

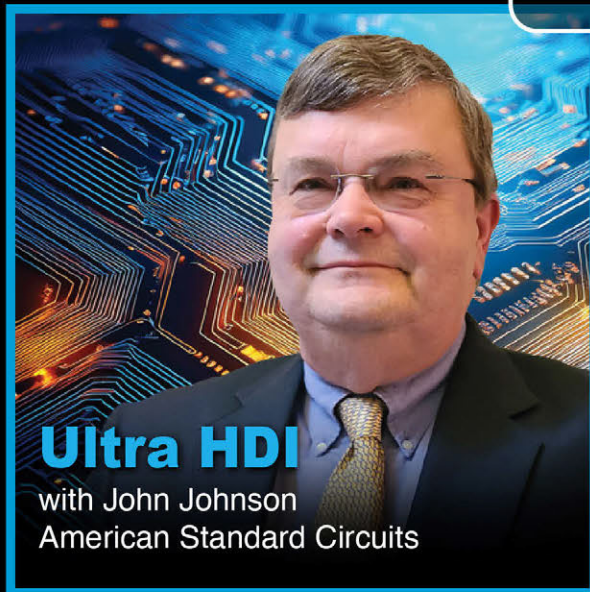
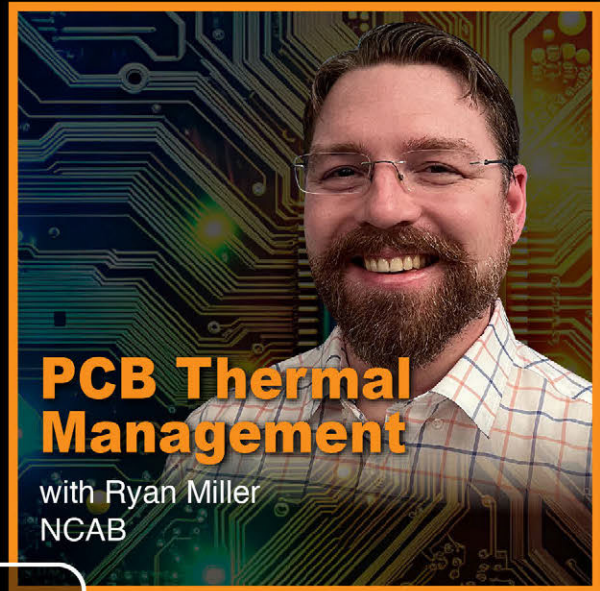
AUGUST 2026

SMT007

MAGAZINE

CMMC 2.0
↑
UPDATE

Now Playing



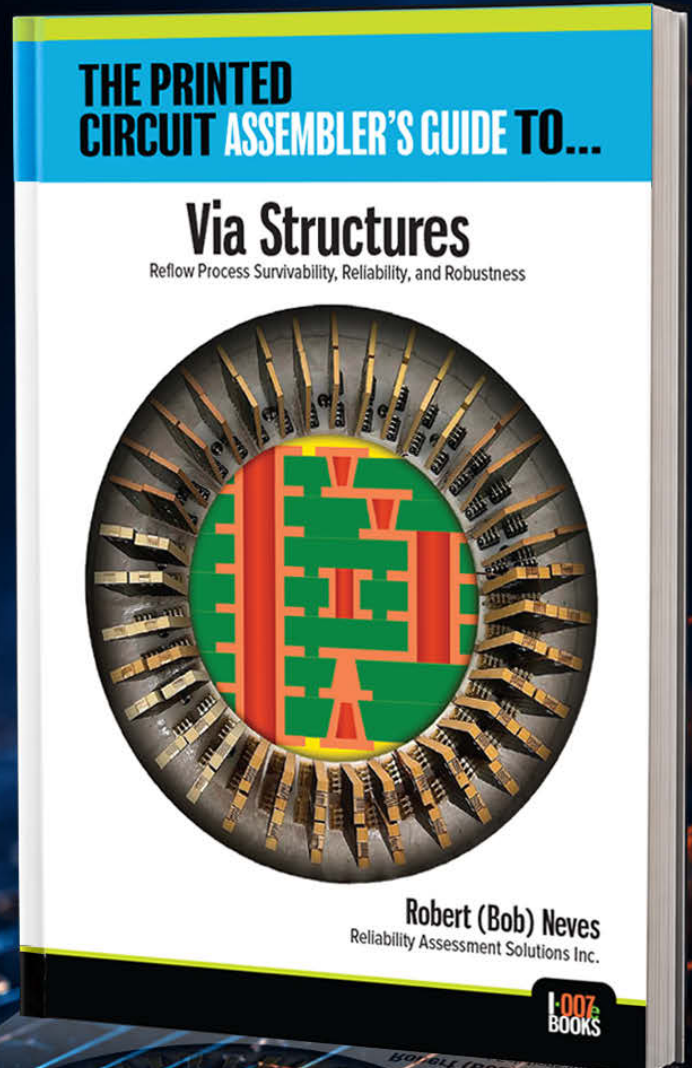
PODCAST SERIES
WITH BONUS COMPANION GUIDES

THE HEAT IS ON. WILL YOUR VIAS HOLD UP?

Learn how to identify **vulnerabilities** and build more robust, **reliable** assemblies.

“Bob Neves makes a compelling case for why single via testing is superior to traditional daisy chains in certain situations.”

—Todd MacFadden, Bose



Available Now 

I-007eBOOKS

Cybersecurity Beyond Compliance

Cybersecurity certification has become a competitive requirement for companies serving defense and other high-reliability markets. This issue explores why CMMC matters, what achieving certification requires, how leading EMS companies are preparing, and why strong cybersecurity practices remain essential even as the Department of Defense (War) reevaluates the certification rollout.

From The Editor

- 6** *Nolan's Notes*
The CMMC Certification Question Mark
by Nolan Johnson

Features

- 10** **CMMC 2.0: The Defense Supply Chain's Next Qualification Requirement**
by Nolan Johnson
- 14** **Naprotek and SemiGen's Path to CMMC Level 2 Certification**
by Tim Filteau
- 26** **How San Francisco Circuits Achieved CMMC Certification**
by Daniel Porton and Alex Danovich
- 30** **EMS Companies Respond to CMMC Suspension**
by Nolan Johnson
- 38** **Decoding the CMMC Suspension**
by Divyash Patel

Articles

- 50** *Tariff Terminal*
USMCA Rules of Origin for Electronics: What Could Change in 2026
by James Kim

Columns

- 42** *Knocking Down the Bone Pile*
Hot Air vs. Infrared PCB Rework
by Nash Bell

August 2026

22 **Omega EMS Advances Toward CMMC Level 2 Certification**
with Chris Alessio

Shorts

- 25** **The Printed Circuit Assembler's Guide to... Design for Test: A Practical Guide to Test and Inspection**
by Bert Horner
- 34** **Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements Implementing the Department of War's CMMC Suspension**
- 41** **Flashback Roundtable: Today's Cybersecurity Strategies**
with Hiroyuki Watanabe, Uday Ali Pabrai, and Divyash Patel

In Every Issue

- 48** MilAero007 Highlights
- 56** Career Opportunities
- 64** Educational Resources
- 65** Advertiser Index

SMT007
M A G A Z I N E

Coming to Technica in September 2026: **The SIPLACE CA2**

A game changer for high speed chip assembly direct from wafer



ASMPT

The SIPLACE CA2 has been designed ground up for chip assembly direct from wafer and smt placement in one machine. The unique buffering system allows the machine to run flip chip at 51,000 cph direct from wafer and die attach at 54,000 cph direct from wafer. Way faster than any die bonder! This allows the machine to run direct in-line for submodule assembly.

What's the benefit to YOU? Huge savings in the taping costs of die into SMT reels.

Book your own private demo, September 21st through the 25th.

Use the QR code or contact Yannick Green, ygreen@technica.com, to schedule.



TECHNICA, U.S.A.

1-800-909-8697 • www.technica.com

The CMMC Certification Question Mark



BY NOLAN JOHNSON, I-CONNECT007

About a year ago, the Global Electronics Association published a report, “Interconnected: Global Electronics Trade in an Age of Disruption,” which made a convincing case that the electronics industry is the most globally interconnected industry on the planet. But those digital connections come with a warning label: Storing and transferring large amounts of intellectual property means facing data security challenges we’ve never seen before.

Cybersecurity is no longer a nice-to-have proposition. You can’t just say, “We’re a little company; the

hackers don’t even know who we are.” That’s simply no longer valid. In fact, cybersecurity experts will tell you that hackers tend to break into value chains more often at small- to medium-sized companies, where security is weakest. Claiming anonymity and obscurity is no longer a choice for these companies.

Recently, I came across a blog post claiming that hackers had stolen schematics for the Apple iPhone 18 from Tata, an Indian supplier in the Apple value chain. I traced the story back to Appleinsider.com, which broke the news. Other mainstream channels picked up the story and added their own



BLACKFOX

Premier Training & Certification

Experience the Blackfox Difference!

Premier IPC Training & Certification

- High quality training and customer service
- Offering 6 certification programs in 6 locations and online
 - *Colorado, Arizona, Guadalajara & Queretaro, Mexico, Malaysia and Singapore*
- Custom courses to fill knowledge & skill gaps
- IPC/WHMA-A-620 Space Addendum for trainers and specialists
- Online store supporting the training industry



[CLICK FOR COURSE SCHEDULE](#)

For more information contact us at
888.837.9959 or sharonm@blackfox.com

www.blackfox.com

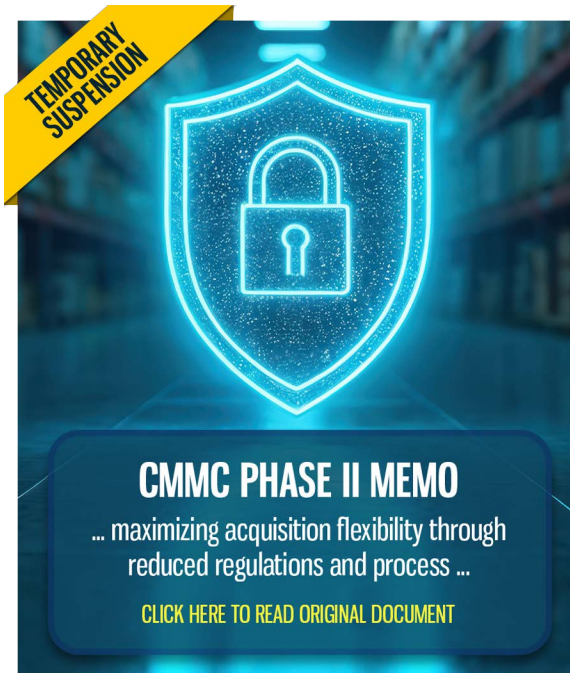


reporting (so some details may be suspect), but the overall story has merit. Tata is a mega-corporation you would expect to have robust cybersecurity, yet it still suffered a breach. Not to be alarmist, but if Tata is vulnerable, so are you, and it's exactly why we're devoting this month's issue to the U.S. Cybersecurity Maturity Model Certification (CMMC) program.

CMMC is the government's system to ensure that if you're handling sensitive information, you're also protecting it. It began as a response to cybersecurity breaches in the U.S. defense industry ecosystem. The U.S. Department of Defense set a Nov. 10, 2026, deadline to comply with its CMMC Phase II requirements, then recently pulled back on that date, and called for a 60-day evaluation. It was a big deadline, to be sure, and many companies of all sizes in the supply chain have been steadily working toward compliance.

That's key to the success of the CMMC program. Even if you don't do direct defense work, you might still need to increase your data security. The Tata iPhone example confirms the value in that. Each of your customers is a separate, distinct value chain. Do you know the full extent of each? How many of those value chains lead to a military application? The military drone teardown videos so popular on YouTube these days show that some surprisingly consumer-level components are now key systems in military assets. One could argue that CMMC is a good idea, no matter where you fit in the EMS value chain.

In this issue, we begin by exploring CMMC's history and implications. Then we talk to three EMS companies pursuing CMMC Level 2 certification: one that has achieved its certs and two that were on track to do so before the November deadline. Each company shares its perspective on the pro-



cess and the implications for its business going forward into 2027. We also include a cybersecurity roundtable from APEX EXPO 2026 in Anaheim, where I moderated a compelling panel discussion on the reasons and practicalities of CMMC certification.

With such important steps in motion, the recent DoD news about the CMMC suspension came as a bit of a surprise. We asked our sources how this news would change their plans, and you'll find those up-

dates in this issue, as well as a reaction piece from recurring CMMC contributor Divyash Patel.

To round out this August issue, tariff expert James Kim continues his discussion of the USMCA, and Nash Bell's column compares hot-air and infrared device removal methods for rework.

Cybersecurity always carries some controversy. Opinions vary on how much money and time must be invested to be the most effective. In this case, however, even the U.S. government is having second thoughts about whether this protocol is appropriate for supporting sensitive military and government work in a sustainable way. Is this our new de facto standard? Perhaps it's too soon to tell, but how will CMMC affect your business? Are you seeking certification? Is CMMC too much, or not nearly enough? Drop me an email at editorial@iconnect007.com.



Nolan Johnson is managing editor of *SMT007 Magazine*. Nolan brings 30 years of career experience focused almost entirely on electronics design and manufacturing. To contact Johnson, [click here](#).

Technology, and People, You Can Trust.

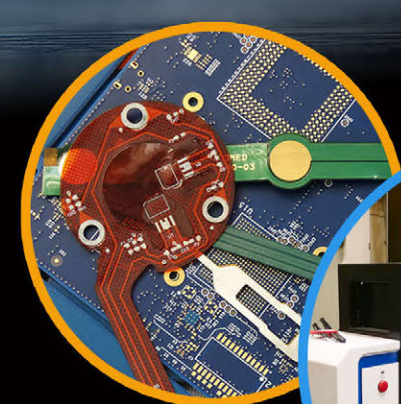
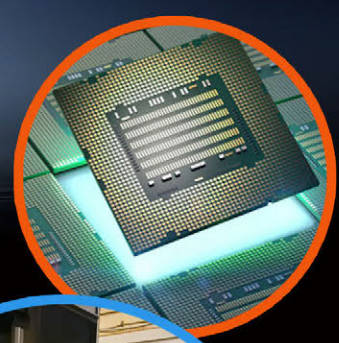


Specialties:

- RF/ Microwave
- UHDI
- Rigid-flex
- High Reliability
- Aerospace/Medical

...and Specialists:

- DFM / DFX Support
- Collaboration
- Project Guidance



asc-i.com



CMMC 2.0

The Defense Supply Chain's Next Qualification Requirement

The U.S. Department of Defense's Cybersecurity Maturity Model Certification (CMMC) program has finally moved from concept to contract language. Cybersecurity compliance for companies hoping to participate in the defense supply chain is now a prerequisite for doing business, right alongside AS9100, ITAR, Nadcap, and IPC standards.

For years, many organizations have self-attested to cybersecurity compliance. Unfortunately, a series of high-profile cyber incidents demonstrated that self-attestation didn't always translate into effective implementation. Sensitive information would leak through vulnerabilities in the Defense Industrial Base (DIB), often via suppliers and subcontractors. The DoD wants verification that



50
YEARS
1976 - 2026



SPEA

SINCE 1976, WE HAVE POWERED THE TECHNOLOGY THAT MOVES THE WORLD.

