

# EXPERT EDITION

## Supply Chain Risk Management

### INSIGHTS ON SUPPLY CHAIN MANAGEMENT FROM:

- DoD
- NIST
- NTIA
- CISA

BROUGHT TO YOU BY:  
**carahsoft.**

# Count on Carahsoft<sup>®</sup> and Our Partners for CMMC Products and Services

Supporting efforts to improve cybersecurity postures  
and ensure compliance

In support of the Defense Industrial Base effort to comply with NIST 800-171, the interim DFARS rules and CMMC, Carahsoft and our reseller and vendor partners deliver products and services to address the cybersecurity controls within the framework. Carahsoft CMMC experts can help organizations identify the services, training and technology — delivered on premises or in the cloud — that will address their specific needs, including solutions from the following vendors:

				
				
				
				View all of our CMMC Vendors: <a href="https://carah.io/CMMC">carah.io/CMMC</a>

To learn more, visit Carahsoft's CMMC resource portal at [carah.io/CMMC](https://carah.io/CMMC) or contact the CMMC Team at (703) 230-7414 or [CMMC@carahsoft.com](mailto:CMMC@carahsoft.com).

**carahsoft** The Trusted Government  
IT Solutions Provider<sup>®</sup>



## TABLE OF CONTENTS

CMMC accreditation body promising more transparency, better results...**2**

3 strategies for remediating cybersecurity risk...**4**

U.S. preparing key supply chain rule changes for this summer...**7**

Automating compliance means security, compliance, and CMMC...**9**

NIST updates 'crawl, walk, run' maturity model for cyber supply chain risk management...**12**

SolarWinds exposed an oversight in CMMC controls that could have serious implications ...**15**

New version of CISA SCRM report includes assessments of impact, mitigation strategies...**18**

CMMC exempts COTS software, but vendors should prepare for change...**20**

NTIA wants to standardize 'list of ingredients' for software supply chain risk...**23**

Government should look to industry for a software supply chain security model...**25**



Concerns about the federal technology supply chain have been growing exponentially over the past decade. But it was only with the SolarWinds incident that agencies and industry grasped the real consequences of the challenge.

This is why there are several complementary initiatives trying to accomplish the same goal: Ensure the software and hardware agencies use is secure from foreign or criminal attack.

The Defense Department's Cybersecurity Maturity Model Certification (CMMC) has received the most attention. DoD is trying to move industry toward a safer posture, particularly in how contractors protect their data. CMMC still is months, if not years, from fully rolling out and Matt Travis, the new CEO of the CMMC Accreditation Body, said the goal is not to waste time or money on the way to that goal.

Other initiatives like the Commerce Department's National Telecommunications and Information Administration (NTIA) software bill of materials and the Cybersecurity and Infrastructure Security Agency (CISA) new threat evaluation guide are trying to address technology vulnerabilities at other points of the supply chain.

Underlying all of these efforts is the National Institute of Standards and Technology special publication 800-161, which outlines evergreen principles for agencies to stand up supply chain risk management program offices. The agency recently released its first major revision to the document, which reflects on a yearlong effort to update the publication with the latest SCRM controls and risk assessments.

This e-book highlights some of the major efforts going on across government to not only secure the technology supply chain, but have a long-lasting impact on all users of technology.

**Jason Miller**  
**Executive Editor**  
**Federal News Network**

# CMMC accreditation body promising more transparency, better results



BY JASON MILLER

**T**he Cybersecurity Maturity Model Certification (CMMC) initiative has been and continues to be the talk of the defense community for much of the past year.

The questions about when, how and who are among the most discussed at each event Defense Department officials speak at and at each CMMC Accreditation Body (CMMC-AB) town hall meeting.

This is why Matt Travis, the new CEO of the CMMC-AB, promised more transparency, more speed without losing any rigor and more results.

"I think I have an innate disposition to want everyone to succeed and get along. I think maybe that that notion of the CMMC-AB being in the center of working with the Department of Defense, working with industry, with the media and Congress watching, we want to make sure this program is being implemented successfully," Travis said at the April town hall. "I want to make sure that all of those stakeholders are being satisfied with how CMMC is being implemented."

So far, the satisfaction of the implementation of the CMMC, particularly by the accreditation body, has been unenthusiastic at best.

**"I want to make sure that all of those stakeholders are being satisfied with how CMMC is being implemented."**

**—MATT TRAVIS, THE NEW CEO OF THE CMMC-AB**

## Ongoing analyses of CMMC

Matt Gilbert, a principal with Baker Tilly's government contracts advisory practice who leads a team that conducts reviews under National Institute of Standards and Technology special publications 800-53 and 800-171, said there are several areas where DoD needs to accelerate its efforts.

"The area in which the DoD should focus is making sure there will be adequate assessors to handle the volume. The DoD might want to consider announcing a gating mechanism. A gating mechanism could restrict assessments to only those contractors that will be awarded one of the pilot contracts with the new DFARS 252.204-7021 clause," Gilbert said in an email to Federal News Network. "Adding to the challenge, if the certified third-party assessment organizations (C3PAOs) are not timely assessed by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), then significant portions of the provisional assessors will be on the sideline. Since all assessments need to be registered with the CMMC-AB, the DoD could give instructions that only those contractors that have the 7021 clause in a pending award should be allowed to proceed with the assessment."

For DoD and the CMMC-AB to speed up the process, it will have to first wait for Defense Deputy Secretary Kathleen Hicks to complete her review of the CMMC program. DoD says Hicks' analysis will look for ways to improve the implementation process.

Additionally, Congress also asked the Government Accountability Office to independently assess and brief Congress within six months of an assessment of each major DoD component.

But beyond the series of ongoing reviews and concerns about the speed of the roll out, Travis also must deal with concerns about the AB itself.

"One, you should expect that this system is going to work; that if you're going to spend your intellectual energy, your time to fill application, your money to go ahead and submit the application that you want to believe, that you should believe that the system is functional and responsive, that you're going to get a fair shake, and an even playing field for the company and every other individual who's applying to be part of this ecosystem. We have to deliver that for you," Travis said. "But you should also expect that we're going to be accessible, and that we're going to listen to you. And then we're not going to be behind some audio/visual wall without accountability to you. I don't think that we have a monopoly on good ideas, I certainly believe in the full on free exchange of ideas. And so we'll be looking to make sure that we're accessible – both me personally as well as the entire professional staff here."

## Recommitment to ethics

Additionally, Travis promised an AB that is ethical, which some have questioned over the past year.

"It's not that there is not a very strong ethical culture here. But I don't think we've communicated exactly where our lines are. If you look at our website, there's nice language about our ethics policy. It talks about our commitment to loyalty, commitment to compliance, commitment to duty, it's all very soaring with eagles. And I'm not saying it's not sincere, but what it doesn't do is give you those very specific lines that we view

**"One, you should expect that this system is going to work that if you're going to spend your intellectual energy, your time to fill application, your money to go ahead and submit the application that you want to believe that you should believe that the system is functional and responsive, that you're going to get a fair shake, and an even playing field for the company and every other individual who's applying to be part of this ecosystem.**

**— MATT TRAVIS, THE NEW CEO OF THE CMMC-AB**



ourselves accountable to. So where are those lines and situations of conflicts of interest that, frankly, have to be avoided, that are untenable?" he said. "What are those conflicts of interest that can be mitigated, and how? If there's a potential breach of those lines, what's the process to investigate, adjudicate those? A lot of those are in place, but we've got to make them clear to you what they are. Any time that I've seen in my career, where there might be an ethical question of something, generally, either because the standards weren't high enough, they weren't properly articulated or understood, or they, frankly, weren't being enforced."

