TRANSCRIPT OF PODCAST

Federal Credit Fridays: Information Security Compliance (3 of 3)

***DISCLAIMER: This is a draft transcript that was automatically generated. It is meant as an accessibility aid for the associated podcast, not an official record.*

00:00:04 Intro

Connecting you with thought leaders and experts in federal loan programs. This is Federal Credit Fridays with your host, Anthony Curcio.

00:00:18 Anthony

Hello, I'm Anthony Curcio and this is the latest episode of Federal Credit Fridays. Over the last two episodes, we've been building a framework for understanding IT compliance and federal credit. We started by exploring what makes this environment different, from the scale and lifespan of the data to the strict requirements around handling controlled and classified information. Then we turned to how organizations are responding, looking at cloud architecture, fed ramp environments, and the practical realities of building compliance systems that can actually perform. Today, we take the final step, and in many ways, the most. What happens when these same compliance challenges intersect with national security priorities? Title credit tools are increasingly used to support national defense and industrial policy objectives. A new layer of requirements is emerging. Programs tied to the Department of War and related initiatives are introducing frameworks such as the Cybersecurity Maturity Model Certification or CMMC, which move beyond self-attestation and towards independently verified compliance. This is a meaningful shift. The expectation is no longer simply that organizations understand and implement security controls, but that they can demonstrate it credibly and repeatedly that these controls are operating. For contractors and advisors working in federal credit, this raises the bar on everything from system design to documentation to day-to-day operations. So my question for us today is, how does the compliance landscape change when federal credit meets national defense? And what does that mean in practice for organizations operating in this space? To help us with this question to close out our three-part series, I'm once again joined by Josh Baker.

00:02:03 Anthony Curcio

Josh brings hands-on experience working with federal cybersecurity frameworks and translating them into operational systems. His work includes supporting environments that must meet evolving standards, such as NIST 800-171, and as I mentioned before, CMMC, where

compliance is not theoretical, but tested, validated, and enforced. Josh, welcome back to the podcast.

00:02:29 Josh Baker

Great to be here, Anthony.

00:02:31 Anthony Curcio

Well, National Defense, it always feels so, but it feels like these days we're living in times of increasing tension around the world and where national defense is a priority. And our leaders and lawmakers, the president and Congress is increasingly reaching to using federal lending and federal credit tools for everything to selling weapons to our allies, to investing in our industrial base, And so what we're seeing, as I mentioned before, you came as an increasing use of federal credit in national security. So I'd like to talk to you about how the stringent standards that you've referenced earlier get even tougher, I think, in a national security environment. So let me just open the door here. I mean, how do you think compliance landscape changes when we start talking about the War Department or national security loan programs?

00:03:26 Josh Baker

We're living through a major change in how the Department of War maintains information security. And that's coming in the form of a program called CMMC, which stands for Cybersecurity Maturity Model Certification. And it's intended to verify that defense contractors are actually protecting the data in the way that they say they are. And so the shift is really coming in the form of third party assessments, no longer allowing contractors to just check a box, sign their names, and claim to be compliant. They're going to actually go in and have some assessors make sure that they're compliant. And so right now that's going through a phased implementation and it's going to be a requirement for anyone that wants to work with the Department of War.

00:04:15 Anthony Curcio

Wow. So let me dig into that a little bit because as I'm obsessed with federal lending, but maybe for just a moment, I'll expand the lens here. The War Department is one of the largest purchasers in the world for contract services, maybe the largest as far as I know. Are you saying that every single contractor will need this certification? And is there any ability to waive it?

00:04:38 Josh Baker

There's no ability to waive that once this program is fully implemented. You know, we are government contractors, we're all familiar with FAR, right? I'm sure you know that one pretty well, Anthony.

00:04:50 Anthony Curcio

Oh yeah.

00:04:52 Josh Baker

Well, you know, DOD has DFARS, which is its own supplemental regulations In 2020, CMMC was put in DFARS as a requirement across the board.

00:05:04 Anthony Curcio

Wow. I mean, that is big. And it's also not something that happened yesterday. It's been around now for, as I've just learned from you, six or seven years. Do you see this as a barrier? Are most contractors who want to provide services, the War Department and other related agencies, defense related agencies, are they complying or is it going to just render some, you know, just left out? I mean, it seems like it would be a barrier to entry.

