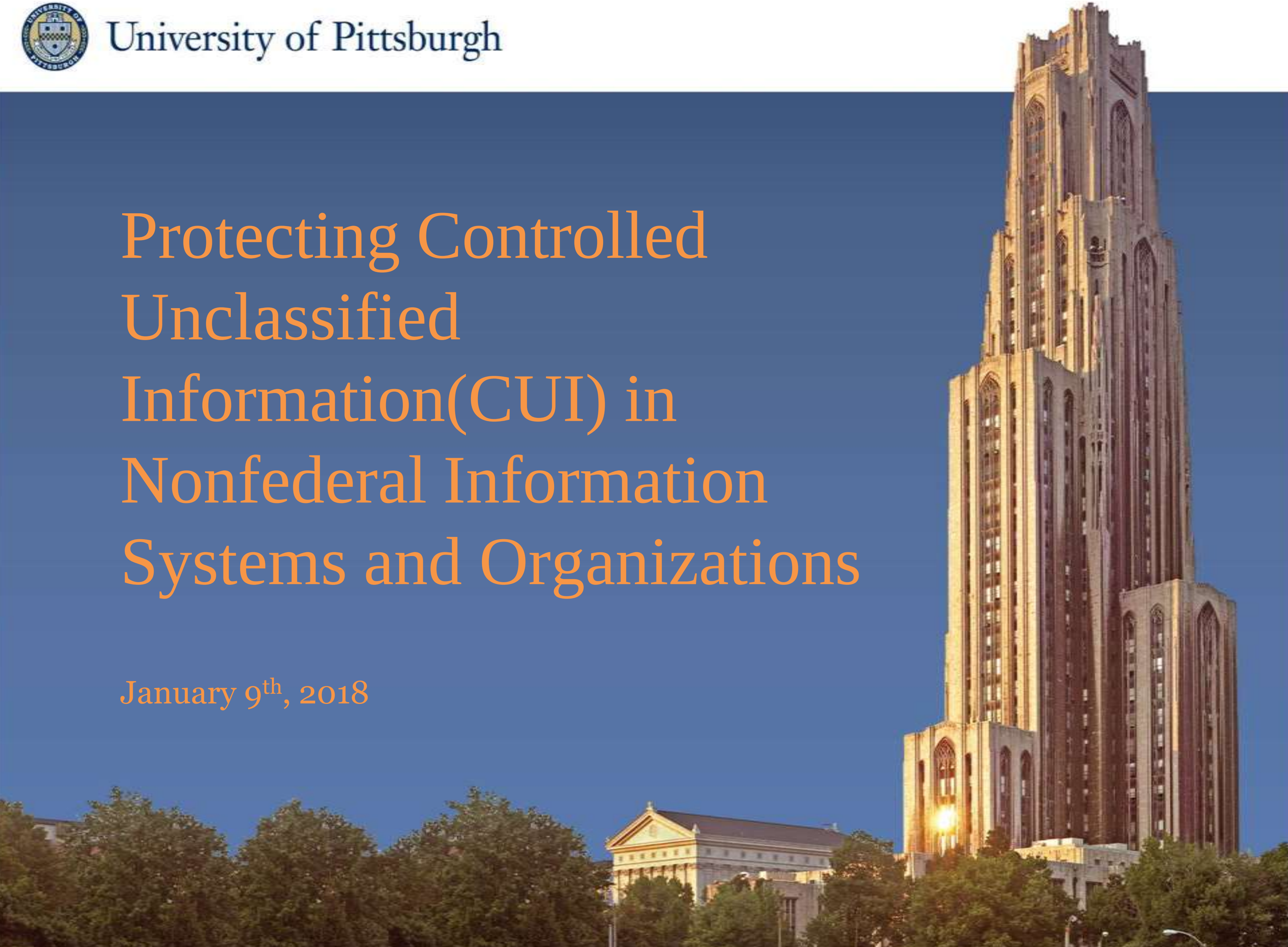
University of Pittsburgh

Protecting Controlled Unclassified Information(CUI) in Nonfederal Information Systems and Organizations

January 9th, 2018



SPEAKER

Chris Seiders, CISSP

Security Analyst

Computing Services and Systems Development (CSSD)

Disclaimer

The views presented are those of the speaker and do not necessarily represent the views of the University of Pittsburgh or its faculty or staff.

The University of Pittsburgh

- 5 Campuses
- 36,028 Students
- 12,646 Faculty and Staff
- Ranked 9th nationally in federal science and engineering funding according to NSF
- Ranked 5th of U.S. universities in terms of grants awarded by NIH

Agenda

- Why Security Frameworks
- Compliance Drivers in Academia and Research
- A Tail of Three Frameworks
- FISMA
- Cyber Security Framework
- NIST 800-171
- Implementation Guidelines

Why Security Frameworks

- Foundation of information security program
- When you want to grow from ‘best practices’
- Method to audit and review existing program
- Guide strategic planning (especially CSF)
- Compliance requirements

Compliance Drivers

"Now, now, now, there's no reason to be intimidated by compliance."

#RegTech
@trulioo

Compliance Drivers

- 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)

Compliance Drivers

baloocartoons.com
by Baloo
©2013 BALOOCARTOONS.COM
Baloo
"...And they're giving us sixty million years to get in compliance."

Compliance Drivers

- As of December 2015, DFARS 225.204-7012 requires contractors to implement NIST Special Publication (SP) 800-171 standards "as soon as practical, but not later than December 31, 2017."

