Constellations Podcast

Episode 105 – Protecting Critical Information, Contracting with DoD and CMMC

Speaker: Justin Padilla, Director, Cybersecurity Services, Kratos – 21 minutes

John Gilroy: Welcome to Constellations, the podcast from Kratos. My name is John Gilroy, and I'll be your moderator. Our guest today is Justin Padilla, Director, Cybersecurity Solutions at Kratos Defense.

John Gilroy: Justin, this is a space and satellite podcast. However, the Department of Defense is a key component in this discussion. The DoD does not manufacture anything. It relies on over 300,000 suppliers to provide goods and services for all its employees. The Pentagon is a hardened target. Our adversaries understand that and view DoD suppliers as the soft target. And that's we're going to talk about today, the soft target. So, to improve the security for suppliers, the DoD has several systems in place. One of the components of that process is a relatively new concept called CMMC or Cybersecurity Maturity Model Certification. That's kind of a mouthful if you've never heard of that before. The CMMC has been in the news of late and will have significant impact on those companies seeking to do business with the U.S. Department of Defense including the satellite industry. And that's what we're going to talk about today.

John Gilroy: Constellations today will break it all down for you. Our guest, again is Justin Padilla. He's the Director of Cybersecurity Services at Kratos. Kratos has recently been named by the Federal Government as one of the first two authorized CMMC third-party assessment organizations, or C3PAO. Justin, who leads the consulting arm of Kratos's commercial cybersecurity business, is going to walk us through what CMMC is and how it will impact your organization. Okay, Justin, let's start off. Give me the scoop here. What's the elevator pitch for CMMC if you just have to meet someone and introduce it to them?

Justin Padilla: CMMC is a maturity model and a benchmark for cybersecurity practices and processes. It's an evolutionary step in the DoD's goal of ensuring that the Defense Industrial Base and Supply Chain is protected at a commensurate level with the type of data that a company processes, stores, transmits, and ultimately protects. It is intended to certify the organizations doing business with the DoD meet a minimum standard and is certified by a third party for what the Office of the Undersecretary of Defense deemed critical for protecting our country's economic and national security.

John Gilroy: So was there an incident? Was there something that precipitated this whole move for CMMC? What got it all started?

KRATOS

Justin Padilla: Yeah, so the DoD has stated that there's over 300,000 companies that make up our Defense Industrial Base and Supply Chain. And it seems like every week we hear about major data breaches, ransomware, and other very targeted attacks on organizations that have become integral components, not only for the DoD's life but our daily lives as well. The troubling thing is, those are just a small portion of the cyber threats and attacks that we actually hear about, right? So, for many years, the organizations doing business with the DoD have been self-attesting to meeting the majority of the requirements that are established within the CMMC. And so, this evolutionary step is now moving away from that self-attestation model to a third-party assessment model that provides greater assurities, that organizations that hold this critical DoD data are doing what they say they're doing and protecting it.

John Gilroy: And that's what we're going to be talking about today, assessment organizations. So Kratos has recently been authorized as a C3PAO, kind of a mouthful but the listeners will get used to it after a while, C3PAO. So what exactly is that?

Justin Padilla: It's not to be confused with a Star Wars Droid.

John Gilroy: It's the first thing I thought of.

Justin Padilla: A C3PAO is a CMMC third-party assessment organization. So, it's a trusted, vetted organization that specializes in assessing compliance of other organizations against a specific framework. In this case, the CMMC security practices and processes.

John Gilroy: So what I understand is that over the years companies have examined themselves and they've been found wanting, so they decided to just bring in a third party, a trusted third party, to do an assessment of their security positioning, their maturity, in cybersecurity, is that right?

Justin Padilla: Absolutely.

John Gilroy: Must be tough to be one of these trusted organizations. So, what do organizations have to do to become authorized as a C3PAO?

Justin Padilla: Well, there are a number of things that aligned really well for us, but I don't want to just speak about us. Kratos is a significant contributor to the Defense Industrial Base, which means that as an organization, we are delta between what we were previously attesting to and where we had to get from CMMC was pretty minimal. But for many organizations that have been doing business with the DoD, they should really be in that same boat, where they've been working towards or have already implemented the NIST SP 800-171 requirements that

were part of the DFARS, and now they're doing that Delta to get CMMC compliance. So one of the first things that a C3PAO has to do is meet whatever level that they're going to be assessing against. In this case, in our case, it was level three, so we had to make sure and validate that our organization, as a whole, was a level three.