Travis said the CMMC-AB started a review of their ethics policy before he joined and the organization will offer more insights in the coming months.

He added the AB is promising to do a better job of articulating and communicating their plans and initiatives with the defense industrial base community. 🤖

So how can federal agencies and contractors move beyond just compliance, and take meaningful steps to a better cybersecurity posture? Steve Baer, chief technology officer for the Americas at Trustwave, breaks it down into what he refers to as “three pieces of pie.”

## 3 strategies for remediating cybersecurity risk

THIS CONTENT HAS BEEN PROVIDED BY TRUSTWAVE



**Steve Baer, chief technology officer for the Americas at Trustwave**

Cybersecurity isn't about eliminating risk, it's about remediating it. Nothing is 100% bulletproof, and what's good today might not be tomorrow. When all is said and done, information has to flow, and cybersecurity is about testing the flows, the outputs and the other pieces and

putting controls around them. The Cybersecurity Maturity Model Certification is a start, but it's important to realize compliance is the floor, not the ceiling.

So how can federal agencies and contractors move beyond just compliance, and take meaningful steps to a better cybersecurity posture? Steve Baer, chief technology officer for the Americas at Trustwave, breaks it down into what he refers to as “three pieces of pie.”

### 1. Test, test and retest

“Test the way a bad guy would. Don't get lured into a false sense of security with some of the compliance based testing,” Baer said. “Not a feel good, warm and fuzzy pen test and map IP ports kind of test, but a realistic risk rating of how resilient is your organization. Can you get knocked over by kids following a YouTube video, or can you withstand 15 minutes of Denial of Service and the backdoor compromises that an adversary would really do?”

Vulnerability scans might work for compliance purposes, but you shouldn't make decisions based off of six month old snapshots. In a hub and spoke scenario, Baer said, ideally everyone involved would have a risk rating of B or better. And while some organizations can be reluctant to spend the budget on this, Baer said that third party testing is the way to go.

It comes down to the idea that compliant does not necessarily equal secure. Plenty of technically compliant organizations have been compromised in the past; credit card organizations are a prime example. New threats and vectors of attack emerge every day. But organizations that are testing effectively are in a continuous improvement model.

## 2. Consulting

Don't know where to start? Having trouble determining the right move? Turn to consultants.

"So policy procedure, does it exist? Is it up to date?" Baer said. "I can't tell you how many times we've been into an organization and we asked about their red book. What's your disaster plan look like? I'm going to pull out a binder and blow all the dust off of it. And you start to go through it and half the people aren't there. Systems have changed. So let's get things back to the right plan, and then testing that plan to make sure it's all effective."

Ideally, organizations would test this plan once per quarter. They also need to think about downstream effects of the longevity of an event. Don't just test the plan; test the failback as well. Organizations need to be diligent about gaming out real-world "what if" scenarios. Consultants can help with that.

## 3. Managed and monitored services

"Managed services and monitored services, that's an uphill battle for a lot of organizations," Baer said. "Most companies, they build a really nice house, and they don't want to pay somebody else to live in it. You put in a lot of infrastructure investment into it. How do you know that you're doing things, right? What we see all the time is organizations buy some fantastic security technology, and they don't use but a third of it. And just because you bought a car doesn't mean you know how to drive."

A lot of organizations have a problem where they've got a ton of data, but they just don't know what to do with it. A lot of times, much of what they've grabbed is worthless from a security events perspective. Managed and monitored services can help organizations get that under control. They can keep an eye on the data 24/7 and report any anomalies. They can also do reporting for third party audits for compliance certifications.

And that's especially useful, because CMMC requires the ability to prove continuous compliance. So organizations may need to show data from months or even years in the past.

"You have to demonstrate that the program is effective, versus just the check the box for compliance," Baer said. "You cleaned up the house before the guest came over. And then once they left you went back to throwing your clothes on the floor. So you have to demonstrate that diligence."

## Just the beginning

The entire Defense Industrial Base is currently focused on meeting CMMC requirements. But CMMC is just the first step, Baer said. He predicted that in a year or two, everyone will be discussing CMMC 2.0, which will bring an evolution of tighter security controls, more diligence, more monitoring and new assets to secure the supply chain.

"Rome was not built in a day," he said. "It's going to take time for all of us to get smarter together and get better together about securing things."



Protect your  
mission  
critical data.

Wherever it is.

---

**GET VISIBILITY, MONITORING  
AND CONTROL OF YOUR  
ENVIRONMENT.**

**[WWW.TRUSTWAVEGOVT.COM](http://WWW.TRUSTWAVEGOVT.COM)**

 **Trustwave<sup>®</sup>**  
Government Solutions





# U.S. preparing key supply chain rule changes for this summer

BY SCOTT MAUCIONE

**T**his summer is shaping up to be a pivotal time for new regulations and reports revolving around how the government will deal with supply chain issues and what it plans to do going forward.

In a few months, the executive branch plans to hammer out the final details of the Federal Acquisition Supply Chain Security Act of 2018, according to Joyce Correll, assistant director for supply chain and cyber at the national counterintelligence and security center for the Director of National Intelligence.

That legislation will let individual agencies make determinations to exclude or remove a particular company from their supply chain.

The authority also provides due process for those companies to challenge an agency's decision to exclude them.

**Correll added that the government is considering how it evaluates “sketchy suppliers” that may need to be restricted, considering it is more a “term of art than of practice.”**

“That’s part of the values that we have as a nation, that under the law there’s a notification process built into the statute to notify the entity that the government is seeking to make such a determination,” Correll said. “And also then allowing that company to have a period of time to say, ‘Wait a minute, you don’t have a fulsome amount of information, we would like to clarify a few things.’”

## Final rule out this summer

Correll said currently the Federal Acquisition Security Council (FASC) has drafted regulations and issued an interim rule, and it expects to issue the final rule later this summer.

Correll added that the government is considering how it evaluates “sketchy suppliers” that may need to be restricted, considering it is more a “term of art than of practice.”

The government is coming up with ways to evaluate technical factors of companies to ensure their viability.

“First and foremost we need to be able to do business with companies that are transparent,” she said. “By transparent, that means we know the ultimate beneficial ownership. We know who the decision makers are, so that we can guard against an untoward amount of foreign ownership.”

Another aspect agencies and industry must take into consideration is responsibility.

“As an example, during a cyber breach a responsible company would immediately notify their customers, their shareholders and the public that something had happened,” Correll said. “For example, I’ll point to what happened with Equifax; they suffered the breach from the Chinese threat actor. A couple years ago, Equifax had been warned that they had poor cybersecurity practices, and they needed to strengthen their cybersecurity. But they didn’t do that. They suffered a breach, and then they sat on it for many days. That’s an example of a company that wasn’t behaving responsibly.”