Compliance Drivers

- Department of Education dropping not-so-subtle hints it may be coming…

- "The Department strongly encourages institutions to review and understand the standards defined in the NIST SP 800-171, the recognized information security publication for protecting "Controlled Unclassified Information (CUI)," a subset of Federal data that includes unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Federal policies."
- "Thus, we **strongly encourage** those institutions that fall short of NIST standards to assess their current gaps **and immediately begin to design and implement** plans in order to close those gaps using the NIST standards as a model."

Dear Colleague Letter

July 1, 2016

DCL ID: GEN-16-12

Compliance Drivers

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

A Tail of Three Frameworks

2013 FISMA Model

- Anticipated that more federal research contracts and grants would mandate following FISMA standards
- Built FISMA infrastructure model to host Federal Information Systems
- If you build it, they may not come

A Tail of Three Frameworks

2015 Cyber Security Framework

- Desire to utilize a standards based approach across the entire University
- Used for both central IT as well as individual colleges and departments
- Gap analysis used for strategic and tactical planning
- Piloted with School of Engineering
- 800-171 was becoming more prevalent

A Tail of Three Frameworks

2017 NIST 800-171

- DOD DFAR Requirements
- Department of Education ‘hints’
- A Better Framework (???)

History of NIST Frameworks

"Federal Bureau of Technological Compliance — May I help you?"

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)

- 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.
- NIST 800-53 is 487 pages long and references numerous other 800-series and FIPS standards

FISMA Controls

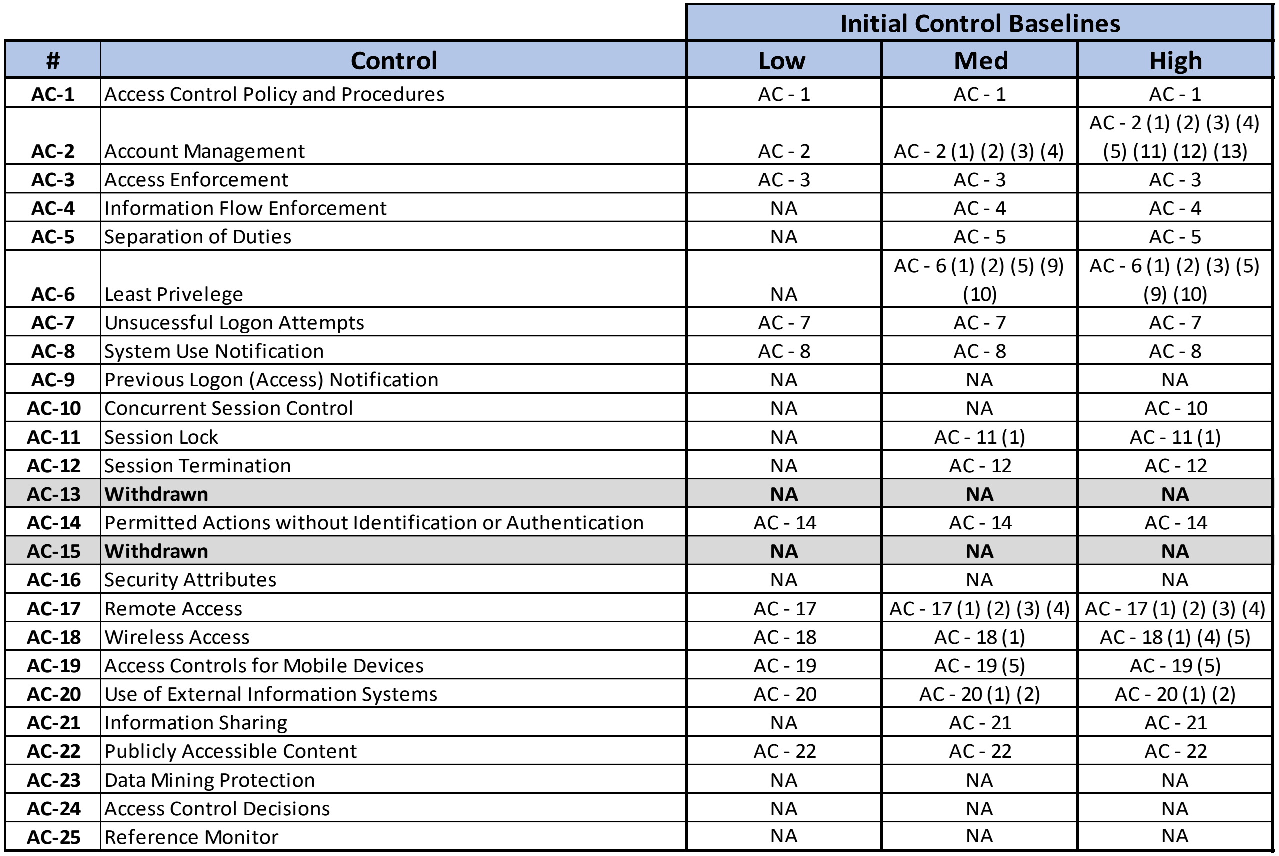
NIST 800-53 High-level Controls

			High- Level	Initial Control Baselines		
#	**ID**	**Family**	**Controls**	**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
  - C-I-A Triad

