Difference between NIST SP 800-171-R2 Level 1 and Level 2

The National Institute of Standards and Technology (NIST) Special Publication 800-171 provides a framework for protecting Controlled Unclassified Information (CUI) in non-federal systems and organizations. It is especially relevant for contractors and subcontractors working with the U.S. Department of Defense (DoD), General Services Administration (GSA), and other federal agencies.

To align with the U.S. government's emphasis on cybersecurity, the Cybersecurity Maturity Model Certification (CMMC) integrates and builds upon NIST 800-171 requirements. In this context, Level 1 and Level 2 security levels reflect different degrees of cybersecurity maturity and protection.

Level 1: (Formerly called "Foundational" now just "Level 1")

Level 1 of NIST 800-171 focuses on the basic safeguarding of Federal Contract Information (FCI). This level includes 15 security requirements derived primarily from Federal Acquisition Regulation (FAR) 52.204-21.

Key Characteristics of Level 1:

- Focuses on basic cyber hygiene.
- Intended to protect Federal Contract Information (FCI) that is not intended for public release.
- Requires organizations to implement and perform 15 security requirements (previously 17 requirements in 2024)
- No formal assessment required beyond self-attestation with accompanying senior company official affirmation of compliance in the Supplier Performance Risk System (SPRS).
- Self-assessment and affirmation is conducted annually.
- Applies to organizations handling FCI.

Level 2: (Formerly called "Advanced" now just "Level 2")

Level 2 corresponds to the protection of Controlled Unclassified Information (CUI) and aligns closely with the full set of 110 security requirements specified in NIST SP 800-171.

Key Characteristics of Level 2:

- Requires implementation of all 110 security requirements from NIST 800-171 Rev. 2.
- Emphasizes documentation, policy development, and process institutionalization.
- Targets organizations that store, process, or transmit CUI data.
- Typically requires a formal assessment or certification under the CMMC framework.
- Represents a higher degree of cybersecurity maturity than Level 1.
- Third party assessments completed every three years with self-assessments and affirmation completed annually.

Differences Between Level 1 and Level 2

Feature Level 1 Level 2

	Level1	Level2
Primary Focus	Federal Contract Information (FCI)	Controlled Unclassified Information (CUI)
Number of Security Requirements	15 requirements in NIST 800-171	110 requirements in NIST 800-171
Assessment Frequency	Annually	Every three years
Assessment Requirement	Self-assessment	Third-party or government assessment
Information Covered	FCI	CUI & FCI
Documentation	SSP is not required, but recommended	SSP is required

Conclusion

NIST SP 800-171 Level 1 and Level 2 represent progressively rigorous approaches to cybersecurity based on the sensitivity of information handled by contractors. Organizations must assess their information environment and compliance obligations to determine which level applies, especially in light of evolving DoD and federal cybersecurity mandates.