Electronics has always been the foundation for invention, innovation, and revolution. Yet, one constant remains: the need for reliable, high-performing, and defect-free devices. Exactly what SPEA testers are engineered to guarantee.



Table 1: Defense-related cyberattacks leading to CMMC certifications

INCIDENT	YEAR	SIGNIFICANCE
Operation Aurora	2009–2010	Targeted technology and defense firms to steal intellectual property; highlighted advanced persistent threats (APTs) and supplier vulnerabilities.
RSA SecurID Breach	2011	Compromise of authentication technology used throughout government and defense sectors.
Lockheed Martin Attack	2011	Attackers leveraged information obtained from the RSA breach to target one of the largest U.S. defense contractors.

contractors handling sensitive information are actually protecting it. CMMC 2.0 is the DoD’s answer.

The CMMC 2.0 framework establishes three levels of cybersecurity maturity:

- **Level 1, Foundational:** Focuses on basic cyber hygiene and protection of Federal Contract Information (FCI). Organizations perform annual self-assessments.
- **Level 2, Advanced:** Aligns with the 110 security controls contained in NIST SP 800-171, the long-established standard for protecting Controlled Unclassified Information (CUI). Depending on the program, organizations may perform self-assessments or undergo third-party assessments by authorized C3PAOs.
- **Level 3, Expert:** Applies to a relatively small group of contractors supporting critical national security programs and includes additional government-led assessment requirements.

The framework may sound technical, but the underlying objective is to establish confidence that sensitive information is protected throughout the defense supply chain.

How We Got Here

The roots of CMMC go back much further than most people realize. In 2010, Executive Order 13556 established a government-wide framework

for handling CUI. Several years later, DFARS clause 252.204-7012 required defense contractors to implement cybersecurity controls in accordance with NIST SP 800-171.

The challenge wasn’t defining the requirements but verifying compliance. As cyberattacks increasingly targeted defense suppliers, the DoD recognized a recurring pattern: Adversaries weren’t always attacking prime contractors directly. Instead, they were looking for easier entry points, such as smaller suppliers, manufacturing partners, design firms, and subcontractors that possessed valuable technical data but often lacked the cybersecurity resources of larger organizations.

In many cases, the weakest link wasn’t at the top of the supply chain, but somewhere in the middle. That realization led to the launch of CMMC 1.0 in 2019.

Why CMMC 1.0 Struggled

When CMMC 1.0 was introduced, industry reaction was immediate. Many organizations supported the goal of improving cybersecurity but raised concerns about the program’s complexity, cost, and implementation. The original model included five maturity levels and a large number of practices and process requirements that many companies found difficult to interpret. Smaller contractors worried about certification costs. Industry questioned whether there were enough qualified assessors to support the entire DIB. Program governance and accreditation processes were still evolving.

Many small and mid-sized manufacturers, which were the most vulnerable to cyber threats, were often the least prepared to absorb the burden of certification because they lacked the infrastructure to manage it. Recognizing these concerns, the DoD paused the rollout and reworked the program. The result became CMMC 2.0.

What's Different About CMMC 2.0?

CMMC 2.0 streamlined the framework from five levels to three. It aligned requirements more closely with existing NIST standards that contractors were already using and reintroduced self-assessments for certain lower-risk environments.

According to affected suppliers, the revised model is easier to understand and more practical to implement, but that doesn't necessarily make it easier to achieve. Organizations that have completed certification efforts consistently report that while the roadmap is clearer, the work remains substantial. Cybersecurity controls still must be implemented, documented, maintained, and demonstrated. In other words, simplification hasn't eliminated the effort required.

Important Notes for Electronics Manufacturers

Many companies in the electronics industry underestimate their exposure to CMMC requirements. A PCB fabricator may not consider itself a defense contractor. An EMS provider may never receive a contract directly from the DoD. A machining supplier or cable-and-harness manufacturer may be several tiers removed from the prime contractor. That distance doesn't matter in a CMMC supply chain.

Defense programs depend on those complex supply chains. Engineering files, Gerber data, fabrication drawings, bills of materials, assembly instructions, test procedures, and revision-controlled documentation move through numerous organizations before a product is delivered. If that information is classified as CUI, then cybersecurity obligations travel right along with it.

The further you look into the defense supply chain, the more likely you are to find companies that don't realize they are supporting defense work at all. Eventually, many of those organizations will be asked to demonstrate cybersecurity compli-

ance. For manufacturers, cybersecurity is becoming a supply-chain issue rather than simply an IT issue.

Phased Implementation

The DoD formally established the CMMC framework through its final rulemaking process, and phased implementation is underway. That matters because requirements are appearing in contracts rather than in guidance documents.

Organizations that wait until a customer requests certification may find themselves behind schedule, or worse, replaced as a supplier. Achieving compliance often requires significant preparation: identifying gaps, implementing controls, documenting procedures, training personnel, and preparing for assessments. Those activities rarely happen quickly.

Companies that start early typically experience fewer disruptions, lower implementation costs, and less risk of losing business opportunities. Companies that wait may find themselves scrambling to catch up.

The electronics manufacturing industry already understands disciplined operational systems. We manage quality systems, maintain traceability, and document processes. We comply with customer, industry, and regulatory requirements every day. CMMC introduces cybersecurity as another operational discipline.

Increasingly, OEMs are evaluating cybersecurity maturity the same way they evaluate quality systems, manufacturing capability, and supplier reliability. Cybersecurity is becoming part of supplier qualification.

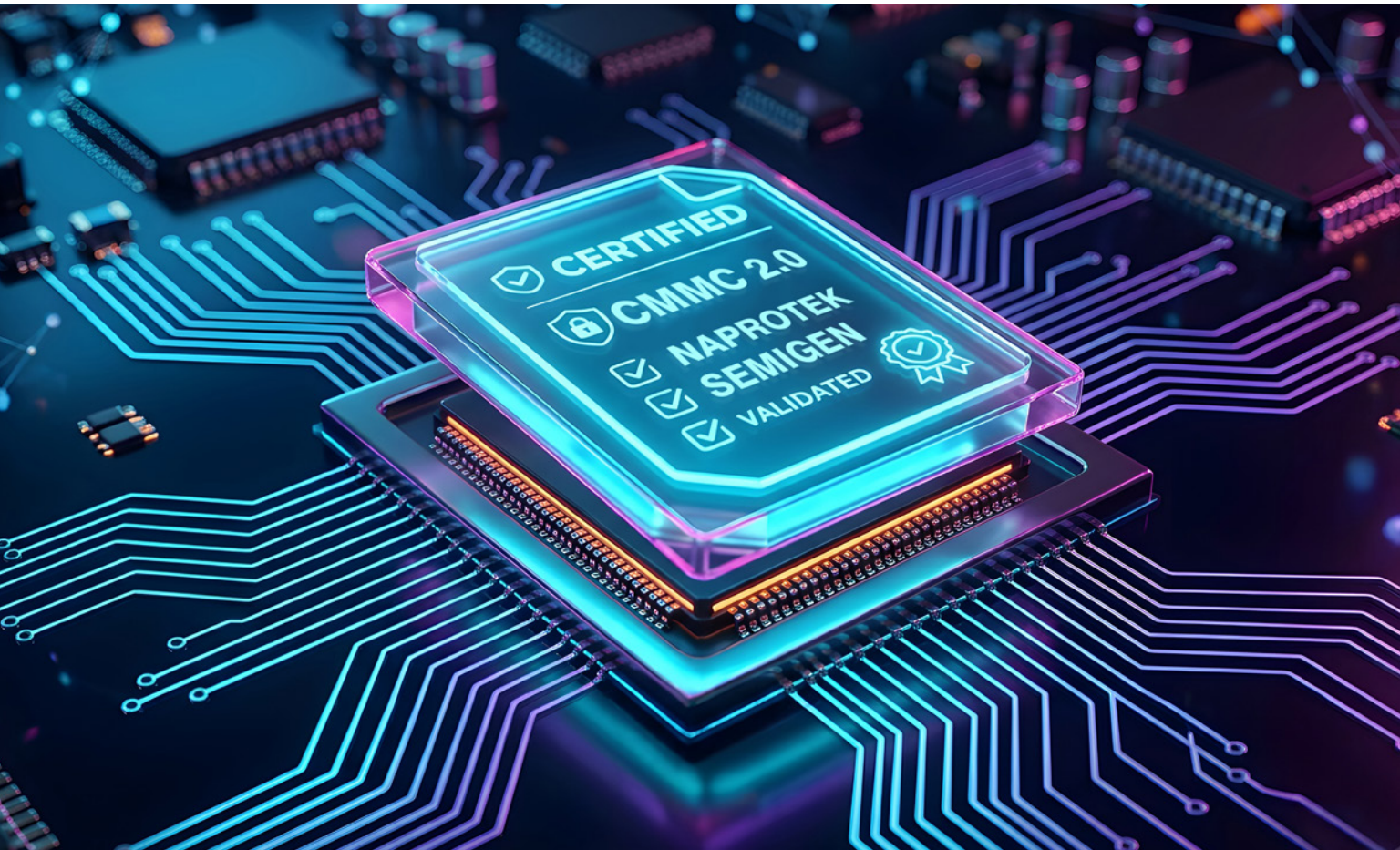
Conclusion

As of July 13, the DoD suspended its Nov. 10 deadline to meet all CMMC 2.0 requirements, specifically aimed at helping small and mid-sized businesses reduce the bureaucracy required for compliance. The pause includes a 60-day study of the future of the program, and the DoD states that all CMMC 1.0 requirements remain in place.

For companies throughout the electronics manufacturing supply chain, however, cybersecurity verification is becoming a routine condition of doing business. The organizations that recognize this shift early will be better positioned to compete for defense-related opportunities in the years ahead.

SMT007

Naprotek and SemiGen's Path to CMMC Level 2 Certification



Editor's note: Naprotek and SemiGen earned their certification in May 2026. Here's what the process required, and what it signals to prime contractors vetting their suppliers.

When Naprotek, LLC and SemiGen, its RF Assembly & Components Center of Excellence, achieved Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 in May 2026, the announcement marked the end of a multi-year effort and the beginning of something more durable: a verified security posture that defense customers can rely on without taking anyone's word for it.

Cybersecurity is foundational to the trust our defense customers place in us. This certification is

the product of a sustained, company-wide commitment to the people, processes, and infrastructure needed to protect controlled unclassified information. We're proud to give our customers across both Naprotek and SemiGen confidence that their data and programs are in accountable hands.

That word "accountable" carries weight in defense manufacturing. Programs don't get second chances. The Controlled Unclassified Information (CUI) flowing through an EMS provider

Where the Electronics Manufacturing Community Connects



TECHNICAL CONFERENCE

35+ sessions across 6 tracks

Deep-dive presentations and research direct from the engineers solving today's challenges

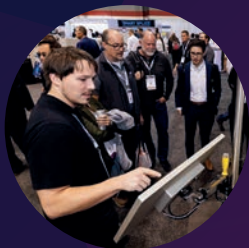


EXHIBIT FLOOR

See equipment in motion

Hundreds of suppliers demonstrating live process, inspection, and assembly solutions on the show floor



PEER NETWORK

Make meaningful connections

Engage with industry peers, collaborators, and potential partners throughout the event



EDUCATION

Hands-on professional development

Application-oriented courses, workshops, and in-depth training led by internationally respected experts

smtai.org

OCTOBER 25 - 29, 2026
ROSEMONT, ILLINOIS, USA

belongs to platforms, contracts, and people who depend on its protection. Accountability, in that environment, is an operating principle before it is ever a certification requirement.

What Level 2 Requires

CMMC Level 2 is among the most demanding cybersecurity standards applied to the Defense Industrial Base (DIB); it's the commercial ecosystem of manufacturers, suppliers, and contractors that keeps the U.S. military equipped and operational. Achieving it requires organizations to implement and demonstrate adherence to all 110 security controls outlined in NIST Special Publication 800-171 Revision 2, codified in Title 32, Part 170 of the Code of Federal Regulations.

Level 2 certification requires an independent Certified Third-Party Assessment Organization (C3PAO) to verify that every control is in place and functioning, and not simply documented on paper. Naprotek's assessment was conducted by KLC Consulting, Inc., an authorized C3PAO. The result: Naprotek's enterprise information environment was confirmed to meet Department of Defense requirements for handling CUI, with certification valid from May 16, 2026, through May 15, 2029.

That distinction carries real weight for procurement teams. CMMC Level 2 requires a qualified outside organization to examine an EMS provider's people, systems, and documented processes before any certification is issued. For prime contractors and program offices managing supplier compliance, a C3PAO-verified certification is a docu-

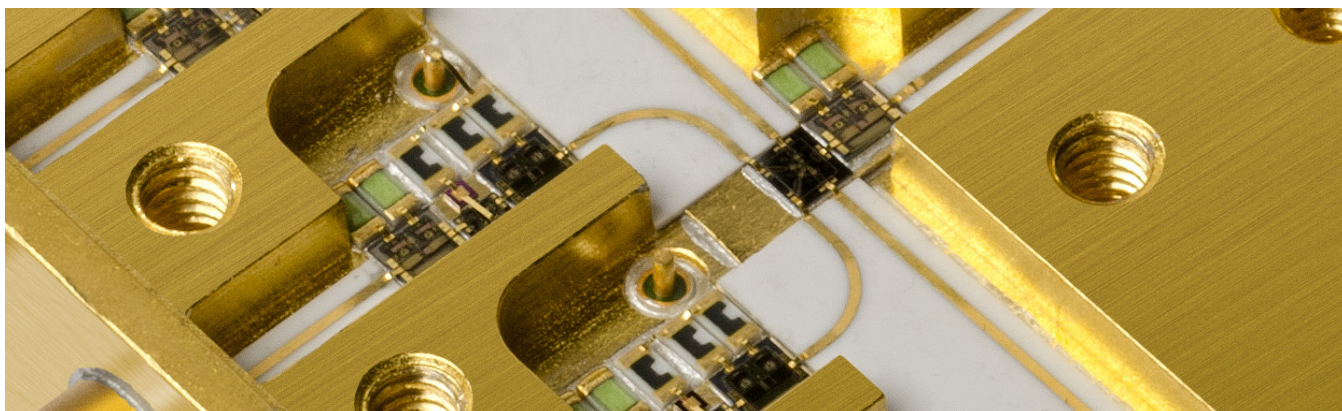


RF board under assembly.

mented, auditable answer to questions that otherwise require time-consuming supplier evaluations.

What Joint Certification Means for Procurement

What makes Naprotek and SemiGen's certification particularly notable for procurement teams is its scope. Both companies achieved certification together, meaning customers working with either entity operate within a single, unified security environment. For procurement teams, that eliminates a step: Rather than evaluating two suppliers separately and managing compliance documentation for both, they have one verified partner that covers two specialized capabilities.



RF microwave assembly close up.



**The Test
Connection, Inc.**

*Leading in quality and test engineering
since 1980*

NEW!



**PRIME X-RAY
SYSTEM**



Test Solutions & Services for
Test Programming, Board Test,
In-Circuit Test, Functional and
Boundary Scan



THE TRAINING CONNECTION, LLC

Knowledge • Training • Certification • Success



Your fast track to hands-on
mastery, industry-recognized
credentials, and career-boosting
confidence.



