

CMMC Readiness: From Certification to Content & Customer Advocacy

How a compliance milestone and customer success narrative generated measurable demand across higher education, government and the Defense Industrial Base

Andrew Mullen Scott
Sr. Content & Digital Strategy
Manager – Public Sector,
Tanium



GOAL

In March 2026, Tanium achieved Cybersecurity Maturity Model Certification (CMMC) Level 2 which validated that the Tanium Autonomous IT Platform itself meets the same compliance standard the company was about to spend the rest of FY27 helping other organizations reach. Rather than treat that certification as a single press release moment, the program built it into the foundation of a full go-to-market campaign: an authoritative white paper connecting real product capabilities to CMMC control families, an FY27 playbook targeting both higher education research institutions and federal defense contractors, a flagship co-branded webinar with Carahsoft pairing a real customer's experience with Tanium's own technical leadership, and a set of sales enablement assets built to carry the momentum into the account team's hands.

The timing mattered. CMMC's phased enforcement timeline requires third-party Level 2 certification starting Nov. 10, 2026 which meant organizations across the Defense Industrial Base and the higher education research community had a hard deadline bearing down on them throughout this campaign's execution. Tanium's own certification, secured months ahead of that deadline, positioned the company to lead the market with proof rather than persuasion.

OBJECTIVES

- Prove platform trustworthiness by achieving Tanium's own CMMC Level 2 certification, then communicate that milestone credibly across the market — the "we did this ourselves" foundation everything else stands on
- Translate that certification into an authoritative technical asset — the CMMC white paper — built and validated with Tanium's federal solutions engineering, architecture, and technical product teams
- Build a full FY27 go-to-market playbook addressing two distinct, high-value audiences — higher education research institutions and federal DIB contractors/subcontractors — each with its own personas, pain points, and sales plays
- Execute a flagship co-branded webinar with Carahsoft that put a real customer (Georgia Tech Research Institute) and Tanium's own technical leadership in front of both audiences simultaneously
- Equip the sales organization with durable enablement assets — an institution-level research tracker and a partnership-model reference guide — so campaign engagement converts into account-level pipeline

Campaign at a Glance

Workstream	Status	Key Date(s)
1. Certification & Announcement	Complete — Launched	Mar 3, 2026
2. CMMC White Paper (Product Marketing)	Complete — Revised with certification	FY26–FY27
3. FY27 CMMC Go-to-Market Playbook	Complete	FY27
4. Carahsoft Webinar	Complete	Jun 2, 2026
5. Sales Enablement	Activated in FY27 Plan	Continuing

STRATEGY & PROGRAM DETAILS

WORKSTREAM 1 OF 5

Foundation: Achieving & Announcing Certification

I spearheaded the communications plan around Tanium's CMMC Level 2 achievement in partnership with Ricardo Quinto, Director of Communications, Public Sector. The announcement, "[Tanium Achieves CMMC Level 2 Certification, Powering Cyber Readiness and Compliance Across U.S. Defense Industrial Base](#)" (published March 3, 2026) positioned the certification not as an isolated security credential but as the credibility anchor for everything that followed: Tanium could not credibly sell CMMC readiness to defense contractors and research institutions without first proving it had met the standard itself.

Tanium CISO Chris Hallenbeck framed the achievement in market terms in the announcement itself: defense contractors need technology partners that meet the same high standards they themselves are required to maintain. That framing — certification as a customer-facing trust signal, not just an internal compliance checkbox — became the throughline for the rest of the campaign.

WORKSTREAM 2 OF 5

Translating Certification into Content: The White Paper

I served as pseudo-product marketing manager and writer of Tanium's official CMMC white paper, "[Achieve CMMC Compliance with Tanium](#)," working directly with Tanium's federal solutions engineering, architecture, and technical product teams to ground every claim in actual platform capability rather than marketing language.

The asset has its own arc worth noting honestly: an earlier version was already in market before Tanium's own certification was achieved. Once certification came through, I revised the paper in tandem with the launch of the press release to reflect industry changes, updated branding, and the certification itself. The final version is a document that matured alongside the achievement it eventually could claim, rather than one written after the fact to fit a marketing narrative.