Justin Padilla: And then, I think another main factor was that we were an early adopter of CMMC, not only from the standpoint of the requirements but also as part of the program itself. So getting involved, working in the community, working with the accreditation body to help them and help us and help the general community get awareness about what these were is really what allowed us to become a C3PAO. There are additional requirements around the company being vetted from a security standpoint, staff being vetted from a security standpoint, and then previous experience, all playing key factors on becoming a C3PAO.

John Gilroy: The reason we have you on the air is because of our listeners. There are listeners to this podcast whose company does business with the DoD, and they're going to be directly impacted by CMMC. Can you explain more detail how this process works at different levels and everything else, please?

Justin Padilla: Yeah. So it's a pretty easy process. If you go to the cmmcab.org, there's a marketplace that identifies different people and resources and different things that help organizations get prepared. It also points you back to the Office of the Undersecretary of Defense's website, which has produced documentation that leads people through the process for getting certified or meeting the requirements to get certified. But in order for an organization to get certified, there's a number of steps that they have to take, including making sure that they actually implement the requirements and then working with the C3PAO to undergo that process.

John Gilroy: So is the process the same for everyone or are there different levels for certification?

Justin Padilla: Yeah. CMMC has five levels of maturity that have increasing security requirements commensurate with the level of data that's associated with the contract. Levels one and two focus on federal contract information, and that information is provided by or generated from the government under contracts that's not intended for public release. Levels three, four, and five is Controlled Unclassified Information. The National Archives and Records Administration goes into great detail defining numerous levels of what qualifies in those various categories. And from a definition standpoint, there's very specific information that would be better looked up than for me to try and voice. But from levels one through three, those are the only ones that can be assessed right now, right?

Justin Padilla: And so levels two and four are eventually going to be, I think, stepping stones, at least that's what I've heard from CMMC-AB, that will allow organizations to not necessarily go from one to three and make that big jump because there's a big difference in security requirements between those levels. And so the level two is there as a stepping stone. Level four and five are not fully finalized yet as far as the requirements to go into that. It's anticipated that its really going to focus on very specific types of CUI. So CUI that has very military or space applications.

John Gilroy: And for the benefit of some listeners, Justin, maybe you can tell us what CUI is.

Justin Padilla: Yeah. So, Controlled Unclassified Information is information that is deemed sensitive to a certain level. I don't have the specific definition.

Justin Padilla: There are some intricacies to it, but it's specifically identified under a specific contract, and it's anything that's generated or produced on behalf of the government in one of any various number of categories.

John Gilroy: You know, Justin, thousands of people from all over the world have listened to this podcast, go to Google and type in “Constellations Podcast” to get to our show notes page. Here, you can get transcripts for all 100 plus interviews. Also, you can sign up for free email notifications for our future episodes.

John Gilroy: There's some terms being used here that not everyone's familiar with, some people are way too familiar with it. I just want to level the playing field for our audience here. Another term you threw out there was assessment. Now I thought back to my math teacher in high school because I never liked assessments, and so what is involved in an assessment? Are there any tips that you can share with companies going through the assessment process? Like what to prepare for? How long does the process take?

Justin Padilla: Yeah. From a tip perspective, I would say that if you haven't started getting your organization ready, start now, even if you don't plan on bidding on contracts or getting assessed, even next year or three years from now. The longer the runway that you have, the easier it's going to be on getting there, right? Whenever time is constrained and you need to do something within a shorter period of time, it makes it much more difficult for an organization to implement. So what's involved, right? There's essentially four phases that are involved with the actual assessment. There's a planning phase, which really outlines the scope of the environment and you'll work with your C3PAO on us. And then there's also a component of identifying any type of objective evidence, such as interview points of contact, documentation, or specific demonstrations of what would be needed during an assessment.

Justin Padilla: And then, the C3PAO works with an organization and helps them confirm that they are ready before actually entering into phase two. So phase two is when we actually conduct the assessment and that requires both an on-site visit to physical locations, where CUI might be stored or with what's defined in your scope or your boundary. And then it incorporates in-depth interviews and reviews of documentation and technical testing, things of that nature. The result of that is basically a pass or fail for each security practice and process that ultimately determines the success or unsuccessful certification recommendation.

Justin Padilla: For phase three, there's reporting of the assessment results, and that is just what it sounds like. It's the organization reporting the final determining factor, right? Whether you passed or failed. And I will note that with CMMC, it's an all-or-nothing thing, right? So an organization has to pass all of the given levels, security practices and processes, in order to be recommended for certification. And so one control failure can and will result in a C3PAO not recommending you for certification, and so that sounds really scary. There is a phase four, which is remediation of outstanding assessment items. And that provides organizations with up to 90 days to resolve any minor issues that might have been found during the assessment.

