Cybersecurity Requirements For Defense Contractors

Pat Toth

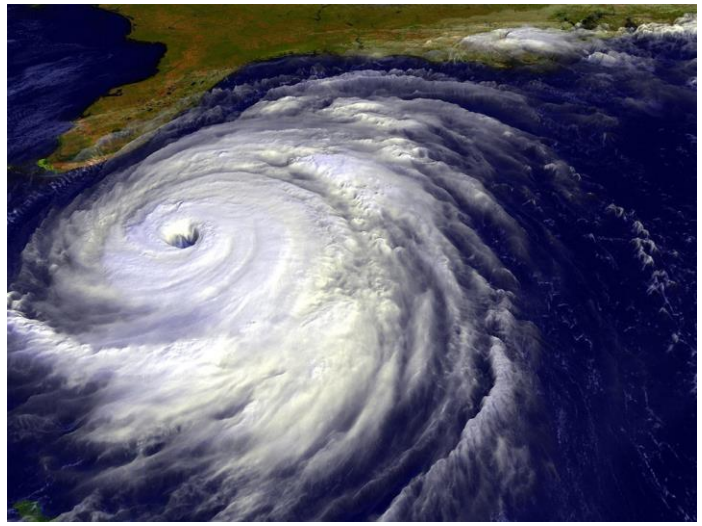
Cybersecurity Program Manager
National Institute of Standards and Technology (NIST)
Manufacturing Extension Partnership (MEP)

Understanding Information Security

Our appetite for *advanced technology* is rapidly exceeding our ability to protect it.

Information technology is fragile and susceptible to a wide range of threats including:

- natural disasters
- structural failures
- cyber attacks
- human errors



Controlled Unclassified Information

Supports federal missions and business functions…

…that affect the economic and national security interests of the United States.

Protecting DOD Information

A Northrop Grumman X-47B (U.S.) and a Lijian Sharp Sword (China)

A Lockheed Martin F-35B Lightning II (U.S.) and a Shenyang J-31 (China)

What is the purpose of DFARS clause 252.204-7012?

- Structured to ensure that:
  - controlled unclassified DoD info residing on a contractor's internal info system is safeguarded from cyber incidents.
  - any consequences associated with the loss of this info are assessed and minimized via the cyber incident reporting and damage assessment processes.

- Also provides single DoD-wide approach to safeguarding covered contractor information systems
  - prevent proliferation of multiple/potentially different safeguarding controlled unclassified information clauses, contract language by various entities across DoD.

What is the DFARS Cybersecurity Requirement?

- Clause 252.204-7012 requires defense contractors and subcontractors to:

1. Provide adequate security to safeguard covered defense information (CDI) that resides on or is transiting through a contractor's internal information system or network.
2. Report cyber incidents that affect a covered contractor information system or the CDI residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support.
3. Submit malicious software discovered and isolated in connection with a reported cyber incident to the DOD Cyber Crime Center.
4. If requested, submit media and additional information to support damage assessment.
5. Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve CDI.

What is "adequate security"?

Contractors should implement, at a minimum, the security requirements in

NIST SP 800-171 rev 1 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations"

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

What is a "Covered contractor information system"?

DFARS 252.204-7012(a): "covered contractor information system"

- "an unclassified info system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense info."
- A covered contractor info system is specifically an "unclassified" info system.
- A covered contractor info system requires safeguarding in accordance with 252.204-7012(b) because performance of the contract requires that the system process, store, or transmit CDI.

What do contractors need to do to ensure compliance with DFARS and when does this apply?

- Defense contractors are required by DFARS to provide ***adequate security*** on all covered contractor info systems.

- Defense contractors must implement, at a minimum, the following information security protections:
  - NIST SP 800-171 rev 1, as soon as practical,
  - but ***not later than December 31, 2017.***

MEP 3-Step Process to Complying with DFARS Cybersecurity Requirements

- **Step 1**:
  - Develop System Security Plan
- **Step 2:**
  - Conduct Assessment
  - Produce Security Assessment Report
- **Step 3:**
  - Produce a Plan of Action

MEP 3-Step Process to Complying with DFARS Cybersecurity Requirements

- **STEP 1**: Develop System Security Plan

- System Security Plan Describes
  - the system boundary;
  - the operational environment;
  - how the security requirements from SP 800-171 are implemented; and
  - the relationships with or connections to other systems