High-level Controls

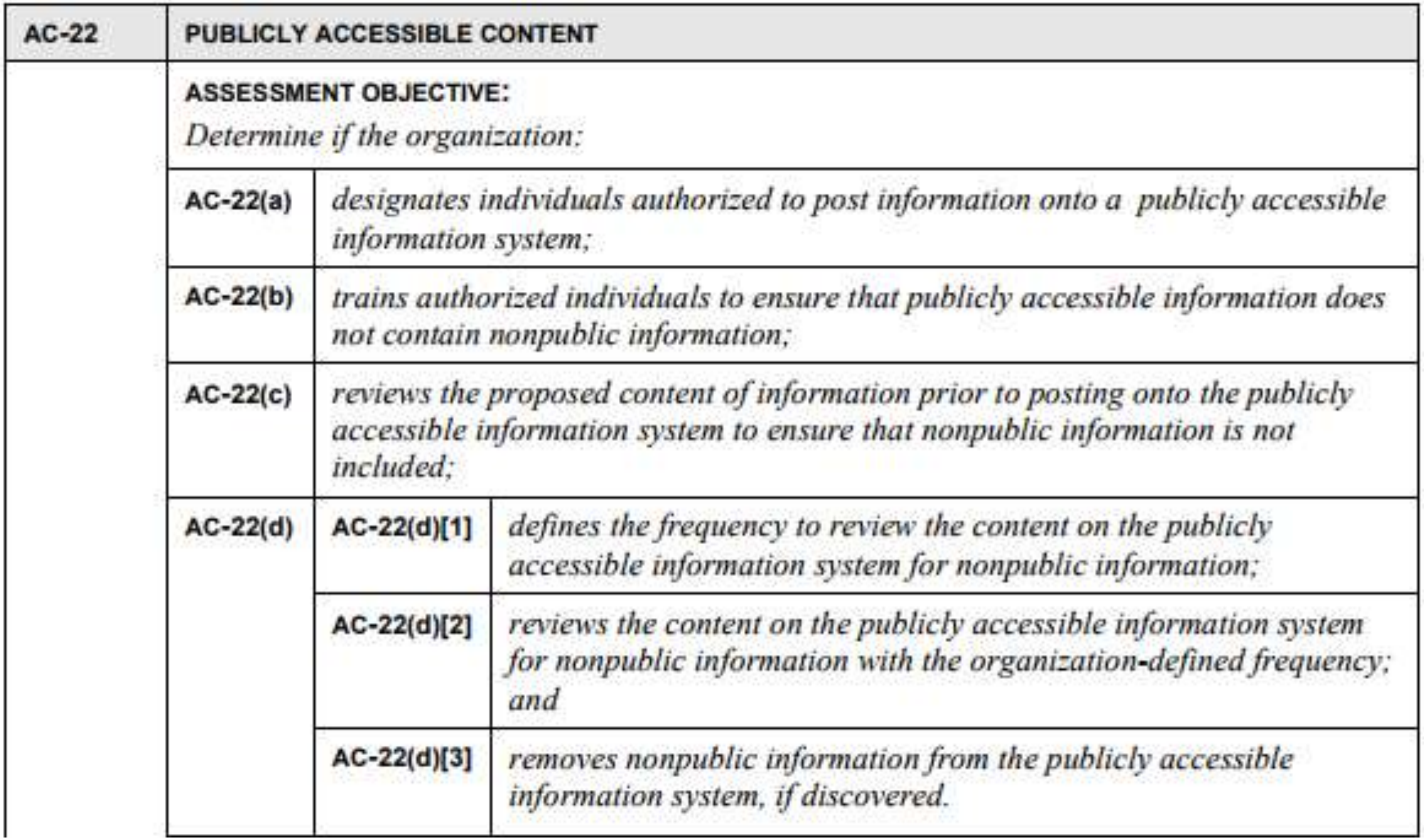
NIST 800-53 – Access Control



		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(#)

