

## TRANSCRIPT OF PODCAST

### Federal Credit Fridays: Information Security Compliance

*\*\*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.*

---

*Intro*

*00:00:04,000*

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

*Anthony Curcio*

*00:00:19,400*

Hello, I'm Anthony Curcio, and this is the latest episode of Federal Credit Fridays. Today we're kicking off a three-part series on a topic that sits just beneath the surface of every federal lending program, information security compliance.

Federal credit programs are at their core financial operations.

It's underwriting loans, managing portfolios, and deploying capital.

*Anthony Curcio*

*00:00:41,841*

But what's often less visible is the technical infrastructure that supports those activities and more importantly, the compliance requirements that govern how that infrastructure is designed and operated.

Unlike many other federal activities, federal lending programs must manage large longitudinal data sets that persist over years and even decades, while remaining subject to evolving audit standards, re-estimate cycles, and strict controls around data security.

This creates a distinctive operating environment where compliance is not simply a matter of policy adherence, but a continuous balancing act between accessibility of that data

*Anthony Curcio*

*00:01:21,881*

performance of the models, and protecting the data itself.

Frameworks such as NIST 800-171 and handling of controlled unclassified information and the broader lifecycle management of federal data impose requirements that are both rigorous and often fundamentally different from what you might encounter in a typical commercial setting or even in other parts of the federal government.

*Anthony Curcio*

*00:01:45,681*

So the question that I'm asking today is pretty simple.

What makes IT compliance in federal credit different, and should we care?

Does it really matter? To help us explore that question, I've invited Josh Baker to join the conversation.

*Anthony Curcio*

00:02:03,042

He's a technical subject matter expert here at Summit who designs and operates compliant IT environments supporting federal lending programs.

His experience spans data architecture, secure data handling, and the practical implementation of federal cybersecurity frameworks.

That includes managing large data sets, controlling CUI, and ensuring those environments meet stringent federal standards.

Josh operates at the point where compliance requirements are translated into real systems that must perform at scale and withstand the scrutiny from auditors and oversight bodies alike.

Let's meet Josh.

Well, Josh, welcome to the podcast.

*Josh Baker*

00:02:46,642

Hey, Anthony.

Thanks so much for having me.

*Anthony Curcio*

00:02:49,362

Well, before you joined, I introduced you and you know, you're an IT specialist and information security specialist.

I don't know if you've noticed, but we love to talk about loans around here. And before you came on board, I was pointing out how the needs around loans are different.

But knowing that they're different is kind of as far as I get sometimes.

So I'm hoping you can shed some light on that.

*Joshua Baker*

00:03:12,242

man, I'm happy to.

And I completely agree that working with loans and especially federal loans, it does seem like a bit of a different beast.

So when I think about that, I think about it from 2 perspectives.

One is that when you are dealing with loan data, it's large data.

It's files that are pretty large and that most people deal with like a Word document, it's a pretty small file.

But if you're receiving a spreadsheet that has millions of loans in it, it can get pretty sizable. And so we have to spend a lot of time thinking about how we're going to store, transmit, and process files of that size. And then when you are adding on to it that it's federal loan data, you have to make sure that you're storing and processing and transmitting that data in a way that's compliant with federal requirements.

*Anthony Curcio*

00:04:14,563

Interesting. Well, Josh, before I, you know, I'm just eager to dive right into some of these questions. How long have you been doing this?

How long have you been doing this in the federal lending space?

*Josh Baker*

00:04:25,923

Yeah, sure. I've been with Summit for right around 10 years, and I've spent that time learning all the answers to what I was just saying.

How do we make this work?

How do we handle such large data sets, give our analysts access to that data in a way that they can use it?

*Anthony Curcio*

00:04:44,404

Well, I didn't tell you I was going to ask you this question in advance, but now I'm kind of interested. Ten years is a long time. As a federal credit expert and someone who deals with federal credit modeling, I think I've detected a big increase in the amount of data that we're using. How do you compare the kind of the levels of data that we're using now to what we were using, you know, 10 or even only five years ago? Has that changed a lot or a little?

What are some of the big trends that you've seen in the size of the data sets that we're using now?

*Josh Baker*

00:05:19,044

Sure. That's a good question. I don't know if it's the individual data sets that necessarily have grown in that time, but certainly, federal loans last for decades. And so when Summit takes on work with the government to help service those loans, we're collecting data across many years. And so there are some projects that we have, that are always just going to have a steady rate of growth in the data.

And if you don't plan for that, you're going to have a situation where you're running around to all of your employees saying, hey, I need you to delete things. I need you to delete things or else we're going to run out of space.

*Anthony Curcio*

00:06:02,005

Yeah.

