



# **DSci526: Secure Systems Administration**

**Security Requirements  
(and Introduction to Virtualization)**

***Prof. Clifford Neuman***

**Lecture 2**  
27 January 2021  
Online



# Course Identification

---

- DSci 526
  - Secure Systems Administration (4 units)
- Class meeting schedule
  - 2PM to 5:20PM Wednesday
  - Online
- Class communication
  - [inf526@csclass.info](mailto:inf526@csclass.info)
  - Goes to instructor and any assistants and is archived.

# General Course Information

---



- Professor office hours
  - Monday 1PM-2:30PM via Zoom
    - Link to be sent in email
  - Other times by appointment
  - E-mail: [dsci526@csclass.info](mailto:dsci526@csclass.info) and [bcn@isi.edu](mailto:bcn@isi.edu)
- TA for the class
  - Not yet assigned
  - Likely to have a lab assistant assigned instead

# Pre-Initial Homework Exercise

(due before 1/27 class and discussed now)

---



- Submit through Drop-box on D2L
- System Structure for Home Network with IoT devices.
  - Enumerate the classes of data
  - Enumerate the classes of users
  - Identify the protection domains
  - Enumerate the systems (hardware)
  - Enumerate the systems (software components)
- This write-up is expected to be about 3 pages in length (could be more or less)
- But we will develop our answer right now (you only need to explain what we discuss).

# Your Organization's Security Policy

---



- First step – Understand Your Organization's Goals for managing risk:
  - <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>
- Write organizational policies that will achieve those goals:
  - [www.GIAC.org/paper/gsec/734/system-security-policy/101613](http://www.GIAC.org/paper/gsec/734/system-security-policy/101613)
- First question for security auditors – do you have a policy?
  - It will guide you in creating categories of data and users
  - This will be important in specifying the system security policies
- Two kinds of Security Policy
  - Specified for evaluation by system components
  - Specified for interpretation by individuals and administrators

# Your Organization's Security Policy



- Should Establish Motivation and Principles, not individual details
  - Computer Security Supports the Mission of the Organization
  - Computer Security is an Integral Element of Sound Management
  - Computer Security Should Be Cost-Effective
  - Systems Owners Have Responsibilities Outside Their Own Organizations
    - To customers
    - To the public and to others that may be impacted by breach
  - Computer Security Responsibilities & Accountability Should Be Explicit .
  - Computer Security Requires a Comprehensive and Integrated Approach
  - Computer Security Should Be Periodically Reassessed
  - Computer Security is Constrained by Societal Factors
    - E.g. privacy and monitoring

# Your Organization's Security Policy



- First document requested by Security Auditors
  - Why?
- Lays out categories of data and users and kinds of access authorized
- Provides specific guidance for security requirements necessary to meet the principles just discussed.
- It will define responsibilities
- It will provide the basis for evaluating your organization's ability to maintain security

Some Guidance in writing a security policy

[www.GIAC.org/paper/gsec/734/system-security-policy/101613](http://www.GIAC.org/paper/gsec/734/system-security-policy/101613)

- I don't agree with all of the above, but it is useful as a basis for discussion.



# A Reasonable Outline(1)

---

- Motivation and Principles
  - Written altruistically, but in reality, the goals are to protect your organization.
  - Mentions Classes of Data and Consequences
    - E.g. Some Material from NIST Risk Management Framework
  - Acknowledgement of the threat environment
    - E.g. The Global System Environment (from GIACS)





# A Reasonable Outline(1)

---

- Description of System (applicability)
  - Inventory: Systems, Devices, Data
- Motivation and Principles
  - Written altruistically, but in reality, the goals are to protect your organization.
  - Mentions Classes of Data and Consequences
    - E.g. Some Material from NIST Risk Management Framework
  - Acknowledgement of the threat environment
    - E.g. The Global System Environment (from GIACS)
- High level assignment of responsibilities



# A Reasonable Outline(2)

---

- Security Requirements and Metrics
  - What is to be protected against what threats
    - Consequences to organization of breaches
  - Required level of protection to each class of asset
    - Required approaches to providing that protection
    - Metric regarding strength of mechanisms to be applied.
- Physical and Personnel Security Constraints
  - Who will have access
  - Access controls on physical systems



# A Reasonable Outline(3)

---

- Requirements on Specific Categories of Controls
  - Access Control
  - Training
  - Audit
  - Configuration Management
  - Identity Management
  - Incident Response
  - Maintenance
  - Vendor Requirements
  - Media Protection
  - Personnel Security
  - Physical Protection
  - Risk Assessment
  - Security Assessment
  - Sys and Comm Protection
  - Integrity
  - Software Requirements



# Access Control

---

- High level rules regarding:
  - Basically a statement regarding least-privilege and need to know, need to access
    - Who has access to physical systems
    - Who has access to classes of data
  - Flow of information between domains
    - System access shall be limited to authorized users, processes, and devices.
    - System access shall be limited to the types of functions permitted to authorized users. (e.g. least privilege)
  - Requirements for mechanisms
    - E.g. encryption, algorithms to be used, etc.
    - Mandatory policies vs discretionary policies



# Information Access

---

- Decide on multiple data classes
  - Public data
  - Customer data
  - Corporate data
  - Highly sensitive data
- Access to each class of data
  - Can you support mandatory policies
  - Otherwise. what discretionary policies apply.
- Domain boundaries
  - Based on users and locations



# Identity Management

---

- High level rules regarding:
  - Password Policies
  - Stronger authentication requirements
  - Multi-factor Authentication
  - When required e.g.
    - Authenticate the identities of users, devices, and processes as a prerequisite to allowing access to organizational information systems.
    - Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- Strength of Mechanism



# Security Requirement's

---

- Personnel Security
  - Including training
- Physical Security
- Monitoring and Audit
- Vendor Requirements
- Accreditation



# Personnel Security

---

- Requirements on credentials and vetting processes for employees with access to different domains.
  - Relates to identity management
  - More as a precursor
- Identity Management about who the user is, PS about vetting and physical access and issuance of ID's.





# Physical Security

---

- Virtual containment of data to domains is useless if access to protected machines can be achieved by failures of physical security. Define controls on placement of hardware and protection of cables, etc.



# Monitoring and Audit

---

- This is how you will know that you have been attacked.
- It is critical to consider these technologies when designing your deployment.
- The monitoring function is part of administration.
  - Responding to alerts
  - False positive vs false negatives
  - Volume of alerts and what is of interest.



# Vendor Requirements

---

- Concern with supply chain subversion, and physical access by vendors on site.
  - Apply personnel security constraints to vendors.
  - Restrict access by vendors and visitors.

# How to Implement: Technological Requirements: Information Access

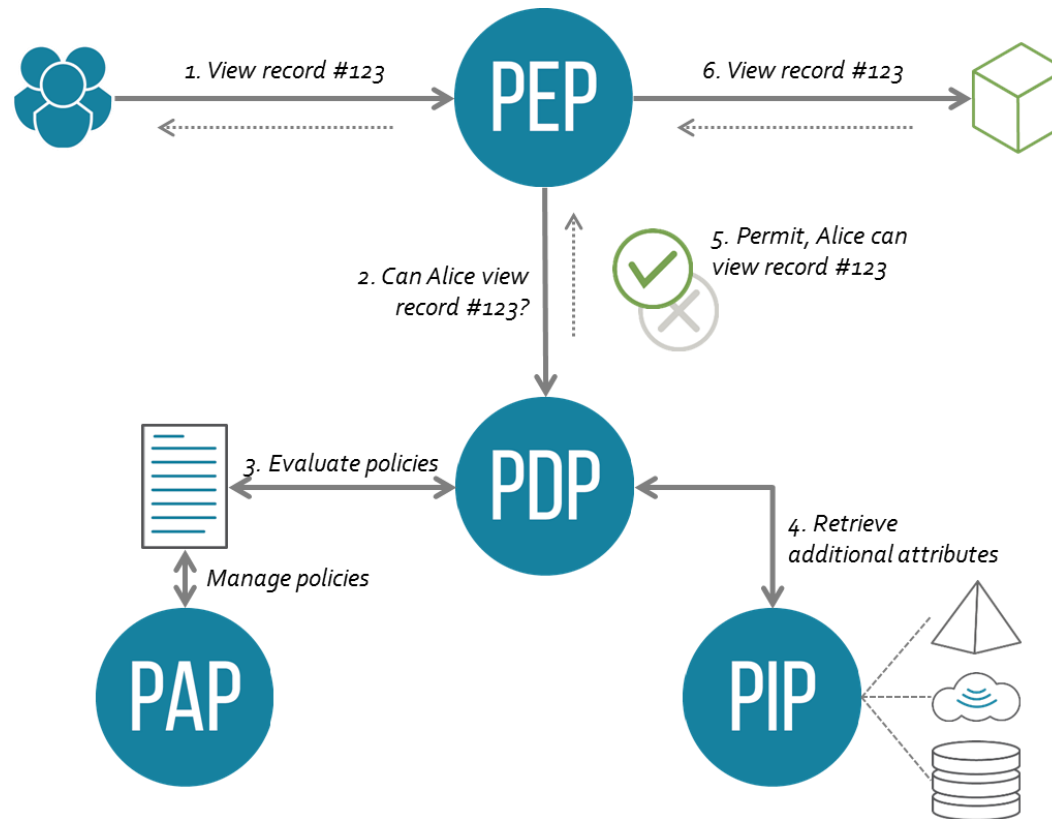
---



- Identity Management
  - Factors / Basis for Authentication
  - Enrollment, Exception Handling
  - Other policy conditions
- Containment
  - Firewalls, VLANs
  - Encryption
- Policy
  - Decision points
  - Specification point (or administration)
  - Enforcement point