FISMA Sample Control



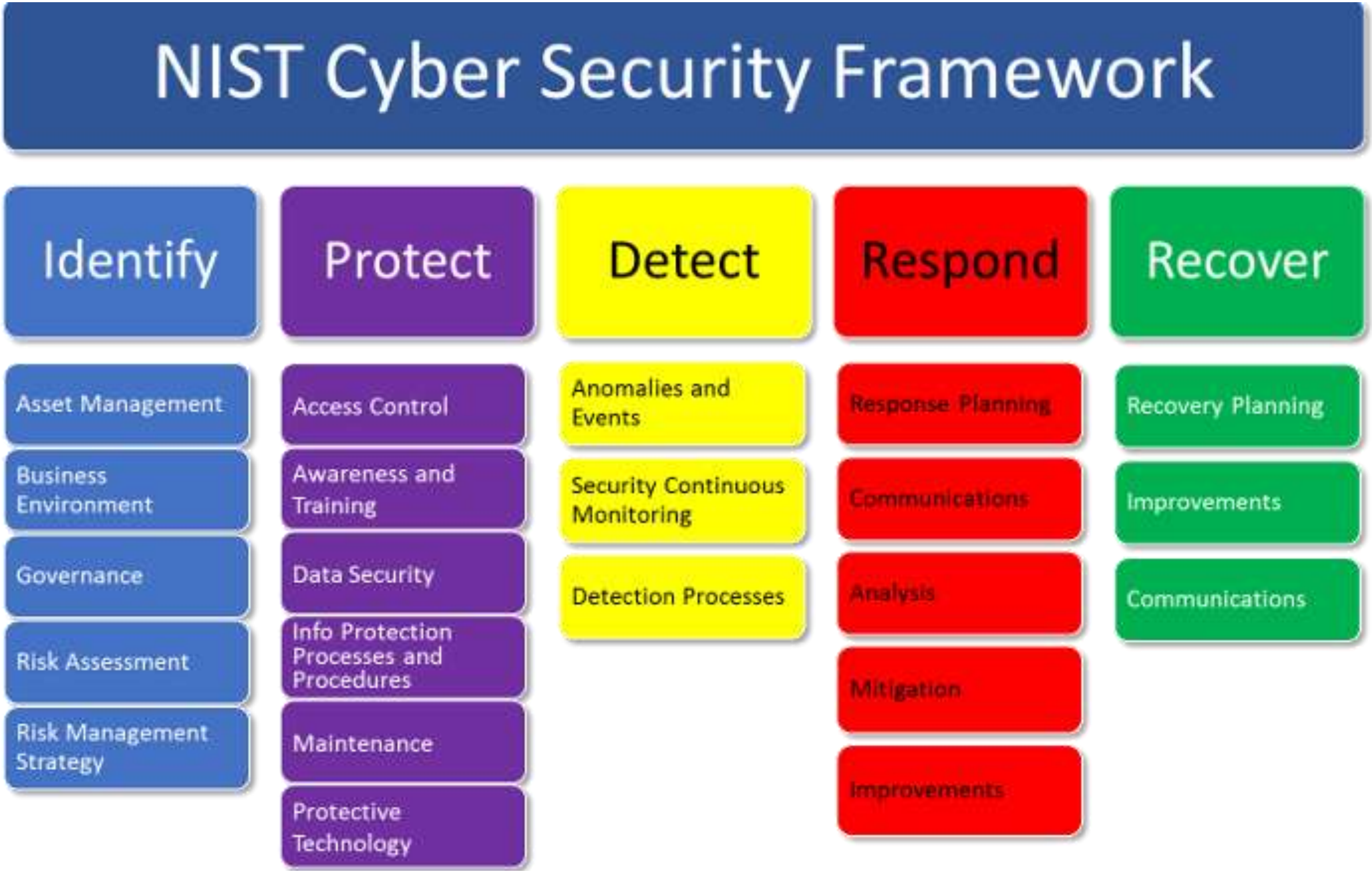
AC-22	PUBLICLY ACCESSIBLE CONTENT		
	ASSESSMENT OBJECTIVE: *Determine if the organization:*		
	AC-22(a)	*designates individuals authorized to post information onto a publicly accessible information system;*	
	AC-22(b)	*trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;*	
	AC-22(c)	*reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included;*	
	AC-22(d)	AC-22(d)[1]	*defines the frequency to review the content on the publicly accessible information system for nonpublic information;*
		AC-22(d)[2]	*reviews the content on the publicly accessible information system for nonpublic information with the organization-defined frequency; and*
		AC-22(d)[3]	*removes nonpublic information from the publicly accessible information system, if discovered.*

History of Cyber Security Framework

- February 2014 based on the previous year's Executive Order 13636.
- Risk-based approach to managing cybersecurity
- Foundation for a new cybersecurity program or a mechanism for improving an existing program.

History of Cyber Security Framework

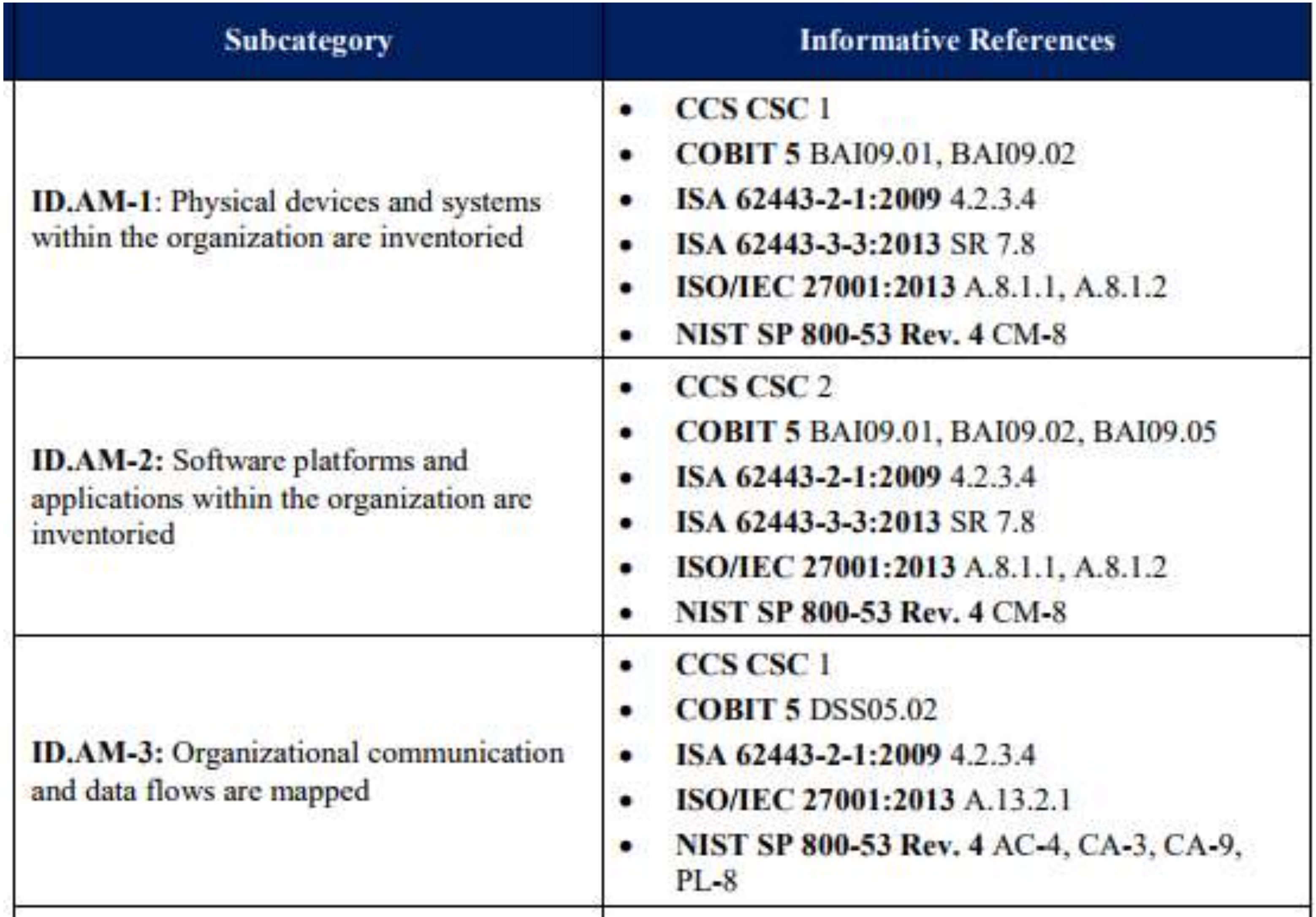
- December 2015 Request for Information
- Cybersecurity Framework Workshop 2016 held at the NIST campus in Gaithersburg, Maryland.
- 2017 draft *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*
- Incorporates feedback since the release of framework version 1.0, 2015 RFI, and NIST Workshop



