**NICE Framework in Focus – Tim Nordvedt**

**Mr. Petersen:** Welcome to the NICE Framework in Focus. The National Initiative for Cybersecurity Education, or NICE, is best known for its NICE Cybersecurity Workforce Framework. Today, we have Tim Nordvedt with us who is going to be describing his role as a Cyber Tools Delivery Analyst with Booz Allen Hamilton. Tim, thank you so much for joining us today and we look forward to learning more about your career.

**Mr. Nordvedt**: Absolutely, it's my pleasure.

**Mr. Petersen**: Explain your role and responsibilities as a Cyber Tools Delivery Analyst.

**Mr. Nordvedt**: To start off, Booz Allen, at its core is a company that solves problems. We try to do so with new and innovative thought processes. I am part of a team that we work with DHS called Continuous Diagnostics and Mitigation. We call it CDM for short. In its simplest form, the purpose of this project is to help strengthen the networks, the cybersecurity posture of multiple government agencies. Currently, CDM (Continuous Diagnostics and Mitigation) project covers over 80 percent of .gov enterprises. My specific role is I consider myself like a filter. When our clients are looking for new network security options, it can be a bit daunting and seem overwhelming when you look at the market place out there. I listened to a talk the other day and the gentleman said by his estimate, there's over 1500 security vendors out there. It's sort of where do you begin? So, what I do is I start filtering through the material. I look at the requirements of our client. I look at what is the legitimate capability of the product, the marketing materials. I try to find out what's really going to work best for the client. That way they don't have to search through hundreds of different vendors. They have a very manageable pool to look at. At the same time, it's not always about buying new products or creating new infrastructure. Sometimes we look at their current infrastructure and it's just a matter of being able to use these tools in a smarter or add some functionality to make it work in a better way without investing new capital. I spend a lot of my time just doing research on that end and develop new solutions for the different kinds of organizations.

**Mr. Petersen**: Thanks Tim. And in fact, your last line about doing the research really reflects the work role that you fill which is technology research and development and then the broader NICE category of Provisioning. You mention client and customers, so that kind of reflects your role at Booz Allen to work with, as a federal contractor, with a client or a customer, you do not do any of the internal operational cybersecurity for Booz Allen, correct?

**Mr. Nordvedt**: That is correct, yes.

**Mr. Petersen**: Very good. So, describe Tim, your career path to becoming a cybersecurity employee at Booz Allen Hamilton.

**Mr. Nordvedt**: Absolutely. Unlike others out there, I had a very unconventional path to the industry. About twenty years ago, I attempted the whole college thing in the late 90s. I ended up being a college drop out. I just started jumping around from job to job and settled on a job as a bookkeeper for a car dealership. I did that job for about 20 years. I actually did that up until the year right before I started with Booz Allen. Then about eight years ago, due to some family circumstances I had to pick up a second job and I became a bicycle mechanic. I worked my way to a master technician and bike shop manager. For the past eight years, by day I was a bookkeeper, and by night I was a bike shop manager. It's not hard to figure out that's an unsustainable life especially with young kids and a wife at home. Roughly the fall of 2017 I realized that I was going to need a career change. I needed to look at doing something different. I knew it was going to be IT-related. I've always had this comfort level around technology. I've worked with computers since the Commodore 64 days. In high school I would write programs to do all my math homework for me. Certainly very tech. I certainly wanted to do something in It. When I started doing my research that's how I was first introduced to the cybersecurity industry. I really became focused on day one. It just seemed like a focus for my skill set and a passion, something I could really enjoy pursuing. In December 2017, I took my first class in network security foundations at Howard Community College. While I really enjoyed my time at Howard Community College, I had some great teachers and they helped lay a great foundation for the skills needed in a career in IT. Early on I knew I would need to do a lot more than just have a career certificate from a community college if I really wanted to get into industry. I really started a rigorous self-study program. For every hour or two of formal classroom study, I probably had eight to ten hours of self-study on my own. I started pursuing a certification path, started developing a nice collection of starter certifications. I really tried to get involved in anything and everything I could that was cyber related just to get more and more exposure.