*Josh Baker*

00:06:02,645

And I say that with. I remember those from the old days.

*Anthony Curcio*

00:06:05,445

Yeah.

*Josh Baker*

00:06:06,085

Well, I was about to say, I, of course, say that without any real-life experience, but we know that's not true.

*Anthony Curcio*

00:06:12,965

Well, so let's get to the compliance requirements, security requirements. You know, what does it mean to support federal lending versus, let's say, a commercial client?

*Josh Baker*

00:06:25,925

Sure. I mean, the truth is, I think about, you know, protecting data, safeguarding data is going to be done in a similar way no matter where you are. But when you are working for the federal government, they have outlined very specific requirements in order to protect, you know, the American people's information. And so we have that added accountability to some of the regulations that come from being a federal contractor. For example, data that is financial in nature is going to fall in the category of controlled unclassified information.

Back in 2010, President Obama signed an executive order that established the CUI program and made it enforceable on all federal contracts, that contractors were required to safeguard that kind of data. Then the National Institutes of Standards and Technology, NIST, has developed a set of security controls in their document, Special Publication 800-171, And that is the expectation that contractors have on them in order to safeguard that data.

*Anthony Curcio*

00:07:42,486

So Josh, I'm going to reach back in the Wayback Machine. I've been doing this stuff for a long time. And I can remember back in a day where, you know, we just encrypt something and attach it to an e-mail. I don't know if you still remember those days, but.

*Josh Baker*

00:07:55,526

Sure.

*Anthony Curcio*

00:07:56,486

That's how we used to solve it. But are there unique compliance challenges that arise when you work in this particular industry? Are there controls that govern how we exchange data? And you know, when I think back to those, the olden days that just don't allow that anymore or is that not really related to standards?

*Josh Baker*

00:08:14,726

no, that's definitely related. There are specific controls in that NIST special publication that speak directly to that question. And the answer is going to depend on the contractor information system and how it's run.

Now, this is where you can talk about the specific challenges of working with federal credit information. We've talked about how large those data sets can be. Well, even if you were able to securely encrypt and attach a file to an e-mail, that's not going to work with our data. And so

we've had to make sure that we know other alternative methods of exchanging information, exchanging data that is protected in transit and at rest. These are all parts of the requirements. So things like SFTP servers, which is the Secure File Transfer Protocol, sometimes SharePoint. It really depends on the client. Anthony, I'm sure you can remember some clients wanted to have an encrypted hard drive hand delivered to them.

*Anthony Curcio*

*00:09:17,687*

I remember that.

*Josh Baker*

*00:09:19,047*

That's also within the realm of possibility.

But you really have to be sometimes creative when you're dealing with large files.

*Anthony Curcio*

*00:09:27,927*

That's interesting. And it sounds like you're talking about large files. You know, I'm obsessed with federal credit. Can we dig into that?

*Josh Baker*

*00:09:34,847*

What about federal credit specifically?

*Anthony Curcio*

*00:09:37,927*

Is are there specific things to federal credit or is this kind of or are these evolving standards around data security?

*Josh Baker*

*00:09:45,928*

Well, those standards are going to apply across the board. And so I think it just comes back to applying those standards in a in an environment that is dealing with federal credit and a specific challenges We've spoken about the data transit challenge. There are also the fact that we deal with loans and loan programs that the government audits on a regular basis. The government will go back and audit a fiscal year, and we are... Responsible for holding on to data from that fiscal year to make sure that it can be audited and reported and referred back to in order to verify and validate results that our analysts come up with, and so... Whereas maybe a normal business can set a data retention lifecycle of three years. After three years, if it hasn't been touched, go ahead and automatically delete it. Well, that doesn't necessarily apply when you're talking about government financial data. And so that's an extra layer that we have to consider in terms of how do we maintain and keep our data and keep it secure, but not beyond the time that would be reasonable.

*Anthony Curcio*

*00:11:04,009*

Well, Josh, as we get close to the end of our time together, I want to invite you back because this is a three-part series, as I warned you before. And in our next time together, I'd like to switch from defining the problem or understanding the challenge and to move to solutions. And I want to talk about cloud computing. Shared responsibility models and FedRAMP. If you're game to come back, I'd like to get back together and talk about some of those solutions. How does that sound?

*Josh Baker*

*00:11:34,449*

Are you kidding, Anthony? It's not often I get asked to talk about this. So I'm happy to come back and discuss it. Absolutely.

*Anthony Curcio*

*00:11:42,569*

No, I'm learning how important this stuff is, whether I like it or not.

*Josh Baker*

*00:11:45,449*

Okay.

*Anthony Curcio*

*00:11:46,409*

Well, Josh, thanks again for joining today's podcast. And until the next time, This has been Federal Credit Fridays.