Download
Your Copy
Now



410-205-7300
112 Lakefront Drive
Hunt Valley, MD 21030

Naprotek brings deep expertise in complex, high-reliability PCBA and RF/microwave assembly for defense, space, medical, semiconductor capital equipment, and test and instrumentation markets. SemiGen serves defense, SATCOM, space, and advanced communications customers as Naprotek's dedicated RF Assembly & Components Center of Excellence. Together, they represent a manufacturing partnership with two distinct specializations and one shared, verified security posture.

For procurement teams already under pressure from supplier vetting requirements, that consolidation has real value. Naprotek and SemiGen are pre-certified, audit-ready, and prepared to provide compliance documentation on request, reducing supply chain risk and simplifying onboarding for programs with CMMC requirements.

CMMC Among a Broader Compliance Portfolio

CMMC Level 2 joins an existing set of quality and compliance credentials, including ISO 9001, AS9100D, ISO 13485, and ITAR registration, that cover the defense, aerospace, and medical markets. Maintaining that range of certifications simultaneously requires its own discipline, documentation culture, and internal ownership. Each standard demands ongoing investment, not a one-time achievement.

That portfolio spans defense, aerospace, and medical markets, each with its own documentation requirements, audit cycles, and internal ownership.

We wanted to proactively meet the mandatory requirements for DoD contracts and demonstrate our continued commitment to quality, security, and compliance.



Naprotek's Facility in San Jose, California.

As CMMC requirements become standard practice across the DIB, suppliers who are certified early will enter competitive procurements with documentation already in order.

Inside the Certification Process

Colby Cail, director of information technology, led the certification effort at Naprotek and SemiGen and is candid about what companies should expect when they begin.

"Getting to Level 2 took sustained effort across the entire organization until the controls became part of how we operate," Cail says. "When you implement 110 controls, you quickly learn that the calendar doesn't care that you're also running production."

Start With an Honest Gap Assessment

The path to Level 2 certification begins with a gap assessment, mapping where the organization currently stands against each required control. For most companies, that assessment is more sobering than anticipated. Controls that appear manageable on paper—access management, incident response, audit logging—frequently reveal systemic gaps in documentation, process, or infrastructure when examined in practice.

"Don't assume you're closer than you are," Cail advises. "The gap between where most organizations start and where Level 2 requires them to be is wider than expected. Build a realistic timeline, and then add a buffer, particularly if the effort will run alongside active production."

Building the Discipline

From there, the work is sustained and multi-phase: policy rewrites, system hardening, physical



SemiGen's Londonderry, New Hampshire facility.

Open the Door to a **WORLD** of PCB Sourcing Solutions



Our staff can open the doors to Asia-based factory solutions not previously available to your purchasing team. We do this with integrity and transparency, as if we were a trusted member of your PCB sourcing team.

[Open the Door and Learn More](#)

Linkage
Technologies

✉ info@linkage-tech.com
🌐 linkage-tech.com



security upgrades, vendor management reviews, and employee training. Then comes the less visible but equally important work of living with those controls long enough for them to become an operational habit. The 110 controls touch HR, physical security, executive accountability, and incident response planning. Every function has a role.

At Naprotek and SemiGen, that meant building cybersecurity awareness into onboarding and ongoing training, implementing documentation discipline that makes every control traceable and auditable, hardening systems against both external threats and insider risk, and developing incident response capability that gets tested regularly rather than sitting in a binder.

“People assume the technology is the obstacle,” Cail notes. “In our experience, the discipline to maintain controls consistently—month after month, while running a manufacturing operation—is where organizations struggle. Executive ownership made the difference for us. When leadership treats cybersecurity as a business priority, the rest of the organization follows.”

Choose Your C3PAO Relationship Carefully

The third-party assessment is what separates certified from claimed, but the C3PAO relationship matters well before assessment day. The organization you work with is a resource, not just a gatekeeper. Cail’s advice is to find a partner that helps your team understand the standard, not simply pass

it. The goal is a durable security posture. A one-time assessment result that doesn’t reflect how your organization operates will not hold up over three years of continuous compliance.

Verified, Not Claimed

CMMC Level 2 certification carries real procurement value. Certified suppliers are better positioned in competitive bids, and that is a legitimate business outcome. But for prime contractors and program offices evaluating their supply chains, the more meaningful result is the removal of uncertainty.

Because the programs depending on that data have no tolerance for gaps, 110 controls are independently verified across people, systems, and operations. Naprotek and SemiGen pursued this certification so their customers don’t have to wonder whether their supplier is ready. An independent third party has examined the environment and confirmed it meets the standard.

In a market where cybersecurity claims are easy to make, that verification is the differentiator that holds. **SMT007**



Tim Filteau is president and CEO of both Naprotek and SemiGen.

SUSTAINABLE CONFORMAL COATING—NO COMPROMISE REQUIRED

Yes, you can use actnano materials with Nordson conformal coating systems.

Sustainability initiatives often stall when they threaten line stability. Nordson engineered its conformal coating platforms to run advanced actnano materials using targeted equipment upgrades—not full system replacements.

From circulating fluid delivery to extraction filtration, you can stay in control of coating quality, uptime, and throughput.

- Compatible with ASYMTEK Select Coat® SL-940 and SL-1040 conformal coating systems and valves
- Supports circulation, agitation, and material stability
- Enables transition to safer, sustainable materials without throughput loss

Download the actnano Upgrade Guide
Equipment options, configurations, and part numbers included.



OMEGA EMS

Advances Toward CMMC Level 2 Certification

In June, Omega EMS announced its intention to achieve CMMC Level 2 before the U.S. Department of Defense's mandatory November 2026 implementation timeline for organizations handling Controlled Unclassified Information (CUI). We caught up with Omega EMS CEO Chris Alessio to discuss the company's certification journey, the investment required, and what CMMC means for Omega's military and aerospace business. *Note: The DoD has suspended its November requirement pending a 60-day review.*

Nolan Johnson: Chris, where are you with the Level 2 CMMC certification?

Chris Alessio: We have successfully completed both our CMMC Level 1 and Level 2 self-assessments. Those assessments identified the remaining gaps, and we've developed a structured remediation plan with clear milestones to achieve formal CMMC Level 2 certification before the Department of Defense enforcement timeline. We expect to complete certification in late September or early October, providing additional schedule margin before enforcement begins.

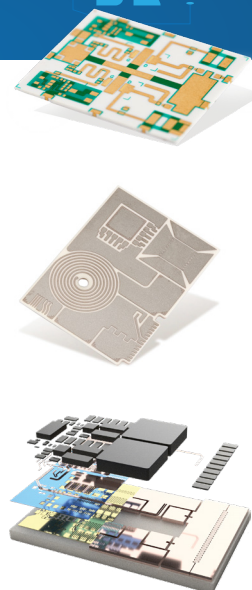
WHEN PCBs WON'T DO, BE CERTAIN WITH CERAMIC.



Working on a design that exceeds the capabilities of ordinary PCB? Remtec's metallized ceramic substrates, components, and packages may **be the solution.** Offering superior thermal conductivity, isolation, and dielectric strength – as well as exceptional mechanical stability, environmental robustness, and plenty of versatility and integration opportunities – Remtec ceramic techniques like Direct Bond Copper (DBC), Active Metal Braze (AMB), and Plated Copper on Thick Film (PCTF) are a powerful option for today's high-power, high-density, microelectronic applications. All from a U.S.-based, ITAR-compliant, and OSAT-ready resource with decades of experience.

PCBs not cutting it? Consider the many advantages of ceramic from Remtec.

Visit remtec.com, call **781-762-9191**, or email sales@remtec.com to initiate a quote.



Visit Remtec.com



Can you help us better understand the CMMC process to become certified?

Our IT and compliance teams have been leading this initiative for several months alongside experienced CMMC advisors. It's a significant investment, not only financially but organizationally, but one we believe is essential.

We've been ITAR-registered for many years and maintain certifications, including AS9100 and ISO 13485. CMMC builds on that foundation by introducing a much deeper level of cybersecurity governance, access control, continuous monitoring, and protection of CUI.

More importantly, it changes culture. As companies grow, processes that worked at \$20 million don't necessarily work at \$100 million. CMMC forces organizations to mature their cybersecurity practices across technology, processes, and people, ultimately making Omega a stronger company.

For final certification, I understand you'll undergo a formal audit. Will that be with the same people who helped with your Level 2 assessment?

No. The formal certification will be conducted by an accredited Certified Third-Party Assessment Organization (C3PAO). Our consultants have helped us prepare for certification, but the actual assessment will be performed independently, as required by the CMMC program.

What are the associated costs, and how soon will you see an ROI?

Initially, we estimated the investment would be approximately \$300,000. As we progressed through the assessment process, we recognized additional opportunities to strengthen our cybersecurity infrastructure beyond the minimum requirements. Today, we expect our total investment to approach \$750,000, with roughly half representing one-time infrastructure and implementation costs and the balance consisting of recurring software subscriptions, monitoring, and compliance services.

We're migrating to Microsoft GCC High, implementing CrowdStrike for endpoint protection, NinjaOne for systems management, Vanta for compli-



Chris Alessio

ance automation, Abnormal AI for email security, and several additional security platforms that collectively provide the controls required for CMMC Level 2.

We don't view this as a traditional ROI investment. We view it as a strategic investment that enables us to compete in markets where CMMC Level 2 certification is a prerequisite for doing business. Over time, these costs will naturally become part of the cost structure associated with serving the defense and aerospace markets.

For a \$100 million company, those recurring costs represent only a fraction of a percent of revenue.

I agree. Our recurring cybersecurity costs are roughly double what they were previously, but in the context of a company our size, they're manageable. More importantly, they're an investment in future growth and customer confidence.

You've publicly committed to this initiative. How close are you?

This is one of the most important strategic initiatives we've undertaken in recent years. Our military and aerospace business continues to grow rapidly, and we're seeing increasing customer demand for CMMC-certified manufacturing partners. We've completed the assessment phase, we're executing against our remediation plan, and we're approximately 80% through our implementation schedule. We're very confident we'll achieve certification on time.

Are customers beginning to require CMMC?

Absolutely. Virtually every new military and aerospace opportunity now includes discussions around CMMC readiness. Existing customers have also made it clear that cybersecurity maturity is an important supplier qualification. Had we not started this journey early, many of those opportunities simply would not be available to us.

How does CMMC benefit customers outside the defense industry?

That's one of the biggest misconceptions about

CMMC. While it was created for the defense industry, the cybersecurity discipline brings benefits to every customer we serve.

Whether you're building medical devices, industrial controls, semiconductor equipment, or defense electronics, intellectual property protection and data security matter. CMMC drives stronger governance around who can access data, where it's stored, how it's monitored, and how it's protected. Those are capabilities every OEM values, regardless of industry.

How will CMMC help Omega move beyond the \$100 million milestone?

The defense and aerospace market represents one of the fastest-growing opportunities in advanced electronics manufacturing. We believe CMMC certification positions Omega EMS to participate in that growth while also making us a stronger partner for customers across every market we serve.

Our objective isn't simply to reach \$100 million in revenue. It's to continue building a world-class manufacturing organization capable of supporting the most demanding customers in the industry. CMMC is one more important step in that journey.

Thank you, Chris, and best of luck.

Thank you, Nolan. We appreciate the opportunity to share our story. **SMT007**

BOOK EXCERPT

The Printed Circuit Assembler's Guide to...Design for Test *A Practical Guide to Test and Inspection*

by Bert Horner, The Test Connection, Inc.

Chapter 6: Measuring Effectiveness With PCOLA-SOQ

In modern electronics manufacturing, success is not measured simply by whether a board powers on; it is defined by the level of confidence in its quality, long-term reliability, and the repeat-



ability of results across every production run. A well-designed test strategy goes beyond defect detection. It provides quantifiable, evidence-based assurance that every critical aspect of the assembly has been verified. This is where PCOLA-SOQ stands out as a robust framework. It transforms testing from a reactive process into a structured, measurable system that evaluates inspection and test effectiveness at both the component and pin level while linking coverage directly to manufacturing risk.

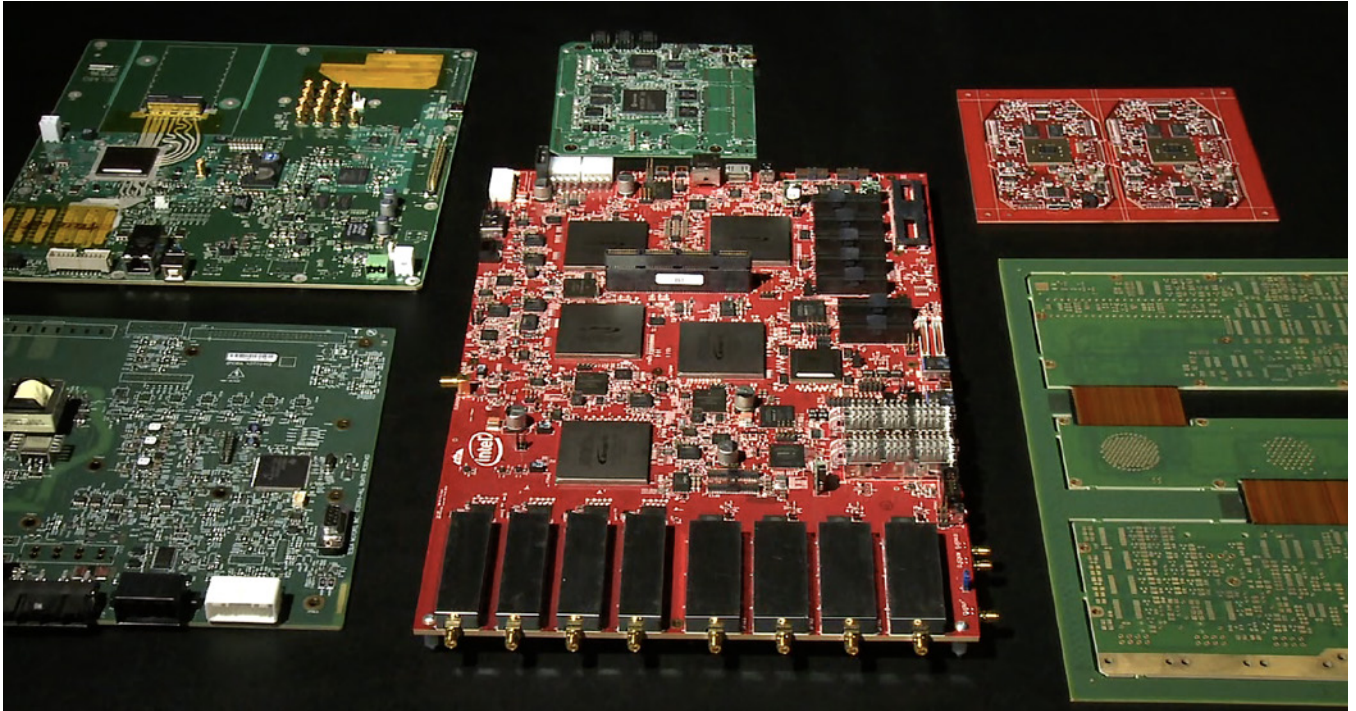
Defining Component and Pin-Level Coverage

PCOLA-SOQ breaks down test and inspection coverage into eight essential attributes that help teams visualize and quantify test completeness.

- **Presence:** Was the component placed?
- **Correctness:** Is it the correct part value/type?
- **Orientation:** Is it installed in the correct direction?
- **Live:** Does the part function electrically under power?
- **Alignment:** Is component correctly aligned to its pads?
- **Shorts:** Is the connection mechanically sound and reliable?
- **Opens:** Are all electrical connections intact?
- **Quality:** Are solder joints present and acceptable?