During this time, I ran across the SANS organization and saw the program that they have in cyber workforce in Maryland, which honestly feels like it was written just for me because the thrust of the program was to help people not in the IT industry to transfer into cybersecurity. You went through a series of qualifiers, some interviews and some assessments. If they felt you had the aptitude for cyber, through the State of Maryland you were given a scholarship to get multiple SANS training for certifications. So, I was able to pursue that. It was basically for about 12 months, I sacrificed and put some stuff on hold and I became, tried to reinvent myself as a cybersecurity professional. So, it was in about December 2018 when I decided I've got a good foundation set. I felt I had a good foundation to make the transition into the cyber workforce. I started putting my resume out there. I'm a big fan of people networking. So, I started reaching out to my network just giving my elevator pitch to a lot of different people. Then I ended up having two different people in my network get me connected with employees from Booz Allen Hamilton in the cyber department here. In January 2019, I interviewed with Booz Allen. I must have impressed somebody, because they gave me an offer. I started here back in February.

**Mr. Petersen**: Well, Tim that's an amazing story and congratulations on your success and your diligence to use a bicycle term to shift careers from what you were doing previously into cybersecurity. I think that is not only unique but that is needed to accelerate learning and skills development to fill the critical shortage. I'd also note for our listeners that Tim and I both probably know each other from our recreation and passionate interest around cycling. I really appreciate your willingness to work hard, and make this career change, if you will. Let's get back to the NICE Cybersecurity Workforce Framework. You've talked about your career path. How do you envision using the NICE Framework to guide your career?

**Mr. Nordvedt**: It took me awhile to realize when I first started my journey, but the term cybersecurity is very vague. It doesn't really describe anything except from like a ten-thousand-foot view and I was going around telling everyone I was going to work in cybersecurity not realizing what a broad stroke I was painting. The more I pursued this path of becoming an expert in cybersecurity, the more I realized that was just an unattainable goal with so many subsets, there was no way a person could be good at them all. When I started looking at the NICE Cybersecurity Workforce Framework it does a great job of breaking down all the subsets and the necessary skills, things to look for, the job description. Right now, I'm wrapping up my bachelor's degree with Western Governors University. As soon as I'm done I know I'm going to need to continue on this education path and like we mentioned before, currently my job role is aligned with "securely provision" technology R&D area, but I have a passion for protect and defend incident response path. I've been looking at that to guide my education plan. Once I finish up on my bachelors, I would use that to start a focus on what to learn next. Because without something like the Framework to just inform my decision, looking at the landscape of possible certifications, bootcamps, conferences it can be a bit overwhelming. You have no idea of what direction to go in. The Framework is a great way to help me focus my studies.

**Mr. Petersen**: That's terrific. You have both a non-traditional path to your career, but also a pretty enlightened perspective on how the NICE Framework can help you advance your career and help you to move along in your career path. Given that you're already doing cybersecurity work, and for many people they might think they have a job and they've arrived, what do you find is necessary to keep your skills sharp and current on an ongoing basis?

**Mr. Nordvedt**: Even before I got into cybersecurity, one of my life mottos was never stop learning. There's just so much life has to offer I just always wanted to learn more and educate myself. What I found especially in this industry it's definitely true. When you look at it from an adversarial aspect there's nation-states that invest heavily that keep their actors relevant on where technology is and where it's going. I want to be at the top of my game and be a valid cybersecurity professional. In today’s environment I need to be constantly evolving myself and stay with the trend. So right now, like I mentioned, most of my focus is on my bachelor's degree. I am attending Western Governors University. I'm getting a degree in cloud and system administration. I'm happy to announce I'm four classes away from graduating and finishing my bachelor's.

