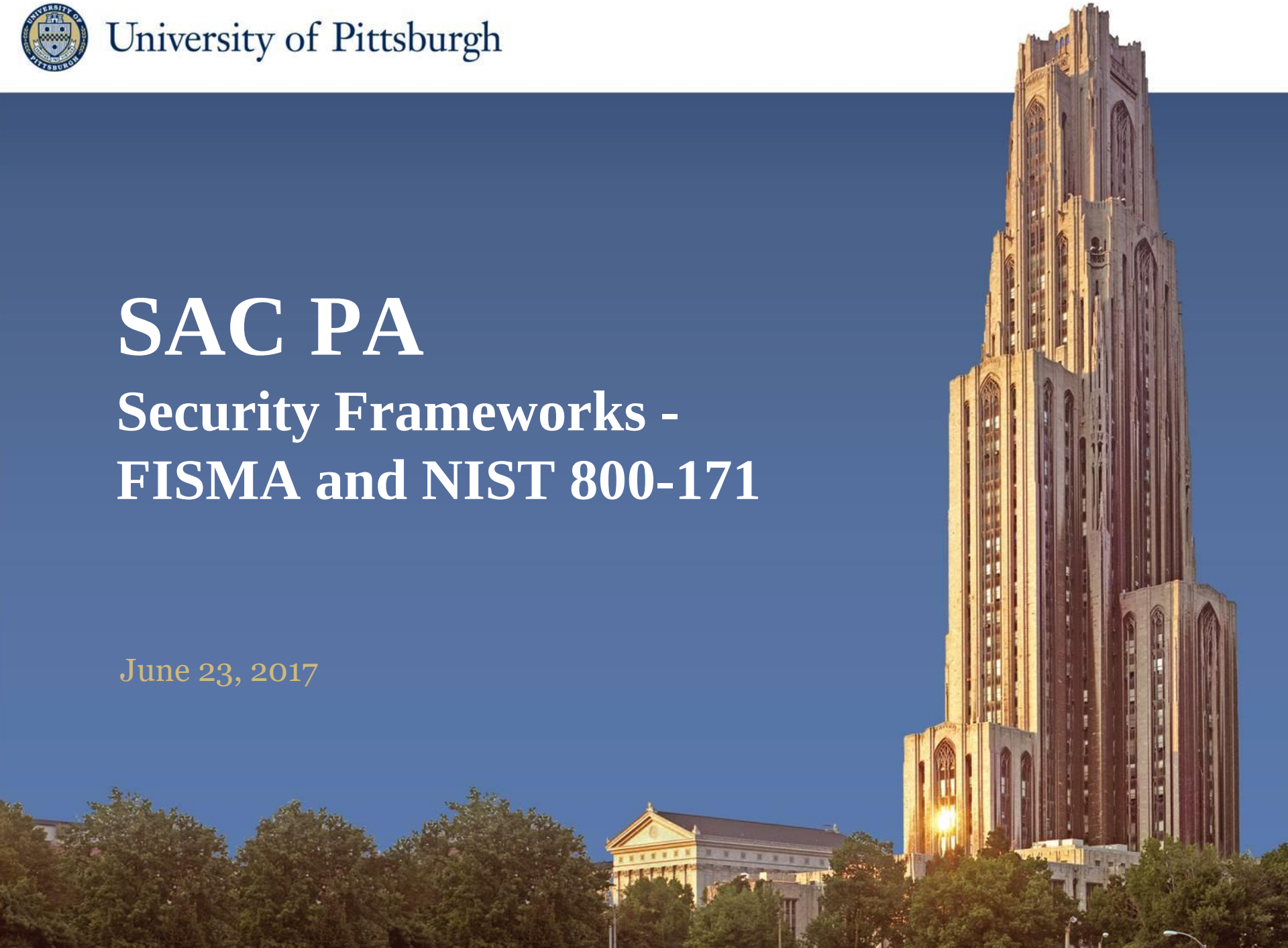
University of Pittsburgh

SAC PA

Security Frameworks - FISMA and NIST 800-171

June 23, 2017



SECURITY FRAMEWORKS

Chris Seiders, CISSP

Scott Weinman, CISSP, CISA

Agenda

- Compliance standards
  - FISMA
  - NIST SP 800-171
- Importance of Compliance
- High-level Controls and Mapping
- Implementation Guidance

