Framework in Focus: Charles Britt
Spring 2021 (publish date: April 2021)

Charles Britt is an Information System Security Officer at the U.S. Food and Drug Administration. In this interview, he discusses his career, the importance of professional skills like communication, and continuous learning, among other topics.

Interview Transcript:

Karen Wetzel: My name is Karen Wetzel. I am manager of the NICE Framework at the National Initiative for Cybersecurity Education at NIST. The NICE Cybersecurity Workforce Framework, published as NIST Special Publication 800-181, establishes a taxonomy and common lexicon used to describe cybersecurity work. The NICE Framework is intended to be applied in the private, public, and academic sectors. In this edition of the NICE eNewsletter series Framework in Focus, it is my pleasure to speak with Charles Britt, Information Systems Security Officer (ISSO) at the U.S. Food and Drug Administration (FDA). Charles, thank you for letting us learn more about your career pathway and understand the NICE Framework from the lens of someone like yourself who is performing cybersecurity work.

Charles Britt: Good afternoon and thank you for the invitation.

Karen: Well let's get to it. I wonder if we can start of by having you explain a little bit about your role and responsibilities as an Information Systems Security Officer at the FDA?

Charles: Yes. I have been at the FDA for a little over two years. I am, as I mentioned, one of about seven or eight ISSOs who are responsible for carrying out cybersecurity activities across different centers and offices across the FDA. My specific role, I am responsible for managing and coordinating the assessment of our security systems against NIST 800-53 standards as well as FDA policies and HHS guidelines. I also provide technical and policy guidance to centers and systems stakeholders to ensure that the application and systems they are using are in compliance with regulations and also they're meeting all of the policy requirements that are set forth as far as privacy, access control, and account management. Also technology evaluations, like any time someone wants to add a new piece of software or hardware to our infrastructure. Those requests come through a standardized system and we are responsible for reviewing and either recommend approving or disapproving based on the business case and its potential impact on our network. Last but not least, I also support incident response. Anytime there is some sort of security incident or breach within our environment, I work very closely with our systems management center to coordinate how we work with all impacted parties within the centers, notifying management in determining whether or not these are the types of issues that may need to be elevated beyond our office on a greater scale.

Karen: Sounds like you have a lot on our plate. That's exciting. Thank you. Does that mean you've got a large team to work with? Can you describe a little about your team and the specific roles?

Charles: Not a large team – a large team of one. Each of us are responsible for our own centers and we do have fairly large portfolios ranging anywhere from one or two systems up to maybe a couple dozen systems that are within our area of responsibility. On our cybersecurity team as a whole we do have approximately 80 individuals across our program that support all aspects of the work that I just talked to

you about. Those individuals consist of cybersecurity engineers, incident response analysts, forensics engineers, SOC analysts or your watch officers who are watching our systems and the perimeters of our network. Other ISSOs like myself, individuals who are also working [with] cloud and emerging technologies, and then of course we've got corresponding senior leadership roles that manage and coordinate all these activities across the program.

Karen: The Information System Security Officer title is one that maybe not a lot of people have heard of. How did you get into this kind of role? What was the career path that you took to get here?

Charles: An interesting one. Initially, I did not anticipate going into cybersecurity. I began my career back in 2003 at the Central Intelligence Agency. I came on board shortly after September 11, as an IT support specialist – as a help desk guy running around installing software, taking care of all of the troubleshooting that was necessary for the particular group and office that I supported during that time. This was leading up to Operation Iraqi Freedom, which most people know is the war on terrorism in Afghanistan and Iraq. We were very busy in leading up to the invasion of Iraq. We were working literally 12-16 hours a day. Once that effort wrapped up, I went to my management and said I needed a new job—I'm burnt out and needed something else to do.

They eventually moved me to a systems administrator type of role. I was behind the scenes, basically working to maintain a lot of our critical systems and infrastructure background, and got in that job and actually missed working with people. That is when an opportunity arose for an ISSO in what was then the growing Information Security Group at the agency. It was growing and they were looking for individuals who wanted to kind of dip their feet into the world of cybersecurity. I accepted the challenge. The key thing to making that transition was both having the technical background but then also really good – at least my management thought – really good communications skills. I jumped into the role of an ISSO and began supporting several of the program offices across the agency. As a result, I then transitioned to move two or three years ago to my role here at the FDA. It's a great position for me because it matches my desire to understand the technology and be able to be impactful in cybersecurity but then also communicate that to individuals within an organization.