- No required format

MEP 3-Step Process to Complying with DFARS Cybersecurity Requirements

- **Step 2:** Conduct Assessment and Produce Security Assessment Report

- Conduct Assessment
  - Develop Assessment Plan
  - Conduct assessment against security requirements in NIST SP 800-171
    - Self-Assessment or
    - Third -Party
  - Determined if security requirements are effective and operating as intended
  - Some requirements may not apply
  - Alternative but equally effective

- Produce Security Assessment Report
  - No Required Format

MEP 3-Step Process to Complying with DFARS Cybersecurity Requirements

- **STEP 3:** Produce a Plan of Action

- Plan of Action describes:
  - How any unimplemented security requirements will be met
  - How any planned improvements will be implemented
  - Detailed milestones used to measure progress

- No deadline for meeting Plan of Action items

MEP 3-Step Process to Complying with DFARS Cybersecurity Requirements

- Submit to DOD Contracting Officer or Prime Contractor:
  - **System Security Plan,**
  - **Security Assessment Report and**
  - **Plan of Action**
- These documents provide evidence to demonstrate compliance with the DFARS.

IMPORTANT: Things to Remember Regarding Compliance with DFARS Cybersecurity Requirements

- Compliance occurs upon approval of the System Security Plan, Security Assessment Report and the Plan of Action.
- Approval of these items comes from the appropriate DOD Contracting Officer, or Prime Contractor – depending upon where a particular manufacturer falls within the supply chain.
- Some plans may need to be reviewed by DOD CIO.
- A contractor's signature on a contract indicates that DFARS cybersecurity requirements have been met.
- No pre-determined audit processes are planned, but audits by DOD may occur as warranted.

NIST SP 800-171 Security Requirements

14 Families

Obtained from FIPS 200 and NIST Special Publication 800-53

- Access Control.
- Audit and Accountability.
- Awareness and Training.
- Configuration Management.
- Identification and Authentication.
- Incident Response.
- Maintenance.
- Media Protection.
- Physical Protection.
- Personnel Security.
- Risk Assessment.
- Security Assessment.
- System and Communications Protection
- System and Information Integrity.

Access Control: SP 800-171 Security Family 3.1

- Access is the ability to make use of any system resource.

- Access control is the process of granting or denying requests to:
  - use information
  - use information processing services
  - enter company facilities

- Logical access controls
  - prescribe who or what can access system resource and
  - the type of access that is permitted.
  - built into the operating system or
  - incorporated into applications programs or
  - major utilities (e.g., database management systems, communications systems), or
  - implemented through add-on security packages.
  - may be implemented internally to the system or in external devices.

Access Control: SP 800-171 Security Family 3.1

- Companies should limit:
  - system access to authorized users
  - processes acting on behalf of authorized users
  - devices, including other systems and
  - the types of transactions and functions that authorized users are permitted to exercise

- Can vary from one system to another.

- It may also be important to control the kind of access that is permitted (e.g., the ability for the average user to execute, but not change, system programs). These types of access restrictions enforce policy and help ensure that unauthorized actions are not taken.

- Controlling physical access to company facilities is also important. It provides for the protection of employees, plant equipment, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to the company.

Awareness and Training: SP 800-171 Security Family 3.2

Information security awareness, training, and education

- Raises awareness of the need to protect system resources
- Develops skills and knowledge so system users can perform their jobs more securely and
- Builds in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems.

All managers and users are aware of the security risks associated with their activities.

Employees are trained to carry out their information security-related duties and responsibilities.

Audit and Accountability: SP 800-171 Security Family 3.3

- Audit
  - Independent review and examination of records and activities
  - Assess the adequacy of system requirements and
  - Ensure compliance with established policies and procedures.

- Audit trail
  - Record of who has accessed system
  - What operations performed during a given period.
  - Maintains a record of system activity
  - Detect security violations, performance issues, and flaws in applications.
  - Ensure that the system not been harmed by hackers, insiders, or technical problems
  - Insurance policy, maintained but not used unless needed (e.g., after a system outage).

- Create, protect, and retain system audit records
- Enables the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity
- Actions of users can be uniquely traced
- Users can be held accountable.