The resulting paper maps Tanium's platform capabilities directly to CMMC control families, including full coverage of the Risk Assessment family and majority coverage of Configuration Management and Incident Response — quantified, specific claims rather than generic compliance messaging:



WORKSTREAM 3 OF 5

The FY27 CMMC Go-to-Market Playbook

The FY27 plan built two parallel audience tracks off the same certification foundation. The higher education track targeted the 148 institutions identified as active U.S. Department of War (DoW) research and funding partners — 120 U.S. institutions plus UK, Australian, Canadian, and New Zealand research partners — spanning DURIP, UARC, MURI, and other DoW-funded research programs that put them in scope for CMMC and NIST 800-171 compliance. The federal track targeted prime contractors, subcontractors, and managed service providers across the Defense

Industrial Base, organized around four campaign pillars: Win the Contract, Pass the Audit, Scale Across the Ecosystem, and Sustain Compliance — each paired with a specific sales play (“Protect the Pipeline,” “Audit Readiness Now,” “Fix Your SPRS Score,” and “Secure the Supply Chain”) targeted to a distinct buying persona.

Urgency for both tracks was anchored to CMMC’s official four-phase DoW enforcement timeline, giving the campaign a hard, external deadline to build messaging around rather than a soft compliance suggestion:

Phase	Effective Date	What Changes
Phase 1 — Initial Contract Requirements	Nov 10, 2025	CMMC requirements begin appearing in new DoW solicitations; self-assessments accepted for Level 1 and some Level 2
Phase 2 — Third-Party Certification for Level 2	Nov 10, 2026	Level 2 contracts involving CUI require formal C3PAO certification
Phase 3 — Level 3 Assessments Begin	Nov 10, 2027	DIBCAC-conducted assessments begin for the most sensitive programs
Phase 4 — Full Implementation	Nov 10, 2028	CMMC becomes a condition of award on all applicable DoW contracts

WORKSTREAM 4 OF 5

Flagship Execution: The Carahsoft Webinar

“[From Requirement to Readiness: Scaling CMMC Level 2 Across the DIB and Higher Education Research Ecosystem](#)” aired June 2, 2026, co-hosted with Carahsoft. Beyond scoping the program, I owned event logistics end to end, wrote all promotional and on-page copy, and coordinated CPE credit eligibility directly with Carahsoft and their NASBA sponsorship which offered attendees one continuing professional education credit, a detail that mattered for pulling in compliance and audit-adjacent titles who need CPE hours to maintain their own certifications.

The session deliberately paired a real customer voice with Tanium’s own technical leadership: Wes Hogarth, Director of Information Systems at Georgia Tech Research Institute (an existing Tanium customer utilizing the platform to achieve CMMC compliance) alongside Ryan Andorfer, Group VP of Tanium Platform. Framed as a cross-sector fireside conversation rather than a policy overview, the format let one session speak credibly to both the higher education and federal DIB audiences the FY27 playbook was built to reach, rather than requiring two separate events.

Notably, the program carried no direct cost to Tanium. As an existing distributor, Carahsoft hosted, promoted, and led registration for the webinar independent of a paid engagement.

WORKSTREAM 5 OF 5

Sales Enablement

Post-webinar nurture drew on a full SDR toolkit built alongside the campaign’s core content, not just a registrant list. Digital Sales Associates and SDRs had direct access to CMMC Tanium Mapping and Guidance Documentation connecting specific control families to platform capability, a recorded CMMC Tanium Dashboard Demo they could send prospects on demand, as well as Tanium’s [NIST Cybersecurity Framework 2.0 white paper](#) as a companion asset alongside the CMMC paper covered in Workstream 2 which gave reps a relevant document for nearly any stage of a compliance-maturity conversation.