Karen: That's really fascinating. There's a lot of talk often around what some call soft skills, professional skills, I've heard them called power skills. Obviously, they seem to have played a big role in where you are now and, as you've said, in your desires of what you want to do in your role. Is that fairly common nowadays in cybersecurity roles, the importance of those kinds of skills in addition to the more traditional type cybersecurity roles?

Charles: Very important because technology is constantly changing, and what we call our stakeholders – or, as some people want to call them, clients – people that we're supporting [who] aren't focused on cybersecurity. At the FDA, they're focused 99% of the time on basically protecting the public health, so they don't have time to keep up with everchanging cybersecurity trends and policy changes. Unlike our organization or individuals who I work with at the agency who are focused on intelligence gathering and sort of protecting our interests around the globe, they don't have that focus. So there is a need for cybersecurity folks who not only understand the technology but also understand how it impacts the business and can explain that to a business owner who is—often in my case, a doctor, a physicist, a chemist, or someone who's background is totally different from my field. I have to be able to explain in a way they understand how the policies and things that we're implementing are impacting the security of

their system and data. I think communications are one of those top skills that, if you can marry with a technical background, you'll be well suited for many roles across the spectrum of cybersecurity jobs.

Karen: When it comes to those technical skills and maybe your communications skills too, what are the kinds of things you do to keep yourself sharp and current in those areas?

Charles: That's a delicate balance. As I mentioned, things are constantly changing, so depending on what your niche is, some people focus on one aspect of cybersecurity or one aspect of technology. The interesting thing about an ISSO role is that you have to know about everything. When someone brings a system to you that needs to be accredited and assessed, they can be using all different types of technologies, some that you may be aware of and some that you're not. You're constantly finding yourself researching, going to training which is used in our office. They provide us great opportunities to go to training and take online courses, both internally as well as externally. Pre-Covid, there was the opportunity of course to attend conferences, and that is something that our staff is constantly encouraged to do so that you can stay up on the latest and greatest. Cyber criminals and those that are performing nefarious acts are definitely keeping up with trends and making some of those trends. As a defender of our network and infrastructure, I, too, have to be well versed on that and, again, in such a way that I can communicate and translate how it affects the work that we do every day.

Karen: It sounds like not only would you need that in order to do your job effectively, but I can see that also being great in terms of career pathing to and being able to understand what's going on out there and being kept apprised of what is most current.

Charles: Yes. It's difficult when you're managing and doing your day-to-day job but then you have to pause all of the activities that I just described to you for a one-week or three-day course and then come back to your regular workload. I'm not saying it's impossible to do, but it does take some balancing. As a matter of fact, today I was speaking with my team lead about the fact that at the beginning of the year I'm going to carve out two or three weeks for training that I've been putting off for a while because the organization has been quite busy. Finding time to get that in is key to your growth. Sometimes you can get stagnant really quick. Taking time off – and she definitely encourages that – putting some time aside to stop and make sure we're keeping our skills up to date, it keeps you competitive but also ensures you're contributing great value to the organization.

Karen: That's great that you're making sure there is time for that and that you have that support. It's that intentionality that can be so very important. When we're talking about the different kinds of jobs—it sounds like you yourself, with your background, you touched on a lot of different kinds of roles. Can you share your own insights about what kinds of cybersecurity jobs you think are most difficult to fill either in your organization now or as you've seen in your roles in cybersecurity?