[Continue reading...](#)

How San Francisco Circuits Achieved CMMC Certification



While CMMC certification requirements have been paused by the U.S. DoW for further consideration and a new timeline, what follows is still relevant and applicable information.

When the U.S. Department of Defense began signaling that cybersecurity self-attestation would eventually give way to mandatory third-party certification, San Francisco Circuits decided to get ahead of it. That decision, made in 2019, shaped everything that followed: the systems we implemented, the partners we engaged, and the audit we ultimately passed. This is the story of that process, including what worked, what added complexity, and what we'd tell other EMS companies and defense suppliers that are now facing the same path.

Defense contractors that handle Controlled Unclassified Information (CUI) are now required to hold CMMC Level 2 certification to win new DoD work, and self-attestation is no longer accepted.

Level 2 requires full implementation of all 110 security practices aligned to NIST SP 800-171, covering every organization in the Defense Industrial Base supply chain that processes, stores, or transmits CUI.

Why It Matters for Defense Programs

For our customers working on defense and government programs, it's not whether their PCB supplier can build the board, but whether that supplier can be trusted with the data surrounding it. Design files, program specifications, and contract information flowing through a supplier's systems are part of the same security perimeter that CMMC is designed to protect.



KOH
YOUNG
TECHNOLOGY



Turn Every Data Point Into a Decision

Go beyond inspection. With AI-driven analytics, Koh Young turns data into insight, helping you predict, optimize, and elevate performance across your factory.

TURN DATA INTO RESULTS



KAP automatically generates inspection programs by recognizing component patterns and validating them against 3D measurement data.

KSMART turns inspection data into real-time insight, improving quality while reducing defects and costs.

SMART REVIEW SMART REVIEW uses AI-powered analysis on an NVIDIA infrastructure to streamline defect verification, reduce false calls, and increase productivity.

KPO Koh Young Process Optimizer, a suite that applies deep learning to enhance surface mount manufacturing.

Measure Everything, **AI** Everywhere

kohyoungamerica.com



america@kohyoung.com

CMMC 2.0 Level 2 certification provides customers with verified assurance that suppliers meet the cybersecurity standards required to handle government and defense program data, and that this assurance is ongoing. As part of the certification, we conduct annual cybersecurity evaluations and must undergo full recertification every three years.

The certification also strengthens supply chain security beyond our own walls. We hold our vendors and manufacturing partners to the same standards, creating consistent security expectations across every link in the chain rather than only at the prime contractor level. For customers working on programs where data protection is a contractual requirement, consistency matters.

A Process That Started Before It Was Required

We didn't start this process because a contract required it. We started it in 2019 because we saw where DoD cybersecurity requirements were headed and recognized that getting ahead of them was the right thing to do for our customers and our business.

We began implementing NIST 800-171 controls in 2019, aligned with early DoD requirements for contractor self-assessment and in anticipation of stricter compliance expectations. Recognizing the scope of the effort, we hired a DFARS compliance firm with more than a decade of influence on federal cybersecurity policy, including involvement in the creation of DIB-CSI, the original DFARS clause, and subsequent updates. That partnership guided the implementation of NIST 800-171 controls, closure of security gaps, and development of formal policies and procedures that would later hold up under audit scrutiny.

By mid-2025, we were positioned to pursue third-party certification ahead of the Phase 2 deadline of Nov. 10, 2026, when we understood that mandatory C3PAO certification requirements would take effect for applicable DoD contracts. (Note: That requirement was suspended on July 13, 2026, pending a 60-day review.)



Achieving CMMC 2.0 Level 2 certification required a sustained, company-wide effort that touched every part of our operations, from IT infrastructure to employee workflows. We started this work years before it became a contractual requirement because we understood what our defense customers needed from a supplier: not just capability but verified accountability.

The Biggest Hurdles in CMMC Certification

For most organizations, the hardest part of CMMC certification isn't understanding the requirements; it's ensuring that technology, process, and documentation all stay aligned at the same time.

On the technical side, we found that existing tools for storing or sharing customer files, whether hosted on-premises or in the cloud, may not meet CMMC requirements. If a current system isn't compliant, the organization must either reconfigure or migrate to a compliant alternative, such as a platform listed on the FedRAMP Marketplace. Either path introduces costs, operational disruptions, and changes to employee workflows that must be managed carefully.

Documentation is another major area that has required significant effort. Auditors review the entire environment, the individual systems within it, and the flow of CUI assessed through a combination of configuration evidence and formal written policies and procedures. What we learned is that documentation can't be an afterthought. Clear, finalized documentation helps auditors understand the environment and gives employees consistent guidance. As systems evolve, keeping documentation aligned with actual configurations is an ongoing obligation, not a one-time deliverable.

Common Issues Companies Face

Beyond the core technical and documentation requirements, several issues come up consistently across organizations pursuing CMMC certification, regardless of company size or how far along they are in the process.



Executive buy-in and organizational alignment: CMMC compliance requires planning, budgeting, and decisions that affect the entire company. Without visible leadership support, employees tend to treat the work as a burden rather than a priority. Leadership will often need to make difficult calls, such as replacing legacy systems, changing established workflows, and allocating resources. The defined CMMC timeline means those decisions can't be deferred.

Legacy systems: Older tools for storing or sharing customer files often fall short of CMMC requirements. Migrating to compliant platforms is time-consuming and costly, and it's one of the most common issues across companies at every stage of compliance readiness.

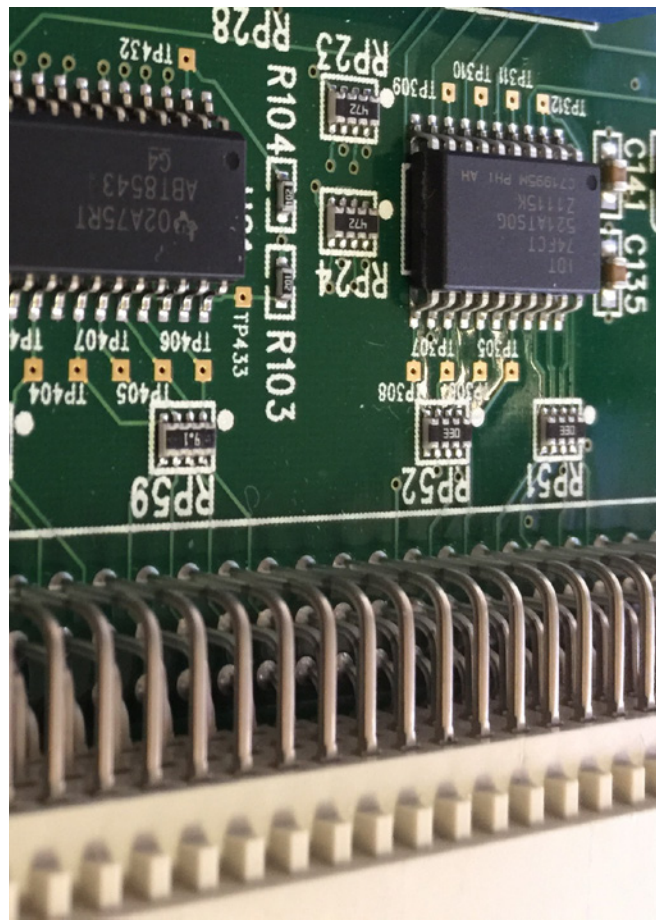
Workforce readiness: Getting employees to consistently follow new workflows after compliant solutions and policies are in place is a separate challenge from implementing those solutions. Behavioral change takes time. Training needs to be ongoing, tailored, and reinforced by leadership because management conformance directly shapes how seriously the rest of the organization takes new procedures.

Sustaining compliance after certification: Treating certification as a one-time event is a common mistake. CMMC requires annual self-attestation and full recertification every three years. Evidence must be maintained, training must continue, and documentation must be updated as systems change. Organizations that don't build this into normal operations typically struggle at reassessment.

Our Certification Process

When we entered the formal certification phase, the preparation we had done over the prior years paid off. With most controls, documentation, and solutions already in place, the certification phase focused on closing remaining gaps and refining existing implementations. New business requirements introduced mid-process necessitated adjustments to several systems and documentation sets, adding complexity for both the compliance team and employees. It's key to remember that no matter how prepared you may be, the organization must be flexible and expect changes.

For the first certification, the standard questions were answered in full. The result was a clean certi-



fication with all requirements satisfied and all documentation complete.

The effort was company-wide. Our IT team worked directly with our compliance partner to plan and implement changes while keeping the business running. Our employees adapted to new tools and procedures and applied them in their daily work rather than as a separate compliance exercise. Our leadership team stayed engaged throughout, from the early planning stages to the final stages of audit preparation.

The Window for Preparation

With fewer than 600 certified assessors available for an estimated 350,000 defense contractors, and C3PAOs already booked well into 2026, wait times for new clients are expected to exceed 18 months by Q3 2026. Companies that have not yet begun the process are working against a shrinking window. **SMT007**

Daniel Porton is the IT manager at San Francisco Circuits. **Alex Danovich** is the CEO of San Francisco Circuits.

EMS Companies RESPOND TO CMMC Suspension



The Department of Defense (War) announced the suspension of CMMC Phase II requirements on July 13, 2026, halting the planned Nov. 10, 2026, transition that would have made third-party assessments a condition of contract award for most DoD solicitations involving CUI.

A new CMMC Reform Task Force has been launched to conduct a top-to-bottom review of the program until mid-September 2026, with a focus on reducing compliance costs and assessment burdens, particularly for small and nontraditional businesses.

So, what does this mean to companies pursuing CMMC? Does it still matter? We asked the three companies showcased in this issue. Here are their answers.

San Francisco Circuits—Daniel Porton, IT manager, Alex Danovich, CEO

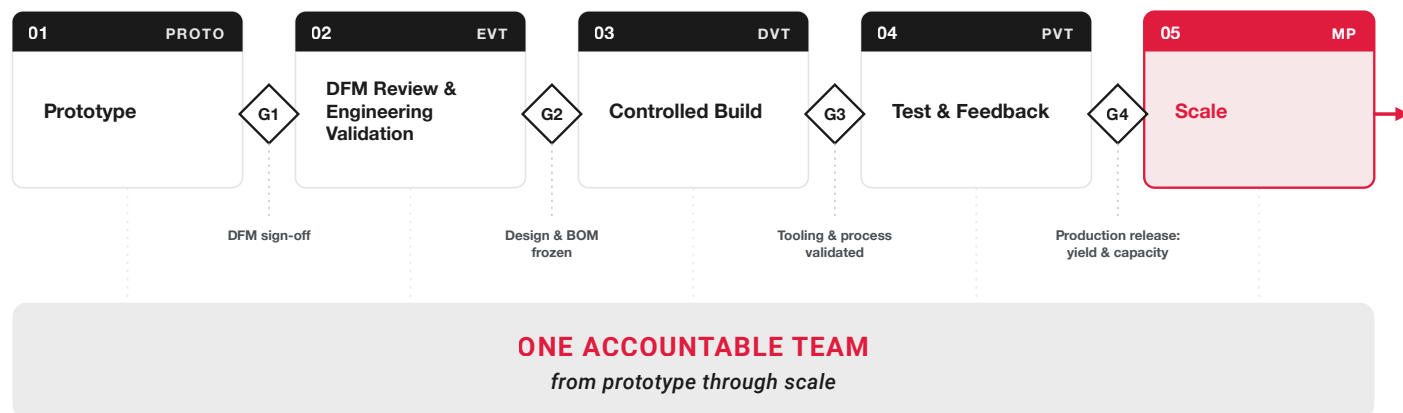
What hasn't changed is the underlying obligation. The suspension pauses one verification mechanism; it doesn't reduce the duty to actually be compliant. Phase I self-assessment requirements

Speed Without Losing Control

Most NPI delays don't come from moving too fast — they come from moving without structure.

Structured NPI System

- ✓ 5 Stages
- ✓ One Team
- ✓ No Handoffs



Let's Review Your Build Today

Visit 🏠

omega-ems.com/contact

Call ☎

408-341-9739

Email ✉

info@omega-ems.com

remain fully in effect. DFARS 252.204-7012 and NIST SP 800-171 Rev. 2 controls are still enforceable, and the Department of Justice has continued its Civil Cyber-Fraud enforcement activity, pursuing contractors who misrepresent their cybersecurity posture or submit inaccurate Supplier Performance Risk System (SPRS) scores.

San Francisco Circuits completed its CMMC 2.0 Level 2 certification before the suspension was announced. That certification remains valid, and the security standards it reflects aren't contingent on what the mandate requires at any given moment.

Omega EMS—Chris Alessio, CEO

While the announcement changes the timing of formal CMMC Level 2 certification, it doesn't change our direction. Omega EMS remains fully committed to completing our cybersecurity roadmap and maintaining compliance with the underlying NIST SP 800-171 requirements (which have always been the technical foundation for CMMC). We made this investment because we believe it's the right long-term decision for our business and our customers, not simply because of a regulatory deadline. We'll continue executing our implementation plan and will pursue formal certification whenever the Department of War resumes the certification process.

Our teams will continue executing against the milestones we've established. Externally, we'll communicate the same message to customers: Omega EMS remains committed to achieving CMMC Level 2 certification and maintaining the highest standards of cybersecurity regardless of changes to the government's implementation timeline. Customers are looking for trusted manufacturing partners, and

that expectation hasn't changed.

During the 60-day pause, very little changes operationally. We've already completed our Level 1 and Level 2 self-assessments and are actively closing all remaining gaps. The temporary pause simply provides additional flexibility in scheduling the formal third-party assessment. We'll use the additional time to further strengthen our cybersecurity posture and ensure we're fully prepared when formal assessments resume.

We certainly appreciate any effort to streamline compliance requirements and eliminate unnecessary administrative burden. If the government can simplify the certification process while maintaining strong security standards, that's a positive outcome for everyone. From Omega EMS's perspective, our investment in cybersecurity isn't changing. Whether the process becomes simpler or more efficient, our customers still expect secure systems, protected data, and a trusted manufacturing partner.

Naprotek

Naprotek is already certified under CMMC 2.0. As such, the suspension has no effect.

Conclusion

For contractors that were preparing for a third-party assessment ahead of the November 2026 deadline, the timing and cost of that assessment may now be worth reevaluating. But the work of implementing controls, maintaining documentation, and keeping SPRS scores accurate remains a live obligation. The companies that treat it that way will be better positioned, in whatever way the program is reshaped. **SMT007**

I-Connect007

Educational Resource Center

Podcasts

White Papers

Roundtables

Books

Webinars

Subscribe

7 FREE COURSES TRANSLATED INTO 5 NEW LANGUAGES.

BUILT FOR ELECTRONICS MANUFACTURING.



More than 3,000 electronics manufacturing companies worldwide rely on our training to build skilled, safety-ready teams. Now that training is even more powerful. As a member, your team gets access to 7 industry-specific courses, now available in English, Spanish, French, German, and Chinese, plus 4 courses newly available in Bahasa Malaysia (Malay). Every course features full native-language narration, not just captions.

