Transcript- What Google Can’t Tell you about NIST 800-171 Compliance – Part 1

00:00:00 Intro

Welcome to Cybersecurity Magnified with Braxton Grant Technologies, where candid cybersecurity conversation needs technical and applicable advice. Investigate with our experts on the latest in the cyber world, including security best practices, compliance guidance, and all things cloud adoption. Thanks for joining the conversation! Let's get started.

00:00:31 Krista, Podcast Host

Hello everyone, welcome to Cybersecurity Magnified. My name is Krista, your podcast host and I'm joined by Josh, one of our cybersecurity engineers here at Braxton-Grant. So, this is our first podcast episode, and we are really excited to be sharing some of our expertise in a new way. So Josh, why don't you give us a little bit of background on how long you've been with Braxton-Grant and in the industry of cybersecurity?

00:01:02 Josh

Sure. First off, thanks for having me on the podcast. I'm really excited today to talk about cybersecurity and compliance in general. Yeah, so I've been working here at Braxton-Grant for the last five years. I've been working in IT and cybersecurity for about 8 to 9 years now. My experience spans, you know, everything from technical expertise in firewalls, teaching courses, working on government sector contracts, and now I'm on my way to working with companies to help with NIST 800-171 and CMMC compliance to help get them in shape and prepared for assessments in the future.

00:01:39 Krista

Awesome, so for our first couple episodes, we're going to be focusing on just that. The NIST-800 171 and compliance, and getting all that up to speed. So, we're going to be covering different things as far as this compliance and what that means for your security environment. Today we are just breaking the surface of what NIST 800-171 and CMMC means, so if that's something that you've been trying to do some research on, then this is the podcast for you.

00:02:11 Krista

First things first. Josh, give us some background on what NIST SP 800-171 is and why it's been such a hot talking point recently.

00:02:22 Josh

Sure, so NIST 800-171 is a set of controls that were put out by the NIST government agency for the protection of unclassified information in non-federal computing systems. And what this refers to is basically all these government contractors out there that are working on different government contracts, specifically for the DoD that handle unclassified information, need to abide by these controls and apply them in their organization to protect that information. The government wants to ensure that you know all these little bits of information out there - while they may not be classified - they are still worthy of being protected. So, NIST 800-171 was put out as a self-adaptation for contractors to basically show that they're compliant, yet not have to have their compliance be done by a third party.

00:03:20 Krista

And you mentioned unclassified information. What does that mean for government contractors?

00:03:27 Josh

So NIST 800-171 applies specifically to controlled unclassified information, and this is information or data that is provided by or created on behalf of a government contract for the DoD for the government. That information needs to be specifically controlled and protected per the contract that you are awarded. For government contractors, that means really identifying what kind of data and information that you or your organization may be handling, storing, and processing or creating on behalf of a government contract and making sure that the NIST 800-171 controls are applied so you know correctly to protect that information.

00:04:15 Krista

So CUI is data that needs protected. Then, if I'm a contractor, how do I know what CUI is?

00:04:22 Josh

So that's the million-dollar question right now. The UI infrastructure is still somewhat in flux. Government contractors have not seen that much in the actual term or the headings to CUI and a lot of information. The DoD is still in the process of setting up their own internal CUI organization that will identify and mark CUI and you know, relay that down through the contracts. So right now, the best thing a government contractor can do would be communicate with their contracting officer and start to talk to them about what CUI might be, created, stored, processed, or handled through that government contract because they are going to be the best resource to really tell you what CUI that you may have or may be handling because right now it hasn't been used previously. This is a new thing, and it's really hard for government contractors to go back retroactively and try to figure out what they have already been doing that might be, you know, considered CUI. Another good resource too is the archives agency. They have all kinds of categorization of what types of information might be considered CUI. That’s a good starting point to try to figure out your business, your service, or products that you supply to the government, would they fall underneath those categories. That still doesn't tell you whether specifically what information is CUI, but it's a good starting point, but really, you know, talking to your contracting officer and have that conversation with them is the best place to start right now.

00:06:10 Krista

You often hear NIST 800-171 and CMMC grouped together. Why are they grouped together and what is the difference between those two?

00:06:20 Josh

Yeah, so is basically CMMC is the next iteration of NIST 800-171. So when NIST 800-171 was first introduced, it was a requirement for defense contractors, but not a requirement to necessarily report their compliance status, or to have a third party come in and evaluate them, so there wasn't really any strict rules around a company's compliance whether they were meeting it or not. CMMC changed that because obviously they realized over time, that was not the best approach and that they needed to make sure that third party was going to come in and improve the compliance for a company that they were actually following the controls and implementing the way that they said they were going to implement them. So CMMC measures a company's, you know, maturity. It really stands for Cybersecurity Maturity Model, and the difference between NIST 800-171 and CMMC is CMMC has the same controls as NIST 800-171. There's 110 controls and CMMC at Level 3 has 130, which is 110 of the NIST ones, plus an additional 20. The another difference there is that the CMMC has a lot more requirements. When you read the verbiage of the controls for more documentation around plans, processes, procedures, and budgeting to really prove a company's maturity in their cybersecurity program. You know companies need to be looking at CMMC because that's now the next thing coming down the road here. We're seeing the CMMC AB, the CMMC board has put out a timeline they're currently working on some professional contracts to, you know, certify those contractors at a certain level for CMMC, and so getting NIST 800-171 and getting your compliance from that in order is going to really help you out to then just be able to switch to the additional 20 controls and really build on your compliance as far as the maturity of your organization and your cybersecurity.

