SEI Webcast

Follow the CUI: Setting the Boundaries for Your CMMC Assessment

by Matt Trevors and Gavin Jurecko

Shane McGraw: Hello, welcome to today's SEI webcast, "Follow the CUI: Setting the boundaries for your CMMC assessment." My name is Shane McGraw, outreach team lead here at the SEI, and I'd like to thank you for attending. We want to make today as interactive as possible, so we will address questions throughout today's talk, and you can submit those questions in YouTube chat area where we will get to as many as we can.

Our featured speakers today are Matt Trevors and Gavin Jurecko. Matt Trevors is the CMMC model architect, is a Technical Manager at the SEI. Matt has more than twenty years of experience in information technology, information security and secure software development strategies. Gavin Jurecko is also the CMMC model architect and a senior member of the technical staff within our CERT division at the SEI. And prior to working at the SEI, Gavin has worked within the nuclear and transportation sectors implementing cybersecurity plans, programs, communications systems designs. Now, I'm going to turn it over to Matt Trevors. Matt, good afternoon, all yours.

Matt Trevors: Great, Shane, thanks very much. Welcome, everyone. Thanks for joining the webcast. It's great to have folks here for a discussion on CMMC. As Shane mentioned, I am joined by my friend and colleague Gavin Jurecko. Gavin, nice to see you again.

Gavin Jurecko: Thank you, Matt. Thanks for having me. I'm looking forward to the scoping discussion we're going to have today.

Matt Trevors: Yes, hopefully we're looking more to this than we had this morning, our very brisk first morning in Pittsburgh where we had the sub forty degree temperatures. So, that was kind of a wakeup call. I don't know how you guys were in the North Hills today, but it was a little brisk.

Gavin Jurecko: Yeah, same. The kids did not enjoy the cold walk to the bus stop this morning.

Matt Trevors: Yeah, I don't blame them. Well, with that let's start right into the topic, as Shane mentioned, follow the CUI, or follow the "cooey" as we may say in the business. We're going to talk to you about how to go about scoping your CMMC assessment. So, that's one thing I've heard a lot about is people trying to determine what's in scope, what's out of scope, how do I determine the answer, and Gavin and I are here to help guide your decision making process. And while we can't give you definitive guidance on what Is to dot and what Ts to cross, we're going to do our very best to give you some things to consider. And in that vein, I wrote a blog post recently that is available at the SEI Insights website discussing this very topic, and this podcast, or webcast, is kind of a continuation of that. So, Gavin, why don't you give the folks some of your initial thoughts on how they can go about scoping a CMMC assessment?

Gavin Jurecko: Yeah so, hopefully today we're going to give you some guidance on different concepts or different tools you can use to think about scoping your assessment boundary. The scoping is the foundational step in your journey to achieve CMMC level certification, and a properly defined boundary is going to allow not only your organization to know what is in scope of the assessment but, more importantly, the C3PAO as well. A properly scoped assessment will also help you avoid scope creep by minimizing assets that may not be in scope of the boundaries, so you wouldn't have to apply whatever the practice, CMMC practice, you may have to that asset.

Matt Trevors: Okay, great. So, Gavin, ultimately don't you think one of the first things the organization should likely address is whether or not they need a single CMMC assessment that goes company wide, or should they consider multiple assessments?

Gavin Jurecko: Yeah, I think that's a really good first step. Ultimately, you want to look at your enterprise network and answer the question, "Does everything you do support the DoD, or do you have different lines of business?" If not, you may want to try and separate the two because CMMC may not be applicable to your other lines of business. So, first of all, I'd look at what DoD contracts do you have. What services are you providing the DoD? Are you providing a special widget for a specific subsystem? Are you developing software? As you start thinking of these services, then you can understand the assets that truly support those services and begin to scope your assessment boundary that way. Perhaps also, since we do have different levels of CMMC relating to basically different information types, where level one really is trying to protect the FCI, the federal contract information, and level three is protecting the controlled unclassified information, maybe it makes sense to do a CMMC level one assessment on your enterprise, and then, for the level three stuff where there is CUI, maybe isolate that off or separate that off into a smaller piece of the assessment puzzle.