COURSE LIST

Newly Spanish, French, German & Chinese:

- Chemical Safety in Electronics Manufacturing
- Introduction to Component Identification for Electronics
- Ergonomics for Electronics Manufacturing
- Introduction to Safety Data Sheets for Electronics Manufacturing

Newly available in Bahasa Malaysia (Malay):

- Safety for Electronics Manufacturing
- Introduction to Component Identification for Electronics
- Foreign Object Debris (FOD) for Electronics Manufacturing
- Electrostatic Discharge (ESD) Control for Electronics Manufacturing

A \$385 VALUE PER EMPLOYEE
included with your membership.



Standardize training across every location,
in every language your team uses.

Electronics U
by Global Electronics Association

Editor's note: The following announcement was released on July 13, 2026, and is published here in its entirety.

FORGING THE ARSENAL OF FREEDOM DEPARTMENT OF WAR SUSPENDS CMMC PHASE II REQUIREMENTS

The Department of War today announces the immediate suspension of the Cybersecurity Maturity Model Certification (CMMC) Phase II requirements, which were originally scheduled to come into effect on November 10, 2026. All Phase I self-assessment requirements remain firmly in place. Additionally, the Department will begin a comprehensive review of CMMC aimed at aligning with Secretary of War Pete Hegseth's Acquisition Transformation System (ATS) directives prioritizing speed to capability, lowering barriers for small, medium, and non-traditional businesses, and replacing bureaucratic compliance with scalable, resilient cybersecurity measures.

Ensuring access to leading-edge commercial capabilities is a critical driver powering the Secre-

tary of War's operational execution for the "Arsenal of Freedom." While the current CMMC program was designed to enhance DIB cybersecurity, instead it has created prohibitive compliance costs and bureaucratic burdens. Recent data, including reports from the Small Business Administration (SBA), confirmed that CMMC compliance is forcing innovative companies out of the Defense Industrial Base (DIB), which will delay the delivery of critical capabilities to the warfighters.

"In support of Secretary Pete Hegseth's directive to reduce compliance barriers for small and medium sized businesses, we are today suspending the CMMC Phase II requirements and initiating a 60-day study of the future of this program," said DoW Chief Information Officer Kirsten A. Davies.



Accelerate Your Next Assembly with a Total Solutions Provider

The Challenge—

Your assembly line is ready for action.
Can your PCB supplier keep up?

- Tight turn-around time for prototypes
- Increasing board complexity
- Supply-chain pressure

The United Electronics Solution—

We're built for your challenges and offer full-scale PCB services from prototype to production.

- Engineering support
- Prototypes in as little as 1 day
- Up to 20 layers, fine line/space, blind/buried/stacked vias
- Advanced materials including Teflon, polyimide, metal core, RF/microwave substrates
- Metal-backed / thermal-management
- ISO 9001:2015, IPC Class 2 & 3, ITAR Registered, UL certified
- Material stocking, JIT inventory, offshore + domestic production

Ready to elevate your success? Learn more now.



UNITED ELECTRONICS
CORPORATION

“Robust cybersecurity and operational resilience remain critical to protecting American innovation and supporting warfighter readiness. We believe the DIB can achieve both, while we reduce unnecessary government red tape.”

Effective immediately, the Department will suspend the transition to Phase II requirements of CMMC, as well as pending and future CMMC implementation milestones across the Department of War solicitations and contracts.

“We have a strategic imperative to reduce bureaucracy as we build the world’s strongest Arsenal of Freedom. The CIO’s decision ensures we maintain a strict security baseline while removing paralyzing costs and keeping innovators and competition growing in the defense supply chain,” said Hon. Michael Duffey, Under Secretary of War for Acquisition and Sustainment.

To realign our cybersecurity posture with the principles of the ATS, the Department CIO is establishing a CMMC Reform Task Force to conduct a comprehensive top-to-bottom review of the certification program. This task force will serve as the central hub for synthesizing industry feedback from

our public Request for Information (RFI) regarding compliance challenges. Using these insights, the team will recommend realistic, scalable security measures that prioritize speed to capability and lower barriers for small and non-traditional businesses, delivering their final report to the DoW CIO within 60 days.

During this interim period, the Department will enforce cybersecurity compliance with the NIST SP 800-171 Rev 2 standard through self-assessments and select government-led assessments, focusing on tangible cyber hygiene rather than administrative overhead.

It is critical to note that this action does not eliminate the requirement for companies to protect federal data. All defense contractors and subcontractors remain contractually obligated to safeguard covered defense information in accordance with DFARS clause 252.204-7012.

The Department of War remains steadfast in its commitment to securing its digital domain while empowering the DIB to rapidly provide the most advanced capabilities to the warfighter. [More information can be found here.](#) **SMT007**

Insight, Delivered

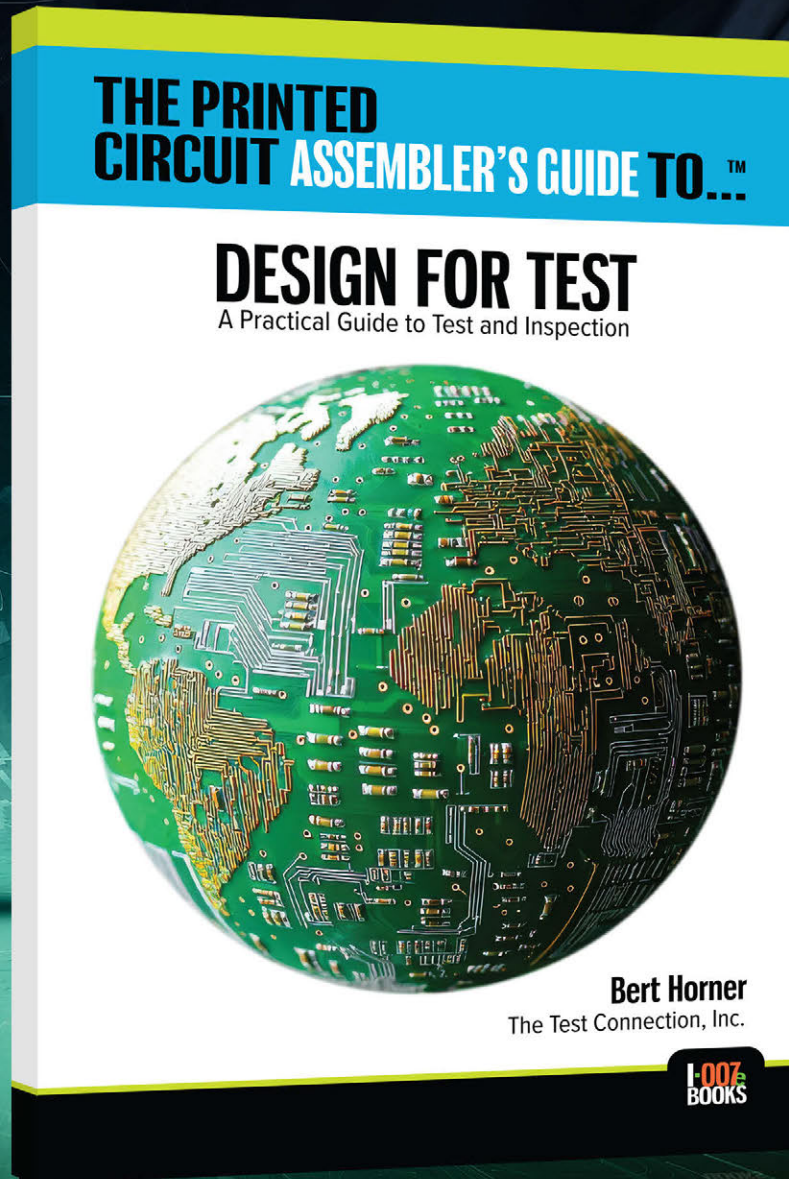
Subscribe to our daily and weekly newsletters, tailored to your interests, and stay connected to what matters most.



SUBSCRIBE NOW →

I-Connect007
The Global Electronics Resource

The Assembler's Playbook for Modern DFT



Look Inside

"Even experienced test professionals will gain valuable insights and fresh perspectives from the author's expertise."

—William E. Webb, Aster Technologies

I-007eBOOKS

Decoding the CMMC Suspension

Since the recent announcement of the CMMC Phase 2 suspension, I have been closely following discussion in the Defense Industrial Base community, including vendors, customers, and cybersecurity specialists. We are all in a state of shock and confusion. In a memo to my clients, I shared some details for the decision. A common theme among those reasons is cost and capacity. We've learned that:

- CMMC has prohibitive compliance costs, with individual bills approaching \$600,000; SBA estimates above \$7 billion annually across the base
- There is a severe assessor shortage; roughly 100,000+ firms need assessments from only about 100 approved organizations
- DoD stood up a 60-day CMMC Reform Task Force to recommend a lower-barrier replacement framework

Even though the assessment timeline has changed, we advise staying the course. Basic cyber hygiene is good for all organizations, and the sus-

pension does not change cybersecurity requirements. Organizations that receive CUI or plan to, should continue to implement NIST 800-171r2. Self-assessments and SPRS score reporting are still required and are not affected by the suspension.

Guidance by Situation

Depending on where you are in the process, the guidance may shift slightly. Here's what we're recommending.

For companies pursuing certification on time

Nothing you did is wasted. The controls you implemented to hit CMMC Level 2 are the same NIST 800-171 controls that remain contractually required today via DFARS and are self-attested. You're now ahead: Your System Security Plan, POA&Ms, and evidence are ready; your SPRS score is defensible; and if certification returns in some form, you'll re-enter near the front of the line. The one thing to pause on is spending: If you haven't yet paid for a C3PAO assessment, hold that check until the 60-day review clarifies what the future model looks like.





inTFlex

INNOVATIVE PRECISION FOR YOUR INNOVATIVE PROJECTS

Industry-leading flex design services, premier in-house manufacturing of flexible circuits and EMS services!



**Global Experts in
Flex Design**



**High Reliability &
Advanced
Manufacturing**



**State-of-the-Art
Facilities**



**Comprehensive
Services**



We provide precision engineering, quality production, and cost-effective solutions that will bring your products to market faster!

CONTACT US FOR A FREE FLEX DESIGN REVIEW

sales@flexiblecircuit.com

763.545.3333

www.flexiblecircuit.com

Table 1: What the memo says

Only self-assessments allowed	During the suspension the only permitted designations are CMMC Level 1 (Self) or Level 2 (Self). Level 2 (C3PAO) and Level 3 (DIBCAC) designations are prohibited.
Level 2 substance survives	Level 2 (Self) remains aligned to the full NIST SP 800-171 Rev. 2 control set. For CUI-handling suppliers, “suspended” does not mean dropping to the light Level 1 FCI baseline. Full Level 2 can still be required, just self-attested.
Baseline stays in force	DFARS 252.204-7012 remains fully in effect.
Contract relief mechanism	Where a solicitation or contract already carries a C3PAO or DIBCAC requirement, program managers must amend it out with active solicitations “as soon as practicable,” existing contracts by modification before the next option exercise or administrative mode.
No waivers	No waivers will be granted during the review. Further guidance follows the 60-day review.
False Claims Act exposure unchanged	Your SPRS score must be accurate and defensible on the evidence, backed by a real System Security Plan and honest POA&Ms. “Phase II is suspended” is never a defense to certifying a number you cannot support.

For companies that would miss the deadline

This is a reprieve, not an exemption. You’ve bought time, but you’re not off the hook. The 800-171 self-assessment baseline still applies, and a low or missing SPRS score is still a contractual and false-claims exposure. Use the runway to close your real gaps rather than treating the pause as a stand-down. Firms that mistake “Phase II suspended” for “cyber-security no longer required” are the ones most likely to get caught out when the reformed rule lands.

Does ‘reducing administrative overhead’ mean a revamp of the certifications?

Yes, most likely. It’s a revamp of the certification mechanism, not an abandonment of the security requirement. The language in the memo (prioritize “speed to capability,” replace “third-party compliance models with scalable, realistic security measures,” focus on “tangible cyber hygiene as opposed to administrative overhead”) signals that DoD wants to keep the 800-171 substance but change how compliance is verified. This will likely lean more heavily on self-attestation, risk-tiering based on data sensitivity, and possibly automated or continuous validation, rather than the point-in-time, pay-a-C3PAO model. Read it as “same controls, lighter and cheaper proof,” not “controls

going away.” The actual shape won’t be known until the task force reports and a new rule goes through rulemaking, which realistically takes many months.

Advice for EMS Suppliers

Don’t stop going on controls, but pause discretionary spend on the certification event. Maintain and improve your NIST 800-171r2 implementation and keep your SPRS score current and honest. Don’t cancel remediation, segmentation, MFA, logging, or SSP/POA&M work. Those are enforceable cyber hygiene. Hold off booking a C3PAO assessment or signing long-term compliance-tooling contracts until the target is defined. Preserve documentation so you can move fast when the new framework drops, and keep flowing requirements to your subcontractors. DFARS 7012 supply-chain obligations did not pause.

Above all, don’t forget the False Claims Act; the suspension does not dismiss honesty in reporting the SPRS score. **SMT007**



Divyash Patel is CEO of MX2 Technology

FLASHBACK ROUNDTABLE: Today's Cybersecurity Strategies



As part of I-Connect007's "Real Time with... APEX EXPO 2026," we conducted a [roundtable of cybersecurity experts](#), Hiroyuki Watanabe, Uday Ali Pabrai, and Divyash Patel, about CMMC certification. The discussion defines CMMC 2.0 and why it matters. The panel demystified much of the CMMC process, and while it may seem that much has changed since this conversation was recorded, what they shared is still just as timely and important as it was then.

AT THE TABLE:

Hiroyuki Watanabe is the executive director, Global Security, at NEC Corporation. He chairs the IPC-1792 cybersecurity standard committee for Trusted Validated Secure Supply Chains. He is committed to assisting critical SME factories and to improving the resilience of the entire electronics manufacturing supply chain.

Uday Ali Pabrai is the CEO of ecfirst, bringing more than two decades of experience delivering advanced AI-powered cyber defense solutions. Pabrai and ecfirst are committed to securing organizations in healthcare, government, and manufacturing, and helping clients achieve compliance with frameworks, like NIST, CMMC, and HIPAA, through tailored strategies and technologies.

Divyash Patel is the founder and CEO of MX2 Technology, Inc., a Silicon Valley-based provider of managed IT, cloud, and compliance services. With over two decades of IT leadership experience, he has positioned MX2 as a trusted partner for organizations in regulated industries. He led the company to achieve HITRUST Certification and CMMC Level 2 certification, helping clients strengthen cybersecurity, meet compliance requirements, and operate with confidence in today's risk-driven digital landscape.