**Mr. Petersen**: Congratulations.

**Mr. Nordvedt**: Thank you very much. Just a side note, whenever I mention that, people kind of assume I want to get into system administration. But kind of the reason I chose that degree, and I hear this a lot with people just trying to get into industry and pursue an education path, they get so security focused that they forget what it is we're actually protecting. It's kind of hard to protect a network if you don't know how a user is authenticating via Active Directory, or how the TCP/IP protocols transfer data between computers. I chose the cloud and system administration, so I could continue to develop my foundational IT skills, so I could know how they do their job, where their vulnerabilities are, and I could better protect them. Outside of that, I'll probably do more of this once I graduate school. But I try a couple times a month - Meetup is a great resource. There are a lot of technical related meetups out there. There can be meetups from lockpicking, to bio-reverse engineering. I was actually at one last night on building temperature sensors with Arduino boards. I think it's a great resource not only to learn stuff, but you can meet people in industry and iron sharpens iron. I'm also a big fan of webcasts. One thing I always like to point out especially with people looking to get into this industry. One of my favorites is John Strand. He is a security practitioner who owns a company, Black Hills Information Security. On his website he has a whole bunch of webcasts. He has a section dedicated towards people new to information security. He has thirty different webcasts on there. He suggests everyone watch it, if you're either trying to get into, or just getting into the industry and that was a big fan of mine. Living in the D.C area, I probably spend a lot of time in the car in traffic so rather than driving around listening to music I basically turn my car into a rolling classroom. I always have podcasts or something security related going on in the background. Just like I said, the enemy never sleeps. They constantly re-evolve themselves, so I know I need to be doing the same.

**Mr. Petersen**: Wow, that's terrific. That's great advice and I can clearly see your enthusiasm and passion for the work you're currently doing. Not that it's not already evident, but can you maybe give us some examples of what you enjoy most about the work you do for Booz Allen and also your cyber tools delivery analyst position?

**Mr. Nordvedt**: Yeah, absolutely. There are so many things I enjoy working for Booz Allen Hamilton, but to be completely transparent, I'll be honest with you. When I first took my job here at Booz Allen, I had the mentality of, I just wanted to get my foot in the door somewhere, so I could start building the experience. In my first job I wasn't really concerned about what it was or where it was or what I was doing, I just wanted to get something on my resume. When I first started here, I really had no intentions of staying here long term. But I've been here a little over five months now, and I truly feel that I won the job lottery in the cyber world. Booz Allen has so much to offer. Booz Allen Hamilton is one of the largest, if not the largest cyber practitioners in the world.

The project that I'm part of, continuous diagnostics and mitigation, is one of the largest cybersecurity undertakings ever. I work with, we really cover all gambits of cyber. I have exposure to every different facet of the Workforce Cybersecurity Framework. Booz Allen Hamilton is also really passionate about lining up people's skills and desires with mission. For example, you know a lot of people on my team know I really desired at one point to move into the incident response path. So, they actively make introductions to people that run a project in those areas, so I can get some exposure, learning some new skills, further my network. Booz Allen Hamilton's motto is, "Empowering people to change the world". It didn't take long for me to realize that's a motto they truly back up with action, that they really are a people-oriented company. Specifically, with the CDM project, I can say it's a job that I'm proud of. I may not be on the frontlines of cyber today, but I do know that when I go home at night that what I’m doing, in a small way, is making a difference in the safety of our country, and it's something I'm excited to keep on doing.

**Mr. Petersen**: That's terrific. It sounds like your employer is super supportive and I would add for our listeners that Booz Allen has been instrumental as a consultant to NIST and the rest of the federal government in the development of the Framework and also have been keynote speakers at our conference to talk about how they are applying it. It's great to hear your testimony about how they are supportive of you and your career. I wanted to end with a question about what type of advice would you give a young person considering a career in cybersecurity, and what would you tell them? I might amend that a little bit because your pathway is not as a young person, but maybe as a middle-aged or mid-career professional. So, both, what would your advice for a young person and maybe person in your shoes, or in your shoes a few years ago that wants to give cybersecurity a try?