Charles: I think a lot of them have to do more with your senior folks. Those that got a really solid technical background who have been working more than likely in IT for years and then have pivoted out of just a general IT role to something that's more cybersecurity focused. That tends to be a challenge. Coming into a larger organization like the FDA or any other large government or private sector organization, there's a lot of institutional knowledge there. For a variety of positions, it's difficult to just bring someone in fresh out of college or right out of a boot camp to really delve deep and fast in the vast networks and infrastructures that these offices are running. For us, I would say it often tends to be roles like mine, the ISSO role. It's often difficult because of that mix between the technical and the project

management and stakeholder management skills that you have to bring to the table. It's across our field in general. I learned this early on in my field: folks who are in technology most often times are not people friendly, aren't the most, you know, who like to engage with the public, at least communicate and engage with the public. They kind of like to do their job, get in, keep their technical focus, and then go home. In my role, we spend a lot of time in meetings with stakeholders, where you're constantly presenting and balancing that while trying to maintain the technology. It's sometimes difficult to find folks who can successfully navigate both.

Another office position that we find is difficult that other organizations talk about is your counter-intelligence folks -- folks that are looking at insider threats. Often times, you'll find those folks have a background in law enforcement or national security – well those aren't just floating around the country. Here in the Washington, DC area we have a lot of those folks because they're retiring from the government or may have held a similar role in a different organization. But across the nation you'd be hard pressed to find a whole lot of folks who have that specialized background and are able to clear the security clearance background. Because there is such a high demand in these very large organizations, such as Amazon and Facebook, for people who are looking at the bigger picture of threats and intelligence, that's another role that you can't just go to a boot camp or take a couple online courses and be well versed in.

Karen: It's interesting hearing you describe all of these different kinds of roles, and it's just that sometimes people who aren't familiar with cybersecurity will come to think of it as more of a one size kind of field. Really there are so many different kinds of roles that people can take on in this space and so being aware of them and knowing maybe what the requirements are for each so you can say "I'm interested in that, I want to talk to someone more about that or take some courses on that or maybe shadow someone"—that's great. Talking a little bit more about workforce, I know there's so many reasons why it's important to have a diverse workforce – just the variety of perspectives that can be brought, effectiveness, and the countless studies. Is that something that you all are focusing on at the FDA? Any kinds of efforts you've been doing in that space perhaps that have been effective?

Charles: Yes, huge focus. Our Chief Information Security Officer has made diversity a huge part of our strategic plan. In the work that we do within our department as well as in our IT division in general, there is a huge focus on bringing in diverse candidates, specifically women. We actually have a very high number of female employees, female cybersecurity professionals within our department. I can say that it is not common across many organizations and agencies, so that is a huge plus for our program and the work that our leadership is doing to ensure that and also overall building an inclusive culture. We've recently had some groups start up, working groups start up that are focused specifically on looking at how we can make our environment more inclusive of the diverse candidates that we're bringing in. So that conversation is happening at lunch hour, after work, about how we can ensure that, once we get candidates in, everyone feels welcome and included in the work that's being done, not just in cybersecurity but across the entire FDA.

Karen: That's so great. I'm glad you mentioned that. I think sometimes people forget the importance of what happens when someone's in the door. You can do everything in the beginning but if you don't have that inclusivity, you're going to lose those people and be in a worse position perhaps than where you were before. I know a number of organizations will do maybe mentoring or again just sort of having

that be a continuous focus. That's great to hear that you are doing that. Can you share a little bit about what you enjoy most about your work? I know you touched on it some, but is there more you can add?

Charles: I've worked for quite some time, and even when I was in high school and in college, I've always had a thing for helping people. It's part of my nature. I enjoy helping people and I enjoy educating people. When I initially entered the IT field, I had a couple internships where my first jobs were the help desk. I did those jobs very well. Again, that's one of the reasons why, when I came onboard at the Agency, they placed me in a help desk job. I had such a really good track record of being that helpful IT guy.

Most people who have ever held a help desk job know that they can burn you out pretty quick and you eventually do move onto something else or become a help desk manager. For me, it's still my passion. It's still my joy doing and that's what I get out of this job. The ability for me to educate our stakeholders by translating technical and the policy guidance in what I call "plain English," where they can take actionable steps to protect their systems and data without a lot of back and forth. Let's sit down, let's talk about the NIST documents. You've seen them, they're long. We have 289 controls that we have to assess systems against. When these folks see this, it's kind of overwhelming. To sit down with them and break it down into very simple plain-English terms about what we're trying to do, about how we want you to manage your accounts, I like being able to do that. I like being able to see that lightbulb go off, where a stakeholder understands, ah, I see why we are doing this, or I see why we should be doing this. Then they take the action and encourage their employees to ensure that once these mechanisms and plans are put into place they stay because they see the value of how these things protect their systems.