NIST Cyber Security Framework

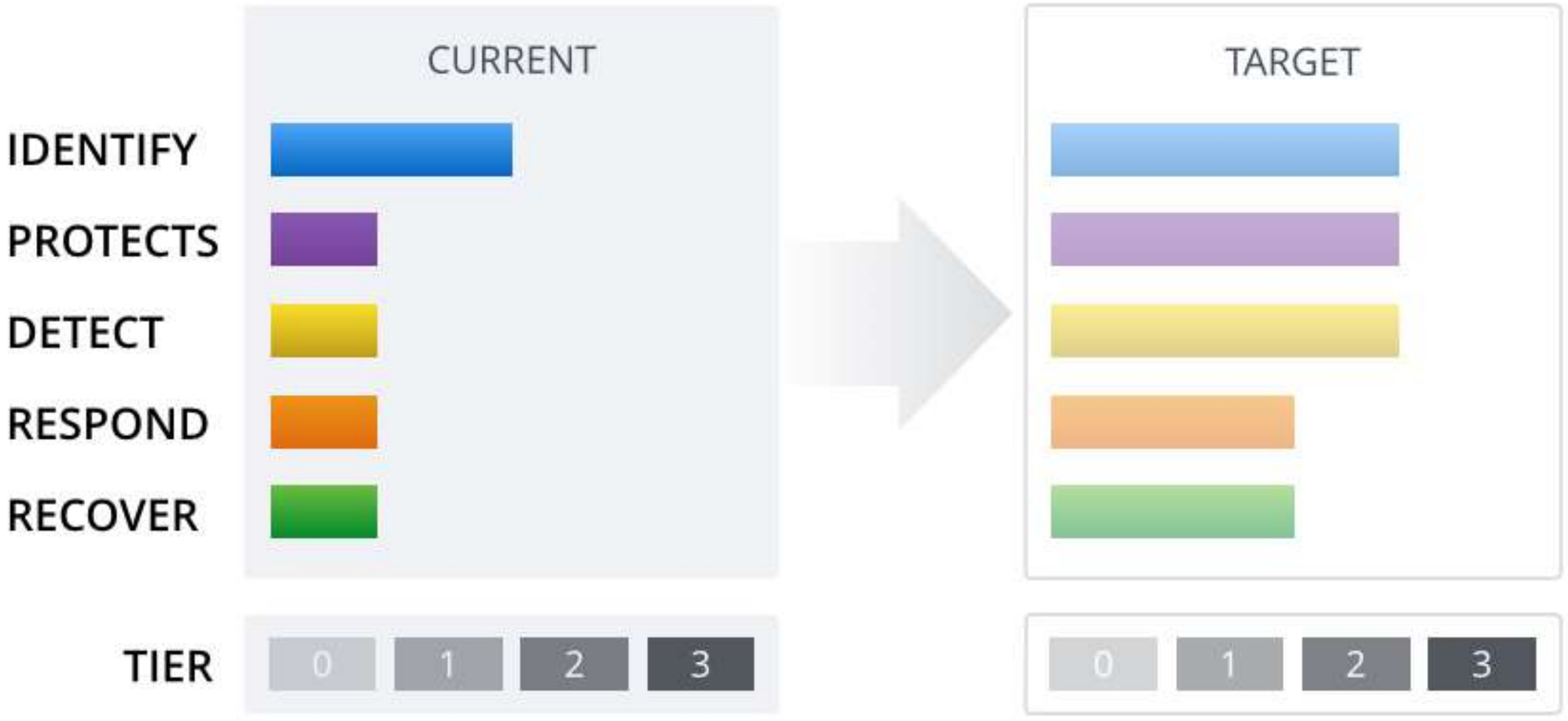
Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

NIST CSF Sample controls



Subcategory	Informative References
ID.AM-1: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8

Cyber Security Framework Profiles



History of 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**.