# Points of Policy



- By Axiomatics - Axiomatics, CC BY 3.0, <https://commons.wikimedia.org/w/index.php?curid=48397652>



# Network Administration

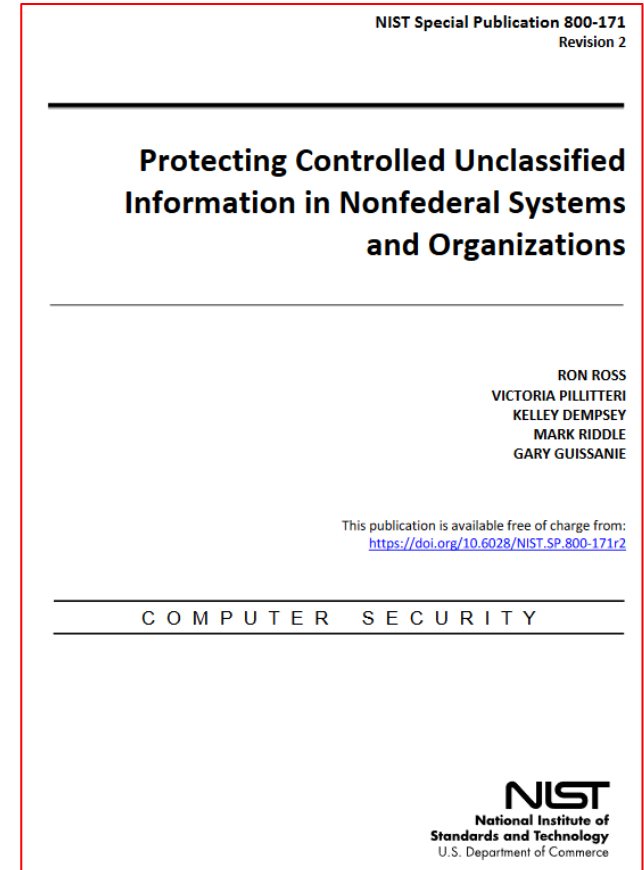
---

- Creation of network protection domains
  - Firewalls
  - VLANs
  - VPNs for access
  - Ipsec
- Define required characteristics
  - Where is encryption required
  - This is policy and administration

# Reading for Next Week



<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>





# DSci526: Secure Systems Administration

(Introduction to Virtualization)

*Prof. Clifford Neuman*

**Lecture 2**  
27 January 2021  
Online





# Virtualization

---

- Operating Systems are all about virtualization
  - One of the most important function of a modern operating system is managing virtual address spaces.
  - But most operating systems do this for applications, not for other OSs.



# Virtualization of the OS

---

- Some have said that all problems in computer science can be handled by adding a layer of indirection.
  - Others have described solutions as reducing the problem to a previously unsolved problem.
- Virtualization of OS's does both.
  - It provides a useful abstraction for running guest OS's.
  - But the guest OS's have the same problems as if they were running natively.



# What is the benefit of virtualization

---

- Management
  - You can run many more “machines” and create new ones in an automated manner.
  - This is useful for server farms.
  - This helps you avoid “errors” in configuration over manual installation of new hardware.
- Separation
  - “Separate” machines provide a fairly strong, though coarse grained level of protection.
  - Because the isolation can be configured to be almost total, there are fewer special cases or management interfaces to get wrong.



# Hypervisors Manage Resources for Guest OS

---

- Same problems
  - Most of the problems handled by hypervisors are the same problems handled by traditional OS's
- But the Abstractions are different
  - Hypervisors present a hardware abstraction.
    - E.g. disk blocks
  - OS's present an application abstraction.
    - E.g. files



# Virtualization

---

- Running multiple operating systems simultaneously.
  - OS protects its own objects from within
  - Hypervisor provides partitioning of resources between guest OS's.



# Managing Virtual Resource

---

- Page faults typically trap to the Hypervisor (host OS).
  - Issues arise from the need to replace page tables when switching between guest OS's.
  - Xen places itself in the Guest OS's first region of memory so that the page table does not need to be rewritten for traps to the Hypervisor.
- Disks managed as block devices allocated to guest OS's, so that the Xen code to protect disk extents can be as simple as possible.



# What makes virtualization hard

---

- Operating systems are usually written to assume that they run in privileged mode.
- The Hypervisor (the OS of OS's) manages the guest OS's as if they are applications.
- Some architecture provide more than two “Rings” which allows the guest OS to reside between the two states.
  - But there are still often assumptions in coding that need to be corrected in the guest OS.



## Partitioning of Resources

---

- Fixed partitioning of resources makes the job of managing the Guest OS's easier, but it is not always the most efficient way to partition.
  - Resources unused by one OS (CPU, Memory, Disk) are not available to others.
- But fixed provisioning prevents use of resources in one guest OS from effecting performance or even denying service to applications running in other guest OSs.





# The Security of Virtualization

---

- +++ Isolation and protection between OS's can be simple (and at a very coarse level of granularity).
- +++ This coarse level of isolation may be an easier security abstraction to conceptualize than the finer grained policies typically encountered in OSs.
- --- Some malware (Blue pill) can move the real OS into a virtual machine from within which the host OS (the Malware) can not be detected.



# Examples of Virtualization

---

- VMWare
  - Guest OS's run under host OS
  - Full Virtualization, unmodified Guest OS
- Xen
  - Small Hypervisor as host OS
  - Para-virtualization, modified guest OS
- Many other hypervisors
- Virtualization is the foundation of cloud computing.



# Xen System

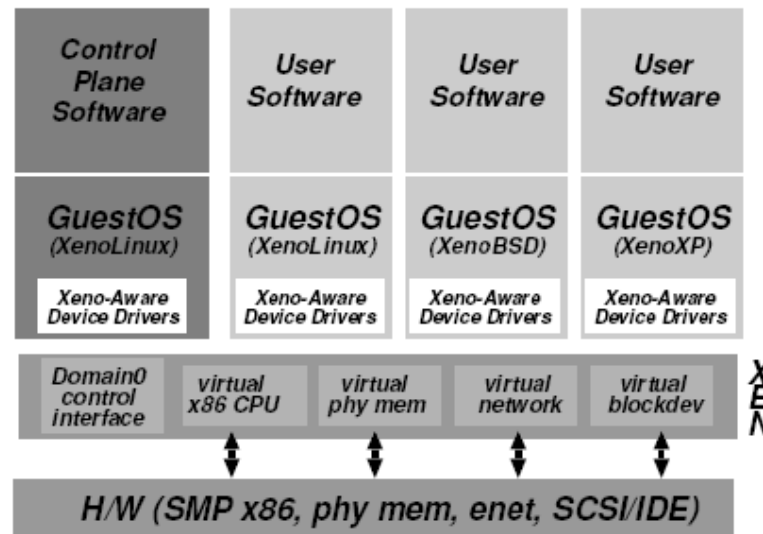


Figure 1: The structure of a machine running the Xen hypervisor, hosting a number of different guest operating systems, including *Domain0* running control software in a XenoLinux environment.