Matt Trevors: Right, understood and just want to backtrack, I'm going to try to hold your feet to the fire Gavin, and do the same for me when you use acronyms. So, C3PAO is CMMC's third party assessment organization. So, again, Gavin, if you catch me, feel free to call me out on that as well.

Gavin Jurecko: Yeah, they're--

Matt Trevors: So, you-- sorry. So, there are-- yeah, there are a number of acronyms in this CMMC. Cybersecurity maturity model certification, there's another one. So, you talked about the various levels and their enterprise network and FCI and CUI. So, that can be very wide. So, there's a breadth to the scope, but they also need to know the levels. So, as we talked about, CMMC is five levels. So, when they're scoping their assessment, they also need to keep that in mind, correct?

Gavin Jurecko: Yeah so, again, whenever we talk about the levels and scoping the assessment, it shouldn't be a trivial decision that the organization makes. The difference between scoping a level one CMMC certification assessment and a level three is around a hundred and ten to a hundred and thirty practices. So, if somebody decides to achieve level one certification, they're required to satisfy seventeen practices at level one. If somebody decides to get certified as a CMMC level three organization, then they're required to comply, or not comply, but satisfy a hundred and thirty practices plus some maturity concepts.

So, that's the other consideration. There is no maturity processes at level one. So, it's really do you do these practices, can you show us evidence that you're doing these practices. When we get to level three, we're going to start looking at maturity concepts, so not only are you doing these practices but how ingrained is it within your organization. Are people following processes, defined processes? Is there a policy from higher level management that signed off on and states the direction of the domain or the CMMC program? Don't necessarily chase green, which is to say, don't arbitrarily set a level without doing some of this pre-planning effort. If you truly don't have CUI, then there may not be a need for your organization to get level three certification, and you can be in the level one range. Preparation is key to before you go out to get CMMC certification.

Matt Trevors: Right, and I just want to-- absolutely right. I know we're talking about seventeen versus a hundred and thirty. There's also level four and five. So, in the entirety of CMMC there's a hundred and seventy-one practices. A lot of those are pulled from, at level four and five, from 172, NIST 800-172, which was the 171 Bravo previously. So, that's really great, and then we're also not really discussing level two, and that is because level two is largely a transitional level. They don't expect to award contracts based on level two, instead they want to use that so that there's a staggered approach or a tiered approach to achieving level three. So, it's not like you're going zero to sixty, from seventeen to a hundred and thirty. As Gavin and I will discuss, there's transitional steps, or there's different ways to measure success. And perhaps if you're at level one aspiring for level three, maybe you start with the practices and processes at level two before achieving level three.

So, Gavin, we talked a lot about big muscle movements, trying to determine the breadth of the assessment, the level to strive for. Do you think it's valuable for the organizations to follow a process such as developed by the NIST cybersecurity framework where you define your current profile, and then you pick a target profile and then build a program to get from A to B?

Gavin Jurecko: Yeah, I mean I think that's essentially the heart of what CMMC intended to do. So, rather than some of the requirements that are out there such as 800-171 as an organization must do all these things, let's take an appropriate approach to see what information organizations actually have and set a profile based on that. So, in essence, again, level one is FCI, federal contract information, and level three is CUI. You need to have a clear picture of what level of certification you would like to achieve. So, some of the questions it's obvious that you need to answer is what CUI does your organization have, if any, what FCI does your organization have if any. The answer to those questions are going to guide you to what level or profile you're going to eventually be at. If you have FCI only, then it's level one. If you have CUI, it's at least level three but maybe a higher level depending on what contract you're supporting.