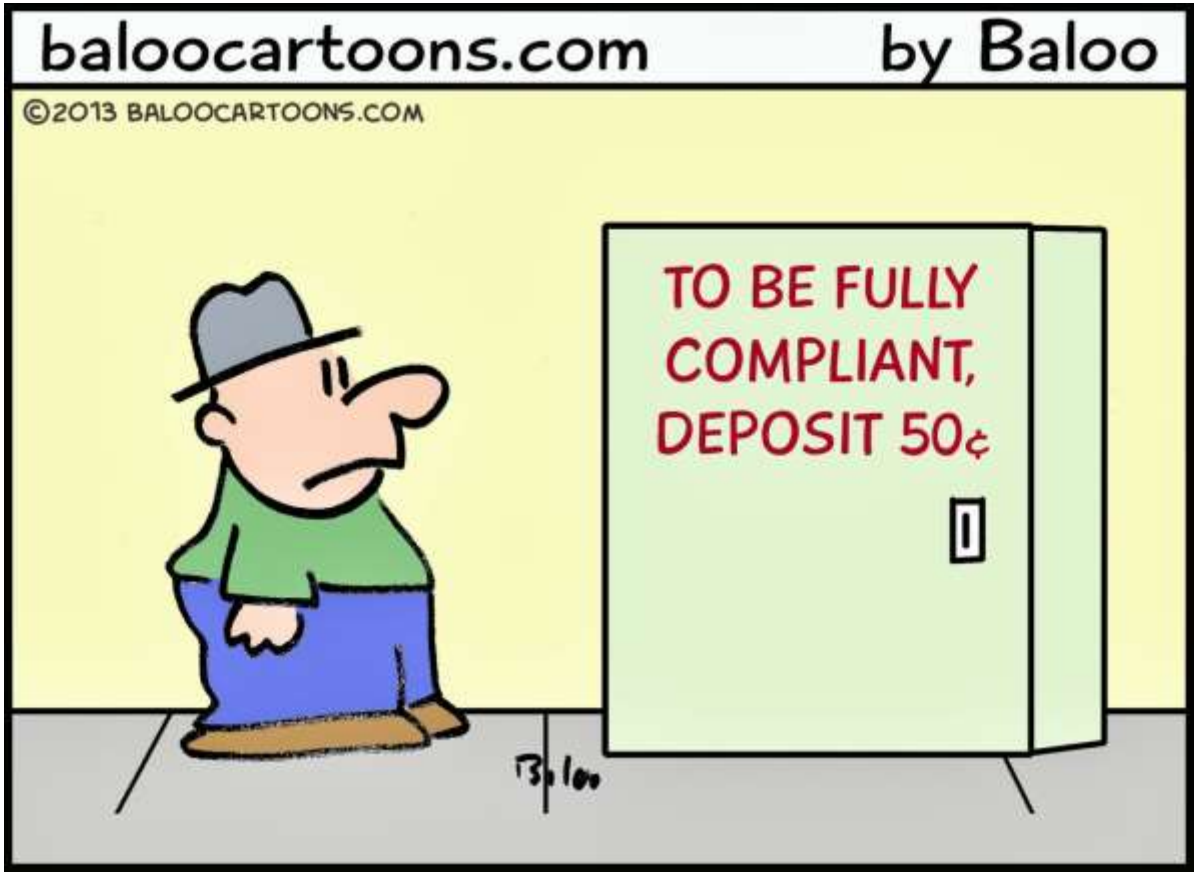
NIST 800-171 is FISMA-lite

History of NIST 800-171

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

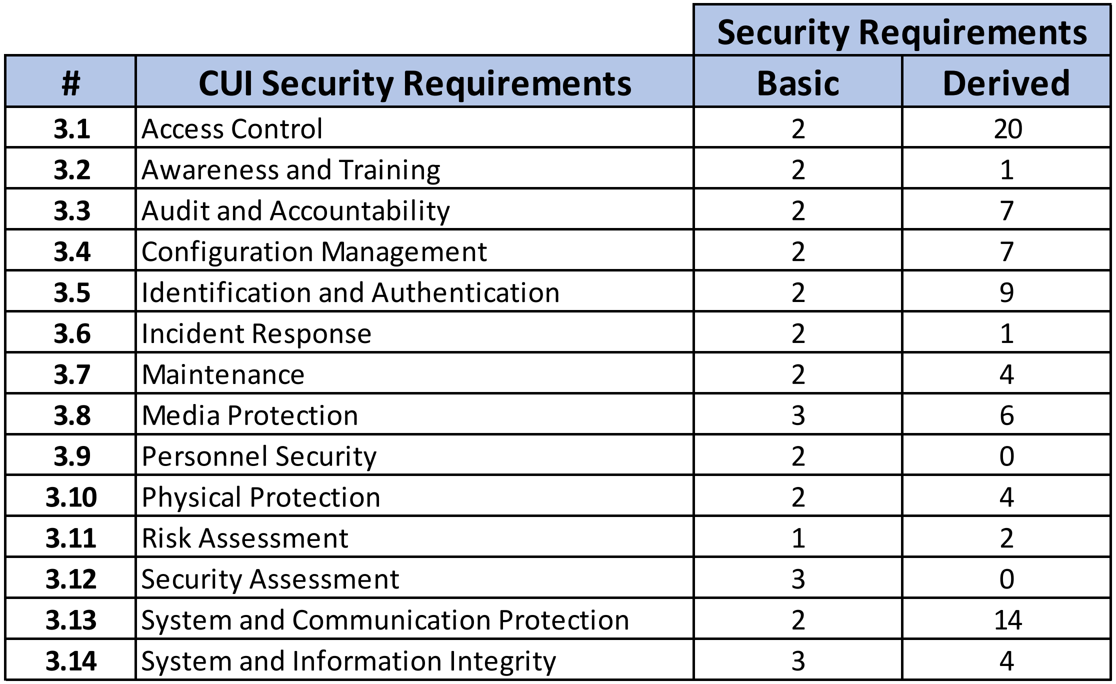
- **Key Requirements for protecting CUI:**
  - Consistent statutory and regulatory requirements for federal and nonfederal systems
  - Consistent safeguards implemented in federal and nonfederal systems
  - Confidentiality impact is no lower than moderate in accordance with FIPS 199
- **Scope:**
  - 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.

