NIST SP 800 – 53 / 171

Controlled Unclassified Information (CUI) - **Security Controls**

Guide

CMMC

NIST SP 800-171

NIST SP 800-53

Cybersecurity Maturity Model Certification (CMMC)

- CMMC is a DoD certification process that measures a DIB sector company's ability to protect FCI and CUI.
- CMMC combines various cybersecurity standards and maps these best practices and processes to maturity levels, ranging from basic cyber hygiene to highly advanced practices.
- The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.
- The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.
- The intent is for certified independent 3rd party organizations to conduct audits and inform risk.

CMMC

CMMC Level 1

CMMC Level 2

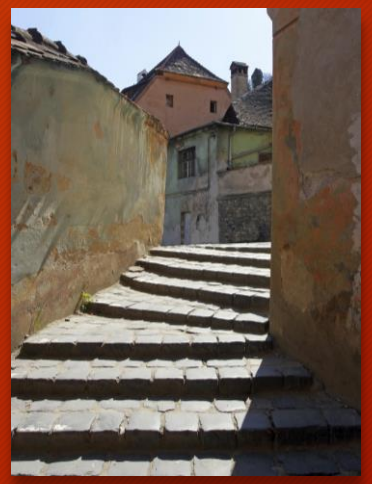
CMMC Level 3

CMMC Level 4

CMMC Level 5

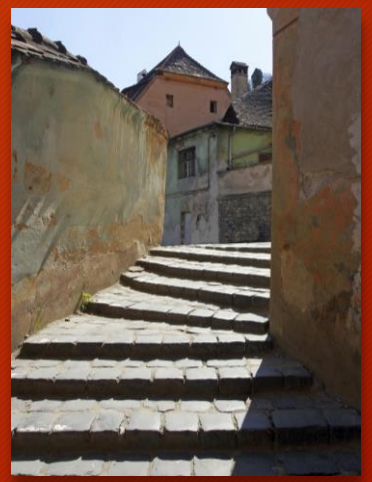
Understanding why you need NIST SP 800-171

When requested, the sysem security plan (or extracts thereof) and the associated plans of action for any planed implementations or mitigations are submitted to the responsible federal agency/contracting office to demonstrate the nonfederal organization's impementation or planned implementation of the security requirements. Federal agencies may consider submitted system security plans and plans of action as critical inputs to a risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization (Reference: NIST SP 800-171).



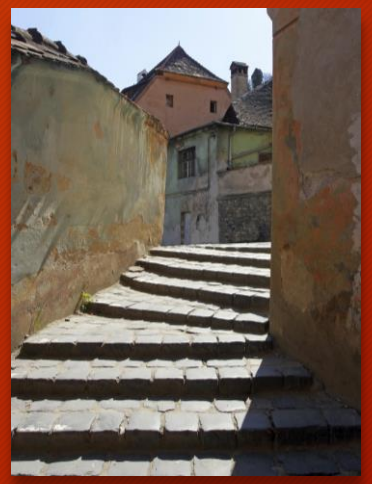
Useful References

- Information Processing Standards (FIPS Publication 199 Standards for Security Categorization Information and Information Systems
- Federal Information Processing Standards (FIPS) Publication 200: Minimum Security Requriements for Federal Information and Information Systems
- NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems an dOrganizations
- NIST Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories



Useful References

- 48 CFR 52.204-21
- NIST SP 800-171 R1
- Draft NIST SP 800-171B
- ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements (second edition)