The institution-level research tracker anchored account prioritization within that toolkit. It was scoped to catalog all 148 identified DoW research institutions (120 U.S., 9 UK, 8 Australian, 7 Canadian, and 4 New Zealand) against

research focus and description, CMMC level relevance and priority, the specific DoW program involved (UARC, MURI, DURIP, and others) and its awarding office, and key personnel, giving SDRs an account-level starting point rather than a cold list of institution names.

On top of that, SDRs and DSAs used a structured discovery script rather than a generic pitch that was designed to open account conversations with informed, consultative questions before moving to Tanium’s CMMC control mapping and a live platform demo. A representative sample from the higher education script:

- What is the risk of CMMC non-compliance to the institution’s reputation and financial stability — considering potential loss of funding and research opportunities?
- What specific DoW-funded research projects or grants currently involve handling CUI and FCI?
- Have you determined what resources — funding, personnel, technology — the institution is prepared to commit to achieve and maintain CMMC compliance?
- Is the institution willing to adopt a unified, platform-centric approach to cybersecurity and compliance that simplifies asset discovery, policy enforcement, and incident response?

Campaign success itself was measured across three dimensions per the FY27 plan: brand and thought leadership visibility through earned media, demand generation pipeline contribution, and nurture tracking via a shared dashboard of combined campaign codes — with regular follow-ups between DSAs and SLED leadership on how campaign-sourced leads were actually converting.

KEY FINDINGS / RESULTS

Key launch results span two distinct data sets: organic social performance for the certification announcement and the webinar promotion, and the webinar’s own registration, engagement, and audience data.

Certification Announcement — Social Performance

Posted to Tanium’s primary corporate LinkedIn page, the [certification announcement](#) reached significantly further than the webinar promotion below — nearly 9x the impressions — consistent with a company-wide credibility milestone traveling further than a niche event invite:

18,338

Impressions

878

Engagements (4.8%)

592

Clicks (3.2% CTR)

Metric	Result
Reactions	235
Comments	4
Reposts	47
Page viewers from post	44
Followers gained	1

Two details are worth surfacing beyond the raw numbers. First, engagement included substantive pushback — one comment noted that “certifications... are not the finish line,” a sign the post reached an informed, skeptical audience rather than an echo chamber. Second, the video’s top viewer metros were Washington DC-Baltimore (7.6%), Dallas-

Fort Worth (6.0%), San Francisco Bay Area (5.9%), New York City (3.6%), and Raleigh-Durham-Chapel Hill (2.9%) — a geographic footprint that tracks the actual DIB and research-institution buyer map, including the Raleigh-Durham market home to NC State University, which became the webinar’s single strongest account signal (see below).

At 4.8%, engagement ran nearly 1.8x above the 2.7% government-industry average LinkedIn engagement rate ([Hootsuite, 2026](#)).

Webinar Promotion — Social Performance

Posted from the smaller Tanium Public Sector page, the [webinar promotion](#) was a deliberately narrower, more targeted push consistent with the campaign’s account-based posture rather than a broad awareness play:

Metric	Result
Impressions	2,113
Engagements	85 (4.0% engagement rate)
Clicks	38 (1.8% CTR)
Reactions	35
Comments	0
Reposts	12
Page viewers from post	2
Followers gained	1

Reposts (12) outperforming comments (0) fits a specialized B2G compliance topic that professionals share directly with colleagues rather than debate publicly — a pattern consistent with the account-based, quality-over-reach approach both the webinar and its promotion were built around.

At 4.0%, engagement still cleared that same 2.7% government-industry benchmark by nearly 1.5x, even against a far narrower, more targeted audience.

Webinar Event Performance

~43	26	85% / 77% / 62%
Registrations (per Carahsoft report)	Peak live attendees (60% attendance)	Retention at 30 / 45 / 57 minutes

Retention held well past the halfway mark before the expected 45-minute drop-off, and structured engagement — 17 responses on the opening poll alone — outweighed live Q&A volume (2 questions), a pattern consistent with a fireside-style format driven by speaker dialogue rather than open floor discussion.

