.

**Mr. Petersen**: You seem pretty enthusiastic and passionate about the work you do. I wonder if you could share with us what you enjoy most about the work you do for CISA as its Mission Systems Branch Chief.

**Gregory Bird**: I would have to say what I really enjoy most is the combination of the overall mission of our agency as well as the privilege and ability to work with highly skilled individuals that I interact with throughout the course of my daily business. The overall goal of our organization is to facilitate the protection of the Nations critical infrastructure through risk advisement an important and vital mission to really sustain the American way of life. Working in this type of environment not only makes the job experience more enjoyable and rewarding but allows me to continue and learn and build upon myself while also challenging myself to do better.

**Mr. Petersen**: That’s great. One of the priorities for both NICE as well as DHS is to increase career awareness particularly among young people. Given all of your experience and your current role, what advice would you give a young person considering a career in cybersecurity? In other words, what would you tell them?

**Gregory Bird**: I actually provide a lot of mentorship to both junior personnel as well as youth in the community. Any time I actually have one considering a career in cybersecurity my first response is awesome, followed very quickly by what they enjoy most about the field. While cybersecurity field as a whole is constantly growing and morphing and we’re in desperate need of smart individuals to assist in our battle. The key is not only getting the right people on the train but also getting them in the correct seats. I’ve seen far too many talented individuals over the years that are just frankly in the wrong job. They’re not working in a position that they were either meant to do or even in the path they want to get to in the end and it results in them burning out in the field or not contributing all that they are truly capable of. It’s kind of like having a chef as a fast food delivery driver. They may get it done but there is so much more they can do. As with any career, but I find it exceptionally true in the cybersecurity field, you need to possess a love and passion for what you do. I’ve been very passionate about what’s now termed as cybersecurity since I’ve started working IT and it’s definitely made all the difference in my personal satisfaction and my drive for the job to do better and my drive to ultimately win the war on the cyberspace battlefront. I constantly look to improve and increase my knowledge and I encourage all those that I provide any type of mentorship to, to do the same because if you truly enjoy and have that passion about what you do you are going to be better at it.

**Mr. Petersen**: Thank you Greg, thanks for your excellent insights, thank you for your service to our country, and for allowing us to feature you and the work you perform as part of our NICE Framework in Focus series.

**Gregory Bird**: Thank you.