Redspin®
A Division of Clearwater

CMMC: The Time Is Now

Redspin's Teague and Graham on How Entities Must Prepare for Compliance

ISMG
INFORMATION SECURITY
MEDIA GROUP

Robert Teague

Teague has over 30 years of leadership in cybersecurity and information technology. He assists clients in understanding, preparing for and achieving CMMC certification for Department of Defense contracts. With a focus on long-term compliance, Teague provides comprehensive guidance and support. His expertise ensures clients are well-prepared and equipped to navigate the complexities of CMMC, enabling them to secure and maintain their contracts successfully.

Thomas Graham

Graham oversees internal security matters at Redspin. He is an expert in CMMC and played a pivotal role in Redspin becoming the first authorized C3PAO and conducting DIBCAC High CMMC assessments under JSVAP. Graham received a FedHealthIT award while supporting the Defense Health Agency and speaks at industry events such as the National Cyber Summit and ISC2 Security Congress.

"Stop waiting; start preparing." This is the message from **Robert Teague** and **Thomas Graham** of Redspin, a division of Clearwater, regarding the U.S. Department of Defense's Cybersecurity Maturity Model Certification. CMMC is coming, they say, and now is the time to get ready.

In this video interview with Information Security Media Group, Teague and Graham discussed:

- The urgency behind CMMC;
- Why CMMC is not going away;
- What "Stop waiting; start preparing" means practically.

“The urgency has to do with the increase in cyberattacks in recent years that served as a wake-up call to the Department of Defense that they needed to shift their mindset from a reactive cybersecurity stance to a more proactive stance.”

– Robert Teague

Status of the CMMC Rule

TOM FIELD: What is the status of CMMC, and why is it so urgent, particularly now?

ROBERT TEAGUE: The CMMC rule is sitting in the White House’s Office of Management and Budget in the division of the Office of Information and Regulatory Affairs. They’ll have it for a 90-day period where they’ll review it. Then they’ll release it for a 60-day public comment period sometime this fall. Once that’s complete, the DOD must address all the comments that have been adjudicated or at least put on for the rule. And then sometime in 2024, that rule should be finalized. By the end of that year, we should see verbiage in the contracts for the contractors.

The urgency has to do with the increase in cyberattacks in recent years that served as a wake-up call to the Department of Defense that they needed to shift their mindset from a reactive cybersecurity stance to a more proactive stance. They are relying on industries such as Redspin and other partners to assist them in this, due to their limited resources within the Department of Defense.

The Joint Surveillance Program

FIELD: Why has the Interim Joint Surveillance Voluntary Assessment Program been so important to this point?

THOMAS GRAHAM: The Joint Surveillance Program, as it’s commonly known, is an early adopter program. Originally, when CMMC came out, it was going to use a phased approach, and within the first year, there was going to be a limited number of contracts that would be those early adopters. Since CMMC has gone through some changes, what can the department do to see if this program is viable? Does it have merit? Are organizations going to be able to get through it? So they came up with the Joint Surveillance Program. It’s a joint assessment via DCMA DIBCAC, which is one of the DOD’s assessment arms, and the C3PAOs, which are the certified third-party assessors for CMMC.

The C3PAOs conduct a NIST 800-171 assessment in conjunction with the DOD DCMA team, performing what’s considered a DIBCAC hot. This is done so that they can see the processes and procedures in action. Are they going to work?

Are there shortcomings or hiccups? If there are, the C3PAOs can then provide information back to the Cyber AB and the DOD, to tweak the program before the final rule goes live or the CMMC assessment process is formally released.

The second part is to get organizations going. Upon successful completion, a couple of things happen. If you pass a joint surveillance assessment in the short term, you receive a DIBCAC high certification. The department and the Cyber AB have told the C3PAOs multiple times that once the final rule is complete, that DIBCAC high will convert to a CMMC Level 2 certification. That gives the early movers an advantage in the ecosystem. It's one of the ways the department is trying to get things moving while we're waiting on the final rule.

CMMC Is Here to Stay

FIELD: So despite the rumors that say otherwise, CMMC is not going away. What does that mean to our audience today?