High-level Controls



High-level Controls

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
- 110 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

NIST 800-171 Control Descriptions

- Limit information system access to authorized users (Access Control Requirements);
- Ensure that system users are properly trained (Awareness and Training Requirements);
- Create information system audit records (Audit and Accountability Requirements);
- Establish baseline configurations and inventories of systems (Configuration Management Requirements);
- Identify and authenticate users appropriately (Identification and Authentication Requirements);
- Establish incident-handling capability (Incident Response Requirements);
- Perform appropriate maintenance on information systems (Maintenance Requirements);
- Protect media, both paper and digital, containing sensitive information (Media Protection Requirements);
- Screen individuals prior to authorizing access (Personnel Security Requirements);
- Limit physical access to systems (Physical Protection Requirements);
- Conduct risk assessments (Risk Assessment Requirements);
- Assess security controls periodically and implement action plans (Security Assessment Requirements);
- Monitor, control, and protect organizational communications (System and Communications Protection Requirements); and
- Identify, report, and correct information flaws in a timely manner (System and Information Integrity Requirement).

NIST 800-171 Control Example

3.1 ACCESS CONTROL	Basic Security Requirements	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
3.1 ACCESS CONTROL	Basic Security Requirements	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
3.2 AWARENESS AND TRAINING	Basic Security Requirements	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.
3.2 AWARENESS AND TRAINING	Basic Security Requirements	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

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.

Frameworks compared

	Control families	Sub-groups	Controls
FISMA	18	3	240
NIST CSF	5	23	109
NIST 800-171	14	2	110