Matt Trevors: Great, and Gavin, with that, we have our first audience question. Tyler P., good afternoon from Pittsburgh, PA. "Can you address scoping for organizations without current contracts that are looking to get into DoD work?" And Gavin, if you don't mind, I'd like to take a stab at this first while you collect your thoughts.

Gavin Jurecko: Sure.

Matt Trevors: So, what I would do, Tyler, is I would honestly determine what your company does, so through your mission statement, or you likely know what your company does, and I would try to find an archive of previous RFPs, where the government has, or the DoD has, spun those out for contracts and just-- then go back and see what part of your organization would help achieve that contract, and usually it's difficult to determine what's FCI versus CUI, but if you're creating bootlaces or just providing a commodity or standard components to the DoD, or to a prime contractor, then it's likely you'll need a level one. However, if you're into more sensitive maybe radar systems or other missile or just basically more advanced products, then you may want to consider yourself for level three, four, and five. Gavin, what are your thoughts on that question?

Gavin Jurecko: So, I kind of hit upon this a little later, but I think you're on the right track. So, looking at the services that your organization does, try and look at what the definition of CUI is. If you look at NARA guidance or ISOO guidance for the defense sector, they do break out what CUI is considered. One of it is control technical information. So, under that, there is engineering drawings, specs, whatnot. I'd then take a look at kind of what Matt was saying as far as the sensitivity of what you're providing them. There might be a barrier depending on if it's a bootlace compared to a specific subsystem of a radar installation. There's not one right answer to see, but you may be able to tell what's more sensitive or not based on your work area.

Matt Trevors: Yeah, and we'll touch on this a little bit in a couple questions, but you really need to determine what parts of your organization-- so we started by talking about do you do a full enterprise-wide assessment, or do you have several enclaves. Maybe you have contracts that you believe are going to be level one, three, maybe even four or five. It's really good to have that stuff documented in data flow diagrams or network diagrams, but I'm getting a little bit ahead of myself, but yeah, Tyler, great question. Thank you very much.

So, let's move on, Gavin. So, you and I have both done assessments supporting various organizations. One that comes to mind are the CRR and CRA, are the cyber resilience review or the cyber resilience analysis, where we go out and evaluate critical infrastructure organizations, but we don't do the entirety of the organization. We spend time helping them scope their critical services, and that's how I think of this. Can you help explain to the audience what a critical service is and why maybe it might be the right way to address scoping?

Gavin Jurecko: Sure, so with the CRR and the CRAs we do not want to go into an organization and look at the entire enterprise. It's a snapshot in time of your cybersecurity practices and your maturity concepts. So, we really need to focus on the scoping, and the way we do that is we bring forth the idea of a critical service. So, a critical service is something that's critical to the success of your organization's mission. It supports the accomplishment of the organization's strategic objectives, and it should be identified, prioritized, and communicated. So, oftentimes, the easiest ones to kind of highlight are those critical services where you're developing a piece of software or you're developing a subsystem for a larger system, stuff like that. As we kind of focus on those critical services, we can then begin to scope the assessment appropriately by not looking everywhere in the enterprise but just focus on the assets that support that critical service. So, each organization may have these critical services defined in many different places. I think Matt's going to also speak to where some of those may be found.

Matt Trevors: Right, great. Thanks for the lead in, Gavin. Thank you very much. So, Gavin's right. So, I have a couple of other places that I help people during the scoping. So, if you review your mission statements at the enterprise level, the department level, or even perhaps the information system level, that will give you a good idea of what your critical services are. So, what I don't want people to walk away with is-- one thing that we often run into is people will start automatically with payroll. Payrolls are critical services or are a critical service because, without the payroll system, people don't get paid, and yes, that would be unfortunate. However, to your customers and your stakeholders, that is not the reason they engage with you. They engage with you for the reasons stated in your mission statement.