00:08:28 Krista

And if CMMC is the new standard for compliance, then where does that leave NIST 800-171 and why are we still talking about it?

00:08:38 Josh

Yeah, so NIST 800-171 is still relevant now. Last year, the DoD put out an interim rule, a DFARS interim rule, that was stipulated that all defense contractors had to have a SVRS score in the database, which that score is derived from the existing NIST 800-171 controls, of which ones have been implemented and which ones haven't, which gives you a calculation of a score and what they stipulated was that if you wanted to be awarded, if a company wanted to be awarded, a contract after November 30th, they would absolutely have to have a score input it into the database. If you do not have school on the database, you will not be awarded a contract. The reason for that is to probably potentially get companies in gear to make sure that they are starting on their NIST compliance, that they have POAMS and milestones that they can figure out how to gain their compliance so that when NIST and CMMC officially rolls out, companies aren't just left way behind and realizing that they have not done anything. So the real key right now for any defense contractor that you have not started on your listing when somebody want compliance now is the time to start. Because waiting until CMMC is just not the best approach.

00:09:57 Krista

So then how do you recommend just getting started?

00:10:01 Josh

So yeah, there's a number of things that will help the company get started and be successful with assessing their NIST 800-171 compliance. It will really put them on the right road for CMMC as well. So one of the first big things is you need a timeline. You need to understand how long it's going to take you to do a self-assessment. And then also to gain 100% compliance because there's going be two parts: It's going to be understanding what you have done, what's completed, what's implemented, but then you need to be able to follow up and finish out everything that's not implemented already.

00:10:35 Krista

So what kind of key status points are usually looking to include in a timeline?

00:10:41 Josh

I think of timeline in this case, like you really want to do an initial first assessment sweep through the controls and I'd really identify what's implemented and what's not. After that, it really comes down to the POAMS you know, planned action, and milestones of the additional projects and implementations that you're going to need to do to get to 100% with NIST 800-171 and really have all those 110 controls implemented. The better you can be realistic and really plan out what projects and what implementations you can realistically accomplish, the more successful organizations are going to be.

00:11:20 Krista

And how rigid and flexible do you recommend when establishing these status points?

00:11:26 Speaker 3

You know, it really takes a lot of buy in from different stakeholders to make sure these things get done so you know there's going to be some project management skills that are going to be required here. Someone's going to need to head this up and they're going to need to hold people accountable to things that that person responsibility. And that's another key aspect too is you know understanding who is responsible for what. So as far as timelines: pick realistic dates. Try to hold people to them, but realize that things that might have to flex. There's going to have to be a little bit of flexibility if things aren't reached.

00:11:59 Krista

Oh yeah, definitely. Do you have any tips of what you've seen for better project management?

00:12:06 Josh

I think they're really one of the biggest keys for project management is really having a designated person that this is their responsibility. And then also delegating out you know different aspects of the controls. Some things may apply to different people within an organization. So really, delegating that to those people that they need to get this done and then holding them accountable for that.

00:12:28 Krista

Is there usually a person who is that point person that's common?

00:12:33 Josh

It depends on the organization. Some organizations are very large and have lots of resources and people to, have this. But a lot of defense contractors are very small businesses, so you have very few people that wear a lot of different hats. They key is whoever is going to take it on, whether that's the owner of the business or whether it's something they delegate, as long as they understand the responsibility they have and know what the expectation is to get it done, that's the key.

00:13:01 Krista

Is this where outsourcing could be a good idea too?

00:13:05 Josh

It can be. You can definitely get a lot of assistance from an outside consultant, especially depending on your familiarity with NIST 800-171 and compliance in general. If this isn't something that the organization has really had to do before, then yes, bring in an outside resource to really help you get your ducks in order and really explain what you need to do and highlight a path forward to gain compliance. It is definitely a good recommendation.

00:13:33 Krista

Yeah, definitely. So covering timeline and getting that point person. I'm kind of taking a step back, but as far as funding goes. Any tips or best practices to inform management on the importance of this?

00:13:47 Josh

Yeah, so you know in any situation where there's a project that needs to be accomplished, you need buy-in from management to get that done and funding is definitely a key part of that. It takes time, money, and resources to do a self-assessment, but then also to accomplish those POAMS and get on top of them and then get to 100% compliance. So yeah, having the buy-in from management and funding is definitely key.