I enjoy that as well as being able to be responsible for a variety of tasks. I don't like coming in and having the same job to do every day, day in and day out. In this job, as I stated at the beginning of our conversation, that's not the case. Every day is different. There's always something going on – new systems being stood up, issues that arise, patches that need to be deployed. Every day the conversations can be different. On any given day, the priorities can change because of what's happening around the world and what's happening in the internet world, so I like that. Being able to help the folks within our agency and other agencies I work in and being able to solve real-world challenges. We hear about certain things on the news or you read about it in the newspaper, and this role puts you on the front lines of a lot of the work that's being done with the Federal Government to protect our systems. I enjoy being that person who can translate that technical knowledge, get the work done, and at the end of the day ensure that we are safe and secure and don't have to worry about finding ourselves on the front page of the paper because of something that's gone wrong.

Karen: You can actually see the impact that you're making and the positive benefits of your role and I can see that being really fulfilling. I'm definitely one of those people who enjoys a variety of different things and certainly in this field you have to want to continuously learn and change so it's not like you can come in and do the same job that you did five years ago

Charles: No, not at all. I started this job in 2018. I had taken a break and I worked in academia at Northern Virginia Community College for five years, helping them develop out cybersecurity programs or programs for youth and young adults that would get them into our program and hopefully out into the workforce. Having come back after five years, yes, a lot changed, and I was shocked at some of the terminology and things that people were saying in meetings. I was like, wait a minute, it was just five years ago, and this stuff was just an idea. Just five years ago, this stuff was in beta testing, and you're

telling me now this is something that the organization is using, and this is where the technologies are going. It blew my mind, and, like you said, as a result of that I talk to folks through the career coaching that I do or the speaking opportunities that I get. I tell them this is one field where you have to be a lifelong learner. For the entire duration of your career, you have to be willing to learn, to learn the technologies, to learn different ways of doing your job because it is going to change. Again, in order for you to be competitive, you have to keep up.

Karen: With your work with the community college and what you've just shared about keeping up and everything, how do you think those training providers and education organizations, how can they make sure that they are helping their students learn things that aren't already too old to apply? That they're keeping up, that they're actually helping their students to be effective in their job when they get lift off?

Charles: That's a really good question. We saw this challenge not only at NOVA but also within the K-12 school divisions with a lot of the materials they were teaching. One year it's the latest and greatest, but by the time they get the curriculum approved, something else has come out. I learned about academia – as it is with the federal government, things move very slow. It can take years to get a curriculum approved to be taught in the classroom and then the technology has changed. We saw that happening, and it does have an impact on the student's preparedness for going into the workforce. The way to keep up with that is to ensure that you're using as many tools and resources to help supplement what's being taught in the classroom – any types of virtual environments, bringing in guest speakers, helping the students connect to some sort of work-based learning experience, connecting with a mentor. All those things are very important to ensuring that although you may not be providing the cutting-edge technology in a community college or a high school classroom, these students are aware that these technologies exist and where they can get more information and connect with individuals that understand it a lot better.

Teacher professional development is important. I fought very hard in my role to provide opportunities for teachers at the high school and collegiate level to be able to attend cybersecurity conferences. They were so used to going to the typical academic conferences within their own network of academia. I certainly stressed many times that they should also attend cybersecurity conferences to skill-up the work that they're doing and information they're teaching in the classroom so they can be more effective teachers to their students. I do understand that's a hard lift sometimes, trying to maintain the job of a teacher but then also keeping up with what's happening in industry. But I can definitely say that the program at Northern Virginia Community College and a lot of the institutions in Northern Virginia and Maryland are doing well with keeping up with the demand for cutting-edge classroom material.