Also, are there companies who may be a little bit more sophisticated or be under regulatory guidance. Business impact analysis is another good place to go identify your critical services and even critical assets. And those would be really good options for reviewing how you may want to go about scoping your critical services. So, Gavin, we talked about business services. Can you talk about some of the assets that we consider important or would be within the scope of the CMMC assessment?

Gavin Jurecko: Yeah, sure. So, typically, when we're talking cybersecurity, everyone focuses immediately on the technology involved, but we also like to consider not only the technology, which is the systems and software that automate or support the service, but also the people that operate and monitor the service. Can they access FCI/CUI? The information obviously is going to boil down to is it FCI or is it CUI, and then also the facilities where the service is performed.

So, obviously, when you're scoping an assessment, this is a data centric model. So, it all goes back to what FCI or CUI you may have. I know there is some pain points right now with CUI and appropriately labeled CUI, but there is guidance out there, and I suggest you be proactive with truly looking at the information that your organization possesses. As I mentioned earlier, the NARA, or the National Archives and Record Administration, and ISOO, Information Security Oversight Office, have high-level definitions of CUI, and specifically that's broken down for different critical infrastructure sectors.

Specifically, for the defense base, we have a couple of overarching categories. One is controlled technical information. So, some of this stuff, whenever you do the research on there, it's research and engineering data, engineering drawings, technical orders, technical reports, datasets, stuff like that. I'd take a look at what data you have, and see if you can apply it to those sets, and that way you can get a better handle on what you have.

Some of the other categories that I see on the site are DoD critical infrastructure security information, naval nuclear propulsion information, and unclassified controlled nuclear information. So, any of those, I didn't go down to the detail, but you can click on those, and they're going to give you examples of what they consider to be some of theirs. So, I think it's really good step to be proactive. I know it's more work, but if you can show that you know where your data is, you're going to have a lot easier time scoping your assessment and limiting the scope of that level three possibly assessment to only the assets that store, process, or transmit that data.

Matt Trevors: Right, great, and Gavin, you just triggered a thought. So, you mentioned it maybe a little bit more work. So, as Shane mentioned in the intro, part of my background is in software development or secure software development, and we have a saying in software development is you want to pull requirements to the left. So, that means, if you're following a system development lifecycle or software development lifecycle, such as discover, design, develop, debug, deploy, maintain, dispose, the earlier on in the process you uncover those bugs or those issues, the less amount of money or time, money, and resources it will cost the organization going forward. So, I think that's a very key point. Although maybe a little bit more effort now, it may be less effort over the long run. Gavin, what do you think? Is that a fair analogy?

Gavin Jurecko: Yeah, I think so. I mean, the more effort you can put into it up front and truly identifying the information you have, I've seen it a number of times over the last couple months of going into an organization and them truly not knowing where the CUI or FCI is. So, ultimately, they want to scope the entire enterprise. I think if we kind of try and move the needle away from that and truly get some proactive thought of what CUI you may have and then begin to kind of trace that through the system, you're going to have a lot better-- you're going to have a lot better success at appropriately scoping an assessment and passing the assessment because you can, without a doubt, then say this is where the information goes.

Matt Trevors: Absolutely. So, we're getting a lot of great audience participation here, Gavin. So, I'll go ahead and read a question from Neel G., and then I will turn it over to you. So, Neel G. says, "Can boundary for CMMC assessment be limited to the personnel who handle CUI, or "cooey" using email and storage solution?" So, if you're speaking strictly from a personnel perspective, I would say as long as you can justify your scoping to your C3PAO, then that would be satisfactory, but I don't know that you'll be able to limit-- so, I'm not sure if the company-- the question is with regards to specifically personnel or that would be the entirety of your scope. So, if it's you can scope it to those people, but it would also include the technology, the information, and the facilities also. Gavin, what are your thoughts on that?