# **DSci526: Secure Systems Administration**

**Standards and Best Practices**

*Prof. Clifford Neuman*

**Lecture 3**  
3 February 2021  
Online

# NIST 800-171 Rev 1



NIST Special Publication 800-171

Revision 1

- NIST SP 800-171 Rev 1 lists 110 controls that correspond to industry best practices and which correspond to “adequate security”.
- For existing DoD contracts it is required that you meet all 110 controls.
- But... at DoD’s discretion, contractors are sometimes permitted to operate with a subset of these controls in place together with a system security plan and plan of action and milestones providing an assessment of which controls are met, and providing a plan to meet the other controls.
- These rules are NOT well defined.
- Rev 2 of NIST 800-171 was issued on 2/21/2020, Rev 1 will be withdrawn on 2/21/2021

---

## Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

---

RON ROSS  
PATRICK VISCUSO  
GARY GUISSANIE  
KELLEY DEMPSEY  
MARK RIDDLE

# NIST SP 800-171

## Minimum Cyber-Security Standards



- NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
  - Lists 110 requirements in 14 areas (sometimes called families)

|                                 |                         |
|---------------------------------|-------------------------|
| Access Control                  | Media Protection        |
| Awareness & Training            | Personnel Security      |
| Audit & Accountability          | Physical Protection     |
| Configuration Management        | Risk Assessment         |
| Identification & Authentication | Security Assessment     |
| Incident Response               | System & Com Protection |
| Maintenance                     | System & Info Integrity |



# The Initial FAR Seventeen

- In this morning session we will discuss the seventeen controls initially called out in the FAR's.
  - These seventeen must be implemented NOW on all covered contractor information systems, as mandated by the FARs.
  - These constitute the most basic security controls that are sometimes referred to as cyber-hygiene and should really be adopted on ALL systems.
  - At present you **must** also have a plan of action and milestones in place to specify your plan for meeting all 110 controls.
- These Seventeen are also part of the CMMC Level One “no-cost” controls.
- This afternoon we will discuss these controls again, in the context of the full set of 110 controls from NIST SP 800-171 which you should implement as soon as possible, and for which you must have a plan of action and milestones in place.

# Access Control and Identity Management



Basic means taken from FIPS 200, Derived means taken from NIST 800-53  
Derived controls elaborate on the basic controls, and may apply  
To certain kinds of access or systems.

| FAR Clause 52.204-21(b)(1)  | NIST 800-171 Reference | Basic or Derived | 800-171 Family                    |
|---|------------------------|------------------|-----------------------------------|
| (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).      | 3.1.1                  | Basic            | Access Control                    |
| (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.                                 | 3.1.2                  | Basic            | Access Control                    |
| (iii) Verify and control/limit connections to, and use of, external information systems.  | 3.1.20                 | Derived          | Access Control                    |
| (iv) Control information posted or processed on publicly accessible information systems.  | 3.1.22                 | Derived          | Access Control                    |
| (v) Identify information system users, processes acting on behalf of users, or devices.   | 3.5.1                  | Basic            | Identification and Authentication |
| (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | 3.5.2                  | Basic            | Identification and Authentication |





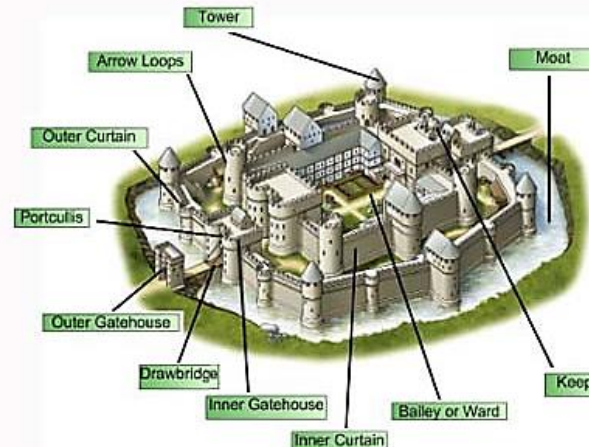
# Control Access to Your Systems

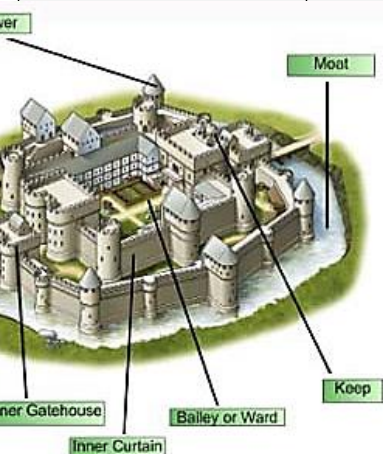
(i) Limit information system access to:

- authorized users,
- processes acting on behalf of authorized users,
- or devices (including other information systems)

Methods:

Account Management  
Firewalls  
Limits to BYOD  
Network Access Control  
Remote access limitations



| SECURITY REQUIREMENTS   | NIST SP 800-53<br>Relevant Security Controls |                    | ISO/IEC 27001<br>Relevant Security Controls |  |
|---|--|--------------------|---|--|
| <u>3.1 ACCESS CONTROL</u>   |  |                    |   |  |
| Basic Security Requirements   |  |                    |   |  |
| <div>3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).</div> <div>3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.</div>  | AC-2   | Account Management | A.9.2.1                                     | User registration and de-registration            |
|   |  |                    | A.9.2.2                                     | User access provisioning                         |
|   |  |                    | A.9.2.3                                     | Management of privileged access rights           |
|   |  |                    | A.9.2.5                                     | Review of user access rights                     |
|   |  |                    | A.9.2.6                                     | Removal or adjustment of access rights           |
|   | AC-3   | Access Enforcement | A.6.2.2                                     | Teleworking                                      |
|   |  |                    | A.9.1.2                                     | Access to networks and network services          |
|   |  |                    | A.9.4.1                                     | Information access restriction                   |
|   |  |                    | A.9.4.4                                     | Use of privileged utility programs               |
|   |  |                    | A.9.4.5                                     | Access control to program source code            |
|   |  |                    | A.13.1.1                                    | Network controls                                 |
|   |  |                    | A.14.1.2                                    | Securing application services on public networks |
|   |  |                    | A.14.1.3                                    | Protecting application services transactions     |
|   |  |                    | A.18.1.3                                    | Protection of records                            |
|   |  | Remote Access      | A.6.2.1                                     | Mobile device policy                             |
|   |  |                    | A.6.2.2                                     | Teleworking                                      |
|   |  |                    | A.13.1.1                                    | Network controls                                 |
|   |  |                    | A.13.2.1                                    | Information transfer policies and procedures     |
|   |  |                    | A.14.1.2                                    | Securing application services on public networks |



# Least Privilege

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

## Methods:

Privileged accounts  
Access Controls  
Information Flow  
Constraints  
Separate server accounts

## Breaches:

SF Muni Hack  
Hollywood Presb Hospital  
Most major ransomware

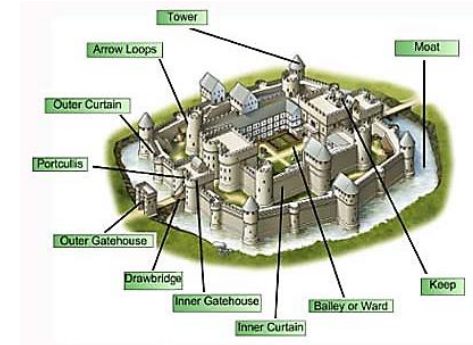
| SECURITY REQUIREMENTS  |       | NIST SP 800-53<br>Relevant Security Controls |          | ISO/IEC 27001<br>Relevant Security Controls      |  |
|--|-------|--|----------|--|--|
| 3.1 ACCESS CONTROL   |       |  |          |  |  |
| Basic Security Requirements  |       |  |          |  |  |
| 3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).<br><br>3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute. | AC-2  | Account Management                           | A.9.2.1  | User registration and de-registration            |  |
|  |       |  | A.9.2.2  | User access provisioning                         |  |
|  |       |  | A.9.2.3  | Management of privileged access rights           |  |
|  |       |  | A.9.2.5  | Review of user access rights                     |  |
|  |       |  | A.9.2.6  | Removal or adjustment of access rights           |  |
|  | AC-3  | Access Enforcement                           | A.6.2.2  | Teleworking                                      |  |
|  |       |  | A.9.1.2  | Access to networks and network services          |  |
|  |       |  | A.9.4.1  | Information access restriction                   |  |
|  |       |  | A.9.4.4  | Use of privileged utility programs               |  |
|  |       |  | A.9.4.5  | Access control to program source code            |  |
|  |       |  | A.13.1.1 | Network controls                                 |  |
|  |       |  | A.14.1.2 | Securing application services on public networks |  |
|  |       |  | A.14.1.3 | Protecting application services transactions     |  |
|  |       |  | A.18.1.3 | Protection of records                            |  |
|  | AC-17 | Remote Access                                | A.6.2.1  | Mobile device policy                             |  |
|  |       |  | A.6.2.2  | Teleworking                                      |  |
|  |       |  | A.13.1.1 | Network controls                                 |  |
|  |       |  | A.13.2.1 | Information transfer policies and procedures     |  |
|  |       |  | A.14.1.2 | Securing application services on public networks |  |



# Containment

(iii) Verify and control/limit connections to, and use of, external information systems.

|        |  |          |  |                           |   |
|--------|--|----------|--|---------------------------|---|
| 3.1.20 | Verify and control/limit connections to and use of external systems. | AC-20    | Use of External Systems                                    | A.11.2.6                  | Security of equipment and assets off-premises |
|        |  |          |  | A.13.1.1                  | Network controls                              |
|        |  |          |  | A.13.2.1                  | Information transfer policies and procedures  |
|        |  | AC-20(1) | Use of External Systems<br><i>Limits on Authorized Use</i> | <i>No direct mapping.</i> |   |



## Prevent Exfiltration

How the data gets out

Could be as simple as apparent web access

Other basic internet services

Definitely SFTP and FTP

Impose policies on use

But what is external?