Configuration Management: SP 800-171 Security Family 3.4

- Determining and documenting the appropriate specific settings for a system,
- Conducting security impact analyses,
- Managing changes through a change control board.
- Allows entire system to be reviewed
- Helps ensure that a change made on one system does not have adverse effects on another system.

Common secure configurations/security configuration checklists:

- provide recognized, standardized, and established benchmarks
- specify secure configuration settings for information technology platforms and products
- can be used to verify that changes to the system have been reviewed from a security point-of-view.

- Help determine if major changes (such as connecting to the internet) have occurred that have not yet been analyzed.
-
- NIST checklist repository, National Vulnerability Database (NVD) https://web.nvd.nist.gov/view/ncp/repository

Identification and Authentication: SP 800-171 Security Family 3.5

- Verifying the identity of a user, process, or device
- Prerequisite for granting access to resources in a system.
- Prevents unauthorized individuals or processes from entering a system.
- Basis for most types of access control and user accountability.
- Identify and differentiate between users
- User accountability requires linking activities on a system to specific individuals
- Authentication presents several challenges:
  - collecting authentication data,
  - transmitting the data securely, and
  - knowing whether the individual who was originally authenticated is still the individual using the system.
- User identity can be authenticated based on:
  - something you know – e.g., a password or Personal Identification Number (PIN)
  - something you possess (a token) – e.g., an ATM card or a smart card
  - something you are (static biometric) – e.g., fingerprint, retina, face, ear, DNA
  - something you do (dynamic biometrics) – e.g., voice pattern, handwriting, typing rhythm

Incident Response : SP 800-171 Security Family 3.6

- Standard operating procedures that can be followed in the event of an incident.
- Addressed in a company's contingency plan.
- Threat events can also result from a virus, other malicious code, or a system intruder (either an insider or an outsider).
- Definition of a threat event is somewhat flexible and may vary by company and computing environment.
- Reoccurrence of similar incidents can make it cost-beneficial to develop a standard capability for quick discovery of and response Closely related to contingency planning.
- Responds to malicious technical threats.

- Incident handling capability includes:
  - adequate preparation,
  - detection,
  - analysis,
  - containment,
  - recovery,
  - user response activities and
  - track, document, and report incidents to company management

Maintenance: SP 800-171 Security Family 3.7

- Controlled maintenance - scheduled and performed in accordance with the manufacturer's specifications.
-
- Corrective maintenance - when a system fails or generates an error condition that must be corrected
- Performed locally or non-locally.
- Nonlocal maintenance - maintenance or diagnostics performed via a network (internal or external)
- Perform periodic and timely maintenance on company systems
- Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Media Protection: SP 800-171 Security Family 3.8

- Defense of system media - both digital and non-digital.
- Digital media - diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks.
- Non-digital media - paper or microfilm.
- Restrict access - Media only available to authorized personnel
- Apply security labels to sensitive information
- Remove information from media so that the information cannot be retrieved or reconstructed
- Physically control system media and ensure accountability
- Restricting mobile devices capable of storing and carrying information into or outside of restricted areas.
- Destroy system media before disposal or reuse.

Personnel Security: SP 800-171 Security Family 3.9

- Users play a vital role in protecting a system
- Personnel security seeks to minimize the risk that staff (permanent, temporary, or contractor) pose to company assets
- A company's status and reputation can be damaged by the actions of employees
- Employees may have access to extremely sensitive, or proprietary information
- Recruiting and hiring new employees
- Employee transfers or is terminated
- Consequences for personnel failing to comply with company security policies and procedures

Physical Protection: SP 800-171 Security Family 3.10

- Protection of systems, buildings, and related supporting infrastructure
- Natural threats
- Man-made threats
- Limit physical access to systems, equipment, and operating environments
- Protect the physical plant and support infrastructure
- Provide backup supporting utilities
- Protect systems against environmental hazards
- Provide appropriate environmental controls in facilities

Risk Assessment: SP 800-171 Security Family 3.11

- Risk assessments identify and prioritize risks to:
  - company operations,
  - assets,
  - employees, and
  - other organizations

- Risk assessment identify:
  - relevant threats or
  - threats directed against other organizations,
  - vulnerabilities both internal and external,
  - impact (i.e., harm) that may occur if threats exploit vulnerabilities and
  - the likelihood that harm will occur.