Compliance Standards

History of FISMA

Federal Information Security Management Act of 2002 (FISMA)

- **Background:** Federal government recognized the importance of information security to the economic and national security interests of the United States and enacted into law under section 44 U.S.C. § 3541 of the E-Government Act of 2002. *(Amended by Federal Information Security Modernization Act of 2014.)*
- **Purpose:** Provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

History of FISMA

Federal Information Security Management Act of 2002 (FISMA)

- **Key Requirements:** National Institute of Standards and Technology **(NIST)** is required to develop a set of information security standards, guidelines, and techniques to reduce the information security risks to an acceptable level
    - In response, NIST developed the following:
        - **Federal Information Processing Standards Publication (FIPS) 200** – Minimum Security Requirements for Federal Information and Information Systems
        - **NIST Special Publication 800-53** – Security and Privacy Controls for Federal Information Systems and Organizations

History of FISMA

- Federal Information Security Management Act of 2002 (FISMA)
  - **Scope:** FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

History of NIST 800-171

National Institute of Standards and Technology (NIST) 800-171

- **Background:** In November 2010, to address an increasing federal government need to protect sensitive, unclassified government information held within the government and with contractors, **Executive Order 13556** was established to standardize the way the Executive Branch handles unclassified information that requires protection, such as personally identifiable information.
  - The National Archives and Records Administration (NARA) was charged with implementing the order.
  - NARA worked with NIST to draft guidelines for protecting controlled, unclassified information (CUI) on information systems outside the immediate control of the federal government based on **FIPS 200** and **NIST 800-53**.

History of NIST 800-171

National Institute of Standards and Technology (NIST) 800-171

- **Key Requirements for protecting CUI:**
  - Consistent statutory and regulatory requirements for federal and nonfederal systems
  - Consistent safeguards implemented in federal and nonfederal systems
  - Confidentiality impact is no lower than moderate in accordance with FIPS 199
- **Scope:**
  - Applies to Controlled Unclassified Information (CUI) shared by the federal government with nonfederal entities such as universities, federal contractors, and state governments.
  - Federal government shares data with institutions for research purposes and for carrying out work on behalf of federal agencies.
  - If no other federal laws or regulations apply to controlling the data (e.g. FISMA), NIST 800-171 applies and addresses how the data must be handled.

Importance of Compliance

- Federal contracts may **require** compliance with FISMA or NIST 800-171
  - Review the contract language to determine if the IT environments must be FISMA or NIST 800-171 compliant
    - Examples include:
      - FISMA may be identified as **NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations** or **NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems**
      - DFARS reference 252.204-7012 -Safeguarding Covered Defense Information and Cyber Incident Reporting
      - Contract terms state NIST 800-171 must be followed
      - Data is specifically identified as Controlled Unclassified Information (CUI)

Importance of Compliance

Example of Federal DOD contract

- PART 4.0 - GOVERNMENT PROVISIONS - NONCOMMERCIAL
- The following clauses set forth in the Federal Acquisition Regulation (FAR) and agency acquisition regulations, as amended and modified below, are applicable as indicated, to this Subcontract. Without limiting the Subcontract provisions, the FAR clauses are incorporated by reference into this Subcontract with the same force and effect as though set forth in full text. The dates of the FAR clauses incorporated by reference are the same as the corresponding clause in the Prime Contract or higher-tier subcontract, unless otherwise provided by law. The following definitions shall apply to this Subcontract Part 4.0 except as otherwise specifically provided.