TEAGUE: The audience should be aware that CMMC is merely a validation of the requirements that are already in place. The DFARS, or the Defense Federal Acquisition Regulation Supplement 252.204-7012, was mandated Dec. 31, 2017. It told contractors they needed to employ NIST 800-171 as a base security network framework. It was originally established that those contractors would self-attest that they are abiding by those 110 practices. But after numerous spot checks and data breaches, loss of funds, etc., the DOD opted to enlist the assistance of industry to help validate those requirements, which is where CMMC is coming from.

CMMC is not going to go away. In fact, many contracting organizations are already talking with the C3PAOs and getting on their schedules now. Many are still waiting for the rule to finalize, and some are listening to those rumors that it's going to go away. This latter group will be stuck in the doors waiting to get in when the rule goes final. The question for them is: What are your competitors doing? If they're already in line, they have an advantage over you.

Stop Waiting; Start Preparing

FIELD: You said, "Stop waiting; start preparing." What does that mean, and what should contractors do first?

GRAHAM: All this comes from the DFAR 7012 requirements, which have been enforceable for multiple years now. This is why every C3PAO out there, as well as various folks from the Department of Defense, continue to say, "Stop waiting; start doing." The requirements have been there for seven years. All of these organizations that are waiting to start are putting themselves in jeopardy of being behind their competitors when the final rule hits and CMMC goes live. And they are also putting themselves at a disadvantage with being able to accurately self-report their NIST 800-171 score into the SPRS system, which is the Supplier Performance Risk System. This is one of the requirements under DFAR 7019, which is already enforceable.

If an organization continues to wait, it will fall farther behind its competitors. On average, it takes eight months to a year to be able to get everything in place. And even for those organizations that have been doing it, as we've been conducting joint surveillance assessments, we're finding they still are having misunderstandings about what the requirements are. So stop waiting; start preparing. Reach out to a C3PAO, the RPOs and all of the folks in the ecosystem. We're here to help you so you don't get in trouble with anybody.

False Claims Act Cases

FIELD: What are your thoughts on the rising allegations under the DOJ Civil Fraud Initiative, particularly related to the False Claims Act and cybersecurity? I'm thinking about the evolving cases of Penn State and Verizon. Do you expect these to become more common in the near future?

TEAGUE: I expect it to be more common and, based on the Department of Justice's website, I believe they are sticking to their guns. According to them, they are ensuring that the citizens' tax dollars are protected from fraud and abuse. That includes those that are not abiding by the current

"If an organization continues to wait, it will fall farther behind its competitors. So stop waiting; start preparing. Reach out to a C3PAO, the RPOs and all of the folks in the ecosystem. We're here to help you so you don't get in trouble with anybody."

– Thomas Graham

regulations for cybersecurity. In the fiscal year ending Sept. 30, 2021, they obtained more than $5.6 billion in settlements and judgments from civil cases involving fraud, False Claims Act cases, and improper cybersecurity practices. It's definitely going to be more common. The False Claims Act is one of the most important tools available to them to deter and hold accountable those who seek to misuse the funds or not comply with the regulations. Also, apparently, they have been increasing their number of personnel, specifically to address the False Claims Act cases and any future findings that come across.

The Redspin Approach

FIELD: Redspin is a division of Clearwater. How are you helping your customers now prepare for CMMC?

GRAHAM: As the first authorized C3PAO under CMMC, Redspin helps our organizations, customers and clients in several different ways. We can help consult with an organization. That means we can help them get ready for an assessment and point out any issues they may have overlooked. We can take all of the information that we've accumulated through doing joint surveillance and being in the ecosystem as long as we have and give them actionable intel. We can point out any shortcomings that they may not have thought of, or things they may have thought were implemented correctly but were not.

The second way that we can help organizations is training. In addition to being an authorized C3PAO, Redspin is also an LTP. An LTP is an organization in the CMMC ecosystem that is authorized to provide certified training that is put in place by the CACO, which is one of the organizations under the Cyber AB. Currently, there are two live certifications – the CCP and the CCA. CCP stands for certified CMMC practitioner.