The FASC, once the rulemaking is done, will collaborate with industry to mitigate risks and find ways to support the vetting of companies.

“There is a requirement to have an information sharing agency to be the executive agent for the government for information sharing,” Correll said. “The Department of Homeland Security and Cybersecurity and Infrastructure Security Agency have been identified as the organizations

for that, but the rules of the road on how that’s going to happen are still being formulated.”

## Supply chain study coming

Agencies will also take into consideration what goods or services a company supplies.

“A mission owner has to be able to assess criticality and the mission owner needs to know what their risk appetite is,” Correll said. “I work in the intelligence community so if I’m buying reams of paper, I really don’t care about risk of those reams of paper. But I do have a very low risk tolerance for IT systems.”

Along with the final rule coming out, the Biden administration plans to release the results of its supply chain study in June.

The White House announced it was going to look into some critical supply chains and beefing up the U.S. industrial base during the first month of Joe Biden’s presidency.

“The goal of these studies is to identify gaps, risks, weaknesses, and try to come up with policy remedies that can be applied to shore up something, maybe some stockpiling is needed,” Correll said. “Also we could put in place some financing if low interest loans are required in a particular area, maybe we have certain trade partnerships with allies.”

She added that over the next year more studies will be conducted on other supply chains. 🚧

**“The goal of these studies is to identify gaps, risks, weaknesses, and try to come up with policy remedies that can be applied to shore up something, maybe some stockpiling is needed.”**

— JOYCE CORRELL, ASSISTANT DIRECTOR FOR SUPPLY CHAIN AND CYBER, NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER, DIRECTOR OF NATIONAL INTELLIGENCE

# Automating compliance means security, compliance and CMMC

THIS CONTENT HAS BEEN PROVIDED BY QMULOS



Automating compliance can make vendors more secure and help them get to CMMC faster.

The Defense Industrial Base is currently focused on achieving the Cybersecurity Maturity Model

Certification (CMMC) as

the Defense Department begins phasing it into contract requirements. Though the certification itself gets a lot of attention, it is important to remember that compliance for the sake of a passing grade should not be the goal. The focus should be about improving operational security, and there is no better way to do that than to track the status of operational security against best practices in real time.

That's actually part of the story for how the SolarWinds hack was discovered, according to Matt Coose, CEO of Qmulos.

"From the stories I've heard, staff at the company who discovered the hack first detected an issue when they noticed one of their administrators was escalating privileges in an account but that admin wasn't supposed to be working. So they called the admin and started investigating. Clearly, they have a robust security program and are monitoring the right things in real-time, but the question is why didn't at least one of the other numerous organizations using SolarWinds catch this?" he asked.

**"Once you automate the collection of security relevant data, you don't have to keep collecting it every time you have an audit. This helps avoid the common 'audit fatigue' that plagues so many companies. You can set it up once, and it's there for you or your auditor's viewing pleasure at any time."**

**— MATT COOSE, CEO OF QMULOS**

There are standard security controls that have been defined for years (see NIST SP800-53) that outline these types of requirements, but not enough organizations actually do them. One specific, relevant example is the AC-02 control, which says you must monitor which admins are taking what actions to create new accounts, delete accounts and modify accounts – which includes escalating privileges.

"The problem is that most organizations still do not, after all these years, actually do this in real-time," Coose said. "Instead they say, 'Hey, give me the Active Directory logs and give me that every three months and give it to me in a paper format. I'll upload it into this static document repository and show my auditor that, yeah, we have that data.' But they're not monitoring it in real time and therefore, are not getting real operational security value out of implementing these controls."

This begs the question: Why not? Coose said there are two ends to the spectrum of organizations who don't do this. On one end are the small contractors, the mom-and-pops with little to no experience with cyber compliance



who are just trying to get to CMMC level one or two. They have to be taught how to start off right and avoid the mistakes of the past in implementing compliance programs. On the other end, there are large organizations who have been doing cyber compliance forever and are stuck in the past, employing legacy products and manual processes.

Both ends of the spectrum can benefit immensely from automating those compliance processes.

"Once you automate the collection of security relevant data, you don't have to keep collecting it every time you have an audit. This helps avoid the common 'audit fatigue' that plagues so many companies," Coose said. "You can set it up once, and it's there for you or your auditor's viewing pleasure at any time."

This approach saves companies quite a bit of money in labor costs. For one, there's no more need for employees to go to operations teams and ask them for outputs from their tools in a static format. And it prevents those operational employees from having to waste time and effort populating spreadsheets with data from their cyber tools in order to satisfy these requests.

Instead, companies as a whole can rely on solutions like Q-Compliance and Q-Audit, Qmulos' real-time compliance software, which sits on top of Splunk and leverages the big data platform to collect technical evidence from any device or tool on the network. Once collected, the data is automatically contextualized into the various security controls and CMMC levels and organized by system and organizational entity to ensure customers are audit ready at any moment. To collect that evidence manually from numerous assets and numerous different data sources for all of the technical controls would otherwise involve logging into dozens of different tools, whereas Qmulos collects them all dynamically in near real time.

"What our customers have seen is that whole problems disappear for the technical controls," Coose said. "We're able to very quickly implement the solution, and show dashboards with data populating in near real time. We eliminate all the labor involved in trying to do that, not only once, but many, many times over the course of however long you want to remain compliant."

"Qmulos' solution enables DoD vendors to achieve CMMC compliance much quicker than traditional methods," Coose said.

Automating the collection of the data could have customers monitoring 30 to 60 technical controls within a week or less. And all it requires is for organizations to leverage Qmulos and make use of their existing tools such as Cisco Products, Microsoft Windows or Linux OS's and Active Directory.

Again, if implemented in a way where the organization isn't just checking a box to meet CMMC compliance, it will make the company more secure. And not just against external threats; monitoring the audit family of controls in real time can give vendors insight into behaviors that could indicate insider threats, such as individuals sending documents outside the network, printing more than normal, or unauthorized file access. These are all controls that are part of CMMC and should be implemented in an operationally valuable way.

"The higher value proposition, beyond just the labor savings and collecting evidence in real time and in perpetuity, is actually the security value an organization achieves by looking at our dashboards and setting up alerts for anomalous events," Coose said. "If you actually implement those 70 technical controls for CMMC Level 3, and you're continuously monitoring them in real time, you're substantially more secure and experiencing ongoing operational security. Yet most organizations still like doing it the manual way. That needs to change to meet the needs of CMMC and the digital age."



# Secure your digital supply chain with real-time visibility.

learn more

You need real-time visibility of your supply chain's security posture because that's what matters. Check-the-box risk management doesn't cut it anymore. Upgrade to Qmulos and find out what you've been missing.

A blurred background image showing a hand interacting with a digital interface. The interface displays lines of code, likely Python, and various data visualizations including bar charts and line graphs. The overall color scheme is blue and teal, giving it a high-tech, digital feel.

```
def operation = "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add back the deselected
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier selected
#mirror_ob.select = 0
done = bpy.context.selected_objects[0]
#the data on which the modifier is applied
```



# NIST updates 'crawl, walk, run' maturity model for cyber supply chain risk management

BY JORY HECKMAN



**T**he discovery of the SolarWinds breach is sparking renewed interest in cybersecurity supply chain risk management (C-SCRM) from agencies and industry.