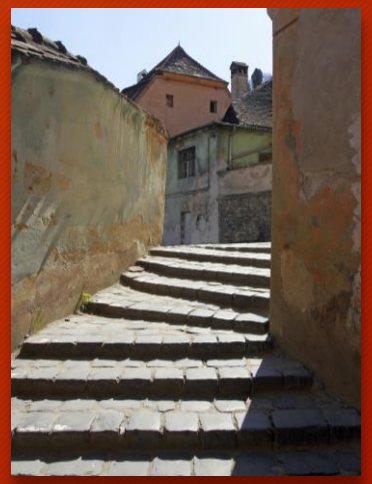


Useful Terms

CUI: Controlled Unclassified Information

FCI: Federal Contract Information

DIB: Defense Industrial Base

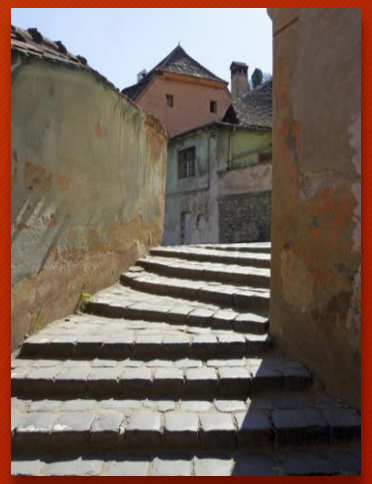


Security Requirements

The security requirements are organized into fourteen families

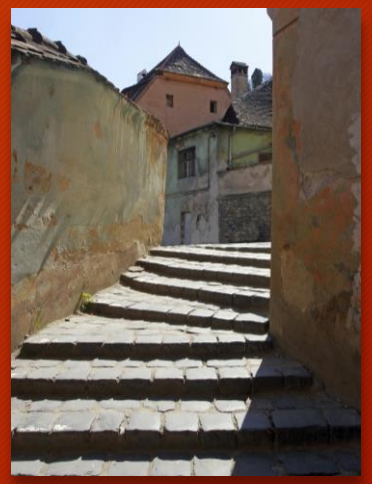
Each family contains the requirements related to the general security topic of the family.

Families are closely aligned with the minimum-security requirements for federal information and systems described in FIPS 200.



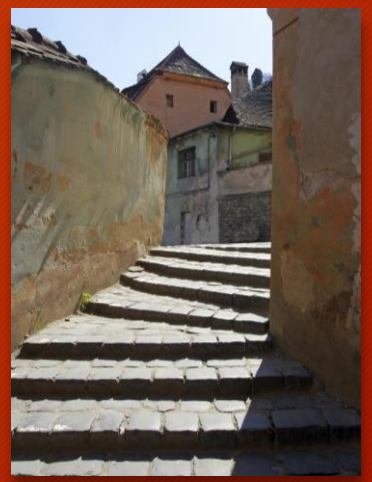
Family (A)

- Access Controls (3.1)
- Awareness and Training (3.2)
- Audit and Accountability (3.3)



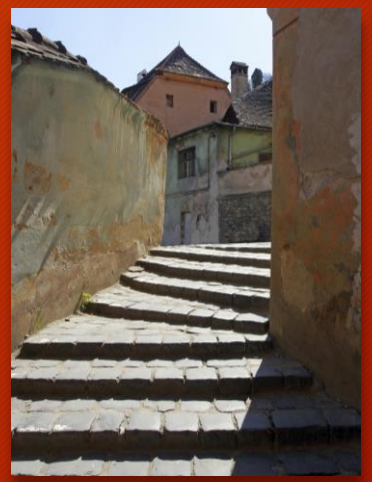
Family (C-I)

- Configuration Management (3.4)
- Identification and Authentication (3.5)
- Incident Response (3.6)



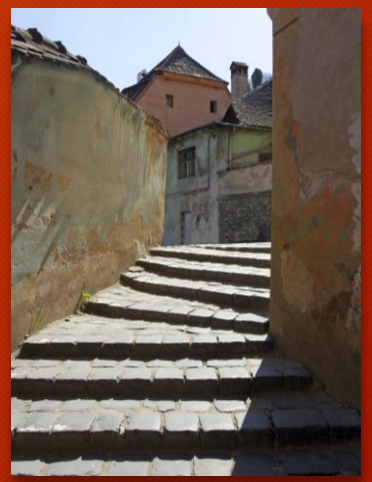
Family (M / P)

- Maintenance (3.7)
- Media Protection (3.8)
- Personnel Security (3.9)
- Physical Protection (3.10)



Family (R / S)

- Risk Assessment (3.11)
- Security Assessment (3.12)
- System and Communications Protection (3.13)
- System and Information Integrity (3.14)



NIST SP 800-53 rev 5 and NIST SP 800-53A

- Controls in this publication are for federal information systems and organizations, state, local, and tribal governments, as well as private sector organizations are encouraged to consider using
- Security and Privacy Controls
- Risk Management Framework (RMF)

Useful References

- OMB Circular A-130
- NIST SP 800-37
- NIST SP 800-160
- FIPS PUB 200

Security and Privacy Control Families

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Assessment, authorization and Monitoring (CA)
- Configuration Management (CM)
- Identification and Authentcation (IA)
- Individual Participation (IP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Privacy Authorization (PA)
- Physical ad Environmental Protection (PE)
- Planning (PL)
- Program Management (PM)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

Type of Controls

- Three types of controls
  - Common controls
    - Security or privacy controls whose implementation results in a capability that is inheritable by multiple information systems or programs
  - System-specific controls
    - Primary responsibility of information system owners and the authorizing officials or those systems
  - Hybrid controls
    - Exists if one part of the control is common and another part of the control is system-specific
    - Example: an organization may implement the Contingency Planning control using a predefined template for the master contingency plan for all organizational information systems with individual information system owners tailoring the plan for system-specific uses, where appropriate

Thank You!

NIST SP 800 53 / 171 and ISO/IEC 27001

Contact
sales@norbecktech.com
301-798-9108