HOT AIR VS. INFRARED

PCB Rework

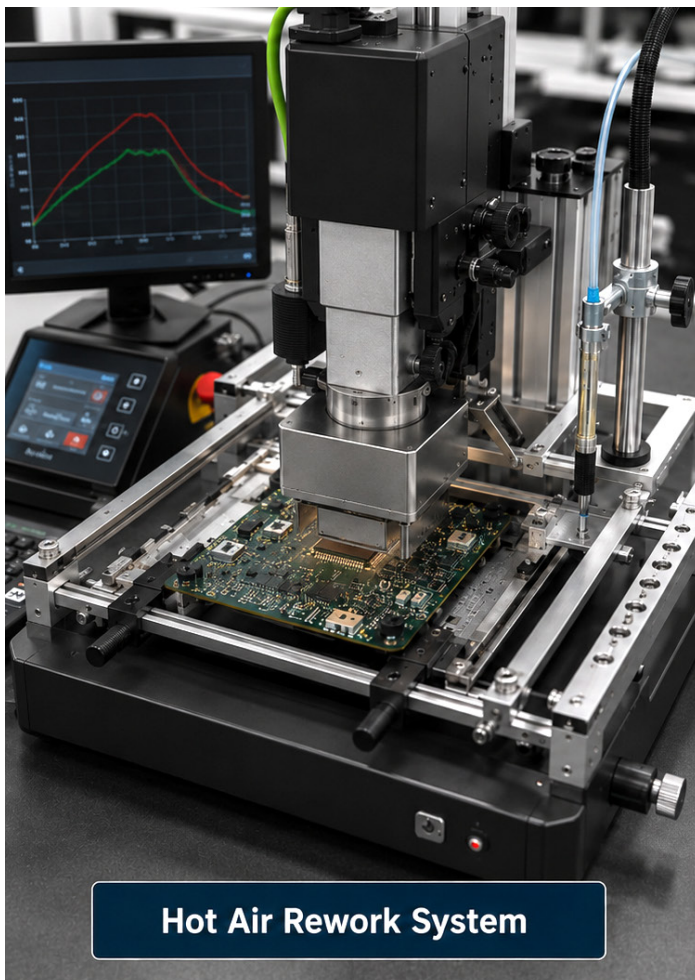
BY NASH BELL, BEST, INC.

Component rework is the controlled process of removing, replacing, repositioning, or repairing electronic components on an assembled PCB. Rework may be required because of component defects, incorrect placement, soldering defects, engineering changes, or damage identified during inspection or testing. A successful rework process uses controlled heating, soldering, cleaning, handling, and inspection

techniques to restore the assembly while minimizing thermal and mechanical stress to the PCB and surrounding components.

Common Rework Methods

Although several methods may be used to rework PCBs, hot air and infrared systems are among the most common for area-array and surface mount components. Hot air rework directs heated air or



Hot Air Rework System



Infrared Rework System

Figure 1: Hot air rework system and IR rework system for removal of electronic devices.

STRONG PARTNERSHIPS GROW LONG BEFORE THEY'RE NEEDED.

Material shortages.
Longer lead times.
Supply chain uncertainty.

These challenges are affecting much of the PCB industry. Preparation makes the difference.

At FSQuality, decades of strategic supplier relationships and global sourcing strength help ensure reliable access to critical materials — keeping your production moving when others slow down.

When the market gets tough, the right partner stands out.



GLOBAL STRENGTH
Local Support



ON-TIME DELIVERY
When It Matters



TRUSTED QUALITY
Every Step



YOUR SUCCESS
Is Our Priority



KNOCKING DOWN THE BONE PILE

nitrogen through a nozzle to concentrate heat around a specific component. Infrared rework uses radiant energy to heat the component and surrounding area without forced airflow, often providing broader heat exposure.

Both types of systems commonly include bottom-side preheating, adjustable board supports, component alignment or placement features, and thermocouple monitoring. These controls help develop and repeat a thermal profile that brings the solder joints to reflow temperature without unnecessarily overheating the component, PCB, or adjacent parts.

Both hot air and infrared systems are accepted rework methods, but neither is the best choice for every assembly. The appropriate method depends on factors such as component construction, PCB thermal mass, surrounding component density, surface finishes, accessibility, and production requirements. The following sections compare the advantages and limitations of each method.

Pros: Hot Air

Targeted heat exposure: Hot air rework is a widely used and accepted method for reworking ball grid array (BGA) packages because it provides localized heating through a targeted nozzle. Nozzles are designed to fit closely around the component perimeter, helping focus heat on the target package while improving access in densely populated assemblies and limiting thermal exposure to nearby components, connectors, and other heat-sensitive features.

Less affected by surface finishes: Another benefit of hot air rework is its ability to accommodate component packages made from a wide variety of materials, colors, and surface finishes. Packages with higher thermal mass, such as ceramic or metal packages, generally require more time and energy to reach reflow temperature than plastic packages. However, hot air heating is typically less affected by differences in surface color, emissivity, and reflectivity than infrared heating.

Repeatable process control: Hot air rework systems provide repeatable process control by allowing key variables such as nozzle temperature, airflow, bottom-side preheat, and profile timing to be

adjusted and documented. Thermocouples can be used to monitor actual temperatures at the component, solder joints, PCB surface, and underside of the board throughout the heating cycle. Once a successful thermal profile is developed, the same process parameters can be saved and repeated on similar assemblies. This improves consistency while reducing the risk of overheating, insufficient reflow, and unnecessary thermal exposure.

Pros: Infrared

Broad, uniform heating: Infrared rework systems apply radiant energy across a wider area, which can help heat the component and surrounding PCB more gradually and evenly. This broader heating approach may reduce steep temperature differences across large components or high-thermal-mass assemblies when the process is properly profiled.

Airflow-free rework: Because infrared systems transfer heat without forced air, they eliminate the risk of airflow disturbing small, lightweight components near the rework site. This can be beneficial in densely populated assemblies containing chip components, fine-pitch devices, or other parts that could shift during reflow.

Reduced dependence on custom nozzles: Infrared systems can accommodate a wider range of component sizes and shapes without requiring a dedicated nozzle for every package. This may reduce setup time and tooling costs, particularly for low-volume work or assemblies containing unusual component geometries.

Faster heating for production work: Infrared systems can heat the component and surrounding PCB more quickly by transferring radiant energy across a broad area at the same time. This can shorten cycle times and improve throughput for repeat production work, particularly when the assembly has consistent materials, surface finishes, and thermal characteristics.

Cons: Hot Air

Risk to adjacent components: Although a targeted nozzle limits the heated area, escaping airflow and radiant heat from the nozzle can still affect nearby components, connectors, or plastics. Improper

REDUCE SOLDER
USAGE UP TO
85%



“Using MS2 Molten Solder Surfactant for Solder Dross Recovery has been extremely efficient and profitable for the company. We are getting 80% +/- recovery.”

David Ramirez
SME Engineer in Guadalajara, Mexico

CALCULATE YOUR SAVINGS



+1 (800) 757-6533 | sales@pkaymetal.com

PK
M · E · T · A · L

www.pkaymetal.com

KNOCKING DOWN THE BONE PILE

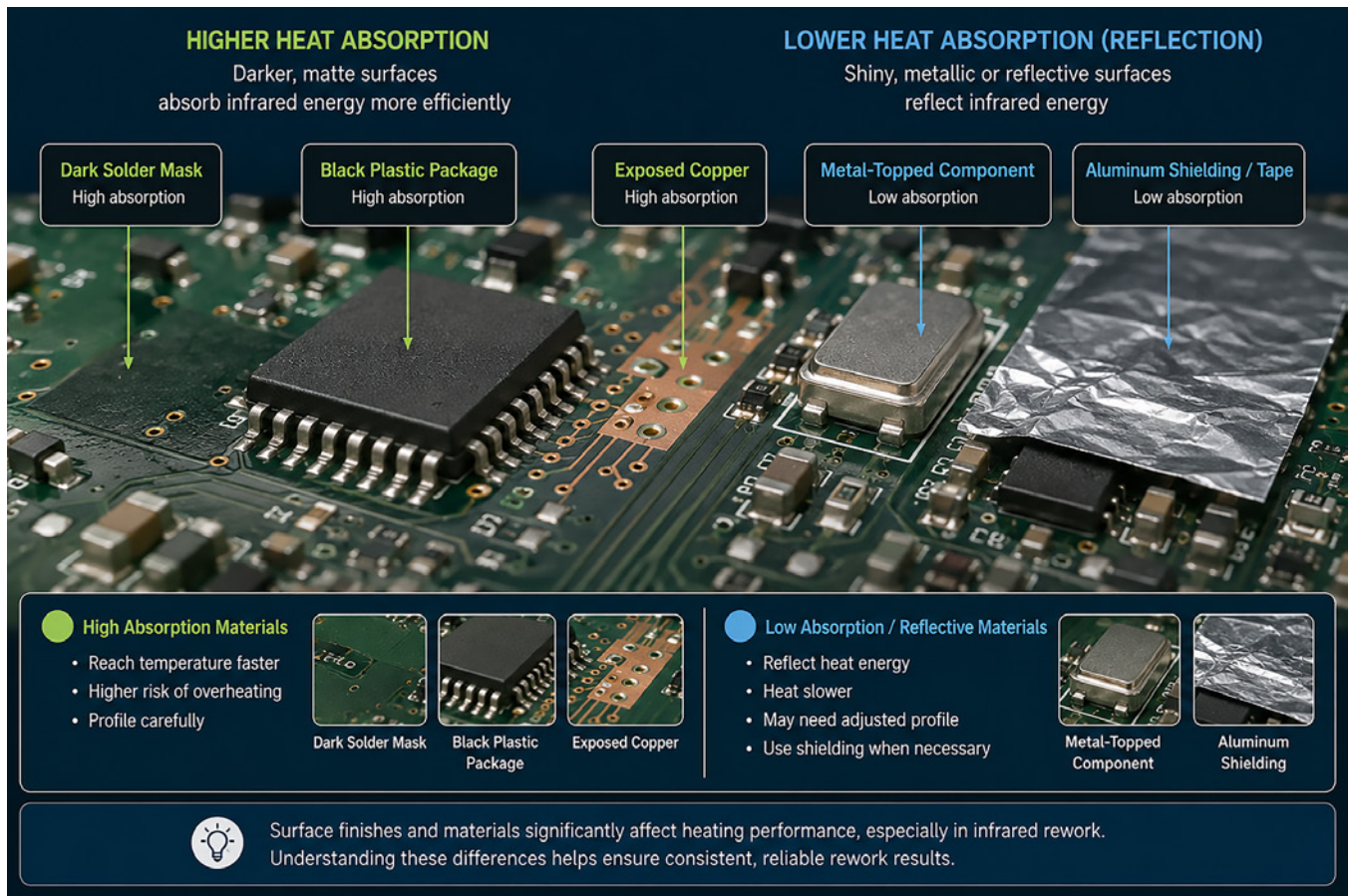


Figure 2: PCB and component surface properties influence infrared heating: Dark, matte materials generally absorb radiant energy more readily, while shiny metallic surfaces reflect more energy and may heat more slowly.

shielding, nozzle selection, or airflow settings may cause adjacent solder joints to reflow or small components to shift.

Custom nozzle requirements: Hot air rework often requires a nozzle sized closely to the target component. Unusual package dimensions or crowded layouts may require custom tooling, increasing setup time, cost, and lead time before rework can begin.

Localized thermal stress: Concentrated top-side heating can create a temperature difference between the component area and the rest of the PCB, particularly when bottom-side preheat is insufficient. Excessive ramp rates or uneven heating can increase the risk of PCB warpage, package warpage, delamination, or damage to the rework site.

Cons: Infrared

Affected by surface properties: Infrared heating is

influenced by the color, emissivity, reflectivity, and finish of the component and PCB surfaces. Dark or matte materials may absorb energy quickly, while shiny metal lids, exposed copper, or light-colored surfaces may reflect energy and heat more slowly, making temperature control less predictable.

Less localized heat control: Infrared systems typically heat a broader area than a fitted hot air nozzle. This can expose nearby components, connectors, and the PCB laminate to additional heat, particularly when the rework site is densely populated or close to temperature-sensitive materials.

Line-of-sight heating limitations: Infrared energy primarily heats surfaces directly exposed to the emitter, while raised components, shields, and surrounding features can block or redirect the energy. This may create uneven heating or require additional shielding and thermal profiling to ensure

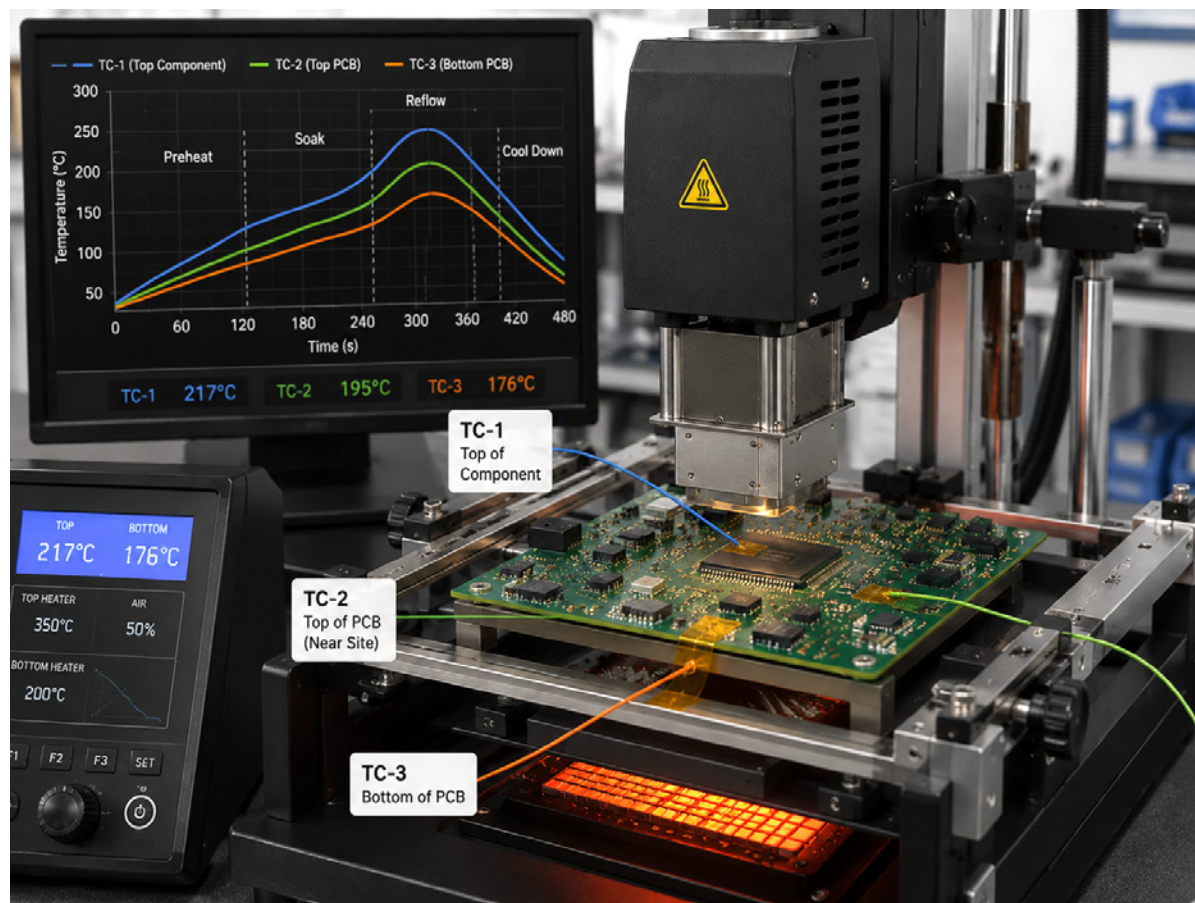


Figure 3: Thermal profiling during BGA rework uses thermocouples at critical locations to verify component, PCB, and bottom-side temperatures throughout the heating cycle.

the solder joints reach reflow temperature without overheating exposed surfaces.

Importance of Thermal Profiling

Regardless of whether hot air or infrared is used, a validated thermal profile is essential to ensure the solder joints reach reflow temperature without overheating the component, PCB, or surrounding parts.