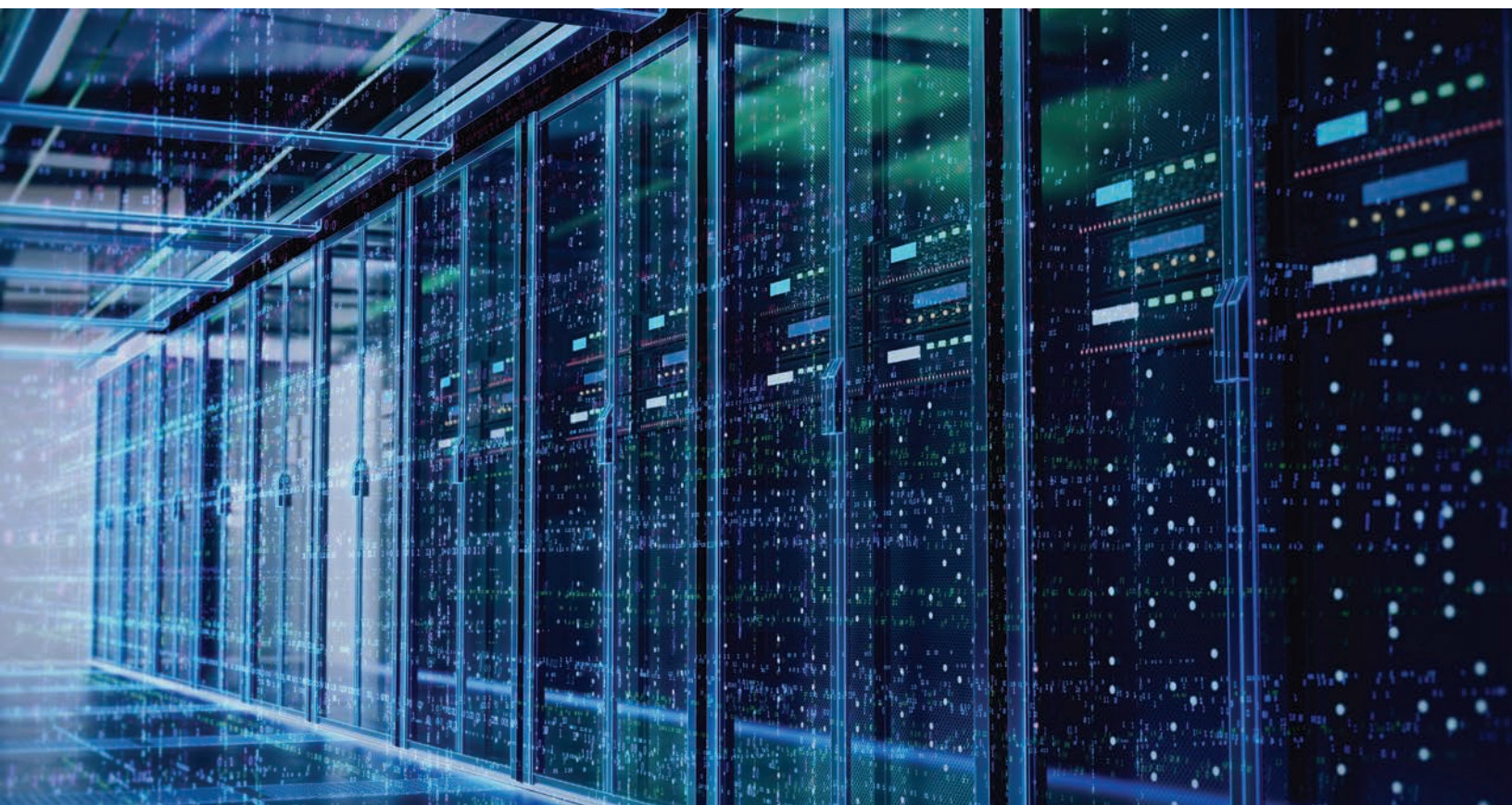
The scope of the breach warrants its high-profile coverage. Anne Neuberger, the White House's deputy national security adviser for cyber and emerging technology, said in February that the breach compromised the networks of at least nine agencies and 100 private-sector companies.

The need to protect federal supply chains from malicious cyber threats, however, has loomed over

agencies years before SolarWinds became a household name.

The National Institute of Standards and Technology released the first version of its Special Publication Special Publication-800-161 in 2015, outlining bedrock principles for agencies to follow in setting up supply chain risk management programs.

The Office of Management and Budget, under the Obama administration, last updated its Circular A-130 memo in 2016 to reflect trends in supply chain risk management and directed all agencies to conduct supply chain management activities.





Despite the rollout of these documents, the Government Accountability Office last year found none of the 23 agencies it reviewed had implemented all seven supply chain risk management practices it identified. More troubling, more than half hadn't implemented any of the SCRM practices.

## High stakes for supply chain attacks

Jon Boyens, the deputy chief of NIST's Computer Security Division, said supply chain threats aren't anything new. In an interview, he said they've been around for the last 5-to-10 years, and while awareness of these threats has grown, so too have the stakes when – not if – something goes wrong.

"Over the last 20, 40, 50 years, technology has grown in its importance and impact. So when that technology fails, the impact to an organization is greater than it ever has been before, because we depend upon those technologies," Boyens said.

While NIST's original SP-800-161 outlines evergreen principles for agencies to stand up C-SCRM program offices, the agency recently released its first major revision to the document, which reflects on a yearlong effort to update the publication with the latest C-SCRM controls and risk assessments.

**"We did a lot of research with departments and agencies before drafting this revision. Most of the changes you will see in this version, the approach is similar to the first draft. However, we've tried to make this version more modular and usable."**

**— JON BOYENS, DEPUTY CHIEF, COMPUTER SECURITY DIVISION, NIST**

Before rolling out SP-800-161 Revision 1, Boyens said NIST spent six months looking at the C-SCRM practices of agencies and gathered feedback on what agencies found lacking in the original SP-800-161 document.

"We did a lot of research with departments and agencies before drafting this revision. Most of the changes you will see in this version, the approach is similar to the first draft. However, we've tried to make this version more modular and usable," Boyens said.

The revision includes different templates for agencies or other organizations to develop C-SCRM strategies and policies.

NIST held a virtual workshop on May 12 to gather feedback from agencies and industry and will accept written comments on the revision through June 14.

In addition to getting feedback from agencies, Boyens said NIST is also looking for feedback from federal vendors to determine what security hurdles they face from their suppliers.

"That's kind of a dual scope that we're looking at from industry -- one as a supplier, and then two as an acquirer themselves within their supply chain," Boyens said.

## Three key practices

The revision also includes key practices generally categorized in three buckets – foundational practices, sustaining practices and enhancing practices. Boyens said these principles follow a "crawl, walk, run, fly approach" to improving maturity.