## Examples of Breaches:

- Use of hacked Samsung TVs
- Target
- Home Depot
- Equifax
- HBO
- Sony

# Stay within the Perimeter



(iv) Control information posted or processed on publicly accessible information systems.

|  |       |                             |                    |
|--|-------|-----------------------------|--------------------|
| 3.1.22 Control CUI posted or processed on publicly accessible systems. | AC-22 | Publicly Accessible Content | No direct mapping. |
|--|-------|-----------------------------|--------------------|

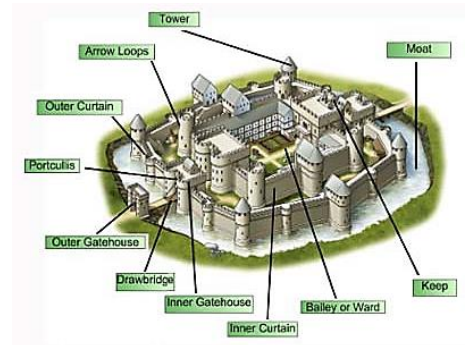
What are “publicly accessible information systems”?

- Your public web server
- Can include any webserver that might be mis-configured to serve data from folders that should be protected
- Can include uploading data to wrong directories

The Cloud (when using public cloud services)

- Amazon S3 Buckets
- Dropbox and similar services
- Gmail and other alternative communications services, e.g. Yahoo

Could also be your employees home machines or laptops



# Attribution and Identification



(v) Identify information system users, processes acting on behalf of users, or devices.

Where:

In log files

In the system itself, for use in access decisions.

Try to avoid group accounts. Group accounts are generally a bad idea, but if present they require careful management.

| SECURITY REQUIREMENTS                        |  | NIST SP 800-53<br>Relevant Security Controls |  | ISO/IEC 27001<br>Relevant Security Controls |  |
|--|--|--|--|---|--|
| <u>3.5 IDENTIFICATION AND AUTHENTICATION</u> |  |  |  |   |  |
| Basic Security Requirements                  |  |  |  |   |  |
| 3.5.1  | Identify system users, processes acting on behalf of users, or devices.  | IA-2   | Identification and Authentication (Organizational Users) | A.9.2.1                                     | User registration and de-registration                    |
| 3.5.2  | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems. | IA-5   | Authenticator Management                                 | A.9.2.1                                     | User registration and de-registration                    |
|  |  |  |  | A.9.2.4                                     | Management of secret authentication information of users |
|  |  |  |  | A.9.3.1                                     | Use of secret authentication information                 |
|  |  |  |  | A.9.4.3                                     | Password management system                               |

# Authentication



(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

| SECURITY REQUIREMENTS                        |  | NIST SP 800-53<br>Relevant Security Controls |  | ISO/IEC 27001<br>Relevant Security Controls |  |
|--|--|--|--|---|--|
| <u>3.5 IDENTIFICATION AND AUTHENTICATION</u> |  |  |  |   |  |
| Basic Security Requirements                  |  |  |  |   |  |
| 3.5.1  | Identify system users, processes acting on behalf of users, or devices.  | IA-2   | Identification and Authentication (Organizational Users) | A.9.2.1                                     | User registration and de-registration                    |
| 3.5.2  | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems. | IA-5   | Authenticator Management                                 | A.9.2.1                                     | User registration and de-registration                    |
|  |  |  |  | A.9.2.4                                     | Management of secret authentication information of users |
|  |  |  |  | A.9.3.1                                     | Use of secret authentication information                 |
|  |  |  |  | A.9.4.3                                     | Password management system                               |

Plus derived controls that tell us how to do this one effectively.

Methods: Strong Passwords (and policies)

Complexity, avoid reuse, sharing, phishing  
Second Factors (cards, biometrics)



# More on Authentication



While not within the 17 initial elements, these provide good advice on how to perform 3.5.2 effectively.

| Derived Security Requirements |   |         |  |                    | SECURITY REQUIREMENTS                 |  | NIST SP 800-53<br>Relevant Security Controls |   | ISO/IEC 27001<br>Relevant Security Controls |                                       |
|-------------------------------|---|---------|--|--------------------|---------------------------------------|--|--|---|---|---------------------------------------|
| 3.5.3                         | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | IA-2(1) | Identification and Authentication (Organizational Users)<br>Network Access to Privileged Accounts                      | No direct mapping. | 3.5.6                                 | Disable identifiers after a defined period of inactivity.  | IA-4   | Identifier Management                                     | A.9.2.1                                     | User registration and de-registration |
|                               |   | IA-2(2) | Identification and Authentication (Organizational Users)<br>Network Access to Non-Privileged Accounts                  | No direct mapping. | 3.5.7                                 | Enforce a minimum password complexity and change of characters when new passwords are created.   | IA-5(1)                                      | Authenticator Management<br>Password-Based Authentication | No direct mapping.                          |                                       |
|                               |   | IA-2(3) | Identification and Authentication (Organizational Users)<br>Local Access to Privileged Accounts                        | No direct mapping. | 3.5.8                                 | Prohibit password reuse for a specified number of generations.                                   |  |   |   |                                       |
| 3.5.4                         | Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.                       | IA-2(8) | Identification and Authentication (Organizational Users)<br>Network Access to Privileged Accounts-Replay Resistant     | No direct mapping. | 3.5.9                                 | Allow temporary password use for system logons with an immediate change to a permanent password. |  |   |   |                                       |
|                               |   | IA-2(9) | Identification and Authentication (Organizational Users)<br>Network Access to Non-Privileged Accounts-Replay Resistant | No direct mapping. | 3.5.10                                | Store and transmit only cryptographically-protected passwords.                                   |  |   |   |                                       |
|                               |   |         |  |                    | 3.5.11                                | Obscure feedback of authentication information.  | IA-6   | Authenticator Feedback                                    | A.9.4.2                                     | Secure logon procedures               |
| 3.5.5                         | Prevent reuse of identifiers for a defined period.  | IA-4    | Identifier Management  | A.9.2.1            | User registration and de-registration |  |  |   |   |                                       |





# Physical, Media, and Communications

|  |                            |         |                                     |
|--|----------------------------|---------|-------------------------------------|
| (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.   | 3.8.3                      | Basic   | Media Protection                    |
| (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.  | 3.10.1                     | Basic   | Physical Protection                 |
| (ix) Escort visitors and monitor visitor activity...<br>...maintain audit logs of physical access, and...<br>...control and manage physical access devices.  | 3.10.3<br>3.10.4<br>3.10.5 | Derived | Physical Protection                 |
| (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | 3.13.1                     | Basic   | System and Communication Protection |
| (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.  | 3.13.5                     | Derived | System and Communication Protection |





# Removing CUI during disposal

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

What is this media:

- CDs or DVD's
- Thumb Drives
- Hard drives inside computers
- Copy machines
- Printers
- Printouts
- Cellphones
- SSD's



| SECURITY REQUIREMENTS       |  | NIST SP 800-53<br>Relevant Security Controls |                    | ISO/IEC 27001<br>Relevant Security Controls |                                    |
|-----------------------------|--|--|--------------------|---|------------------------------------|
| <u>3.8 MEDIA PROTECTION</u> |  |  |                    |   |                                    |
| Basic Security Requirements |  |  |                    |   |                                    |
| 3.8.1                       | Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. | MP-2   | Media Access       | A.8.2.3                                     | Handling of Assets                 |
|                             |  |  |                    | A.8.3.1                                     | Management of removable media      |
|                             |  |  |                    | A.11.2.9                                    | Clear desk and clear screen policy |
| 3.8.2                       | Limit access to CUI on system media to authorized users.   | MP-4   | Media Storage      | A.8.2.3                                     | Handling of Assets                 |
| 3.8.3                       | Sanitize or destroy system media containing CUI before disposal or release for reuse.                      |  |                    | A.8.3.1                                     | Management of removable media      |
|                             |  |  |                    | A.11.2.9                                    | Clear desk and clear screen policy |
|                             |  | MP-6   | Media Sanitization | A.8.2.3                                     | Handling of Assets                 |
| A.8.3.1                     | Management of removable media  |  |                    |   |                                    |
| A.8.3.2                     | Disposal of media  |  |                    |   |                                    |
| A.11.2.7                    | Secure disposal or reuse of equipment  |  |                    |   |                                    |

What about encrypted drives.

e.g. Whole disk encryption

Other forms of encryption

If properly implemented, these ensure the information remains protected even if media are not destroyed. It can also simplify the process of destroying information. But Sanitize anyway.