So when it comes to doing a self-assessment and identifying where the shortfalls with gaps are, understanding what it's going to take to get that control implemented is key. And understanding what it’s going to cost. The more concrete cost you can identify, the more realistic management is going to approve it if they really understand what it’s going to gain them in the end and what is a realistic cost.

00:14:43 Krista

And along the same lines of just making sure that management is ready to conduct a risk assessment, is this something that can be done internally, or why or why not would you recommend doing so?

00:14:56 Josh

Yeah, so you know risk assessment is a good key point to bring up. A lot of the controls are security-related controls, and to really effectively apply security controls, you really need to understand the risks on assets and then that will help guide you to apply the appropriate security controls based on risk. There is a risk assessment component of NIST 800-171 and CMMC, so you're going to have to have done at risk assessment and regularly do them, whether it's on an annual basis or biannual basis to ensure that you understand what the risks are to your assets and are applying the appropriate security controls to those. So, management needs to understand that that's going to involve management to help identify what's the important assets or the potential risks, and then how to apply the best possible security controls to reduce risk.

00:15:54 Krista

And this relates back to what we were discussing earlier with CUI. So obviously risk assessments are super important to NIST 800-171 and CMC, so how do those two relate together?

00:16:07 Josh

Yeah, so CUI is Controlled Classified Information, in which information or data can be considered an asset when you generally do a risk assessment. You identify assets and then you identify threats to those assets to determine what the risk is. So, doing a risk assessment and identifying the threats to identify the risks and then apply appropriate security controls helps to follow that path, that methodology, to apply the appropriate controls. So understanding CUI in your organization and what CUI is that you are handling, where you are storing it, who is processing it, what systems does it pass through, is a pretty big first step too as well. You can't apply the appropriate controls if you don't know where the information or where the data rests. So understand that the CUI in your organization is a big key factor as well to accomplished NIST 800-171 and CMMC.

So an organization is going to need to have some policies and procedures around how CUI and sensitive data is handled within their organization. Policies and procedures are big part of NIST and CMMC compliance, and that's a big lift for a lot of companies that are smaller and maybe don't have those sorts of things already sorted out. Where technical controls are implemented: and if you look at NIST and CMMC a lot of people just assume it's a lot of technical, IT related controls which a good part of it is, but really a big secondary part of that is the policies and procedures that dictate how these things are implemented, and that's a big part of NIST and especially CMMC.

So organizations are going to need to make sure that they have a mature set of policies and procedures that really showcase what the expectation is from management on how information and things are protected and then also the procedures to back that up on how those things are actually done on a day-to-day basis.

00:18:07 Krista

Do you have an example of one of those non-technical controls?

00:18:12 Josh

Absolutely, so one of the controls in NIST 800-171 and CMMC specifically refers to an on boarding of a new employee. Are you verifying that that person is who they say they are? Are you verifying that they are authorized to access your computer systems and data? And generally, you're going to have an HR process for on boarding people: an interview is conducted, management interviews that person they give the go ahead, the person gets hired, that gets moved on to HR. HR starts to do the onboarding and does the background checks and all that. So you know, that's one of those things where that's not a technical control, but that is a procedure that you're going to prove that you follow and that’s going to be something that has to be documented, it has to be written down, to show and have evidence of that. That’s a natural one for most companies, but a lot of these other controls for small businesses is where a lot of effort needs to be put in. Because what we’re hearing out of the CMMC pilot programs right now, those contracts that they decided to test and initially pilot CMMC compliance, is that documentation is what’s really lacking for a lot of businesses. And that’s here a lot of efforts are going to need to be put into have those policies and procedures that are not normally documented for a small business because it is all just word-of-mouth, or people just don’t have the time to do all that paperwork, and that’s a big lift for small business to write all that stuff out, to have everything documented about how they do everything day-to-day operations and all that stuff.

And that could be a good opportunity for a company to bring in an outside resource to help them with all that documentation, to really tie all this stuff together, all controls together into policies and procedures which they can actually leverage on a day-to-day basis that makes sense for them.

00:20:01 Krista

Yeah, and I think that's a great transition to what our next episode is actually going to be, which is diving into that role of what documentation plays into being NIST and CMC compliant. So stay tuned for that! But for now, Josh, thanks so much for joining us. Thanks for all of our listeners and stay tuned for next episode going over that documentation compliance.

00:20:34 Outro

Thank you for listening to Cybersecurity Magnified. Make sure to subscribe wherever you get your podcasts, so you're up to date with our newest episodes. And if you found this episode helpful, share it on social media. Braxton-Grant is an experienced cybersecurity solution provider with over 20 years of experience in the government and commercial space. To learn more about us, visit braxtongrant.com or find us on LinkedIn. Thanks again for listening!