Gavin Jurecko: Yeah, it's hard to say without having some of the background knowledge of Neel's specific business, but at a high-level I think that's kind of where you want to start going with your assessment boundary. If you're truly only have personnel that are accessing CUI through email or storing it, and you're not leveraging that or creating something and whatnot, then it would be appropriate to start thinking of where the CUI is in those respects, but that's kind of where I'm getting at as far as what CUI you have. If you can appropriately define where that's stored, you're going to have a lot better chance with the assessor to say this is in bounds, and this is out of bounds because this is how we use it, or, by policy, we're doing things this way.

Matt Trevors: Right, great, and then we have a follow up question from Neel G., what is the best way to define boundary for CMMC assessment for small organizations with all remote workers using cloud software as a service services for handling CUI. So, Neel, follow the CUI. So, if you have CUI in your email system or basically, as we have been talking about, or we will talk about, data flow diagrams will help you find the best way to scope your assessment. Gavin, any additional thoughts on that?

Gavin Jurecko: Yeah, so there's currently a lot of work going on to discuss cloud providers and all of that. And it's even something we were going to discuss at a high-level later on, but I think the biggest thing that I want to point out here is just because you use a cloud provider to satisfy some of the CMMC level three requirements, there still is that process maturity piece. So, while they may be providing you the technical solutions to satisfy some of these practices, it's still on your organization to be mature enough to plan around this process, define the processes and procedures on how you access the CUI, how you do different configurations of your technology, as well as the policy for each of these CMMC domains.

Matt Trevors: Okay, perfect. A couple more audience questions, and then we'll get back to the interview. So, Brett Z., part of his question is, "Is it safe to assume that GFE will be out of scope for an organization's assessment for CMMC?" And Gavin, I'm going to say to Brett I would not assume that anything is out of scope until you can convince the C3PAO that you have appropriately scoped your assessment. What are your thoughts, Gavin?

Gavin Jurecko: Yeah, unfortunately, there's still some decisions being made where we can't definitively say one way or the other, but, again, this all starts with talking with your assessor and letting them know what you have, what other requirements you may be required to meet for GFE equipment. Sometimes, that equipment isn't allowed to be updated, or it's an old operating system because it's meant to support an existing system that's out in the field, and you can't. So, there are discussions about this in place, but I don't think Matt or I can leave any definitive guidance on that subject today.

Matt Trevors: Right, right, thank you, Gavin. And then from Rick G., "How does CUI marking and FOUO, I'm assuming that's for office or official use only, coexist, or does CUI guidance replace FOUO?" So, as Gavin and I have spoken about, the CMMC largely focuses on FCI and CUI, so federal contract information and controlled unclassified information. And what we can say emphatically is all CUI is considered FCI, but not all FCI is considered CUI, and FOUO doesn't really come into the vernacular of CMMC. So, if it's for official use only, you're going to have to classify that information as FCI, CUI, or another type of data. Gavin, what are your thoughts?

Gavin Jurecko: I'm going to defer to you on that. I don't-- I'm not a documents marking expert. So, I don't really have anything to add to that.

Matt Trevors: Okay, so let's get back to the question and answer portion of this. Great questions from the audience. Thank you so much. It really makes this-- you're really testing to make sure that Gavin and I are truly model architects, I think. So, thank you very much for those questions. So, we've talked about data flow diagrams a little bit, Gavin, in this discussion. And when I-- we talked about us doing CRRs and CRAs in the past. I've always found it extremely helpful to draw a diagram up front as part of the scoping exercise. Can you-- what are your thoughts on drawing data flow diagrams to help folks scope their assessment.

Gavin Jurecko: Yeah, so it's never a bad idea to have a data flow diagram or a network diagram. I know some of these specific practices that relate to that, having the information flows and the diagrams, may only show up in level three, but it's just god practice to have your network mapped out so you can explain to the assessor what the boundaries may be. So, a high-level diagram can be worth a thousand words, or, as they say, a picture is worth a thousand words, but when you're looking at the high-level network diagram, it's not that you must have every single component diagrammed out, but think of it from a system or a subsystem point of view. A system or a subsystem is going to have many different components that underlie in that subsystem, and maybe a different drawing can show all the details of that, but when you're trying to scope the assessment boundary, you want to look at what can have the FCI, what can have the CUI, and the high-level network diagram that shows hey, this can only have bidirectional, or this can only have what unidirectional communication, or this is segmented differently, those relationships are going to be super important when discussing these things with your assessor.