Audience Composition: A Deliberately Diversified Room

The audience spanned six distinct segments — higher education, existing customers, federal systems integrators and defense contractors, federal civilian agencies, state and local government, and K-12 — evidence the campaign’s dual-track (higher ed + federal) strategy pulled a genuinely mixed room rather than a single-segment audience:

Segment	Registrants	Attended
Higher Education Prospects (excl. existing customers)	9	8
Existing Customers (Higher Ed research institutions)	6	3
FSI / Defense Contractors	5	3
Federal Civilian	2	2
State & Local Government	1	0
K-12	1	1

The organization list itself is the clearest evidence of how deliberately cross-sector this room was. NC State University sent five attendees which was the strongest single-organization signal of the event, indicating active internal evaluation already underway rather than casual interest. They were alongside fellow research institutions Southern Methodist University, Purdue University, Oregon State University, the University of Arkansas, UNC Wilmington, and Northern Illinois University. On the FSI and defense contractor side, attendees came from Presidio, Guidehouse, DRI (Disaster Recovery Institute), Arcadian Pursuits, and White River Resources Group. Federal civilian representation included the DHS Office of Inspector General and the Defense Health Agency, and DeKalb County School District (Georgia) represented the K-12 segment. Existing Tanium customers Georgia Tech Research Institute and the University of Texas at Arlington rounded out the room.

Registration data extended that diversity even further: the City of New York registered but did not attend. Given the historically difficult NYC/NY State market, that registration alone was treated as a strategic re-engagement opportunity worth direct follow-up. Major defense contractor L3Harris and global consulting firm Deloitte also registered without attending, underscoring that the event's pull extended well beyond the core research-institution audience it was built around.

Poll Insights

Poll 1 — How soon is your organization pursuing CMMC Level 2? (n=17)	% of Respondents
Less than 6 months	47%
6–12 months	18%
Not planned	35%

Poll 2 — Biggest barrier to CMMC compliance? (n=7)	Responses
Resource or staffing constraints	3
Lack of visibility into assets/CUI	2
Budget constraints	2

Poll 3 — Interested in a CMMC readiness assessment? (n=7)	Responses
Yes	1
Maybe	4
No	2

Nearly half of poll respondents placed themselves inside a six-month compliance runway, and the leading stated barrier — lack of visibility into assets and CUI — maps directly to Tanium’s core platform value proposition rather than a generic pain point, giving follow-up conversations a natural, product-relevant opening. These insights were instrumental in determining next phase nurture processes.

Post-Event Satisfaction

Anonymous post-event survey responses were collected on a 1–5 scale (5 = Strongly Agree / Very Valuable):

Survey Question	Avg. Score
Learning objectives were met	4.8 / 5 — Excellent
Prerequisite requirements were appropriate	4.8 / 5 — Excellent
Program materials were relevant and contributed	4.6 / 5 — Excellent
Time allotted was appropriate	4.6 / 5 — Excellent
Presenter — Wes Hogarth — was effective	4.8 / 5 — Excellent
Presenter — Ryan Andorfer — was effective	4.75 / 5 — Excellent
Overall webinar value	3.6 / 5 — Good

As reported by Carahsoft; the overall-value question used a slightly different scale than the rest of the survey, which is reflected verbatim here from the source report rather than normalized.

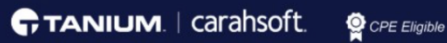
PARTNERS

Tanium: Program led by Andrew M. Scott (Sr. Content & Digital Strategy Manager, Public Sector), with Holly Hein (Marketing Manager, SLED) and Kristin Starkel (Sr. Public Sector Marketing Director) contributing across planning and execution. Ricardo Quinto (Director of Communications, Public Sector) led certification announcement communications strategy alongside Andrew M. Scott. Tanium’s federal solutions engineering, architecture, and technical product teams supported certification achievement and white paper development. Ryan Andorfer (Group VP, Tanium Platform) served as featured webinar speaker given his direct ties to CMMC and Tanium’s FedRAMP solution capabilities.

Georgia Tech Research Institute: Wes Hogarth, Director of Information Systems, served as featured customer speaker.