An agency setting up a C-SCRM program management office meets the criteria for a foundational practice, for example, while NIST considers an agency relying on third-party assessments and formal certification processes to assess critical suppliers a sustaining practice.

**“How can we automate a lot of these functions and practices, capabilities and processes, and then starting to get into the quantitative risk analysis and metrics and measurement to see how efficient and useful some of these practices are?”**

**— JON BOYENS, DEPUTY CHIEF, COMPUTER SECURITY DIVISION, NIST**

Boyens said enhancing practices focus on an agency addressing these C-SCRM problems at scale and building out these principles with automation in mind.

“How can we automate a lot of these functions and practices, capabilities and processes, and then starting to get into the quantitative risk analysis and metrics and measurement to see how efficient and useful some of these practices are?” Boyens said.

As a general guiding principle, however, Boyens said organizations need to follow good cyber hygiene before demanding it from its vendors.

“You can’t ask a supplier to have better cybersecurity practices when the acquiring organization has horrible cybersecurity practices,” he said.

Part of the challenge in standing up a robust C-SCRM program within an organization, Boyens said, is that it requires input from a wide range of disciplines. The Venn diagram, he said, includes an overlap of traditional information security, supply-chain logistics and enterprise risk management.

It also includes input from an agency’s legal department, systems engineers and systems architects.

“So there’s a whole host of folks that should really be brought in. I think some of the challenge is just the very

nature of organizations. Organizations are formed with silos, and so it’s not really breaking down those silos, it’s dealing with the nature of silos,” Boyens said.

## **24 recommendations from government, industry**

Agencies can also borrow from lessons learned in the private sector. Boyens, in a NIST publication released in February, identified 24 key C-SCRM recommendations gathered from industry observations.

The leading industry practice is to integrate C-SCRM through a risk council that brings together different disciplines to focus on the problem.

NIST’s SP-800-161 Revision 1 calls on agencies and industry to take internal risk management steps, like identifying which critical business functions depend on which information systems.

“It’s really trying to find out what are their critical assets within an organization, which they need to spend a greater amount of resources or have more rigorous security around those resources to protect them,” Boyens said.

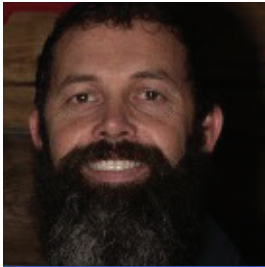
Agencies and industry, looking externally, can apply that same critical approach to their supply chains to identify which vendors supply critical technology.

Boyens said the risk calculus should also consider whether one vendor supplies a huge quantity of products that, on their own, would not be considered critical products or services

“Ultimately, it’s having an organization both looking internally at its critical information systems and components, and then externally looking at those critical suppliers,” Boyens said. 🚫

# SolarWinds exposed an oversight in CMMC controls that could have serious implications

THIS CONTENT HAS BEEN PROVIDED BY ZSCALER



**Patrick Perry,**  
director of emerging  
technology for DOD  
and the Intelligence  
Community, Zscaler

Vendors in the Defense Industrial Base have been preparing for the Cybersecurity Maturity Model Certification for quite some time. But the SolarWinds hack exposed a major oversight in the CMMC process. CMMC was designed to ensure the DIB protects the Defense Department's controlled

unclassified information and its federal contracting information. But it only applies to vendors who actually handle that information directly. Any contractors that provide hardware or software to the DoD and DIB but never handle DoD data aren't subject to CMMC.

And that's a problem, as the SolarWinds breach illustrated in no uncertain terms.

"There is a difference between how the software operates, regardless of its configuration, and then how it's implemented, i.e., how the customer configures it," said Patrick Perry, director of emerging technology for DoD and the Intelligence Community at Zscaler. "The actual environment itself is not your problem, or even how the software was written; it's that user part."

He likened it to the frequent exploitations of AWS S3 buckets. The problem wasn't the underlying code; the problem was user responsibility. Admin passwords weren't changed, access wasn't properly restricted,

and machines caching SAML tokens weren't safeguarded.

"Now shift it back to CMMC and the separation between the CMMC controls, which is a lot more configuration," Perry said. "I would submit to you that the way that CMMC is written implies validating the configuration of or the implementation of software. Say your control is how you block or control split VPN capability. No solution, just by plugging it in, will do that. It's all based on the user configuration and validating that. So that implies that the user's configuration of the software is being validated. That does not, though, imply how the software is working underneath the hood, is actually being validated."

And it's beaconing that's the real threat, Perry said. That's what happened with SolarWinds. The software was exploited, but only to embed infiltration. No damage occurred to any environments until the command and control channel was beacons back out to the adversary. That's when they got access to the environment and began to spread and inflict damage.

"Arguably, CMMC kind of gets to that," Perry said. "There are many controls that involve secure communication, the SC control family, where it says only authorized protocols get through your environment, deny by default, permit only by exception connection requests. So while it kind of gets after the aftermath of the exploit – the destruction phase – it still would have never ever solved the SolarWinds code compromise or the SolarWinds exploit being found within the environment."



This comes back to the fact that hardware and software should require better validation, even if it doesn't directly touch CUI or FCI. Perry said there needs to be another control family of third party hardware and software utilization, because it only takes one weak link to completely compromise the supply chain.

Perry said there are a couple of different ways this could be done. The code itself could be audited.

But that's a massive task due to the sheer amount of code used by some of these vendors, not to mention the intellectual property concerns. Sandboxing and monitoring a capability for beaconing or other malicious activity could be another option. Agencies and DIB vendors could also set more stringent requirements on software, but that too is no easy task.

But Perry also said having a zero trust mindset could have mitigated a lot of the damage done by the SolarWinds exploit. Just because a software has been running in an environment for some time doesn't mean it should be automatically flagged as friendly. Access should be transactional.

Perry also offered some steps for agencies and vendors looking to protect against these kinds of exploits moving forward. First, they need to know their environment. You can't secure something you don't know. Then they should adjust their strategy in how they construct their security as an overlay across their environment. The new reality is that security capabilities become obsolete quickly. This may be painful, Perry warned, but

in the end will not only result in higher security posture, but a simplified approach. With all good things, partnerships should be one of the foundational aspects of this strategy shift, as defense in depth is imperative.

"It's back to the weakest link. One bad partnership in your ecosystem could corrupt your entire risk value chain," he said. "Unfortunately, security needs to be tightened while not impacting

user experience too much or security will be bypassed for convenience. And you have to get better visibility into what you're really doing."

The reality is that these supply chain impacts could potentially delay the adoption of CMMC, Perry said. That would impact roughly 300,000 companies worldwide in a market worth \$300-400 billion per year.

**"Something as catastrophic of a gap as supply chain management within the CMMC process may draw a lot of concern and a lot of angst out there. Where do organizations start with meeting CMMC? What should they prepare for if CMMC changes because of the supply chain?"**

**— PATRICK PERRY, DIRECTOR OF EMERGING TECHNOLOGY FOR DOD AND THE INTELLIGENCE COMMUNITY AT ZSCALER**

"Something as catastrophic of a gap as supply chain management within the CMMC process may draw a lot of concern and a lot of angst out there. Where do organizations start with meeting CMMC? What should they prepare for if CMMC changes because of the supply chain?" Perry said. "Everybody is being forced to pay for a new assessment that might not have actually provided the value expected, which in this case is the security that is required."