With hot air systems, the profile focuses heavily on nozzle temperature, airflow, bottom-side preheat, and the temperature difference between the component and PCB. Infrared profiling requires additional attention to surface color, emissivity, reflectivity, component height, and line-of-sight exposure because these factors can cause different areas to absorb radiant heat at different rates. Thermocouples should be placed at critical locations to confirm actual temperatures rather than relying only on the machine's programmed heater settings.

Selecting the Appropriate Rework Method

Both hot air and infrared systems can produce reliable BGA rework results when properly applied and thermally profiled. Hot air is generally preferred for localized, predictable heating, while infrared may be advantageous for broader, airflow-free heating or improved production efficiency. The most appropriate method depends on the component construction, PCB thermal mass, surrounding layout, surface finishes, and production requirements. Ultimately, successful rework depends less on the heating technology itself and more on controlled heat delivery, accurate temperature monitoring, and a repeatable process. **SMT007**



Nash Bell is president of BEST, Inc. To read past columns, [click here](#).

As SpaceX Goes Public, the Market Hunts for the Next Investable Launch Company ▶

When SpaceX went public, the effect was immediate and structural: For the first time, the market had a public reference price for the launch economy, and every other space stock suddenly had a benchmark to be measured against. Now, what are some of the other companies to consider?

Ukrainian Drone Manufacturer UDD Selects Northwest Ohio as First U.S. Assembly and Manufacturing Center ▶

UDD has chosen Northwest Ohio as its first major U.S. assembly and manufacturing center after receiving its first Pentagon contract. UDD is expected to make a multimillion-dollar investment in the new production project in the Village of Holland, creating at least 300 new jobs.

JetZero Breaks Ground on First Aircraft Factory in Greensboro, North Carolina ▶

JetZero broke ground on its first manufacturing and final assembly campus, an 8-million-square-foot factory on more than 600 acres in Greensboro, North Carolina. The project is supported by the largest-ever state-level incentive package for any startup in any industry. With a projected staff of 14,500 over the next 10 years, JetZero will make the Z4 in Greensboro. It's designed for the unserved commercial middle market, with 250 passenger capacity on a range of up to 5,000 nautical miles.

Saab Receives Order for Giraffe 1X Radars from Denmark ▶

The Danish Armed Forces engaged Saab to deploy several Giraffe 1X systems for surveying both civil and military infrastructure. Saab responded promptly, and after successfully operating the systems for over six months, the Danish Ministry of Defence Acquisition and Logistics Organisation (DALO) has now placed a permanent order for the systems.

Boeing Lab Tests Mark Major Step Toward Space-based Quantum Network ▶

Boeing announced that its Q4S quantum networking satellite system successfully demonstrated

high-fidelity entanglement swapping during ground testing on a compact, space-qualified payload. This result marks a major step toward proving quantum networking in orbit.

Muon Space Officially Opens High-Mix Satellite Manufacturing Facility in San Jose ▶

Muon Space, the Mission Foundry for high-performance satellite constellations, announced the grand opening of its new advanced manufacturing facility in San Jose, California. The 130,000-square-foot facility significantly expands Muon's manufacturing capacity and positions the company to meet growing demand for satellite constellations across national security, civil, and commercial markets.

Lockheed Martin, GM Defense Team up on U.S. Defense Manufacturing ▶

Working under a memorandum of understanding (MOU), Lockheed Martin and GM Defense will explore opportunities to accelerate the delivery of critical capabilities and innovation by combining Lockheed Martin's defense production expertise with General Motors' advanced industrial capabilities in high-rate commercial manufacturing and engineering.

Teledyne FLIR Defense Wins \$28.8M CBP Contract for Mobile Surveillance Systems ▶

Under the 24-month contract, Teledyne FLIR Defense will deliver an advanced version of its Lightweight Vehicle Surveillance System (LVSS), a highly mobile, multi-sensor platform designed to provide situational awareness and boost operating efficiency for Border Patrol agents.

NASA Selects Rocket Lab to Launch Sun, Earth Sciences Missions ▶

Rocket Lab will fly two back-to-back Electron launches for NASA's PoISIR mission from Launch Complex 1 in New Zealand no earlier than June 2027. A separate Electron launch for NASA's TSIS-2 mission will take place from the same launch site in early 2027.



Elevate your PCBs

A Total PCB Solution from a Single Manufacturing Partner.

Rigid. Flex. Rigid-Flex. HDI. RF. Assembly.
Quick-turn Prototypes. Volume Production.

Summit Interconnect is the largest, privately held PCB manufacturer in North America. With eight high-tech facilities and thousands of employees, we work alongside customers to push the boundaries of what is possible, helping to create inventive and transformative electronic products.

Proudly serving high-growth markets including:



Aerospace & Defense



Medical



Industrial



Semiconductor



Automotive



Space



Consumer Electronics



Computing & Datacom

 summitinterconnect.com

Your trusted manufacturing
partner for mission-critical PCBs.





USMCA Rules of Origin for Electronics

What Could Change in 2026

Editor's note: Tariff Terminal is a series exploring how trade policy, tariffs, and customs developments impact the electronics manufacturing industry. This is the second of a two-part look at the USMCA review.

In my [first article on the USMCA](#), I explained why the USMCA six-year review matters to the electronics industry and where the negotiations currently stand. Now I want to get under the hood, because the most consequential changes for electronics manufacturers are in the rules of origin, the technical framework that determines whether your product gets duty-free treatment under USMCA.

Rules of Origin 101

Free trade agreements don't just lower tariffs; they also determine what counts as an "originating" product. Without rules of origin, an importer could potentially route non-qualifying goods through an FTA country, change the label, and claim duty-free treatment. So, every FTA contains product-specific rules (PSRs) that define

YOUR SYSTEM IS LIMITING YOUR CEILING.

There are cracks in the foundation.
It may be time to stop working around them.

TAKE A LOOK AT HOW YOUR SYSTEM HOLDS UP:

01

BUILT ON OUTDATED ARCHITECTURE

Costly to maintain. Difficult to change.

02

DISCONNECTED ACROSS THE BUSINESS

Departments, data, and processes live in separate places.

03

NOT ALIGNED TO ELECTRONICS MANUFACTURING

Requires workarounds to handle high-mix contract manufacturing.

04

DEPENDENT ON SPREADSHEETS

Critical data lives outside the system, relying on manual effort and tribal knowledge.

05

STRUGGLES TO SUPPORT GROWTH

New contracts, industries, and processes push beyond system limits and capabilities.

WHAT TO EVALUATE →

cetecerp.com/industries/electronics-manufacturing-ems-pcba/

how much production must occur within the trade bloc for a good to “originate” there.

USMCA uses two main tests, applied alternatively: a tariff shift test (the non-originating inputs must change classification under the Harmonized Tariff Schedule when they’re transformed into the finished good), and a regional value content (RVC) test (typically 60% under the transaction value method or 50% under the net cost method). Some products require one or the other; many allow either.

“**Free trade agreements don’t just lower tariffs; they also determine what counts as an ‘originating’ product.**”

Article 2.10 and General Note 11(p): The IT Industry’s USMCA Backstop

Buried in USMCA Article 2.10 (and implemented in U.S. law as General Note 11(p) of the HTSUS) is a provision that does something unusual. For a defined list of information technology products, the goods are deemed originating simply by being imported into the United States from Mexico or Canada. No tariff shift analysis or no RVC calculation is needed.

The list is squarely an IT industry list. It covers automatic data processing machines (laptops, servers, and the like), digital processing units, input/output units, storage units, ADP-type displays and monitors, parts of those displays, parts of ADP machines, parts of printers and copiers, parts of LAN equipment, and computer power supplies.

The legal effect is striking. U.S. Customs and

Border Protection has confirmed in published rulings that even Chinese-origin IT goods within the enumerated categories—for example, ADP machines, processing units, storage units, computer power supplies, and LAN parts—qualify for USMCA preferential treatment under GN 11(p) when shipped to the U.S. from a Mexican facility, even where the Mexican operation consists only of sorting, picking, packing, and shipping. The goods are treated as originating because they fall within the enumerated categories and are shipped from a USMCA country, full stop.

Why does this rule exist? It’s a direct descendant of NAFTA Annex 308.1, which the three countries adopted in the early 1990s to harmonize their external tariffs on computer goods. The logic was that if all three NAFTA countries applied roughly the same MFN tariff to imported ADP goods, there was no risk of trade deflection, so the usual rules of origin weren’t needed. When the WTO Information Technology Agreement subsequently brought MFN tariffs on those same goods to zero globally in 1997, the policy basis became even stronger. USMCA carried the rule forward in 2020 and modernized the product list.

If the 2026 review tightens or narrows GN 11(p), the impact on importers of finished computers, servers, displays, and IT subassemblies will be immediate.

The Standard PSRs: A Mixed Bag for Electronics

Outside the GN 11(p) list, electronics products are governed by the standard PSRs under the agreement. A few patterns matter for SMT and EMS readers.

Semiconductors enjoy the most permissive treatment. Diodes, transistors, integrated circuits, and electronic microassemblies require no change in tariff classification at all, and an explicit transit/transshipment exception even allows further production outside USMCA (think wafer testing or back-end packaging in Asia) so long as the further processing doesn’t kick the goods into a different category. These rules are the rules-of-origin counterpart to the WTO International Technology Agreement’s broader liberalization of semiconductor trade.

Telecom and networking goods, such as smart-

We are dedicated
to excellence through

innovation, technology and most importantly, service.



COMMERCIAL • MILITARY • MEDICAL • BAREBOARD



U.S.CIRCUIT

www.uscircuit.com



phones, switches, routers, and base stations, generally require a subheading-level tariff shift. That's achievable through real PCB assembly and integration in North America, but not through repackaging or light-touch finishing.

Insulated wire and cable harnesses carry an unusual rule that excludes copper and aluminum wire inputs from the upstream raw metal categories. For harness makers sourcing copper conductors from Asia, this matters.

Transformers and power-supply parts became materially harder to originate as of July 1, 2025. The rules for finished transformers and their parts were tightened to exclude inputs from certain steel categories, and the RVC threshold jumped from 60%/50% to 65%/55%. This was scheduled into USMCA from the start (a hint at where the negotiators see strategic value), and it is now stacking on top of the new Section 232 metals tariffs covered in my first installment.

What To Watch Out For

The U.S. negotiating priorities suggest several possible directions:

- **Higher RVC thresholds in strategic electronics sectors.** Power conversion, magnetics, and certain finished IT products are obvious candidates given the administration's "U.S. content" framing.
- **A new U.S. content requirement layered onto RVC.** This would be a sharp departure from how USMCA currently treats U.S., Mexican, and Canadian content as interchangeable.
- **Narrowing or conditioning GN 11(p).** If the goal is to stop Asian goods from using Mexico as a "side door," the deemed-originating rule for finished IT products is an obvious target. Tightening it would force importers back into the standard PSRs, which is a much harder bar.
- **Tighter material origin rules for steel and aluminum inputs.** Building on the 2025 changes to the transformer and power-supply rules, "melt-and-pour" and "smelt-and-cast" requirements for raw metal inputs could creep into electronics-relevant PSRs.

- **Changes to Mexico's IMMEX, PROSEC, and Rule 8 programs.** These programs are how most U.S.-owned maquiladoras bring non-originating components into Mexico at reduced or suspended duties. IMMEX suspends import duties on inputs that are subsequently exported, PROSEC permanently reduces Mexican MFN duties on specified inputs for designated sectors (including electronics), and Rule 8 allows duty-free import of inputs unavailable in sufficient quantity in North America. In combination, these programs let non-originating inputs flow into U.S.-bound goods at little or no Mexican duty. USTR could make these Mexican export promotion programs a point of contention, with direct consequences for electronics importers sourcing Asian components for Mexican assembly.

Conclusion

Rules of origin are often an overlooked aspect of trade policy, but for electronics manufacturers, they are where the math is done. The 2026 review has a real chance of moving that math in ways that change sourcing economics, qualification documentation requirements, and cost structures across the SMT and EMS world. Companies that depend on the current GN 11(p) pathway, or on the standard PSRs for telecom, networking, power conversion, and magnetics product families, should map their product lines against the existing rules now and be ready to model the impact of likely changes well before they're finalized.

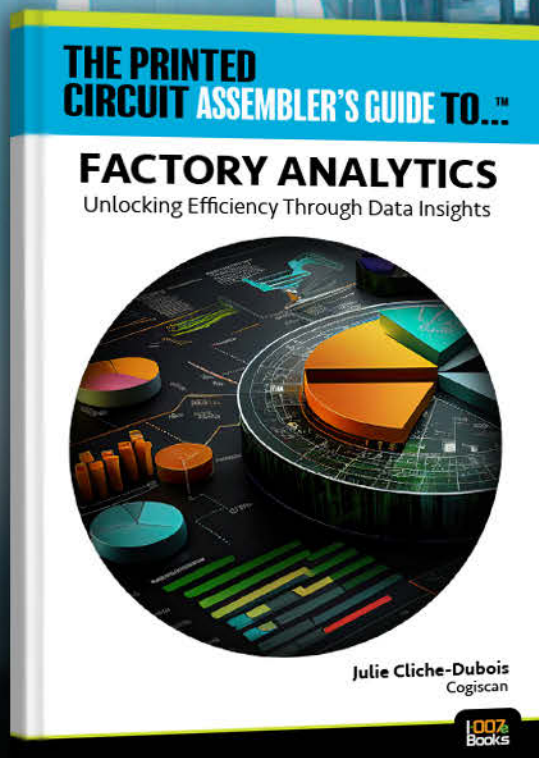
In the next installment, I'll turn to the Section 301 investigations and their impact on electronics supply chains, and how those interact with USMCA preferential treatment. The trade architecture keeps getting denser, and the electronics industry is sitting at the intersection of nearly every piece of it.



James Kim is an international trade lawyer at ArentFox Schiff LLP. He can be reached at james.kim@afslaw.com.

“I would recommend that any data-driven engineers focused on taking their manufacturing operations to the next level read this book.”

Jason Sciberras
Emerald Technologies



**Download
Now**

I-007eBOOKS

Find Industry-experienced Candidates at jobConnect007



For just \$975, your 200-word, full-column ad will appear in the Career Opportunities section of our monthly magazines, reaching circuit board designers, fabricators, assemblers, OEMs, suppliers and the academic community.

In addition, your ad will:

- be featured in at least one of our newsletters
- appear on our jobConnect007.com board, which is promoted in every newsletter
- appear in our monthly [Careers Guide](#), emailed to 26,000 potential candidates

Potential candidates can click on your ad and submit a resume directly to the email address you provide, or be directed to the URL of your choice.

No contract required. Just send over your copy and company logo and we'll do the rest!

Contact barb@iconnect007.com to get your ad posted today!

CAREER OPPORTUNITIES



FAE Wanted

San Francisco Bay Area, United States

PCB Recruitment Ltd - **the global PCB and electronics industries recruitment specialists** - are working in partnership with our client to source a world-class FAE in the Bay Area.

Outstanding Field Application Engineers in the San Francisco Bay Area – we have an exceptional opportunity that's well worth your attention.

Join one of the world's leading manufacturers of high-performance server PCBs at a pivotal stage of growth.

We're looking for someone with **specialist expertise** in high-speed signal PCBs and experience supporting AI infrastructure, GPUs, 800G–1.6T networking, or similar high-performance computing applications.

Salary: \$250,000–\$300,000 plus an excellent, industry leading benefits package.

For a confidential, no-obligation conversation, contact william@pcbrecruitment.co.uk.