# Physical Access

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

How easy would it be for someone to plug a USB device into one of your systems.

| SECURITY REQUIREMENTS   |      | NIST SP 800-53<br><i>Relevant Security Controls</i> |                    | ISO/IEC 27001<br><i>Relevant Security Controls</i> |  |
|---|------|---|--------------------|--|--|
| <u>3.10 PHYSICAL PROTECTION</u>   |      |   |                    |  |  |
| Basic Security Requirements   |      |   |                    |  |  |
| 3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. | PE-2 | Physical Access Authorizations                      | A.11.1.2*          | Physical entry controls                            |  |
|   | PE-5 | Access Control for Output Devices                   | A.11.1.2           | Physical entry controls                            |  |
|   |      |   | A.11.1.3           | Securing offices, rooms, and facilities            |  |
| 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.                                 | PE-6 | Monitoring Physical Access                          | No direct mapping. |  |  |

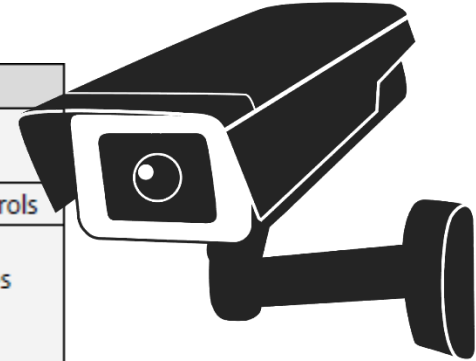
Visibility of input and output devices from beyond the perimeter.

# Building Access



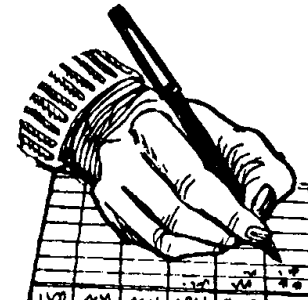
(ix) Escort visitors and monitor visitor activity... maintain audit logs of physical access, and...control and manage physical access devices.

| Derived Security Requirements                        |      |                         |          |   |
|--|------|-------------------------|----------|---|
| 3.10.3 Escort visitors and monitor visitor activity. | PE-3 | Physical Access Control | A.11.1.1 | Physical security perimeter             |
| 3.10.4 Maintain audit logs of physical access.       |      |                         | A.11.1.2 | Physical entry controls                 |
| 3.10.5 Control and manage physical access devices.   |      |                         | A.11.1.3 | Securing offices, rooms, and facilities |



Physical access devices:

- Metal keys (hard to manage 3.10.4)
- Proximity cards (can be copied) – can require passcode too, still not perfect
- Locks – manage centrally based on identity of authorized individuals



| VISITOR      |          |
|--------------|----------|
| Name:        |          |
| Destination: |          |
| Date:        | Time In: |

# Cyber Perimeter Monitoring/Control



(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

- Firewalls
- VLANs
- Network architecture
- VPNs
- Network access controls
- Security for WiFi and physical network ports

| SECURITY REQUIREMENTS  |      | NIST SP 800-53<br><i>Relevant Security Controls</i> |          | ISO/IEC 27001<br><i>Relevant Security Controls</i> |  |
|--|------|---|----------|--|--|
| <u>3.13 SYSTEM AND COMMUNICATIONS PROTECTION</u>   |      |   |          |  |  |
| <i>Basic Security Requirements</i>   |      |   |          |  |  |
| <b>3.13.1</b> Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | SC-7 | Boundary Protection                                 | A.13.1.1 | Network controls                                   |  |
|  |      |   | A.13.1.3 | Segregation in networks                            |  |
|  |      |   | A.13.2.1 | Information transfer policies and procedures       |  |
|  |      |   | A.14.1.3 | Protecting application services transactions       |  |
| 3.13.2 Employ architectural  |      |   |          |  |  |

# Guests and the DMZ



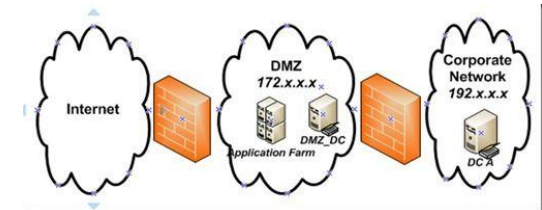
xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Multiple networks  
Not just VLANs

|   |      |                     |          |  |
|---|------|---------------------|----------|--|
| 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. | SC-7 | Boundary Protection | A.13.1.1 | Network controls                             |
|   |      |                     | A.13.1.3 | Segregation in networks                      |
|   |      |                     | A.13.2.1 | Information transfer policies and procedures |
|   |      |                     | A.14.1.3 | Protecting application services transactions |

## Consider 3 or 4

- Operational network for those needing access to CUI
- Operational network for your other employees – protects your other assets
- Optional third network if you need to provide “guest” access to outside.
- Public facing servers can go on 4<sup>th</sup> network in the “DMZ” between public and NON-CUI network



# System Integrity and Subversion



|  |        |         |                                  |
|--|--------|---------|----------------------------------|
| (xii) Identify, report, and correct information and information system flaws in a timely manner.   | 3.14.1 | Basic   | System and Information Integrity |
| (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.                                      | 3.14.3 | Basic   | System and Information Integrity |
| (xiv) Update malicious code protection mechanisms when new releases are available.   | 3.14.2 | Derived | System and Information Integrity |
| (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. | 3.14.5 | Derived | System and Information Integrity |



# Patching and Sharing

(xii) Identify, report, and correct information and information system flaws in a timely manner.



Patches

e.g. **Equifax**

To patch or not to patch:

e.g. **cCleaner, Peyta**

Malware hitched rides on software updates.

**Conclusion – Know your updates.**

- Vulnerability and breach reporting.
  - 72 hours

| SECURITY REQUIREMENTS   |      | NIST SP 800-53<br><i>Relevant Security Controls</i> |          | ISO/IEC 27001<br><i>Relevant Security Controls</i>                |  |
|---|------|---|----------|---|--|
| <u>3.14. SYSTEM AND INFORMATION INTEGRITY</u>   |      |   |          |   |  |
| <i>Basic Security Requirements</i>  |      |   |          |   |  |
| 3.14.1 Identify, report, and correct information and system flaws in a timely manner.                 | SI-2 | Flaw Remediation                                    | A.12.6.1 | Management of technical vulnerabilities                           |  |
| 3.14.2 Provide protection from malicious code at appropriate locations within organizational systems. |      |   | A.14.2.2 | System change control procedures                                  |  |
| 3.14.3 Monitor system security alerts and advisories and take appropriate actions in response.        |      |   | A.14.2.3 | Technical review of applications after operating platform changes |  |
|   |      |   | A.16.1.3 | Reporting information security weaknesses                         |  |
|   | SI-3 | Malicious Code Protection                           | A.12.2.1 | Controls against malware  |  |
|   | SI-5 | Security Alerts, Advisories, and Directives         | A.6.1.4* | Contact with special interest groups                              |  |



# Antivirus and More



(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

Protection =

- Anitvirus
- Anti-malware
- Isolated execution environments
- Least privilege
- Network isolation

| SECURITY REQUIREMENTS   | NIST SP 800-53<br><i>Relevant Security Controls</i> |   | ISO/IEC 27001<br><i>Relevant Security Controls</i> |   |
|---|---|---|--|---|
| <u>3.14 SYSTEM AND INFORMATION INTEGRITY</u>  |   |   |  |   |
| <i>Basic Security Requirements</i>  |   |   |  |   |
| <b>3.14.1</b> Identify, report, and correct information and system flaws in a timely manner.<br><br><b>3.14.2</b> Provide protection from malicious code at appropriate locations within organizational systems.<br><br><b>3.14.3</b> Monitor system security alerts and advisories and take appropriate actions in response. | SI-2  | Flaw Remediation                            | A.12.6.1   | Management of technical vulnerabilities                           |
|   |   |   | A.14.2.2   | System change control procedures                                  |
|   |   |   | A.14.2.3   | Technical review of applications after operating platform changes |
|   |   |   | A.16.1.3   | Reporting information security weaknesses                         |
|   | SI-3  | Malicious Code Protection                   | A.12.2.1   | Controls against malware  |
|   | SI-5  | Security Alerts, Advisories, and Directives | A.6.1.4*   | Contact with special interest groups                              |



# AV and Attack Signatures



(xiv) Update malicious code protection mechanisms when new releases are available.

| Derived Security Requirements   |      |                           |          |                          |
|---|------|---------------------------|----------|--------------------------|
| 3.14.4 Update malicious code protection mechanisms when new releases are available. | SI-3 | Malicious Code Protection | A.12.2.1 | Controls against malware |
| 3.14.5 Perform periodic scans of  |      |                           |          |                          |

- We all know this right?
- What if you are using Kaspersky?
  - Remove it

As with any software – some update types can carry malicious code.