# IT STARTS WITH ZERO

Cybersecurity Maturity Model  
Certification & Zscaler.



IMPROVED USER  
EXPERIENCE



BETTER SECURITY



LOWER COST &  
INFINITE SCALABILITY



REDUCED RISK



IT MODERNIZATION



AUDITING SIMPLIFIED

Already meeting the highest levels of government compliance, The Zscaler Zero Trust Exchange will speed up your organization's efforts to meet CMMC accreditation.

Learn more at [zscaler.com](https://zscaler.com)



Certified

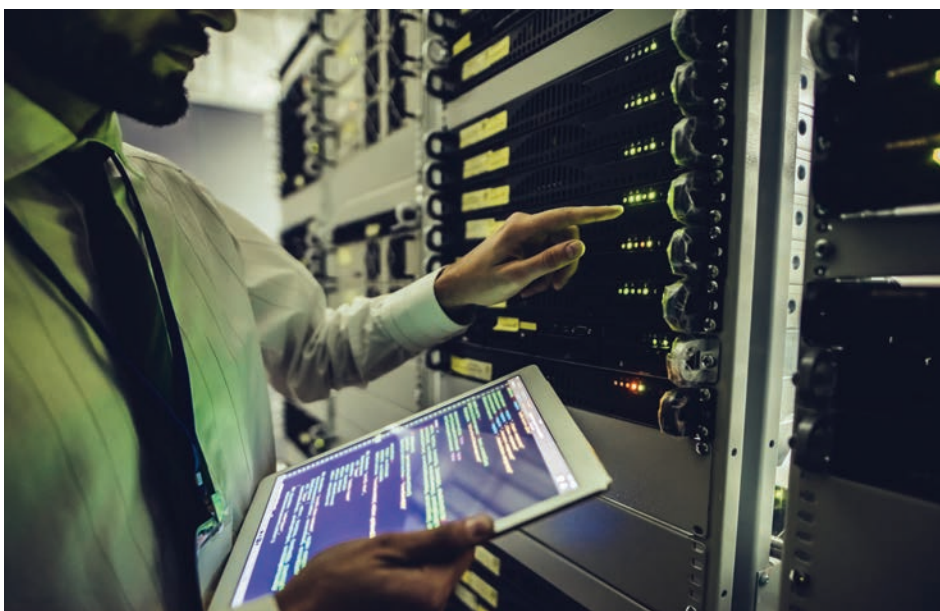
# New version of CISA SCRM report includes assessments of impact, mitigation strategies

BY DAVID THORNTON

The Cybersecurity and Infrastructure Security Agency has expanded one of its task force's reports on supply chain risks. CISA's Information and Communication Technology SCRM Task Force Working Group on Threat Evaluation added new information on threat evaluations, including impact assessments and potential mitigation strategies to its Threat Scenarios Report.

"Whether it's the packets of data that enable the operational functionality of connected infrastructure; or whether it's sensitive data, things like intellectual property and personal preferences and identifiers; whether it's monthly firmware or software updates; one overarching takeaway becomes abundantly clear: Data is increasingly becoming the currency of economic security, our national security, and our public health and safety," said Bob Kolasky, the director of the National Risk Management Center at CISA, during a recent CISA virtual event.

The task force's year two report, which came out in December, highlighted the work it conducted in 2020, including the creation of a vendor SCRM template, which is a standardized set of questions to communicate ICT supply chain risk posture and analyze comparative risk among all types and sizes of organizations, to enable increased transparency in managing ICT outsourcing risks, and a threat evaluation working group. That committee conducted an assessment of threats to and from products and



**"Whether it's the packets of data that enable the operational functionality of connected infrastructure; or whether it's sensitive data, things like intellectual property and personal preferences and identifiers; whether it's monthly firmware or software updates; one overarching takeaway becomes abundantly clear: Data is increasingly becoming the currency of economic security, national security, and our public health and safety."**

**— BOB KOLASKY, DIRECTOR OF THE NATIONAL RISK MANAGEMENT CENTER, CISA**





services, evaluating those threats with a scenario-based process, which released in February 2020.

It also created a risk and mitigation resource by leveraging threat groupings and applying the National Institute of Standards and Technology Risk Management Framework described in NIST SP 800-161. CISA released the second version of that committee's report, which includes the assessments of impacts and mitigating controls, in February 2021.

The report is essentially a threat evaluation guide. The task force identified a few hundred reference threats for supply chain, then boiled those down into several major threat groups:

- **Counterfeit parts:** These involve the replacement of trusted components, products or services with those from untrustworthy sources.
- **External attacks on operations or capabilities:** These involve the uses of vulnerabilities or malware by an external actor in order to compromise the supply chain.
- **Internal security operations and controls:** These are similar to external attacks, but involve insider threats due to poor cyber hygiene or phishing attacks.
- **System development lifecycle products and tools:** These threaten the ability of providers to develop products or services, such as the inability to detect malware or use of vulnerable open source libraries.
- **Insider threats:** These threats include intentional tampering or interference from trusted staff.
- **Economic risks:** These threats involve the financial status of providers and the impacts of their potential failures, such as single source suppliers or resource constraints.
- **Inherited risks:** These threats consider the scope of the supply chain, and the difficulty in extending

**“With this reality in mind, ICT supply chain risk management can no longer be looked at as a largely independent discipline. It is simply a new layer on top of existing cybersecurity risk management and critical infrastructure protection activities that must be undertaken. These all must be thought of holistically to drive security and resilience results.”**


**— BOB KOLASKY, DIRECTOR OF THE NATIONAL RISK MANAGEMENT CENTER, CISA**

controls and best practices to every layer and component.

- **Legal risks:** Suppliers may be vulnerable to legal concerns, such as regulation or intellectual property considerations.
- **External end-to-end supply chain risks:** These include natural disasters, geopolitical issues and other similar events that may disrupt the supply chain.

The task force's report breaks each of these threat groupings down into more specific individual threats, including whether it's adversarial or accidental and who the most likely culprit is.

The group then assessed each threat grouping, determining the source, the impact, the vulnerability, a description of what the event might look like, and provided potential strategies and controls for mitigating the risk. These range from strategies to identify counterfeit parts to implementing specific cybersecurity provisions and identity access and management controls.

“With this reality in mind, ICT supply chain risk management can no longer be looked at as a largely independent discipline,” Kolasky said. “It is simply a new layer on top of existing cybersecurity risk management and critical infrastructure protection activities that must be undertaken. These all must be thought of holistically to drive security and resilience results.” 

# CMMC exempts COTS software, but vendors should prepare for change

THIS CONTENT HAS BEEN PROVIDED BY SOLARWINDS



**Tim Brown, vice president of security at SolarWinds**

The Cybersecurity Maturity Model Certification is quickly becoming the law of the land for the Defense Industrial Base. This is the first year of the Defense Department's five-year phased rollout, and RFIs and RFPs will soon begin requiring

CMMC compliance. But there's one exemption: commercial off-the-shelf software. That's because it's not just about the software itself, but about the implementation as well.