Importance of Compliance

Example of Federal DOD contract

DFARS Reference	*Title of Clause*
252.203-7000	Requirements Relating to Compensation of Former DoD Officials
252.203-7001	Prohibition on Persons Convicted of Fraud or Other Defense Contract-Related Felonies (If Order exceeds simplified acquisition threshold)
252.203-7002	Requirement to Inform Employees of Whistleblower Rights
252.203-7004	Display of Fraud Hotline Posters (if Subcontract exceeds $5.5 million)
252.204-7009	Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting
252.204-7014	Limitations on the Use or Disclosure of Information by Litigation Support Contractors

Importance of Compliance

252.204-7012	**Safeguarding Covered Defense Information and Cyber Incident Reporting**

- 252.204–7012 Safeguarding of unclassified controlled technical information. As prescribed in 204.7303, use the following clause: SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (NOV 2013)
- Section (b) *Adequate security item 2 subsection (i):*
- (i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

Importance of Compliance

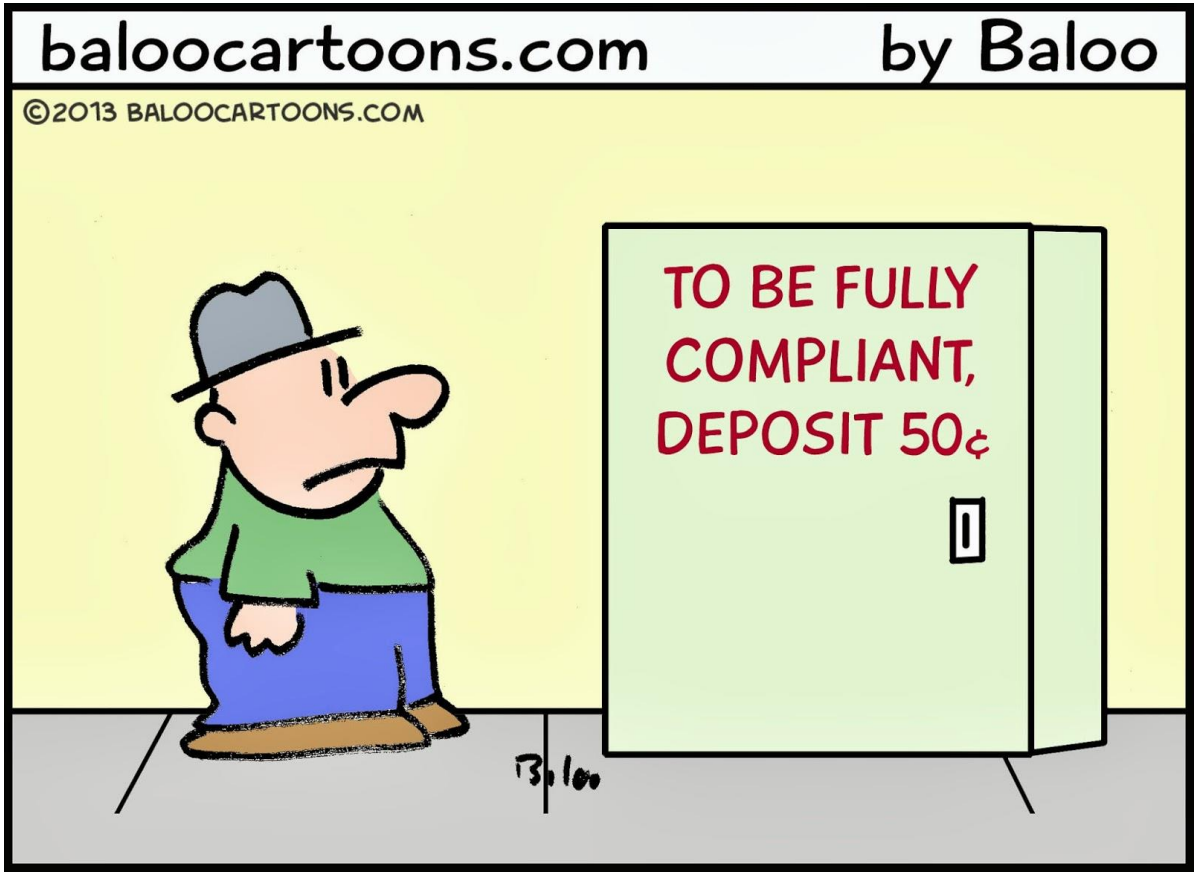
Controlled Unclassified Information (CUI)