# Apply Live AV and Scanning



xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Scans of system:

- AV
- Tripwire or AFIK
- Check integrity

| Derived Security Requirements  |      |                           |          |                          |
|--|------|---------------------------|----------|--------------------------|
| 3.14.4 Update malicious code protection mechanisms when new releases are available.  | SI-3 | Malicious Code Protection | A.12.2.1 | Controls against malware |
| 3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed. |      |                           |          |                          |

## As files are downloaded, opened, or executed

- Most AV systems will do this
- But, also apply scanning in servers and proxies (email, web proxies, firewalls)



# Intrusion Detection

- Beyond the 17 Initial FAR controls covered this morning, consider network-based intrusion detection tools.

|  |         |   |                    |
|--|---------|---|--------------------|
| 3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | SI-4    | System Monitoring   | No direct mapping. |
|  | SI-4(4) | System Monitoring<br>Inbound and Outbound<br>Communications Traffic | No direct mapping. |
| 3.14.7 Identify unauthorized use of organizational systems.  | SI-4    | System Monitoring   | No direct mapping. |



- Some subversions detectable through command and control detection.
- Consider detection based on your knowledge of partners – what communication is odd (anomalous)

# You must perform a Risk Assessment



- Start with a list of all your assets, especially CDI, FCI, and CUI. Where is it resident on your systems.
  - Who needs access, and who does not.
  - Can you segregate the computers that need access to CUI.
- Assess the controls in place on each of your system components against the 110 controls in NIST 800-171, but especially the 17 controls discussed today.
  - What's missing – i.e. what don't you meet.
  - What do you need to do to meet these requirements
  - Are there interim steps you can take (e.g. segregation – don't process CUI on some systems).
- Complete a System Security Plan
  - This will be covered this afternoon.



# Question on the Initial 17 Requirements





# What about the Cloud

- Many small businesses necessarily use cloud services to support their day to day operations. Can the cloud be used to process CDI and CUI.
  - Some providers may claim compliance to NIST SP 800-171 (or other NIST standards, for PCI standards or HIPAA standards) – what does this mean.
    - Don't believe that by using such "compliant" cloud systems that your handling of CDI is automatically compliant.
    - You must ensure (contractually with the vendor) that the specific systems they are providing meet the flow down requirements. (You may need to pay extra for the segregated and compliant servers).
    - You must also ensure that the communication and local processing of such data by your own systems, and by your applications that run on the cloud services are similarly compliant.
  - See [FEDRAMP](#) for an example of how the government accredits and contracts for such services.

# One example



## AWS GovCloud (US) Region

Designed to address the specific regulatory needs of United States federal, state and local agencies, education institutions and the supporting ecosystem.



AWS GovCloud (US) Region:

Subject to FedRAMP High and Moderate baselines

Allow customers to host sensitive Controlled Unclassified Information (CUI) and all types of regulated workloads

Operated by employees who are U.S. citizens on U.S. soil

Only accessible to vetted U.S. entities and root account holders, who must confirm they are U.S. Persons to gain access

### Requirements for access to AWS GovCloud (US)



US person  
(account holder)



US entity on US soil



Can handle export  
controlled data



# One example

Gives vetted government customers and their partners the **flexibility to architect** secure cloud solutions that comply with:



Federal Risk and Authorization Management Program (FedRAMP) Moderate and \*\*High. [Learn](#)



Federal Information Security Management Act (FISMA) Low, Moderate and \*\*High



Department of Defense Security Requirements Guide (SRG) Impact Levels 2, \*\*4 and \*\*5. [Learn more.](#)



U.S. International Traffic in Arms Regulations (ITAR)



\*\*Department of Commerce Export Administration Regulations (EAR)



\*\*IRS-1075 Encryption Standards for Federal Tax Information (FTI) Section 6103 (p)



\*\*Department of Justice Criminal Justice Information Service Security Policy



\*\*National Institute of Standards and Technology (NIST) SP 800--53 (rev4) and SP 800-171



\*\*Federal Information Processing Standard Publication



\*\*Defense Federal Acquisition Regulation Supplement (DFARS)



Healthcare Insurance Portability & Accountability Act Privacy Standards



Payment Card Industry Security Standards

Other Vendors may provide similar services and it is up to you to validate the accreditation of such services (including this example).



# Shared Responsibility Matrix for Cloud Services



**Cloud Responsibility Matrix**

|  | IaaS                  | PaaS                  | SaaS                  |                       |
|--|-----------------------|-----------------------|-----------------------|-----------------------|
| Security Governance, Risk and Compliance (GRC) | CSC Responsibility    | CSC Responsibility    | CSC Responsibility    | CSC Responsibility    |
| Data Security                                  | CSC Responsibility    | CSC Responsibility    | CSC Responsibility    | CSC Responsibility    |
| Application Security                           | CSC Responsibility    | CSC Responsibility    | Shared Responsibility | Shared Responsibility |
| Platform Security                              | CSC Responsibility    | Shared Responsibility | CSP Responsibility    | CSP Responsibility    |
| Infrastructure Security                        | Shared Responsibility | CSP Responsibility    | CSP Responsibility    | CSP Responsibility    |
| Physical Security                              | CSP Responsibility    | CSP Responsibility    | CSP Responsibility    | CSP Responsibility    |



---

# Lightning Round Discussion of all 110 Controls in NIST SP 800-171

(Assessment and security  
plan covered later)



# NIST SP 800-171 Controls

## What to Expect



- Most Government and Prime Contractor Customers presently require supplier Assertions regarding which of the 110 controls in NIST SP 800-171 are fully **implemented** in your organization.
  - You MUST implement at least the Initial FAR required 17.
  - You must have performed a security assessment.
  - You MUST have a plan of action and milestones for the remaining controls.
- What does fully implemented mean?
  - You have processes in place to ensure that the control is met
    - And that you honestly consider the process that is in place to be sufficient (adequate)
  - It does not mean that the process is fool-proof
- Different ways to meet the control:
  - Configuration, Hardware, Software, or Policy
  - Policy may simply involve not using systems for certain purposes

# It's not as hard as it seems



- Many of the controls remaining from the 110 are refinements to the Initial FAR 17
  - Dictating specific approaches for certain environments
  - Specifying configuration options, etc.