"I'm handing you a piece of software. And how do I know you configured it appropriately? How do I know that you have given the right people access to it? Think of an operating system: You can make it as secure as you'd like when you install it. So that's the reason why you have that exemption today," Tim Brown, vice president of security at SolarWinds, said. "If you look at a lot of the language in CMMC today, it's how is the service configured? Is the service configured appropriately? Who has access to that service? Have you made sure that your administrators are treated differently than new users?"

However, Brown said there's currently talk about how to update CMMC – as well as other regulations – to account for COTS software. And that could take a different approach, focusing on what goes into the software rather than how it's configured and exists in the environment. Assessments could look at what safeguards go into place during the creation of the software, and what third parties are utilized.

But while these gaps are being investigated in order to discover how to make software more resilient, the other side of the coin is, it cannot negatively affect innovation. So the big question is how to increase transparency and visibility into software providers without reducing productivity?

"That's the question," said Brown. "Does it take the form of a different type of regulation? Does it take the form of amendments to CMMC? Does it take the form of other certifications that need to be put in place? Those are the types of debates that are going on right now."

**"That's the question. Does it take the form of a different type of regulation? Does it take the form of amendments to CMMC? Does it take the form of other certifications that need to be put in place? Those are the types of debates that are going on right now."**

— TIM BROWN, VICE PRESIDENT OF SECURITY AT SOLARWINDS

The problem is, it took a long time to get to CMMC. It took years to get the documents and testing centers and Certified Third-Party Assessor Organizations in place and ready to go. Similarly, any adjustment to account for COTS will take time, starting with understanding what the appropriate level of certification is. Then certifying bodies have to be put in place, along with a model for what audits look like.

In the meantime, vendors should begin preparations so that they're ready to respond when this does take place. And that, Brown said, means starting with internal audits.

"One of the things that we're doing and that others are doing is being prepared to talk about our engineering processes, to talk about our testing process, to talk about our build processes, and our supply chains, and really preparing internal audits in the preparation for external audits," he said. "A number of the external audit companies are not as prepared for this type of audit. It's just not natural today for somebody to say, 'I'm going to go and audit how you build your software components and produce your report on that.' It's not a general practice today."

And because it's so early in the process, no one knows yet where the standards are going to come from. CMMC is already in place both from an audit perspective and from a testing perspective, so some have proposed that it would make the most sense to adapt that. Others, however, have advocated standing up a completely separate process. So ownership of this is still murky.

Part of the problem is, currently, different agencies have different processes in place to look at this. There's a lack of governmentwide consistency. DoD has its own testing lab; it has specialized questionnaires for when it's looking at software. But the questions vary, the level of detail varies, and the level of inspection varies across different types of software. So there's very little consistency even internally. And every agency has its own process.

"That lack of consistency hurts measurement, and that lack of consistency makes it harder for vendors to inform, and that lack of consistency makes for varying degrees of risk," Brown said.

That's really what drives the expectation that within a few years, things will change. Controls will be put in place, and regulations will be put on software providers. That's why it's important for vendors to start preparing now.

"That's the important part for other vendors to realize that they need to do, is be able to fully explain their development process, fully explain their bill of materials, fully explain what their test programs and security programs look like," Brown said. "And be very open with that, because that will help everyone prepare for this next stage, which will be when we do have regulations and official external audits."



# Secure by Design

Leading the way to safer IT

[solarwinds.com/secure-by-design-resources](https://solarwinds.com/secure-by-design-resources)



Scalable, end-to-end IT monitoring software from [solarwinds.com/government](https://solarwinds.com/government)



# NTIA wants to standardize ‘list of ingredients’ for software supply chain risk

BY DAVID THORNTON

Supply chain risk management is at the top of the to-do list for every federal agency’s cybersecurity division right now, as the list of vulnerabilities and breaches continue to pile up. The Commerce Department’s National Telecommunications and Information Administration (NTIA) is exploring the value of increased software transparency in helping to avoid these vulnerabilities or mitigate them quicker. Distilled to its most basic level, the concept is that agencies need to know what they have before they can secure it.

“For me, it’s really baffling that very few organizations can quickly and easily answer a simple question: ‘Hey, this new vulnerability, am I affected? Whether I make the software or whether I buy the software or operate the software, am I affected?’” said Alan Friedman, director of cybersecurity initiatives at the NTIA during a recent FCW event. “That should be the easy part. But surprisingly, that’s the hard part.”

That’s where the idea of a software bill of materials (SBOM) comes in. It’s much like a hardware bill of materials, where any company that builds something has to list the materials and where it bought them from, and potentially even track components. Software, the NTIA argues, should be treated the same way. That means more visibility into things like libraries, executables and source code.



The benefits NTIA lists include reduced cost and reductions in multiple kinds of risk, including security, and the use cases range from supply chain management to software development to procurement. Proofs of concept are already demonstrating value in the healthcare, automotive and energy industries.

“So why aren’t we doing this today? Well, first and foremost, the more venal reason is licensing concerns and open source restrictions have made a lot of organizations reluctant to say what they’re using. That’s a much better understood problem today. There are commercial off the shelf tools to help manage it. There are international initiatives and ISO standards like OpenChain that helps people understand their obligations,” Friedman said. “Now, it’s also a chicken and egg issue. No one’s asking for this data, so no one’s applying it. No one’s applying it so no one’s asking for it. How do we get started?”

**“This has to fit in with upstream solutions, downstream solutions, tooling, vendors, existing manufacturers. If we try to get everyone to adopt something brand new that’s against what they’re already doing, we’re simply not going to succeed.”**

— ALAN FRIEDMAN, DIRECTOR OF CYBERSECURITY INITIATIVES, NTIA

## Automation is key

To start with, any organization looking to create an SBOM has to understand it will only work if automation is applied. That means data has to be in machine readable formats and widely interoperable.

Then there's the question of scope. An SBOM isn't limited to just open source, or middleware, or proprietary software. It has to cover the entire supply chain.

NTIA also recognized that it has to be modular.

"This has to fit in with upstream solutions, downstream solutions, tooling, vendors, existing manufacturers. If we try to get everyone to adopt something brand new that's against what they're already doing, we're simply not going to succeed," Friedman said.

But Friedman was also quick to clarify that this is not about regulation, though he acknowledged there are regulators watching the process closely.

"This is not a regulatory process. This is not about source code disclosure," he said. "This is not about solving all software supply chain issues or assurance issues. Our goal here is to really empower your project, your initiative, your product."


And an SBOM accomplishes that by making a minimum amount of information more transparent: supplier, component name, version number. And if there are known unknowns, those get tagged as well. So if, for example, it's unknown whether a certain piece of software has any dependencies, that would be tagged. That way, even if the information is not available, the risk is clear.

## Transparency is a standard practice

And this kind of transparency is standard practice across almost every industry already, Friedman said, from 50 gallon drums of chemicals to diesel generators. Even Twinkies come with a list of ingredients.