- Periodically assess risk

Security Assessment: SP 800-171 Security Family 3.12

- Testing and/or evaluation of the management, operational, and technical security requirements
- Determine if requirements are:
  - implemented correctly,
  - operating as intended, and
  - producing the desired outcome with respect to meeting the security requirements for the system.
  - most effective and cost-efficient solution
- Continuous basis to support a near real-time analysis of security posture.
- Company makes the decision to operate (for a new system) or to continue to operate.
- Document actions in the System Security Plan.

System and Communications Protection: SP 800-171 Security Family 3.13

- Confidentiality of information at rest and in transit.
- Physical or logical means.
- Establishes boundaries that restrict access to publicly-accessible information within a system.
- Monitor and control communications at external boundaries and key internal boundaries within the system.
- Employ architectural designs, software development techniques, and systems engineering principles

System and Information Integrity: SP 800-171 Security Family 3.14

- Guarding against improper information modification or destruction.
- Data can only be accessed or modified by the authorized employees.
- Assurance that information being accessed has not been meddled with or damaged by an error in the system.

Companies should:

- Identify, report, and correct information and system flaws in a timely manner
- Provide protection from malicious code at appropriate locations within company systems and
- Monitor system security alerts and advisories and respond appropriately.

NIST Handbook 162

- Step-by-step guide to performing a self-assessment against NIST SP 800-171
- Available at http://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf
- Downloaded over 13,000 times

Security Requirement

Awareness and Training Example

Basic Security Requirements:

3.2.1 Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those organizational information systems.

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Derived Security Requirements:

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Security Requirement

Awareness and Training Example 3.2.2

Security Requirement:

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Meeting the Requirement:

- Basic security awareness training to new employees.
- Security awareness training to users when information system changes.
- Annual security awareness refresher training.

Security Requirement

Awareness and Training Example 3.2.2

MEP Self-Assessment Handbook

Do employees with security-related duties and responsibilities receive initial and annual training on their operational, managerial, and technical roles and responsibilities? Does the training cover physical, personnel, and technical safeguards and countermeasures?

Yes No Partially Does Not Apply Alternative Approach

Does the training address required security requirements related to environmental and physical security risks?

Yes No Partially Does Not Apply Alternative Approach

Does the training include indications of potentially suspicious email or web communications, to include suspicious communications and other anomalous system behavior?

Yes No Partially Does Not Apply Alternative Approach

Is security-related technical training provided before authorizing access to the system or performing assigned duties, when required by system changes and on a periodic basis?

Yes No Partially Does Not Apply Alternative Approach

Security Requirement

Awareness and Training Example 3.2.2

Where to Look:

• security awareness and training policy • procedures addressing security awareness training implementation • appropriate codes of federal regulations • security awareness training curriculum • security awareness training materials • security plan training records • other relevant documents or records

Who to Talk to:

• employees with responsibilities for security awareness training • employees with information security responsibilities • employees with responsibilities for role-based security training • employees with assigned information system security roles and responsibilities • employees comprising the general information system user community

Perform Test On:

• automated mechanisms managing security awareness training • automated mechanisms managing role-based security training

Security Requirement

Configuration Management Example

Basic Security Requirements:

3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational information systems.

Derived Security Requirements:

3.4.3 Track, review, approve/disapprove, and audit changes to information systems.

3.4.4 Analyze the security impact of changes prior to implementation.

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

3.4.5 ……

Security Requirement

Configuration Management Example 3.4.1

Basic Security Requirements:

3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Meeting the Requirements:

- Develops, documents and maintains a current baseline configuration of the information system
- Configuration control in place.

Security Requirement

Configuration Management Example 3.4.1

Basic Security Requirements:

3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Meeting the Requirements:

- Configuration management policy; procedures and plan.
- Documentation for Enterprise architecture or information system design.
- Information system configuration settings and associated documentation.
- Change control records.
- Personnel with configuration management responsibilities.
- System/network administrator.