Karen: Do you see that the Framework is helping in that regard? One of the things we've been trying to do with the Framework is we have these building blocks of Tasks, Skills, and Knowledge that basically almost serve as a bridge at times between the employers and the learners. Do you see that being helpful?

Charles: Very helpful. It's my go-to. I literally had sheets that I would paste on my board at work where I would have the NICE Framework, so anytime someone brought up cybersecurity I said, "Let's start with the NICE Framework." Honestly, it is a very simple way to look at how the build is divided up and understand at least the tasks, as you mentioned, responsibilities, and skills that are needed. Then using that to marry up which degree program a student may need to pursue or which job they may be interested in or whether or not the skills and interests that they have match the type of job they had in

mind. As you mention, every type of cybersecurity job is not the same. A lot of times we notice that with students and sometimes people in academia, within cybersecurity you automatically think you know a forensics analyst or someone who is protecting the firewalls and not talk about all these vast other components of that. I often used the NICE Framework—and still do to this day—to help break it down. I'm glad to see the revisions that have been made, which have made it even easier to really help pinpoint and use some of the online resources to say this is the track that you want to look at if this is where you'd like to see yourself or other options you may have. Give someone a roadmap to look at and help them. Before this Framework, it made it very difficult [for people] like myself. I just landed in the ISSO role. I had no clue what it took to get there or some of the other roles that were evident in my organization.

Karen: Well, we try. That's great to hear that it's being effective. You've talked a bit about people just entering this field and the support you've provided to folks who are coming in here, so if you had just one piece of advice to give someone who's considering a career in cybersecurity what would you say?

Charles: Definitely be specific about what you're looking to do. It's a very broad field. As I mentioned, when I'm doing presentations and speaking with folks, they always say they want to get a cybersecurity job, but they have no idea of what they specifically want to do. In a presentation that I gave a couple weeks ago for National Cybersecurity Careers Awareness Week, I told the audience that you have to go back to the basics. What is it that you are really good at and what is it that someone is willing to pay you for? Those are the basics of defining a really good career. In cybersecurity, the good thing is, whatever you're good at there is going to be something in cybersecurity that there is a need for and will pay you well. So you can't go wrong. It's just really a matter of: Are you a people person? Do you like to communicate? Or do you like to write? Are you creative? Do you like to present? Are you more of an introvert and prefer to work by yourself?

All of those factors really play into how successful you are in a lot of these different roles, and a lot of folks don't know what those paths look like. They see the skills, but there is also those personality traits and those innate abilities that individuals have that will help propel them either faster ahead or actually hold them back. I often tell folks if you can be a little more refined and specific about the paths you'd like to go down, you're going to be a lot better off finding a job. That's not to say that you have to stay in that particular role. The other beauty of the field is that if you don't like it and it's not a good fit, there are tons of other opportunities that are available to you. But throwing a blind dart at a board and saying I want to get into cybersecurity and whatever job becomes available is the one I want is not the best approach. Be specific about that but then also flexible when it comes to opportunities. I think that would work well for most folks who are looking to launch a career in cyber.

Karen: That really works well for both the employer and the learner in that case. You want to be in a job that's fulfilling and is making the most of your abilities, so thinking that carefully through at the beginning versus just going for, oh I've heard this title before. Especially since titles from organization to organization can be totally different.

Charles: Totally different. They change the requirements a lot of times. They'll throw in the entire kitchen sink at a job description. You don't know what you're getting into. But if you understand the basics of that role and what the organization is looking for through that interview and asking the right questions, you'll see they're asking for all of this but the real person that they need is this. You can then craft your job search to ensure that you're not being pigeonholed into a job that sounds really good – it

has a lot of technical buzz words – but then find out you're not doing and performing the tasks that you had in mind. No one wants that. No matter how much money you're making, you still want to be in a role that you enjoy doing every day and that you are not setting yourself up for failure because you've limited your options.

Karen: It sounds like you found yourself a role like that and I really appreciate you sharing with us about it. I had not heard the ISSO title before, so I really appreciate hearing from you today, Charles. Thank you so much for your time.

Charles: You're welcome. Thank you Karen. It's been my pleasure.