"The goal of this list of ingredients is to put the information in the hands of those who are in the best position to make a risk-based decision based on their own profile and their own needs," Friedman said during a Cybersecurity and Information Systems Information Analysis Center webinar last fall. "And for me, it's kind of crazy that we have this for our delicious snacks in the snack aisle. But we don't have this in the most important systems that are running our critical infrastructure, and that are supporting our national interest in the national defense community."

Multiple formats for this data already exist. Two prominent ones are the Software Package Data Exchange (SPDX), which is open source and used as a standard by the Linux foundation, and Software Identification (SWID), which is an industry standard used by commercial software publishers. NTIA's position has been, rather than coming down in favor of one format or the other, to help the different communities work together and collaborate rather than viewing each other as competitors.

"Everyone needs to understand software supply chain risks and transparency is a key part of that," Friedman said. "We're basically helping the entire world create a common set of practices and market expectations." 

**"The goal of this list of ingredients is to put the information in the hands of those who are in the best position to make a risk based decision based on their own profile and their own needs."**

**— ALAN FRIEDMAN, DIRECTOR OF  
CYBERSECURITY INITIATIVES, NTIA**

If federal agencies are breached, they lose data and trust, while if vendors are breached, they lose customers and revenue. Government can learn a lot from industry, since many have proven approaches in place to mitigate future software supply chain risk management attacks.

# Government should look to industry for a software supply chain security model

THIS CONTENT HAS BEEN PROVIDED BY MICRO FOCUS GOVERNMENT SOLUTIONS

Government has a tendency, especially in the wake of a major cyber breach, to focus solely on



**David Wray, public sector chief technology officer, Micro Focus**

the immediate, reactive problem. In the months since the SolarWinds breach, government has primarily focused its attention on remediation and detection, rebuilding trust stores, and other operational activities. But little focus has been paid to proactively preventing breaches like this in the first place.

Industry, on the other hand, has a financial incentive to be proactive. If federal agencies are breached, they lose data and trust, while if vendors are breached, they lose customers and revenue. Government can learn a lot from industry, since many have proven approaches in place to mitigate future software supply chain risk management attacks.

"Our focus has been on SolarWinds, and most recently Codecov because of the stealthiness, and the successful techniques our adversaries were able to exploit to penetrate environments and break into trust stores," said David Wray, public sector chief technology officer at Micro Focus. "In both scenarios, adversaries attacked the software build process and were able to gain high level access to both commercial and government organizations for months before being discovered."

Agencies also need to consider any open source code they use, Wray said. The open source community simply doesn't have the funding to keep pace with security threats. Since the code base is shared, it makes it easier to write malicious software, as well as inject into the tooling and/or environment that modern DevOps teams use every day. Agencies need to be using immutable source code control and auditing all code transactions during software builds just like industry does today.

There's also the problem of how many development teams agencies have. Some have as many as 300, each with its own supporting contractor, software factory or CI/CD automation scripts. Multiply that by the number of different tools and processes used in these software builds, and you've got thousands of attack vectors for adversaries to target.

"At Micro Focus, shortly after the HPE acquisition a couple of years ago, this was our situation: costing us too much money, having hundreds of tools and well over 2000 processes to do software builds across 300 products was just wasteful," Wray said. "So we took an effort to consolidate a lot of these products and built enterprise services for DevSecOps that all development teams must use. Next, we created standard policies, and support service owners around that, which is our production support software factory today. Now we have robust services that all development teams must use, mostly supported by our own IT Products from our portfolio. So in order to do a product build, development teams have to use our



defined process. We have over a dozen enterprise services for development teams today, from source code control, to security scanning, through integration/performance testing and production deployment."

Wray said Micro Focus got down to approximately a dozen products that are leveraged enterprisewide. This significantly reduced the available attack vectors, cost, energy and risks.

There are a number of other actions agencies can take, depending on the threat vector, Wray said. For example, providing a common build environment for all teams allows agencies to reduce the risk of introducing malicious code or compromised libraries that may exist on local build environments. Agencies can also limit access to code repositories and leverage insider threat modeling and other forensic tools to audit and monitor activity during builds to ensure they are safe.

"For example, if we control the build environment, nobody should be able to modify the binary repo," Wray said. "If you touch a binary, it should be something that goes through change control, is hardened, and goes through code inspection before it gets into the binary repo. Yes, it'll slow you down. But we must make sure that it's not going to interject something into a production product. The libraries that are shared by many development teams are an ideal attack vector. In many government environments all developers have access to all source code libraries, including binaries. And many popular open source development tools and add-ins for DevSecOps pull the latest libraries from the internet, not a controlled repo. Hence, it's very important to have a continuous monitoring and audit trail process for the entire software supply chain and a "Kill-Chain" in place."

Some organizations also provide a centralized testing-as-a-service function to run automatic functional tests once a build is completed and provide feedback to DevOps teams. That keeps individual teams from creating their own testing environments and using production data for testing. Local test environments may not be secure and could expose production data to adversaries.

"At Micro Focus, we leverage our own cloud-based performance testing service, as well as

our software assurance/scanning cloud services, and have made these available for customers to leverage as well," Wray said.

It all boils down to having enterprise capabilities, consistent measurements and governance across all development teams and eliminating potential attack vectors. Otherwise each team has to be secured independently, which isn't efficient, nor feasible in many government organizations. Today, most agencies don't always think that way, and many programs are awarded to separate contractors that have their own software build capability; hence IT leadership needs to rethink/configure service contracts to enforce enterprise services for DevSecOps in order to achieve the same success that industry leverages.

These are just a few of the threat vectors that federal agencies need to address. Others include suppliers and third-party components, software integrity and availability, infrastructure and data privacy. Many of the mitigation strategies for these threat vectors overlap, but agencies need to take a proactive approach to begin securing them before the next breach like SolarWinds, Codecov, Microsoft Exchange or the most recent fuel pipeline ransomware attack.

President Biden signed an executive order aimed at hardening the federal government's cybersecurity defenses to help the government assess, grade and rank software vendors on their supply chain security during their production process. There was no mention of new requirements for hardening the plethora of software builds that occur annually within a large federal agency.

"I am worried about a lot of these federal agencies, as well as the defense industrial base because they've never produced commercial products, and they write a whole lot of custom software," Wray said. "To me, it's an easier attack surface for a nation state to go after. I believe that's why we have seen so many CVE's introduced into development tools, especially open source software that is heavily used during the build process. I believe we will continue to see adversaries target the software supply chain until we start building safer digital software factories that are based upon enterprise services and secure tools -- the SolarWinds incident was simply the beginning."

# Powering a Secure Digital Transformation

Protecting what matters most:  
Identities, applications, and data

The digital transformation journey is promising but perilous. We know it well and we can help. Our solutions cover every challenge your agency may face—from modernizing critical infrastructure to protecting against cybersecurity threats. Let us smooth the way.

## Cybersecurity needs:

### Manage Identities

by governing privileges, enforcing access controls, and unifying identity stores.

### Secure Applications

by embedding strong security and best practices into DevOps processes.

### Data Protection

by discovering where it is, determining who has access, and guarding it wherever it resides.



Learn more: [mfgsinc.com](https://mfgsinc.com)

Discover more innovative solutions:

| Enterprise DevSecOps | Hybrid IT Management | Security, Risk and Governance | Predictive Analytics