This opportunity is not to be missed and could be an immense step in your career.

Apply Now!



TECHNICAL SALES MANAGER

Arlon Electronic Materials. Rancho Cucamonga, CA

Arlon Electronic Materials, a subsidiary of Elite Material Co., Ltd., is the #1 PCB laminate supplier by revenue worldwide, the #1 rigid CCL supplier, and the #1 supplier of AI data center PCB material. We are hiring a Technical Sales Manager to drive growth across the U.S. defense, aerospace, and high-reliability electronics market.

In this role you will generate revenue across Defense & Aerospace OEM and PCB fabricator accounts, serve as the technical liaison between customers and Arlon's engineering team, and build long-term strategic partnerships that support mission-critical programs. It is a hunter-farmer role for someone who can translate material science into customer value, with roughly 50% travel to customers and industry events.

We welcome experienced engineers and technical professionals from the PCB/PCBA industry ready to step into sales. Requirements: a BS or MS in Engineering, Science, or an equivalent technical field; 5+ years in the PCB/PCBA industry; and strong written and verbal communication. Must qualify as a U.S. Person per ITAR.

Compensation: base \$105K–\$161K, with OTE of \$150K–\$200K+ and uncapped bonus potential.

Apply today: recruiting@arlonemd.com

This position is subject to ITAR/EAR regulations. Arlon EMD is an Equal Opportunity Employer.

Apply Now!

CAREER OPPORTUNITIES



ventec
INTERNATIONAL GROUP

Director – OEM Sales and Business Development

Full-time, USA

Ventec International Group is a global leader in high-performance PCB materials, serving aerospace, defense, AI, automotive, industrial, medical, and high-speed digital markets.

We're seeking an accomplished sales leader to drive OEM business across the United States. This is a business development role focused on winning design-ins, building executive relationships, and securing long-term strategic partnerships with leading electronics companies.

Key Responsibilities

- Win new OEM opportunities across Ventec's product portfolio
- Develop relationships with OEMs, PCB manufacturers, and technology partners
- Drive specification wins in advanced electronics applications
- Lead and develop our manufacturer representative network
- Partner with technical teams to deliver customer solutions
- Contribute to commercial strategy, forecasting, and market intelligence

About You

You have at least five years' experience selling to OEMs within the electronics or PCB industry, with a proven record of winning new business and delivering sustained growth. You're commercially driven, confident engaging senior decision-makers, skilled at solution selling, and able to understand technical products while working independently and within global teams.

Why Ventec?

You'll work alongside senior leadership, influence major global programmes, and help shape the future of advanced electronics while making a direct commercial impact.

Apply Now!



Senior Thick Film & Microelectronics Quality Engineer

Remtec is growing and has an exciting opportunity at our dynamic, team-oriented tech-manufacturing company, based in our newly renovated headquarters in Canton, MA, just south of Boston.

The Senior Thick Film & Microelectronics Quality Engineer ensures product quality and AS9100 compliance across thick film fabrication and microelectronics assembly, including printing, firing, laser trimming, plating, wire bonding, soldering, assembly, testing, and inspection.

Responsibilities include:

- managing nonconforming materials
- leading root cause investigations
- conducting audits
- developing control plans, PFMEAs, and inspection procedures to ensure customer and regulatory requirements are met

The role partners with production and suppliers to establish quality standards and improve supplier performance and yield, reduce waste, and support continuous improvement overall.

The ideal candidate has a bachelor's degree in engineering or a related technical discipline, at least three years of quality engineering experience in microelectronics, semiconductor, or PCB manufacturing, and hands-on knowledge of thick film processes, quality systems, and problem-solving.

Preferred skills include AS9100/ISO 9001 systems; nickel, gold, and silver plating and surface finishes; GEA and MIL testing and inspection standards; and statistical software.

Join Remtec and contribute to a collaborative culture focused on quality, integrity, and innovation.
Learn more and apply here:

Apply Now!

CAREER OPPORTUNITIES



TECHNICA, U.S.A.

Various Positions

For 40 years, Technica USA has been providing products, equipment, and services to the printed circuit board fabrication and assembly markets.

Working with our worldwide partners, we offer our customers solutions through best-in-class product lines.

Technica has offices in San Jose, Calif, and Rancho Cucamonga, Calif.

We are expanding and looking for highly qualified Business Development/ Account Managers for both the PCB and PCBA markets.

We are adding to our growing national equipment service coverage and looking for experienced Equipment Service Technician/Engineers.

Are you a PCBA equipment applications expert with experience in component placement and inspection? We are looking for Equipment Product Specialists to work within our San Jose, Calif., PCBA Equipment Demo center.

Please visit www.technica.com/careers to learn more about these positions and submit your resume today!

Apply Now!



eptac

TRAIN. WORK SMARTER. SUCCEED.

Instructor – Electronics Manufacturing

EPTAC is seeking experienced professionals from the electronics manufacturing industry to join us as Instructors. This role offers flexible part-time or full-time opportunities. Ideal candidates will have expertise in soldering, quality control, PCB design, or related fields.

Responsibilities:

- Teach IPC Certification and electronics manufacturing related courses
- Travel as needed to teach at EPTAC locations or customer sites across the U.S.
- Contribute to the development of new training programs and enhance existing courses
- Stay current with industry trends, emerging technologies, and best practices to refine instructional techniques
- Provide hands-on demonstrations and supervise use of industry tools
- Foster a positive learning environment, enforcing classroom and safety rules

Requirements:

- 10+ years experience in the electronics manufacturing industry
- Current or past IPC Certification
- Bachelor's degree or equivalent
- Excellent communication, instructional, and organizational skills
- Practical, quick, and hands-on approach to problems
- Unrelenting drive to understand and meet student needs

EPTAC is the leader in Electronics Manufacturing Training and Certification in North America with 24 locations. Our headquarters is in Salem, NH. We offer a modern, positive environment with benefits including health care, paid time off, retirement savings, and professional development.

Email careers@eptac.com to apply.

Apply Now!

CAREER OPPORTUNITIES



Independent Sales Representatives Wanted

P. Kay Metal / MS2 Technologies, headquartered in the United States, is seeking established **independent sales representative firms** to add a proven, patented product to their portfolio.

We manufacture and supply **MS2® Molten Solder Surfactant**, a patented solution designed for both **Tin/Lead and Lead-Free soldering processes**, delivering measurable performance and cost benefits to electronics manufacturers.

MS2® already has successful customer installations throughout the United States, as well as a growing international footprint with active customers in Mexico, El Salvador, Honduras, Ecuador, and the Dominican Republic. We ship globally and support customers worldwide.

This opportunity is ideal for rep firms currently calling on electronics manufacturing, PCB assembly, soldering, or process engineering accounts who are looking to expand their offering with a differentiated, high-value consumable.

Strong technical products, international growth potential, and factory support provided.

To learn more about our company and technology, visit **www.pkaymetal.com**.

Interested firms are encouraged to reach out for additional details to Gladys Flores at gladysflores@pkaymetal.com.

Apply Now!



Rewarding Careers

Take advantage of the opportunities we are offering for careers with a growing test engineering firm. We currently have several openings at every stage of our operation.

The Test Connection, Inc. is a test engineering firm. We are family owned and operated with solid growth goals and strategies. We have an established workforce with seasoned professionals who are committed to meeting the demands of high-quality, low-cost and fast delivery.

TTCI is an Equal Opportunity Employer. We offer careers that include skills-based compensation. We are always looking for talented, experienced test engineers, test technicians, quote technicians, electronics interns, and front office staff to further our customer-oriented mission.

Associate Electronics Technician/ Engineer (ATE-MD)

TTCI is adding electronics technician/engineer to our team for production test support.

- Candidates would operate the test systems and inspect circuit card assemblies (CCA) and will work under the direction of engineering staff, following established procedures to accomplish assigned tasks.
- Test, troubleshoot, repair, and modify developmental and production electronics.
- Working knowledge of theories of electronics, electrical circuitry, engineering mathematics, electronic and electrical testing desired.
- Advancement opportunities available.
- Must be a US citizen or resident.

Apply Now!

CAREER OPPORTUNITIES



Quality Assurance Specialist—Bare Board PCB Manufacturing

Accurate Circuit Engineering seeks an organized, technically proficient Quality Assurance Specialist dedicated to bare board PCB production. You will champion compliance with industry standards, lead internal audits, manage certifications, and drive continuous improvement based on product performance data and customer feedback.

Key Responsibilities:

- **Standards Compliance & Certification:** Enforce IPCA600, IPC6012 (CIS/CIT preferred), and ISO 9001 quality standards throughout fabrication
- **Internal Process Auditing:** Conduct scheduled and ad hoc audits of incoming materials, fabrication stages, testing protocols (etest, AOI), and documentation traceability
- **Employee Training & Development:** Create and deliver training programs for inspectors and production staff on IPC standards, quality procedures, and inspection tools to maintain certification
- **Failure Analysis & Corrective Actions:** Investigate nonconforming boards—including internal findings and customer returns/RMAs—analyze root causes, and lead corrective/preventive actions (8D/CAPA)
- **Procedure Optimization:** Analyze quality trends and RMA data to update processes, inspection checklists, and control plans

Qualifications:

- Associate degree or equivalent experience in electronics manufacturing
- 3+ years in bare board PCB QA, with IPCA600/ CIS and IPC6012 certification
- Strong auditing, training, documentation, and cross-functional collaboration skills
- Proficient in rootcause failure analysis

Join us to ensure rigorous compliance, elevate fabrication quality, and continuously improve manufacturing standards.

Contact brandon@ace-pcb.com and James@ace-pcb.com to apply.

Apply Now!



Are You Our Next Superstar?!

Insulectro, the largest national distributor of printed circuit board materials, is looking to add superstars to our dynamic technical and sales teams. We are always looking for good talent to enhance our service level to our customers and drive our purpose to enable our customers to build better boards faster. Our nationwide network provides many opportunities for a rewarding career within our company.

We are looking for talent with solid background in the PCB or PE industry and proven sales experience with a drive and attitude that match our company culture. This is a great opportunity to join an industry leader in the PCB and PE world and work with a terrific team driven to be vital in the design and manufacture of future circuits.

Apply Now!

CAREER OPPORTUNITIES

ARLON ELECTRONIC MATERIALS

Multiple Positions

At Arlon EMD, we support aerospace, defense, and next-gen technology. We're looking for people who show up, take ownership, and get the job done on the production floor and beyond. No fluff. Just real work, real impact, real opportunity.

Now hiring for roles like:

- Field Application Engineer
- Technical Sales Manager
- Maintenance Technician
- Machine Operator
- Customer Service Representative
- Accounting Manager
- Senior Accountant
- Entry level Sales Engineer

Arlon is a major manufacturer of specialty high performance laminate and prepreg materials for use in a wide variety of PCB (printed circuit board) applications. Arlon specializes in thermoset resin technology including polyimide, high Tg multifunctional epoxy, and low loss thermoset laminate and prepreg systems.

View all open roles and apply here:
<https://www.linkedin.com/company/arlon-emd/jobs/>

Apply Now!

I-Connect007
The Global Electronics Resource

THE ELECTRONICS INDUSTRY'S HIRING NETWORK

**Your Next Opportunity
Starts Here.**



START HIRING



IPC BUILDS STANDARDS DEVELOPMENT COMMITTEE MEETINGS

19-24 September 2026 | H4 Wyndham Paris Pleyel, Paris, France

YOUR SEAT AT THE STANDARDS TABLE IS COMPLIMENTARY

The future of electronics manufacturing does not just happen — it is **built by experts like you.**

Join industry leaders from around the world at **IPC Builds 2026** to collaborate on the standards that drive quality, innovation, and reliability across the electronics industry.

- **Influence** future standards
- **Share** your expertise
- **Connect** with global industry peers
- **Help** shape what is next

Committee participation starts here!
Register today at electronics.org/ipc-builds

EDUCATIONAL RESOURCES



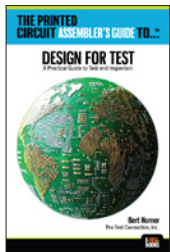
THE HEAT IS ON. WILL YOUR VIAS HOLD UP?

Available Now

THE PRINTED CIRCUIT ASSEMBLER'S GUIDE TO...
Via Structures
Reflow Process Sustainability, Reliability, and Robustness
Robert (Bob) Neves
Reliability Assessment Solutions, Inc.

Learn how to identify **vulnerabilities** and build more robust, **reliable** assemblies.

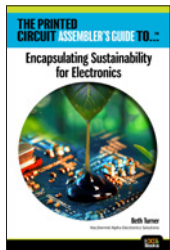
I-007eBOOKS



Design for Test: A Practical Guide to Test and Inspection

by Bert Horner

This book presents a practical roadmap for integrating DFT into PCB and CCA development, emphasizing early test strategy rather than adding it after design completion. The author highlights the cultural shift required to make DFT a shared responsibility across engineering, manufacturing, quality, and leadership teams. [Download your copy today!](#)



Encapsulating Sustainability for Electronics

by Beth Turner, MacDermid Alpha Electronics Solutions

This book discusses the growing demand for sustainable solutions in the market and highlights examples of bio-based resins and the demand from emerging technologies. [Read it now!](#)

PODCAST SERIES



Executive Director | Managing Editor
MARCY LARONT
marcy@iconnect007.com • (480) 280-5229

Managing Editor
NOLAN JOHNSON
nolan@iconnect007.com

Associate Editor
MICHELLE TE
michelle@iconnect007.com

Technical Editor
PATTY GOLDMAN

Contributing Technical Editor
HAPPY HOLDEN
happy@iconnect007.com

Business Development Manager
BARB HOCKADAY
barb@iconnect007.com

Marketing Services Manager
TOBEY MARSICOVETERE
tobey@iconnect007.com

Digital Marketing Manager
BRITTANY MARTIN
brittany@iconnect007.com

Art Director | Production Manager
SHELLY STEIN

Magazine Layout
TYLER ZAPOLUCH

Ad Design
TOBEY MARSICOVETERE

Director of Digital Operations
and Media Systems
BRYSON MATTIES

Cover Design
SHELLY STEIN

Cover Image
ADOBE STOCK © MUHAMMAD

SMT007 MAGAZINE®
is published by IPC Publishing Group, Inc.,
3000 Lakeside Dr., Suite 105N, Bannockburn, IL 60015

© 2026 IPC Publishing Group, Inc. does not assume and hereby disclaims any liability to any person for loss or damage caused by errors or omissions in the material contained within this publication, regardless of whether such errors or omissions are caused accidentally, from negligence, or any other cause.

August 2026, Volume 41, Number 8
SMT007 MAGAZINE is published monthly,
by IPC Publishing Group, Inc., dba I-Connect007.

ADVERTISER INDEX

American Standard/ASC Sunstone.....	9
Blackfox Training Institute.....	7
CETEC ERP	51
Flexible Circuit Technologies	39
FS Quality	43
Global Electronics Association.....	33, 63
I-007eBooks	3, 37, 55
Koh Young Technology	27
Linkage Technologies.....	19
Nordson.....	21
Omega EMS	31
On the Line with.....	2
P Kay Metal	45
Remtec.....	23
SMTA.....	15
SPEA	11
Summit Interconnect	49
Technica USA	5
The Test Connection, Inc.....	17
U.S. Circuit	53
United Electronics Corporation.....	35

SMT007

M A G A Z I N E



Problems solved!