You want to be sure to include stuff like cloud instances that you use, any type of remote access methods, especially now in our current-- with working from home and with COVID going on, remote access has become a big thing. So, any of those types of methods, you want to point out on these high-level diagrams. Managed service providers, you're going to want to call out those in the high-level diagrams. Make sure that you make an effort to kind of truly show a depiction of what you're network looks like, so you and the assessor can have a common picture of what you're going to be talking about for however long that assessment is going to last.

You can also then, depending on your organization, break that down into lower level network diagrams to show individual components. You can start to include ports, protocols, services, whatever. As you begin to discuss some of those higher level CMMC practices, you may be able or you may have to show how you're protecting or dealing with some of those things as well. So, again, it's not a requirement at the lower levels of CMMC to have these diagrams, but it's highly recommended that somebody takes the time to appropriately document these things so you and your assessor can be on the same page.

Matt Trevors: All right, couldn't agree more, and I think the analogy of moving everything to the left applies here as well. Just because you don't have to do it at level three-- or level one, doesn't mean you shouldn't. If you have the bandwidth, I strongly encourage you to take these efforts and bring them to your assessment because you-- it is incumbent upon you to ensure that the assessor or the C3PAO has enough evidence for them to have you be marked as satisfied for each of the practices. So, I think it's key that if you do a little bit of extra work, it's going to show that you're more prepared, you're taking it seriously, and you may have the C3PAO at ease. So, I think that's great.

So, we have another question from the audience. So, Chinho K., "What about how do you usually deal with FedRAMP environments?" So, I think the question is if they are a company that deals with a FedRAMP moderate or a FedRAMP high environment, how do we treat that? So, I will say that that is part of our reciprocity initiative, and I believe Miss Arrington, the SYSO for OUSD Acquisition has stated publicly that FedRAMP is one of the primary regulations that we will be mapping to so that we have a good-- so that the community has a good understanding of how those two standards relate. Gavin, any other thoughts on that?

Gavin Jurecko: Yeah, so work is ongoing on that. There are specific practices that we expect to be satisfied by cloud instances that are FedRAMP moderate, and the details between that are currently being worked out.

Matt Trevors: Okay, great. All right, so back to the Q and A. So, Gavin, one of the terms that I see very often misused is level one, level three, FCI, CUI with regards to assessments. So, I just wanted to take a moment to wax poetic on that for a sec. So, level three, as most of you are aware, consists of all hundred and ten 171 controls or requirements in addition to twenty additional. So, some of these practices ended up at level one through the work of the model architects. So, those controls or requirements or practices, whatever term you use, still apply to CUI. It just so happens that they also more directly apply to FCI. So, Gavin, any thoughts on FCI, CUI, level one, level three?

Gavin Jurecko: Yeah, so I'd like to just try and clear up-- so, the CMMC was written as well because there was a-- not every organization handles the same type of information, and then even more so not every organization, depending on what they do, should have to satisfy all of the requirements of 800-171.

So, with that being said, one of the principles that we wanted to use for CMMC level one was to relate it to the FAR requirements. That's where we got the seventeen practices. So, CMMC level one relates to the seventeen FAR practices, and a level one organization is required to satisfy those practices. Now, when they go to level three, since the model is cumulative, they'll still have to comply with or satisfy the level one, level two, and also the level three practices. What we're trying to say, too, with the scoping boundary is just because your organization handles both FCI and CUI, CUI has a higher barrier to entry to protect. So, if you choose to get a CMMC level three assessment or certification, you need to meet all of the practices at CMMC level three. It doesn't matter if you have co-mingled data in the level three environment, FCI and CUI. Since it's cumulative, everything would have to be protected using all of the practices. So, that's where it kind of behooves an organization to say okay, well maybe we do have these different boundaries, and FCI doesn't permeate everywhere, there's lower sensitivity information. The barrier to satisfy those requirements is a lot lower. So, that's where you get into maybe having two assessment boundaries, where you have a level one assessment boundary for your enterprise, and then you isolate the CUI further to do the level three assessment since there's more practices that have to be satisfied at level three.