Carahsoft: Distribution and demand generation partner; hosted and co-branded the webinar, managed CPE credit sponsorship (NASBA), and provided post-event registration and engagement reporting.

MEDIA — WEBINAR LANDING PAGE



Webinar

From Requirement to Readiness: Scaling CMMC Level 2 Across the DIB and Higher Education Research Ecosystem

[Register Now](#)


What Defense Industry and Higher Ed Leaders Need to Do Next

Featured Speakers:

Wes Hogarth, *Director, Information Systems*, Georgia Tech Research Institute

Ryan Andorfer, *Group VP*, Tanium Platform, Tanium

Tuesday, June 2, 2026

11:00am - 12:00pm ET;
8:00am - 9:00am PT

Online

[Register Now](#)

CMMC is here, and organizations must now show measurable progress toward Level 2 compliance while managing complex, distributed environments.

Join experts from Georgia Tech Research Institute and Tanium for a practical discussion on turning compliance into a continuous, scalable capability.

[Reserve Your Spot](#)

What You'll Learn:

- How CMMC Level 2 is impacting contractors, higher ed and research
- Steps to move from planning to audit-ready execution
- Challenges in securing CUI across distributed environments
- How automation and real-time visibility reduce compliance burden
- Best practices for aligning IT, security and governance teams

Get the insights you need to accelerate your path to compliance.



Please don't hesitate to **reach out** with any questions.

carahsoft.

Daniel Lyons
571-662-3312
www.carahsoft.com/tanium

We are pleased to offer 1 continuing professional education (CPE) credits to those that attend the event. For more information on the CPE credit we are offering, our CPE sponsor (NASBA) and the submission process, please visit our **CPE information page**.



Carahsoft and our partners have assembled products and services to help the Defense Industrial Base address the processes and practices of CMMC. View more on our **CMMC website** where you can search for solutions addressing any of the 14 capability domains and view additional resources.

Click [here](#) to update your email preferences

By supplying my contact information, I authorize Carahsoft and its vendors and partner community to contact me with personalized communications about their products and services. Please review our [Privacy Policy](#) for more details or to [opt-out](#) at any time

MEDIA — SOCIAL MEDIA POSTS


Tanium
5mo · Edited ·

We're proud to announce that Tanium has achieved Cybersecurity Maturity Model Certification (CMMC) Level 2. This milestone assures the Department of War (DoW), defense contractors, subcontractors and research institutions that the Tanium Autonomous IT Platform can protect Controlled Unclassified Information (CUI) and operate confidently within DoW compliance frameworks.

"Achieving CMMC Level 2 demonstrates Tanium's deep commitment to securing the confidentiality of government data used by organizations that support the nation's defense mission," said [Chris Hallenbeck](#), chief information security officer at Tanium.

"Defense contractors need technology partners that meet the same high standards they themselves are required to maintain. This certification further gives our customers confidence that Tanium supports their most sensitive environments while helping them accelerate their compliance efforts."

Beyond validating Tanium's own security posture, this achievement delivers immediate value to [Tanium Public Sector](#) customers across the U.S. Defense Industrial Base. Under CMMC flow down requirements, defense contractors must ensure their partners and tools also meet CMMC standards.

Learn more: <https://bit.ly/4u7bsfA>



PRESS RELEASE

Tanium Achieves CMMC Level 2 Certification, Powering Cyber Readiness and Compliance Across U.S. Defense Industrial Base

TANIUM


 235
 4
 47

Comment as Tanium



Most relevant ▾


Archived
849 followers
5mo ...

Certifications like this matter, but they are not the finish line. Compliance proves you met a standard at a point in time. Security is about what happens the day after. The real test is whether those controls hold up under real pressure, not just audit conditions.

Like | Reply


Igor Kovalenko · 3rd+
Engineering Quality Leader | Driving Impact with End-to-End QA for ...
5mo ...

Congrats on reaching CMMC Level 2, that's a serious bar to clear and a big trust signal for defense-focused customers.