|                     | AC       | AT    | AU    | CM    | IA      | IR    | MA    | MP      | PS    | PE       | RA     | CA       | SC       | SI       |
|---------------------|----------|-------|-------|-------|---------|-------|-------|---------|-------|----------|--------|----------|----------|----------|
| Basic<br>(FIPS 200) | 3.1.1 +  | 3.2.1 | 3.3.1 | 3.4.1 | 3.5.1 + | 3.6.1 | 3.7.1 | 3.8.1   | 3.9.1 | 3.10.1 + | 3.11.1 | 3.12.1   | 3.13.1 + | 3.14.1 + |
|                     | 3.1.2 +  | 3.2.2 | 3.3.2 | 3.4.2 | 3.5.2 + | 3.6.2 | 3.7.2 | 3.8.2   | 3.9.2 | 3.10.2   | 3.11.2 | 3.12.2   | 3.13.2   | 3.14.2 + |
|                     |          |       |       |       |         |       |       | 3.8.3 + |       |          | 3.11.3 | 3.12.3   |          | 3.14.3   |
|                     |          |       |       |       |         |       |       |         |       |          |        | (3.12.4) |          |          |
| Derived<br>(800-53) | 3.1.3    | 3.2.3 | 3.3.3 | 3.4.3 | 3.5.3   | 3.6.3 | 3.7.3 | 3.8.4   |       | 3.10.3 + |        |          | 3.13.3   | 3.14.4 + |
|                     | 3.1.4    |       | 3.3.4 | 3.4.4 | 3.5.4   |       | 3.7.4 | 3.8.5   |       | 3.10.4 + |        |          | 3.13.4   | 3.14.5 + |
|                     | 3.1.5    |       | 3.3.5 | 3.4.5 | 3.5.5   |       | 3.7.5 | 3.8.6   |       | 3.10.5 + |        |          | 3.13.5 + | 3.14.6   |
|                     | 3.1.6    |       | 3.3.6 | 3.4.6 | 3.5.6   |       | 3.7.6 | 3.8.7   |       | 3.10.6   |        |          | 3.13.6   | 3.14.7   |
|                     | 3.1.7    |       | 3.3.7 | 3.4.7 | 3.5.7   |       |       | 3.8.8   |       |          |        |          | 3.13.7   |          |
|                     | 3.1.8    |       | 3.3.8 | 3.4.8 | 3.5.8   |       |       | 3.8.9   |       |          |        |          | 3.13.8   |          |
|                     | 3.1.9    |       | 3.3.9 | 3.4.9 | 3.5.9   |       |       |         |       |          |        |          | 3.13.9   |          |
|                     | 3.1.10   |       |       |       | 3.5.10  |       |       |         |       |          |        |          | 3.13.10  |          |
|                     | 3.1.11   |       |       |       | 3.5.11  |       |       |         |       |          |        |          | 3.13.11  |          |
|                     | 3.1.12   |       |       |       |         |       |       |         |       |          |        |          | 3.13.12  |          |
|                     | 3.1.13   |       |       |       |         |       |       |         |       |          |        |          | 3.13.13  |          |
|                     | 3.1.14   |       |       |       |         |       |       |         |       |          |        |          | 3.13.14  |          |
|                     | 3.1.15   |       |       |       |         |       |       |         |       |          |        |          | 3.13.15  |          |
|                     | 3.1.16   |       |       |       |         |       |       |         |       |          |        |          | 3.13.16  |          |
|                     | 3.1.17   |       |       |       |         |       |       |         |       |          |        |          |          |          |
|                     | 3.1.18   |       |       |       |         |       |       |         |       |          |        |          |          |          |
|                     | 3.1.19   |       |       |       |         |       |       |         |       |          |        |          |          |          |
|                     | 3.1.20 + |       |       |       |         |       |       |         |       |          |        |          |          |          |
|                     | 3.1.21   |       |       |       |         |       |       |         |       |          |        |          |          |          |
|                     | 3.1.22 + |       |       |       |         |       |       |         |       |          |        |          |          |          |

+ FAR Clause 52.204-21 maps to these NIST SP 800-171 requirements

|  |                |  |                                       |
|--|----------------|--|---------------------------------------|
|  | Policy/Process |  | Policy or Software Requirement        |
|  | Configuration  |  | Configuration or Software             |
|  | Software       |  | Configuration or Software or Hardware |
|  | Hardware       |  | Software or Hardware                  |

Source: DoD 23 Jun 17 Industry Information Day slide deck

AIA members noted hardest and costliest

# Set 3.1 - Access Control (1 of 4)



Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 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.
- 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 nonsecurity functions.

LEAST PRIVILEGE

# Set 3.1 - Access Control (2 of 4)



Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

Access control and  
privilege policy

Notice of policy

Autologout / lock

- 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.
- 3.1.9. Provide privacy and security notices consistent with applicable CUI rules.
- 3.1.10. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.
- 3.1.11. Terminate (automatically) a user session after a defined condition.



## Set 3.1 - Access Control (3 of 4)

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.1.12. Monitor and control remote access sessions.
- 3.1.13. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- 3.1.14. Route remote access via managed access control points.
- 3.1.15. Authorize remote execution of privileged commands and remote access to security- relevant information.
- 3.1.16. Authorize wireless access prior to allowing such connections.
- 3.1.17. Protect wireless access using authentication and encryption.
- 3.1.18. Control connection of mobile devices.
- 3.1.19. Encrypt CUI on mobile devices and mobile computing platforms.



## Set 3.1 - Access Control (4 of 4)



Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.1.20. Verify and control/limit connections to and use of external systems.
- 3.1.21. Limit use of organizational portable storage devices on external systems.
- 3.1.22. Control CUI posted or processed on publicly accessible systems.

Manage remote access

Manage data on remote/mobile devices

Controls on portable storage

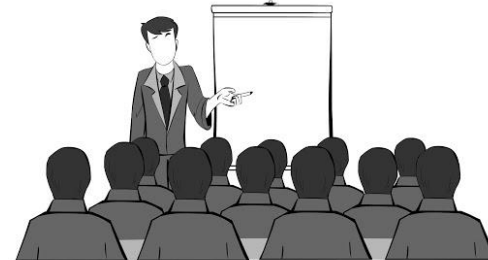
Control of information on publicly accessible servers.

## Set 3.2 Awareness and Training



Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.2.1. Ensure that managers, systems administrators, and users of organizational 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 systems.
- 3.2.2. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- 3.2.3. Provide security awareness training on recognizing and reporting potential indicators of insider threat.



# Set 3.3 Audit and Accountability



Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.3.1. Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.
- 3.3.2. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
  - 3.3.3. Review and update audited events.
  - 3.3.4. Alert in the event of an audit process failure.
  - 3.3.5. Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
  - 3.3.6. Provide audit reduction and report generation to support on-demand analysis and reporting.



Manage system logs

Protecting them

Monitoring them

What they contain

Alert on log failure

Automated tools

Common time base

Who managed logs

## Set 3.3 Audit and Accountability



Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.3.7. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
- 3.3.8. Protect audit information and audit tools from unauthorized access, modification, and deletion.
- 3.3.9. Limit management of audit functionality to a subset of privileged users.

Manage system logs

Protecting them

Monitoring them

What they contain

Alert on log failure

Automated tools

Common time base

Who managed logs

## Set 3.4 Configuration Management (1 of 2)



Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.4.1. Establish and maintain baseline configurations and inventories of organizational 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 systems.
- 3.4.3. Track, review, approve/disapprove, and audit changes to organizational 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 organizational system.
- 3.4.6. Employ the principle of least functionality by configuring organizational system to provide only essential capabilities.



## Set 3.4 Configuration Management (2 of 2)



Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.4.7. Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.
- 3.4.8. Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- 3.4.9. Control and monitor user-installed software.

Manage the software, hardware and configurations of the systems running on your network.

# Set 3.5 Identification and Authentication



- 3.5.1. Identify system users, processes acting on behalf of users, or devices.
- 3.5.2. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.
- 3.5.3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- 3.5.4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
- 3.5.5. Prevent reuse of identifiers for a defined period.
- 3.5.6. Disable identifiers after a defined period of inactivity.
- 3.5.7. Enforce a minimum password complexity and change of characters when new passwords are created.



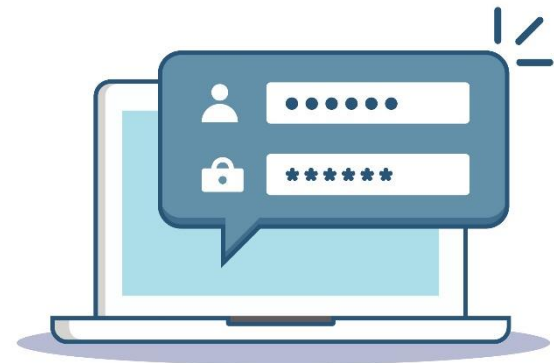
# Set 3.5 Identification and Authentication (2 of 2)



Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.5.8. Prohibit password reuse for a specified number of generations.
- 3.5.9. Allow temporary password use for system logons with an immediate change to a permanent password.
- 3.5.10. Store and transmit only cryptographically-protected passwords.
- 3.5.11. Obscure feedback of authentication information.

Multi-factor authentication  
Password Policies  
How passwords entered  
Resistance to various attacks





## Set 3.6 Incident Response



Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.6.1. Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
- 3.6.2. Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.
- 3.6.3. Test the organizational incident response capability.



3.6.1 (and 3.6.3) is a 3 hour lecture in and of itself.

3.6.2 follows from the plan.

This will be good for your organization in general, independent of the CUI requirements.

But it will be time and labor intensive.



## Set 3.7 Maintenance

Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.7.1. Perform maintenance on organizational systems.
- 3.7.2. Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
- 3.7.3. Ensure equipment removed for off-site maintenance is sanitized of any CUI.
- 3.7.4. Check media containing diagnostic and test programs for malicious code before the media are used in organizational system.
- 3.7.5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
- 3.7.6. Supervise the maintenance activities of maintenance personnel without required access authorization.



Remove disks before sending equipment back for repair.

Easier said than done.

Equipment maintenance personnel need to be supervised.

Remote desktop for maintenance is problematic.