John Gilroy: Well, what people are thinking is, what about pricing? For a small company, will CMMC put an undue burden on companies in the Defense Industrial Base that will need the certification?

Justin Padilla: Organizations should have been meeting or close to meeting the previous DFARS requirements that incorporated that NIST SP 800-171. So realistically, there should only be around a delta of around 20 security controls in order for organizations to get to a CMMC level three requirement. Practically, I don't think that companies, I'm sorry, I do think that companies are going to have to invest some money into it just to kind of tie up potential loose ends or potential POA&M items that they had on their lists. But from an assessment perspective, I don't see CMMC assessment costs being drastically different from other certification costs that organizations would normally go through. And the DoD has also said that it may be reimbursable at some point, although I'm not the one to speak on that or how that might work, but I think that's a potential there too.

John Gilroy: Although you would think that a normal company would understand the concept of changing their passwords regularly, two-factor authentication, and tagging documents carefully, and this is really just like showing up and having shoes and socks on for cybersecurity. So this is the minimum requirements or some of the baselines here. What I've investigated in CMMC, it seems like there's assessment services, but also advisory services available. So what's the difference here? And does a company do both or just one?

Justin Padilla: Organizations can be both, right? An RPO is a Registered Provider Organization, and they provide various consulting or advising services to organizations with the intent of getting them fully prepared to undergo a CMMC assessment. That can be anything from helping an organization interpret security controls to integrating security solutions, conducting gap assessments, anything of that nature, right? With a real intent to get them to the point that they can pass a CMMC assessment. When it comes to a C3PAO, that function is solely reserved for assessment period, right? And that can be readiness assessments or even the full on certification assessments. I think the key thing here is that a C3PAO, when performing in that role, cannot provide guidance or recommendations, right? They're only there to assess whether or not you are meeting or not meeting a given requirement. And so for organizations that are both a C3PAO and an RPO, they cannot serve in both capacities for the same organization, so it's either one or the other.

John Gilroy: You've seen enough of these assessments in your business dealings here. So what are some of the top challenges here for CMMC compliance?

Justin Padilla: For CMMC, it continues to evolve and will likely do so over the next few years, right? As things get more flushed out. But as we've been working with companies, CUI handling and marking and the protections both from a physical and an electronic standpoint, has areas of challenges. In large part, because many times we should be receiving, organizations should be receiving information from the government that identify specifically whether or not it is or it is not CUI. In many cases, that's not happened and so organizations have a really difficult time with making sure that they are properly handling and marking information that would be classified as CUI.

Justin Padilla: From a technical standpoint, there are aspects that have proven to be difficult. Multifactor authentication is one. Whitelisting and blacklisting of applications is another one. Surprisingly, being able to gather a complete and comprehensive inventory of an organization's assets has proven to be challenging for many organizations. And then there's also the aspects of documentation. Documentation in itself isn't hard, right? Because you're really documenting what you do as an organization, but it is time-consuming, especially whenever you consider all the different requirements that you're documenting against.

John Gilroy: Now, Justin, a lot of companies are listening to this interview and maybe you want address them. Could you give us some advice for companies that are seeking a C3PAO for an assessment?

Justin Padilla: Yeah, as I mentioned before, there's a standard process that all C3PAOs are going to from a process perspective, you shouldn't see that much variance between one organization or another. I think where it really comes into play is the organization's experience with the type of business they're working with,

right? As a services organization, that type of business is very much different than somebody that is manufacturing a piece of equipment. And so, working with a C3PAO, making sure that you get all of your questions answered, making sure that you feel comfortable with that organization, and then also making sure that they have relevant experience in assessing environments such as your own, I think is pretty critical.

John Gilroy: Justin, this podcast, the Constellations Podcast is focused on the satellite and space industry, you know that. So are there any special CMMC considerations that companies in this particular sector should be aware of?

Justin Padilla: Yeah. I touched on specialized CUI, specifically designating that as Control Technical Information. As I mentioned, that is applicable to military and space applications. So while I don't think that everybody listening to this podcast is going to have to meet a higher level of CMMC requirement, level four and five, I would imagine that many organizations that support the space industry are working on stuff that is highly sensitive, that may not be classified but is pretty close, right? And if you're in that situation, as you're working towards your level three certification right now, you should also be planning for those higher levels of requirements just to kind of extend that runway as I mentioned before, a little bit longer, so that you have better planning and better options for implementing the solution that'll get you to where you need to be.

John Gilroy: Great, Justin, you just gave our listeners a better handle on critical thinking for cybersecurity maturity for suppliers to the Federal Government. I'd like to thank our guest, Justin Padilla, Director, Cybersecurity Solutions at Kratos Defense.