Like | Reply


Sergio Ivan Garcia · 3rd+
Enterprise Technical Sales en Hitachi Vantara -SSA
6mo ...

Amazing!!

Like | Reply


Benjamin Bota · 2nd
Customer Success Leader | Enterprise SaaS & Cybersecurity | Driving ...
6mo ...

This is huge, Craig! Congrats!

Like | Reply


Tanium Public Sector
3mo ·

With CMMC Phase 2 enforcement on the horizon this November, organizations across the Defense Industrial Base and higher education research ecosystem face a clear mandate: demonstrate measurable, auditable progress toward Level 2 compliance—or risk contract eligibility.

Our upcoming fireside webinar featuring technology leaders [Wes Hogarth, Georgia Tech Research Institute](#) and [Ryan Andorfer, Tanium](#), dives into how both organizations are navigating these challenges in real operational environments.

This isn't a policy overview. It's a cross-sector conversation on what compliance execution actually looks like—and what it takes to build it as a continuous capability.

What to Expect:

- ◆ How CMMC Level 2 is impacting contractors, higher ed and research
- ◆ Steps to move from planning to audit-ready execution
- ◆ Challenges in securing CUI across distributed environments
- ◆ How automation and real-time visibility reduce compliance burden
- ◆ Best practices for aligning IT, security and governance teams

Join us: <https://lnkd.in/eZ8pkCXP>

We're proud to co-host this webinar along with our partners at [Carahsoft](#).

#CMMC #CMMCcompliance #DIB #highered #EdulT #eduresearch #cyberdefense #defenseresearch #defensetech



TANIUM | **carahsoft** 

Webinar

From Requirement to Readiness:
Scaling CMMC Level 2 Across the DIB and Higher Education Research Ecosystem

Tuesday, June 2, 2026
11:00am - 12:00pm ET; 8:00am - 9:00am PT

Speakers ▸


Wes Hogarth
Director, Information Systems,
Georgia Tech Research Institute


Ryan Andorfer
Group VP, Tanium Platform,
Tanium




 35

 12

Comment as Tanium Public Sector



Achieve CMMC Compliance with Tanium

Address certification requirements for continuous visibility, control and compliance.



Navigating CMMC with confidence

For organizations that process, store, or share Controlled Unclassified Information (CUI) for the Department of War (DoW), achieving Cybersecurity Maturity Model Certification (CMMC) compliance is a strategic imperative, and essential for securing DoW contracts. These organizations need a solution that protects them from cyberattacks and ensures that they are handling sensitive information while meeting specific cybersecurity requirements.

Tanium's Autonomous IT Platform supports many CMMC compliance requirements by providing comprehensive endpoint visibility, automated security controls, and streamlined reporting capabilities to address core compliance requirements with confidence. By consolidating capabilities into a single platform, Tanium simplifies IT security management while cutting costs. The result is improved efficiency without compromising protection.



Tanium supports key technical requirements outlined in CMMC (relative to Tanium products), including:

- 100% of the Risk Assessment family requirements
- Over 75% of the Configuration Management family requirements
- Over 65% of the Incident Response family requirements



Tanium is CMMC Level 2 Certified

How does Tanium help achieve CMMC compliance?

The Tanium platform provides an integrated solution that aligns directly with many of CMMC's technical controls while delivering significant operational benefits:

- **Real-time visibility:** Tanium offers continuous monitoring of all endpoints, ensuring that organizations have real-time visibility into their IT environment. This is crucial for maintaining asset management and security controls required by CMMC.
- **Proactive security hygiene:** By continuously assessing and improving the security posture of endpoints, Tanium helps organizations maintain strong security hygiene, which is essential for meeting the CMMC foundational cybersecurity requirements.
- **Autonomous endpoint management:** Tanium automates patch and configuration management, ensuring that all systems are up-to-date and compliant with security policies. This helps meet the configuration management and maintenance requirements of CMMC.
- **Automated incident response:** Tanium provides tools for rapid detection and response to security incidents, helping organizations quickly mitigate threats. This capability supports CMMC incident response and risk management requirements.
- **Continuous compliance reporting:** Tanium generates detailed compliance reports and audit trails automatically, simplifying the process of demonstrating adherence to CMMC standards. This aligns with the audit and accountability requirements.

