CIRCUIT NEWS 3.7

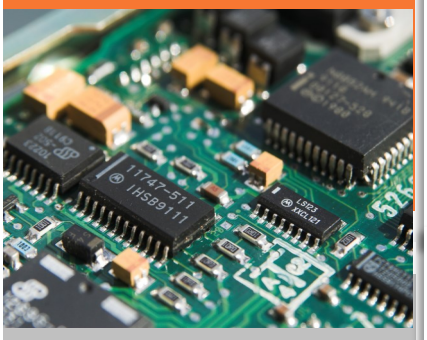
December 2025

NIST Compliance Tips:

Through SoPark working on NIST compliance, we have gained knowledge of some helpful approaches we would like to share. First and foremost is that NIST compliance is a key reference point for Cybersecurity Maturity Model Certification, Level 2.0 (CMMC).

NIST is related to compliance while CMMC is a certification with annual assessments by a third party auditor. It is important to keep this certification in mind that has three tiers or levels starting with basic level, then broad protection of Controlled Unclassified Information (CUI), and finally higher level protection of CUI against advanced threats.

CMMC has its own regulating body. The Department of War will define the level needed in the procurement process. Organizations seeking CMMC certification must align with NIST standards as well. For more information on CMMC visit: *CIO - About CMMC*



Check our website for past Circuit News issues…

Quick link:

News | SoPark | Electronics Contract Manufacturer

NIST 800-171:

This standard and its compliance are specifically related to the protecting controlled unclassified information (CUI). The standard provides a structured approach to ensure that non-federal organizations handling CUI can maintain its confidentiality. The standard was first issued by the US Department of Defense (DoD) in 2015. It became mandatory for their contractors in 2017.

The framework specifies 110 controls divided across 14 security requirement families ranging from access control to system integrity. For PCB manufacturers specifically it means maintaining and controlling a security system and plan for critical customer information such as Gerber files, sensitive emails, sensitive contact information, other design or related information.

The 14 Security Requirement Families:

- ***Access Control*** **-** Restrict system access to authorized users and processes only.
- ***Awareness and Training*** **-** Ensure all personnel and subcontractors understand cybersecurity risk and policies.
- ***Audit and Accountability*** **-** Maintain logs and ensure accountability for system activities.
- ***Configuration Management*** **-** Enforce secure configurations for systems and software.
- ***Identification and Authentication–*** Use strong authentication methods for system access.
- ***Incident Response*** **-** Establish procedure for detecting, reporting and responding to security incidents.
- ***Maintenance*** **-** Performing system maintenance while safeguarding sensitive data.
- ***Media Protection*** **-** Securely handle and dispose of physical and digital media.
- ***Personnel Security*** **-** Screen individuals accessing CUI.
- ***Physical Protection–*** Restrict physical access to systems containing CUI.
- ***Risk Assessment*** **-** Regularly evaluate risks to organizational systems.
- ***Security Assessment–*** Periodically review security measures for compliance.
- ***System and Communications Protection*** **-** Securely transmit data.
- ***Systems and Information Integrity*** **-** Promptly detect and respond to security vulnerabilities.

For more information visit these links and sources:

What Is the NIST SP 800-171 and Who Needs to Follow It? | NIST

NIST 800-171 Compliance for PCB Manufacturers: Protect Your Data & Contracts

NIST 800-171 Compliance Checklist: Tutorial & Best Practices - Device42