- Any federal information that is not in the classified category
  - 22 approved CUI categories with 85 Subcategories

CUI Categories	
1. Agriculture	12. Law Enforcement
2. Copyright	13. Legal
3. Critical Infrastructure	14. NATO
4. Emergency Management	15. Nuclear
5. Export Control	16. Patent
6. Financial	17. Privacy
7. Foreign Government	18. Proprietary
8. Geodetic Product Information	19. Safety Act Information
9. Immigration	20. Statistical
10. Information Systems Vulnerability Information	21.Tax
11. Intelligence	22. Transportation

Subcategory Examples
Bank Secrecy
DNA
Investigation
Financial
Health Information
Personnel
Census
Investment Survey

High-level Controls and Mapping



High-level Controls and Mapping

NIST 800-53 High-level Controls

#	ID	Family	High- Level Controls	Initial Control Baselines		
				Low	Med	High
1	AC	Access Control	23	11	17	18
2	AT	Awareness and Training	4	4	4	4
3	QU	Audit and Accountability	16	10	11	12
4	CA	Security Assessment and Authorization	8	7	7	8
5	CM	Configuration Management	11	8	11	11
6	CP	Contingency Planning	12	6	9	9
7	IA	Identification and Authorization	11	7	8	8
8	IR	Incident Response	10	7	8	8
9	MA	Maintenance	6	4	6	6
10	MP	Media Protection	8	4	7	7
11	PE	Physical and Environment Protection	19	10	16	17
12	PL	Planning	6	3	4	4
13	PS	Personnel Security	8	8	8	8
14	RA	Risk Assessment	5	4	4	4
15	SA	System and Services Acquistion	20	6	9	13
16	SC	System and Communications Protection	41	10	19	21
17	SI	System and Information Integrity	16	6	11	12
18	PM	Program Management	16	16	16	16

- 18 Control Families with 240 high-level controls
- 3 levels of Initial Control Baselines (Low, Medium, High)
- Baseline level selected based on business's
  - Priorities
  - Information system functions
  - Information system environments

High-level Controls and Mapping

NIST 800-53 – Access Control

		Initial Control Baselines		
#	Control	Low	Med	High
AC-1	Access Control Policy and Procedures	AC - 1	AC - 1	AC - 1
AC-2	Account Management	AC - 2	AC - 2 (1) (2) (3) (4)	AC - 2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	AC - 3	AC - 3	AC - 3
AC-4	Information Flow Enforcement	NA	AC - 4	AC - 4
AC-5	Separation of Duties	NA	AC - 5	AC - 5
AC-6	Least Privelege	NA	AC - 6 (1) (2) (5) (9) (10)	AC - 6 (1) (2) (3) (5) (9) (10)
AC-7	Unsucessful Logon Attempts	AC - 7	AC - 7	AC - 7
AC-8	System Use Notification	AC - 8	AC - 8	AC - 8
AC-9	Previous Logon (Access) Notification	NA	NA	NA
AC-10	Concurrent Session Control	NA	NA	AC - 10
AC-11	Session Lock	NA	AC - 11 (1)	AC - 11 (1)
AC-12	Session Termination	NA	AC - 12	AC - 12
AC-13	**Withdrawn**	**NA**	**NA**	**NA**
AC-14	Permitted Actions without Identification or Authentication	AC - 14	AC - 14	AC - 14
AC-15	**Withdrawn**	**NA**	**NA**	**NA**
AC-16	Security Attributes	NA	NA	NA
AC-17	Remote Access	AC - 17	AC - 17 (1) (2) (3) (4)	AC - 17 (1) (2) (3) (4)
AC-18	Wireless Access	AC - 18	AC - 18 (1)	AC - 18 (1) (4) (5)
AC-19	Access Controls for Mobile Devices	AC - 19	AC - 19 (5)	AC - 19 (5)
AC-20	Use of External Information Systems	AC - 20	AC - 20 (1) (2)	AC - 20 (1) (2)
AC-21	Information Sharing	NA	AC - 21	AC - 21
AC-22	Publicly Accessible Content	AC - 22	AC - 22	AC - 22
AC-23	Data Mining Protection	NA	NA	NA
AC-24	Access Control Decisions	NA	NA	NA
AC-25	Reference Monitor	NA	NA	NA

- Controls may have control enhancements which may vary by level
- Control enhancements are indicated by AC-X(#)

High-level Controls and Mapping

NIST 800.53 – Access Control – AC 1

Access Control Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [Assignment: organization-defined frequency]; and
2. Access control procedures [Assignment: organization-defined frequency].