## Set 3.8 Media Protection



Which of the following NIST SP 800-171 controls are fully implemented in your organization?

Manage, Label, Control access to, and Encrypt media and destroy in appropriate manner.

- 3.8.1. Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
- 3.8.2. Limit access to CUI on system media to authorized users.
- 3.8.3. Sanitize or destroy system media containing CUI before disposal or release for reuse.
- 3.8.4. Mark media with necessary CUI markings and distribution limitations
- 3.8.5. Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
- 3.8.6. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

## Set 3.8 Media Protection (2 of 2)



Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.8.7. Control the use of removable media on system components.
- 3.8.8. Prohibit the use of portable storage devices when such devices have no identifiable owner.
- 3.8.9. Protect the confidentiality of backup CUI at storage locations

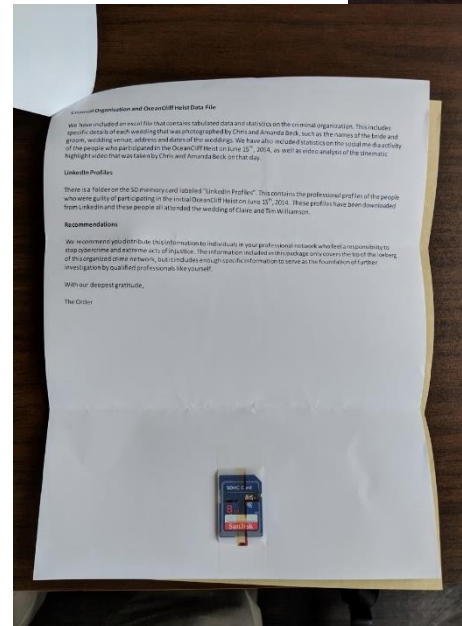
Manage, Label, Control access to, and Encrypt media and destroy in appropriate manner.



# Set 3.8 Media Protection EXAMPLE



- 3.8.7. Control the use of removable media on system components.
- 3.8.8. Prohibit the use of portable storage devices when such devices have no identifiable owner.



## Set 3.9 Personnel Security



Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.9.1. Screen individuals prior to authorizing access to organizational systems containing CUI.
- 3.9.2. Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.



## Set 3.10 Physical Protection



Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.10.1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
- 3.10.2. Protect and monitor the physical facility and support infrastructure for organizational systems
- 3.10.3. Escort visitors and monitor visitor activity.
- 3.10.4. Maintain audit logs of physical access.
- 3.10.5. Control and manage physical access devices.
- 3.10.6. Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).

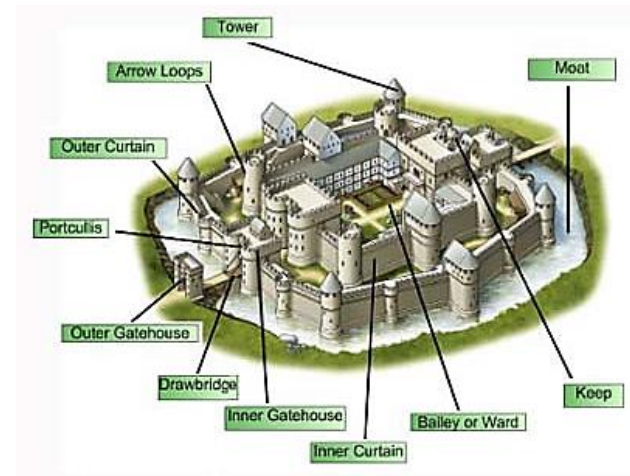




# Set 3.13 System and Comm Protection

Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.13.1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
- 3.13.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
- 3.13.3. Separate user functionality from system management functionality.
- 3.13.4. Prevent unauthorized and unintended information transfer via shared system resources.
- 3.13.5. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.





## Set 3.13 System and Comm Protection (2 of 3)



Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.13.6. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
- 3.13.7. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks.
- 3.13.8. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
- 3.13.9. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
- 3.13.10. Establish and manage cryptographic keys for cryptography employed in organizational systems.

## Set 3.13 System and Comm Protection (3 of 3)



Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.13.11. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. (for now this means AES and appropriate PK systems)
- 3.13.12. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
- 3.13.13. Control and monitor the use of mobile code.
- 3.13.14. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies
- 3.13.15. Protect the authenticity of communications sessions
- 3.13.16. Protect the confidentiality of CUI at rest.

# Set 3.14 System & Information Integrity



Which of the following NIST SP 800-171 controls are fully implemented in your organization?

- 3.14.1. Identify, report, and correct information and system flaws in a timely manner.
- 3.14.2. Provide protection from malicious code at appropriate locations within organizational systems.
- 3.14.3. Monitor system security alerts and advisories and take appropriate actions in response.
- 3.14.4. Update malicious code protection mechanisms when new releases are available.
- 3.14.5. Perform periodic scans of organizational system and real-time scans of files from external sources as files are downloaded, opened, or executed.
- 3.14.6. Monitor organizational system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
- 3.14.7. Identify unauthorized use of organizational system

# Risk Assessment and Security Plan

---

- Start with a list of all your assets, especially CDI, FCI, and CUI. Where is it resident on your systems.
  - Who needs access, and who does not.
  - Can you segregate parts of the system needing CUI.
- Assess the controls in place on each of your system components against the 110 controls in NIST SP 800-171.
  - What's missing – i.e. what don't you meet.
  - What do you need to do to meet these requirements
  - Are there interim steps you can take (e.g. segregation – don't process CUI on some systems).
- Complete a System Security Plan
  - This will be a focus later in today's lecture

# Set 3.11 Risk Assessment

---



- 3.11.1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.

## ***DEFINE YOUR PERIMETER***

- 3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.
- 3.11.3 Remediate vulnerabilities in accordance with assessments of risk.



# Risk Management

---

The goal of security in all organization is to manage risk.  
The first step in managing risk is your risk assessment  
(3.11.1)

Once risks are assessed, characterized, and quantified, your organization takes steps to mitigate those risks, balancing the cost of the mitigation against the potential loss resulting from the risk.

In the case of CDI, the requirements are that you apply adequate (e.g. industry best practices as identified in NIST SP 800-171) to mitigate all identified risks to CDI from your risk assessment.

# Set 3.12 Security Assessment



- 3.12.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
- 3.12.2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
- 3.12.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- 3.12.4. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

## 3.12.4 System Security Plan



NIST has released a template which you can use as the basis for writing your system security plan.

See:

<https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-1/final/documents/CUI-SSP-Template-final.docx>



## 3.12.2 Plan of Action and Milestones

NIST has release a template (blank table) for your plan of actions and milestones:

<https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-1/final/documents/CUI-Plan-of-Action-Template-final.docx>

Most Federal sites have Cyber Security Resources and some additional materials are noted below and in the References section at the end of this training. The documents below are Plans of Actions and Milestones from some other problem domains, and they may be useful to you as examples. They are not intended to be copied for use as your own plan.

[FedRAMP Plan of Action and Milestones \(POA&M\) Template](#)  
[Centers for Medicare & Medicaid Services - Plan of Action and Milestones Process Guide](#)



# A Case Study

- <https://money.cnn.com/2018/08/06/technology/tsmc-chip-supplier-virus/index.html>

Taiwan-based chip manufacturer TSMC warned that the infection, which was eventually contained, will delay shipments of its products and could wipe as much as \$171 million off its revenue. The virus hit the company's computer network late Friday and spread to machines used to make chips and processors, TSMC (TSM) said in a press conference on Monday. TSMC said the virus caused equipment to crash or repeatedly reboot and was a variant of WannaCry, which targeted more than 300,000 computers in 150 countries last year. TSMC blamed the infection of its computer systems on "misoperation during the software installation process" for new equipment.

The equipment in question was "not first isolated and confirmed to be virus-free," the company said, allowing the virus to enter as soon as the equipment was connected to the company network. The virus was stored in the equipment and didn't come from a hack or cyberattack, a spokeswoman for TSMC said. The company added that its primary computer systems that store production and customer data were not affected, and no confidential information was compromised.

TSMC, short for Taiwan Semiconductor Manufacturing Company, is the main manufacturer of processors for Apple's (AAPL) iPhones and iPads. It's also the world's largest maker of made-to-order chips, which involves manufacturing products designed by companies like Qualcomm (QCOM) and Nvidia (NVDA). TSMC spent the weekend scrambling to get its operations back to normal. Most of the affected systems were up and running again by Sunday afternoon, and the company said they were fully recovered Monday. It plans to give customers details in the coming days on when they can expect to receive the delayed shipments. TSMC said Monday that the disruption is expected to knock 2% off its third-quarter revenue, which it had previously forecast would be in the range of \$8.45 billion and \$8.55 billion.