The CCP is the entry-level certification for any individual that wants to operate within the ecosystem, potentially as an assessor. We advocate for any of our clients or customers to send somebody to CCP training because it provides an overview of how we got to this point, what the governance is and how to do scoping and go through the process. It goes through all 110 practices in 800-171 from both a consulting standpoint as well as a practitioner standpoint. For those folks that want

to take it a step further, there is the CCA, or CMMC Certified Assessors certification. CCAs are the individuals that perform the Level 2 assessment of an organization that stores, processes and transmits CUI, under the requirements of CMMC.

The third way that we can help organizations is that, as an authorized C3PAO, we can certify. We can do the assessments, which are based on the CMMC assessment process that will be published after rule-making by the DOD and the Cyber AB. We also offer managed services – full-service, cost-effective, managed services, cloud services and managed security and compliance services that have been built from the ground up with CMMC in mind.

One of the prevailing questions is: Once the final rule comes out, to what standards will the MSPs, MSSPs or other external service providers be held? Because we have built services related to CMMC from the foundation, our customers can be assured that once they go for assessment, having these third-party services will not be a detriment but rather an asset to their organization.

Next Steps for CMMC

FIELD: What do you see on the CMMC horizon?

TEAGUE: First of all, the rules have to get finalized, which should be sometime early next year.

From there, they need to continue building the ecosystem. Right now, I believe, there are 48 certified third-party assessing organizations. There are about 150 certified assessors, and only a limited number of them have been blessed by the Department of Defense. That ecosystem definitely has to grow in order to tackle the number of assessments that have to be conducted for all these contractors.

Once that's done, NIST 800-171 Revision 3 is going to be released around the same time the CMMC rule goes final. That is going to have to be adjusted into the program and revamped at the end of next year or sometime in the following year. Then, the DOD needs to shift its focus to our overseas partners in Australia, Germany, Japan, etc., who are providing valuable services to the Department of Defense and the organizations overseas. Therefore, they will have to fall in line with the CMMC assessments.

About Redspin, a Division of Clearwater

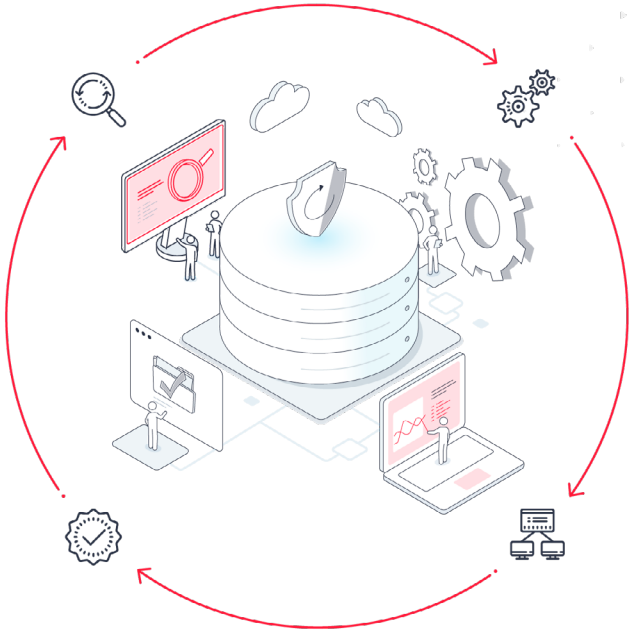
Redspin, a division of cybersecurity and compliance company Clearwater focuses on improving the cyber readiness and resiliency of federal and Defense Industrial Base (DIB) organizations. As the first Authorized CMMC Third Party Assessment Organization (C3PAO), Redspin has the expertise and experience to help organizations achieve CMMC compliance, minimize cyber risks, and protect sensitive information. To learn more, please visit **www.redspin.com**.

Assessments

Our collaborative approach ensures a smooth assessment for your organization's certification needs, no matter the Level.

Training

Help your company prepare for CMMC. Learn from a true CMMC expert trainer and assessor.



Managed Services

Full-service, cost-effective CMMC targeted Managed Security, IT, and Compliance services.

Consulting

Understand my gaps and where I need to prioritize my team's efforts to remediate in preparation of certification.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach TODAY (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io