00:05:32 Josh Baker

Well, I know that they don't want it to be a barrier for entry for organizations that are securely handling data, but I do get the sense that there are some who are working to implement this program who are unsure of how seriously contractors are taking it. I know that there is a push very hard right now as it's being implemented through these phases to get contractors to understand that this is going to be a real thing. And so at Summit, we're taking that very seriously, and we are making sure that we're ready for that. Now, there's also three different levels for CMMC. And let's say that you are a landscaping organization for the Department of War. You are not going to be handling most likely controlled unclassified information, but you do handle government contracts, contracts with the Department of War. So they've put out a level one, which basic safeguarding requirements around contract data.But for an organization like Summit, where we deal in federal lending and any federal financial information falls under a category of CUI, our work would require a level 2 certification from a third party assessor.

00:06:52 Speaker 2

And so they're trying to make allowances for organizations depending on the type of work that they do. And if you handle CUI, CMC is the NIST 800-171 controls, which really you should be implementing anyway.

00:07:09 Anthony Curcio

Exactly. And I just want to point out that this is distinct from concepts like facilities clearance or even secret clearances for staff.

00:07:20 Josh Baker

It is, yeah. So the National Archives and Records Administration, NARA, was actually put in charge of the CUI program, and it's up to them to decide what those different categories of CUI are. So when I say that federal financial information is a category of CUI, it means that it is listed in the NARA's CUI registry. And so when you start talking about top secret or secret clearances,

you're talking about classified information. And the CMMC program is designed specifically for contractors that handle unclassified but controlled information.

00:08:01 Anthony Curcio

Right, that's exactly the kind of challenge that a national security infrastructure of our government that is dealing with private companies that may be innovating new technologies or may be securing America's critical supply chains. These are private companies. And so the information about those companies is not necessarily going to be secret or top secret, but it's going to be controlled on classified data, which I guess leads us back to the need for the CMMC.

00:08:30 Josh Baker

That's exactly right. You have blueprints or plans that they need to build something for the Department of War, and it may not be categorized as classified, but it's still very sensitive information that the Department of War needs to know that you're not just saying that you protect it and safeguard it, but that you can prove to a third party that you do those things.

00:08:55 Anthony Curcio

Interesting. And as I'm sure the type of data that we're dealing with primarily in a loan program is financial data about applications, applicant materials, which could contain sensitive information about plans for those project sponsors.

00:09:11 Josh Baker

That's right. You're going to have in financial information probably various types of personal identifiable information, business sensitive information. So all of that is going to be considered CUI.

00:09:26 Anthony Curcio

And it sounds like this is a step up. I'm sure that, I'm not sure, but I'm guessing that the War Department and, which including the Defense Department goes back, generations has been concerned about this information before. I'm sure this is not the first generation. So why do you think we're tightening up or buckling down? Like what was it? Why the change, I guess, in 2020? I ask you to speculate maybe.

00:09:52 Josh Baker

That's a good question I mean, my understanding is that we just have had too many instances of defense contractors having data breaches. And when looked at more closely, their self-attested controls were not implemented in reality. And so It just became, I think, that the stakes are too high for the government and specifically the Department of War to just allow their contractors to say that they're compliant without actually showing it.

00:10:30 Anthony Curcio

Got it. Well, Josh, It's time for us to wrap up. I don't want to wear our listeners out for too long. Let me ask you, are we ready?

00:10:38 Josh Baker

Oh, absolutely, So CMMC pulls on NIST 800-171 controls. Those are not new to Summit Those are things that we are familiar with. We also hold an ISO 27001 certification, which has a lot of similar best practices. We are well positioned to participate in the CMMC program and bid on work for the Department of War.

00:11:03 Anthony Curcio

Okay. It's a great place to wrap it up. Josh, once again, I want to thank you not only for today, but for this three-part series. It's been great and I've learned a lot.

00:11:11 Josh Baker

Awesome. Thanks so much for having me, Anthony. It's been fun.

00:11:14 Anthony Curcio

Until the next episode, this has been Federal Credit Fridays.