Matt Trevors: Right so, Gavin, what I hear you saying is that they would pursue two assessments. It's not like they could do both of those at once. They would likely go for their CMMC level one enterprise first, and then, once that is achieved, then they would use-- they would follow or pursue a CMMC level three for their enclave, correct?

Gavin Jurecko: Correct.

Matt Trevors: Okay, perfect. So, while we're on this enclave kick, let's talk a little bit about cloud providers. So, we've had a question from Chinho about FedRAMP and you talked briefly about cloud. How will the use of cloud impact an organization in their scoping of an assessment?

Gavin Jurecko: Yeah, so I kind of think of this in two ways. You're either going to have a cloud provider or an MSP that has an associated CMMC certification, so whether that's level one, three, or higher. That becomes a little easier to say then okay, here's how we use them. They have level three certification. They've been assessed and show that they meet all these requirements, but then you get into this instance where they may not need to have that certification. So, you may be pulling this MSP in, depending on the size, of course. This is all dependent on specifics of your instance, but maybe they won't have to have a CMMC certification then. If you appropriately define the boundaries on how they connect to your systems, appropriately identify the people, you can apply the controls to them and make sure that, via policy/procedures, that whatever service they're providing you is within your assessment boundary and you're protecting that information appropriately. It may be it's ensuring that they can't access the CUI, stuff like that. So, just because you're achieving level three certification doesn't necessarily mean that every MSP or cloud provider is going to have to have that same level of certification.

Matt Trevors: And we have a couple more questions, Gavin. So, another question from Neel G., "How do you craft boundary diagrams, network and/or data flow, when the sensitive information is being handled at endpoints, phones, tablets, and mobile devices?" And that's a great question. So, one of the early places I started to build data flow diagrams was in STRIDE threat modeling, and in STRIDE threat modeling, for those who aren't familiar, it's a process that was built in the late '90s by Microsoft, and it stands for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. You have four different objects on STRIDE diagrams, so external entities, processes, data stores, and data connections. So, Neel, what I would do is start to build out a diagram that maybe consists of those four pieces.

Then we also talked about technology information, people, and facilities. With your phones, obviously, they're likely to use a cellular network. I'm assuming they're not just Wi-Fi. So, you're going to have your mobile device management section. You're going to likely need to have some form of encrypted tunnel, so a VPN running over top of that. It's absolutely doable. You may not want to draw every phone, but instead group them into a logical group for phones, maybe tablets, other mobile devices. It's very, very doable. It may result in a large diagram. You may need to consider; this may be a good opportunity to consider multiple CMMC assessments. Gavin, what are your thoughts?

Gavin Jurecko: Yeah, I think you're on the right track. There's no right or wrong way to do it, but depending on the size of the organization, the intent isn't to put every specific endpoint, but really is there a specific aggregation point that they all have to communicate through to get to another portion of the network. That's how you're going to want to start thinking of crafting your boundary diagrams.

Matt Trevors: Right, okay. All right, next-- sorry, go ahead.

Gavin Jurecko: I think there's a question from Scott DeWerth. "Is that a change? Our 3PAO did not state we would need two separate reviews for level three certification." I don't want it to seem like I was saying that you need two separate reviews. All I was saying was if you have FCI and CUI, then the barriers, even though you have FCI in your level three environment, it still has to be assessed via all hundred and thirty practices plus the maturity processes at level three. So, depending on your boundary, it may be easier for your organization to say we only have FCI over here. Let's do a level one assessment, and then we have an enclave where we only have CUI, therefore that would be the second assessment. Ultimately, it's going to be up to you how you want to handle your certification, but there are ways to maybe lower the barrier of entry because the FCI does not have to meet as high of a bar as the CUI as far as practices.