Security Requirement

Configuration Management Example 3.4.1

MEP Self-Assessment Handbook

Are baseline configurations developed, documented, and maintained for each information system type?
Yes No Partially Does Not Apply Alternative Approach

Do baseline configurations include SW versions and patch level, configuration parameters, network information including topologies, and communications with connected systems?
Yes No Partially Does Not Apply Alternative Approach

Are baseline configurations updated as needed to accommodate security risks or software changes?
Yes No Partially Does Not Apply Alternative Approach

Are baseline configurations developed and approved in conjunction with the CISO (or equivalent) and the information security owner?
Yes No Partially Does Not Apply Alternative Approach

Are deviations from baseline configurations documented?
Yes No Partially Does Not Apply Alternative Approach

Is the system managed using a system development life-cycle methodology that includes security considerations?
Yes No Partially Does Not Apply Alternative Approach

Security Requirement

Configuration Management Example 3.4.1

Where to Look: • configuration management policy • procedures addressing the baseline configuration of the information system • procedures addressing configuration settings for the information system • configuration management plan • Security plan • enterprise architecture documentation • security configuration checklists • evidence supporting approved deviations from established configuration settings • change control records • information system audit records • information system design documentation • information system architecture and configuration documentation • information system configuration settings and associated documentation • change control records • other relevant documents or records

Who to Talk to: • employees with configuration management responsibilities • employees with security configuration management responsibilities • employees with information security responsibilities • system/network administrators

Perform Test On: • processes for managing baseline configurations • automated mechanisms supporting configuration control of the baseline configuration • processes for managing configuration settings • automated mechanisms that implement, monitor, and/or control information system configuration settings • automated mechanisms that identify and/ or document deviations from established configuration settings

Security Requirement

Access Control Example

Basic Security Requirements:

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Derived Security Requirements:

3.1.3 Control the flow of CUI in accordance with approved authorizations.

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

3.1.6 Use non-privileged accounts or roles when accessing non-security functions.

3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

3.1.8 Limit unsuccessful logon attempts.

Security Requirement

Access Control Example 3.1.8

Derived Security Requirements:

3.1.8 Limit unsuccessful logon attempts.

Meeting the Requirements:

- Limit number of consecutive invalid logon attempts allowed during a time period.
- Account lockout time period automatically enforced by the information system when max number of unsuccessful logon attempts is exceeded.
- Locks the account/node until released by an administrator.
- Delays next logon prompt according to the organization-defined delay algorithm.
- Access control policy and procedures addressing unsuccessful logon attempts.
- Personnel with information security responsibilities; system developers; system/network administrators

Security Requirement

Access Control Example 3.1.8

Derived Security Requirements:

3.1.8 Limit unsuccessful logon attempts.

Meeting the Requirements:

- Access control policy and procedures addressing unsuccessful logon attempts.
- Personnel with information security responsibilities; system developers; system/network administrators

Security Requirement

Access Control Example 3.1.8

MEP Self-Assessment Handbook

Is the system configured to limit the number of invalid login attempts?
Yes No Partially Does Not Apply Alternative Approach

Is the system configured to lock the logon mechanism for a predetermined time after a predetermined number of invalid login attempts?
Yes No Partially Does Not Apply Alternative Approach

Is the system configured to lock users out after a predetermined number of invalid logon attempts?
Yes No Partially Does Not Apply Alternative Approach

Does the system enforce a limit of a defined number of consecutive invalid access attempts during a defined time?
Yes No Partially Does Not Apply Alternative Approach

Security Requirement

Access Control Example 3.1.8

Where to Look: • access control policy • procedures addressing unsuccessful logon attempts • security plan • information system design documentation • information system configuration settings and associated documentation information system audit records • other relevant documents or records

Who to Talk to: • employees with information security responsibilities • system developers • system/network administrators

Perform Test On: • automated mechanisms implementing access control policy for unsuccessful logon attempts

Meeting SP 800-171

- Emphasis is risk management for a particular operating environment.
- Some security controls may not be applicable to your environment.
  - Remote access
- Build off what you are currently doing.
- Security controls are intended to be flexible
  - Other ways to meet the requirements.
  - Implement alternative, but equally effective, security measures.

Meeting SP 800-171

- Cost effective approaches
  - Isolate CUI into its own security domain by applying architectural design concepts.
  - Security domains may employ physical separation, logical separation, or a combination of both.
  - Use the same CUI infrastructure for multiple government contracts or agreements.

Contact Info:

Pat Toth
NIST MEP
ptoth@nist.gov
301 975-5140

or

David Stieren
NIST MEP
david.stieren@nist.gov
301-975-3197