Mastering CMMC compliance maturity with automation

CMMC's tiered model reflects increasing levels of cybersecurity maturity across organizations supporting the DoW. At Level 1, organizations must demonstrate basic cyber hygiene. At Level 2, the focus shifts to establishing a robust IT management framework. Level 3 raises the bar even further, requiring automated, continuous assessment and enforcement of security controls.

By integrating AI and intelligent automation, Tanium provides the ability to meet these evolving requirements with confidence—delivering broad technical capability, engineered automation, and real-time reporting across the entire endpoint estate.

Tanium directly supports critical Level 3 controls, including:

- Automated detection and remediation of unauthorized or misconfigured systems (CM.L3–3.4.2e)
- Continuous discovery and inventory of system components (CM.L3–3.4.3e)
- Policy enforcement restricting access to only trusted, compliant systems (IA.L3–3.5.3e)
- Advanced analytics to identify and predict risks (RA.L3–3.11.3e)
- Integration of threat intelligence for proactive detection and hunting (SI.L3–3.14.6e)

Additionally, Tanium helps organizations accelerate CMMC readiness and scale compliance efforts with:

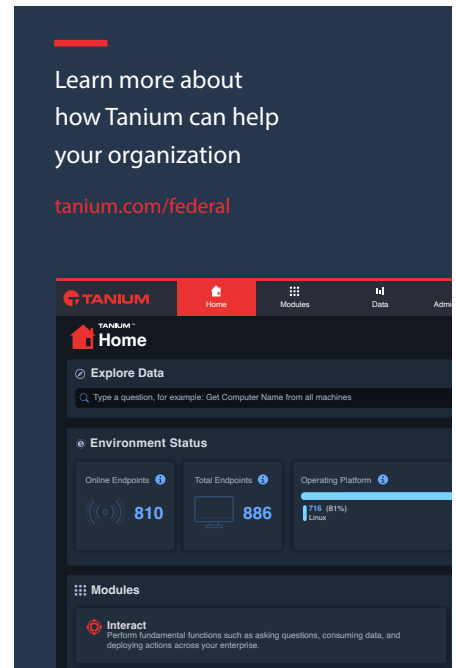
- Supplier Performance Risk Scoring System (SPRS) optimization: Monitor compliance posture, identify gaps, and close Plan of Action and Milestones items within required timelines
- Supply chain compliance enforcement: Oversee subcontractor compliance and fulfill critical flow-down requirements
- Assessment readiness enablement: Provide the evidence you need to streamline Certified Third-Party Assessor Organization (C3PAO) and Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessments and stay certification-ready year-round

Secure CUI and maintain DoW engagements with Tanium

Protecting CUI is not just a compliance checkbox—it's a security imperative at the heart of national defense operations—and the cornerstone of maintaining trust with the DoW. The Tanium platform empowers organizations to achieve CMMC compliance and secure CUI with confidence, enabling organizations to continue vital partnerships, research, and processing data with the DoW while meeting or exceeding CMMC requirements.

By combining real-time visibility, automated management, and proactive risk mitigation, Tanium reduces IT risk, strengthens security resilience, and protects sensitive data. With Tanium, defense contractors and subcontractors can proactively safeguard critical information, accelerate compliance, and sustain long-term mission readiness in an evolving threat landscape.

* Percentages of product coverage is based on current product capabilities relevant to Tanium product offerings and is subject to change as product offerings evolve.



Tanium is the Autonomous IT company. Driven by AI and real-time endpoint intelligence, Tanium Autonomous IT empowers IT and security teams to make their organizations unstoppable. Many of the world's leading organizations trust Tanium's single, unified platform for endpoint management and security to innovate faster, stay resilient and move business forward with confidence, at scale.

Visit us at www.tanium.com and follow us on [LinkedIn](#) and [Twitter](#).

© Tanium 2026