High-level Controls and Mapping

NIST 800-171 – High-level Controls

		Security Requirements	
#	CUI Security Requirements	Basic	Derived
3.1	Access Control	2	20
3.2	Awareness and Training	2	1
3.3	Audit and Accountability	2	7
3.4	Configuration Management	2	7
3.5	Identification and Authentication	2	9
3.6	Incident Response	2	1
3.7	Maintenance	2	4
3.8	Media Protection	3	6
3.9	Personnel Security	2	0
3.10	Physical Protection	2	4
3.11	Risk Assessment	1	2
3.12	Security Assessment	3	0
3.13	System and Communication Protection	2	14
3.14	System and Information Integrity	3	4

- 14 Security Requirement Families
- 109 Security Requirements
- Two types of Requirements
  - Basic
    - Based on FIPS – 200
    - High-level security requirement
    - What needs done
  - Derived
    - Based on NIST 800-53
    - Supplement the Basic requirements
    - How it can be done

High-level Controls and Mapping

NIST 800-171 – Access Control and 800-53 Mapping

800-171 Access Control		NIST 800-53 Control (s)
	Basic Security Requirements	
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)	AC - 2, AC - 3, AC - 17
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	AC - 2, AC - 3, AC - 17
	Derived Security Requirements	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	AC - 4
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC - 5
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC - 6, AC - 6(1), AC - 6(5)
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions	AC - 6(2)
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	AC - 6(9)
3.1.8	Limit unsuccessful logon attempts.	AC - 7
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	AC - 8
3.1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	AC - 11, AC - 11(1)
3.1.11	Terminate (automatically) a user session after a defined condition	AC - 12
3.1.12	Monitor and control remote access sessions	AC - 17(1)
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC - 17(2)
3.1.14	Route remote access via managed access control points.	Ac - 17(3)
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	AC - 17(4)
3.1.16	Authorize wireless access prior to allowing such connections.	AC - 18
3.1.17	Protect wireless access using authentication and encryption.	AC - 18(1)
3.1.18	Control connection of mobile devices.	AC - 19
3.1.19	Encrypt CUI on mobile devices.	AC - 19(5)
3.1.20	Verify and control/limit connections to and use of external information systems	AC - 20, AC - 20(1)
3.1.21	Limit use of organizational portable storage devices on external information systems.	AC - 20(2)
3.1.22	Control information posted or processed on publicly accessible information systems.	AC - 22

While the 800-171 requirements are high-level, the mapped 800-53 controls provide guidance for implementing the controls.

Implementation Guidance

Implementation Guidance

- Obtain Executive buy-in and an Executive sponsor
- Assign dedicated resources
- Determine the scope (entire environment, specific systems)
- Determine costs/budget
- Identify key owners/contacts
  - Infrastructure (networking, server teams, provisioning, security)
  - Human Resources
  - Internal Audit
  - Office of Research/Researchers

Implementation Guidance

- Perform a gap analysis
- Develop remediation plans with target completion dates
- Develop or update policies, standards, guidelines, and procedures
- Institute a continuous monitoring program along with a risk assessment process
- Communicate risks to Executives on a regular basis
- Develop relationships with researchers, so they will communicate project changes which may require IT control changes

References

- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- http://csrc.nist.gov/groups/SMA/forum/documents/feb2014/pviscuso_cui-briefing.pdf
- http://csrc.nist.gov/groups/SMA/fisma/faqs.html
- http://csrc.nist.gov/groups/SMA/forum/documents/aug-2016/tues400_sp800-171_dempsey.pdf
- http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
- https://library.educause.edu/~/media/files/library/2016/4/nist800.pdf
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

Thank You