**Mr. Nordvedt**: This a question I get asked often, because I've had a fairly quick and successful transition into the industry from something totally unrelated. I have three things I always tell people whenever they ask me this question. The first thing is you have to make sure you enjoy it. It's real easy, you look at this industry and you think about, you hear about, yes, you can make a nice paycheck in the industry. Companies are willing to pay people with validated skills. You hear about the workforce gaps, so you can see job security. But if you don't enjoy it, it's not a fun way to live life. I always tell people, security is not a Monday through Friday nine to five gig. Security is 24/7. It doesn't mean you're working 24/7 in fact, Booz Allen discourages you from working overtime. It wants you to have a balance. As a security professional, you never know when you're going to need to be on call. You never know when it's going to be "go" time. You've got to be prepared at all times. If you don't enjoy it, it kind of makes it hard to do. I always tell them make sure you enjoy it before you pursue it.

The second thing I always tell people is network. I mean, people network. This is especially true for people like me that already have experience in something totally unrelated. When I first got started I got some basic certification, I knew that my resume was easily going to be overlooked. We hear about the workforce gap, but I always tell people you have to look at that carefully. It's not a people gap, it's a skills gap. There's always plenty of people that want to get in this industry. What we're lacking is the people with the skills. If you talk to anyone that's in a hiring position, and you open up anything cyber-related, you're going to get a hundred plus resumes in a very short period of time. Someone with a resume like myself, when you look at it, you may see one or two certifications on there but then you see twenty years as a bookkeeper, and eight years as a bicycle mechanic. You don't blame the HR person for just flipping my resume and moving on to the next person.

I knew I had to have someone on the inside who believed in me, who was willing to help sell me to the company. So, I worked really hard at developing my elevator pitch and I told it to anyone and everyone. I always tell people, don't just focus on IT because someone who's not in IT, knows someone who is in IT. I grabbed a lot of cups of coffee. I probably told my elevator pitch hundreds of times over the course of a couple months building this network. Like I mentioned before, it led me back to two different people in Booz Allen Hamilton that both happened to work in cyber. I was able to sell myself to them. They in turn, turned around and believed in me. Yes, it was uncomfortable talking to people, telling my story to people I didn't know, but once you have someone on the inside that believes in you, your resume automatically is worth a lot more to that company. You're more likely to be looked at.

The last thing I always tell people, like I mentioned already, is fall in love with learning. This is a life-long educational path you're going to be on. The attacks of today are not the attacks of tomorrow. The technology of today is not what we're going to see tomorrow. Yesterday we were talking about cloud, today we're talking about AI, tomorrow we'll be talking about who knows what, uplinks, something else. We don't know what tomorrow brings. In order to stay on top of the game as a valid security professional, you're going to have to be learning for the rest of your life, so you might as well fall in love with it again. It took some sacrifices, it took a lot of hard work to get where I am, but now that I'm on the inside looking back I'd do it all over again. I would tell everyone, it's worth what you have to do to get in this position. If you truly find some joy here and you want to pursue it, I can honestly say now that I've found a career that I will spend the remainder of my working life pursuing and enjoying it.

**Mr. Petersen**: Well, Tim, that is really terrific. If I could summarize your three points with three "P's": Passion- you're doing something you really enjoy; Pursue - pursue people, developed relationships and pursued organizations where you eventually found a home; and you persisted both through your career path, but also through your ongoing love of learning, so congratulations on your success as well as your insights for people who might want to consider cybersecurity as a career. We've been speaking today with Tim Nordvedt who is a cybersecurity delivery analyst with Booz Allen Hamilton. Tim, thank you so much for joining us and being part of our NICE Framework in Focus.

**Mr. Nordvedt**: Absolutely. It was my pleasure.