Matt Trevors: Right, and just to call out, 3PAO sounds an awful lot like C3PAO, but the 3PAO are, and Gavin correct me if I'm wrong, they're the third-party assessment organization's charged with evaluating organizations for FedRAMP, correct.

Gavin Jurecko: That sounds right to me.

Matt Trevors: All right, great. Another question from Chinho K., "Do you think use of G Suite, FedRAMP moderate, to use for the CUI environment?" So, I don't think either of us can answer that, Chinho. I think that would largely depend on how the reciprocity mapping between CMMC level three and FedRAMP moderate fleshes out. I don't really know that we have information beyond that. Gavin, anything to add?

Gavin Jurecko: No, I can't really add anything more to that.

Matt Trevors: Yeah, folks, we know that there's still some stuff outstanding. We wish we could give you more definitive answers, but this is a very quick moving system, and we're trying to get to it as quickly as we can. As you see, there's CMMC accreditation body is now helping in this effort. So, hopefully that will help us pick up the pace a little. So, Gavin, with that, we've covered a lot of ground. Scoping is vital to the success of an assessment. I think we've proven that. Do you have any other gotchas or things people should keep in mind when they're scoping a CMMC assessment?

Gavin Jurecko: Yeah, I think primarily for the organizations that are at level one, they tend to not have as much experience with implementing some of these requirements. So, I hope today we've kind of broken this down, giving you different tools through the network diagrams, through thinking of what services you provide, not only thinking of your technology assets, but also the people that access them, the information, the facilities they reside, kind of taking a different perspective on how you can think about these and begin to define your boundary. There are another-- there's a number of self-assessment tools out there that can quickly give you an idea on how far you are from your target. The cyber resilience analysis is a great tool to baseline your capabilities. This is a tool that's available through DC3, the center for cybercrimes through DoD, where you can get an independent third-party to give you a fresh set of eyes on how you're doing things. A lot of the maturity concepts are included in this tool. So, you know, I don't think there's a one size fits all for this, but there's definitely tools you can use to make your (inaudible), and we want to (inaudible) network. I think there's some tools that organizations may be using, and they can leverage to help guide the conversation to the appropriate assets that store, process, transmit FCI or CUI.

Matt Trevors: Great, thanks, Gavin. Before we wrap up, I just wanted to commend the audience on some great questions. Obviously, we understand that there is a fair number of organizations, upwards of three hundred and fifty thousand companies, that may have to adhere to CMMC in one way, shape, or form. I think that's not slated for the next five years to get to that sort of level, but I can appreciate the anxiety that people are experiencing as they stare down the barrel of this new assessment. We went to great lengths to make sure that the practices and processes within the model would help you achieve better cybersecurity outcomes. In no way was it punitive. Please remember that. This was not punitive. We're merely trying to help folks establish more sophisticated and effective cyber programs. With that, Shane, thanks very much for having us, and everyone have a good day.

Shane McGraw: Yeah, Matt and Gavin, great discussion today. Thank you for sharing your expertise. Matt did mention his blog post early on in the webcast. That is in the chat. So, make sure you guys find that link and read that blog post as well. Lastly, I'd like to thank you guys for attending, all great questions. Upon exiting today, please hit the like button and share the archive of this if you found value. Also, you can subscribe to our YouTube channel by clicking the SEI seal in the lower right corner of the video window, and that will subscribe you to our channel. And lastly, please join us for our next webcast, which will be on October 6th. The topic will be threats for machine learning with Mark Sherman, but we will email everyone a link to that registration. So, that's all the time we have for today. Thanks, everyone. Have a great day.

DM20-0788