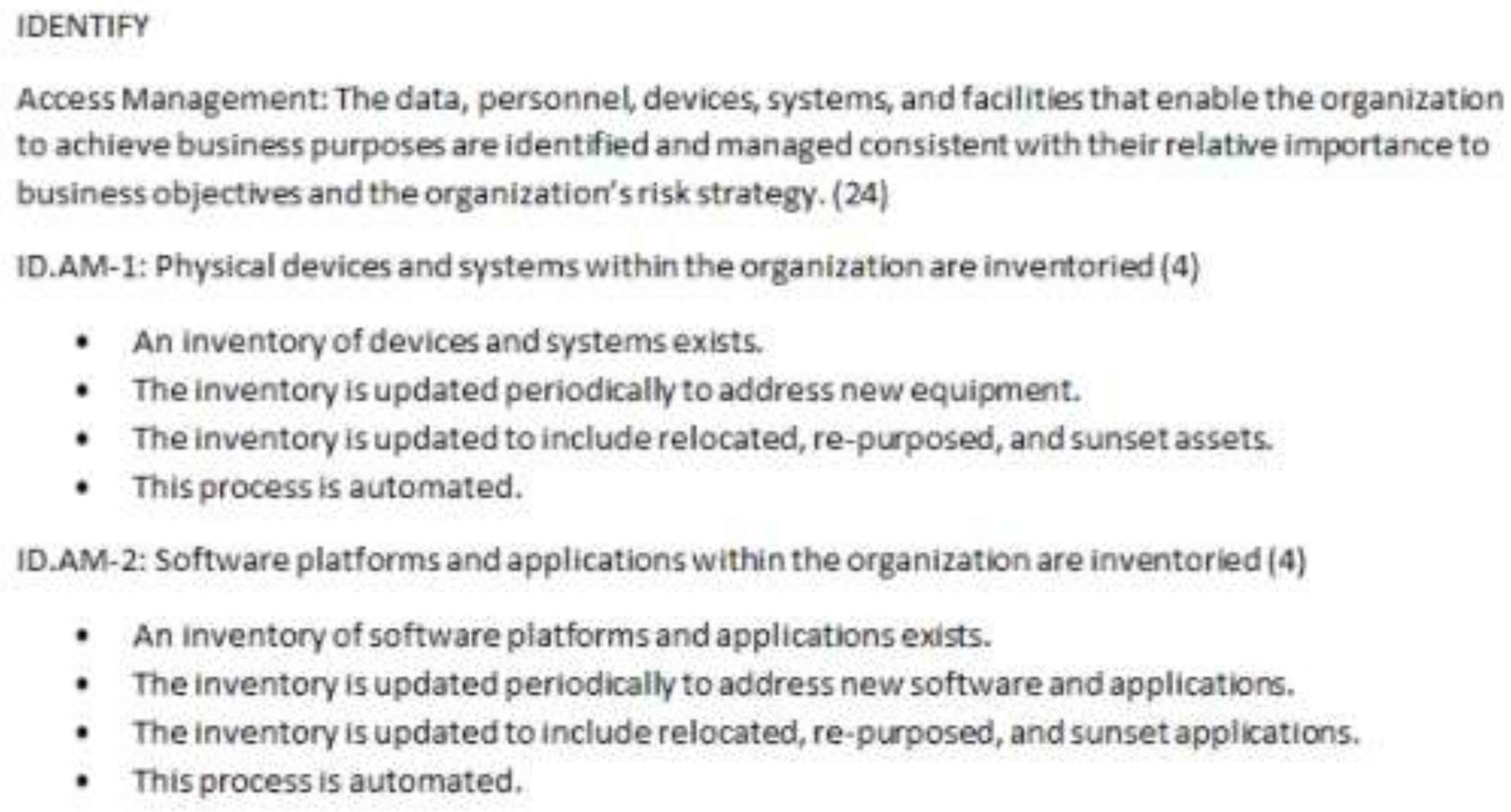
Implementation Guidance
Our approach

- FISMA
- Build an isolated environment dedicated for FISMA projects
- Charge-back model due to costs and administrative overhead
- Successful, but few projects implemented

Our approach

- NIST Cyber Security Framework
- Self-service questionnaire
- Multiple choice of various maturity levels of each control
- Current and Target profiles
- Didn’t roll out, but still might have value

CSF Self-service example questions



IDENTIFY

Access Management: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. (24)

ID.AM-1: Physical devices and systems within the organization are inventoried (4)

- An inventory of devices and systems exists.
- The inventory is updated periodically to address new equipment.
- The inventory is updated to include relocated, re-purposed, and sunset assets.
- This process is automated.

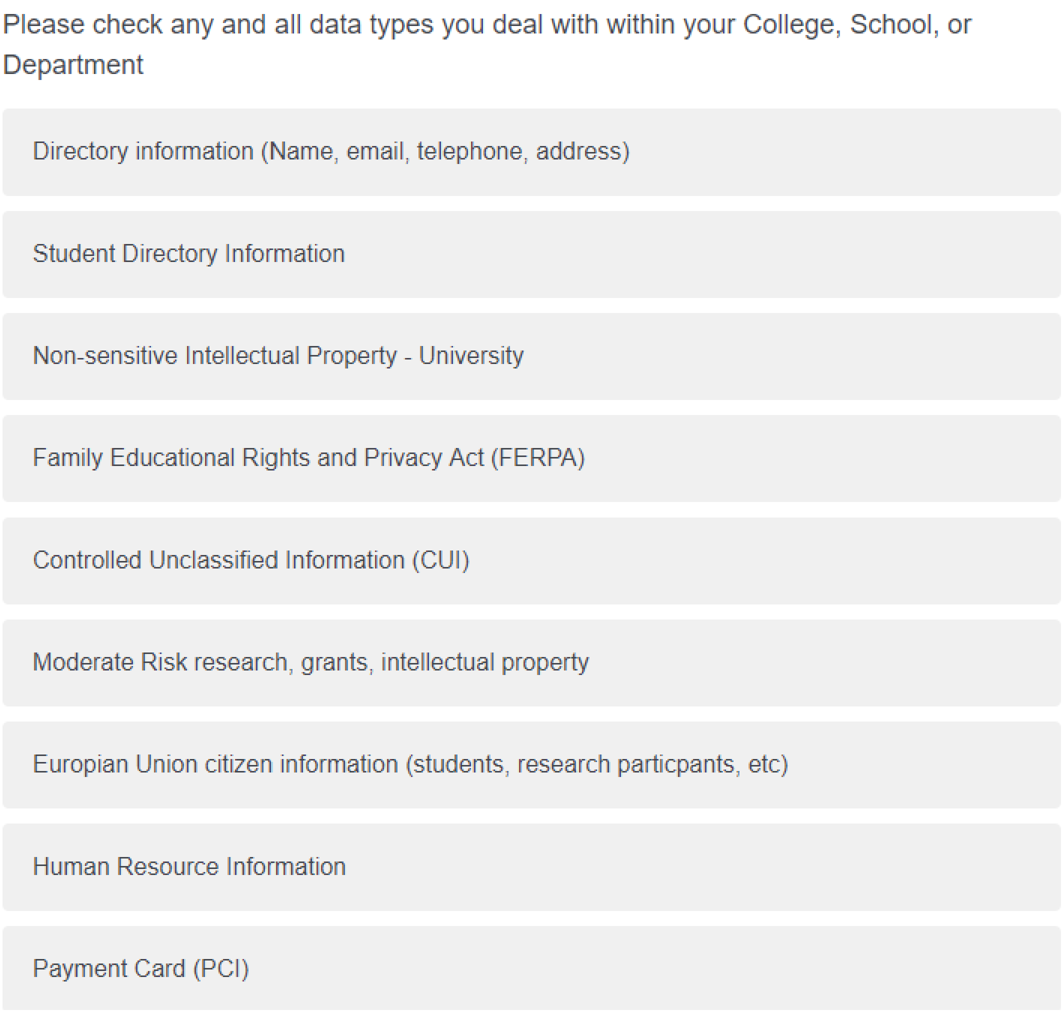
ID.AM-2: Software platforms and applications within the organization are inventoried (4)

- An inventory of software platforms and applications exists.
- The inventory is updated periodically to address new software and applications.
- The inventory is updated to include relocated, re-purposed, and sunset applications.
- This process is automated.

Our Approach

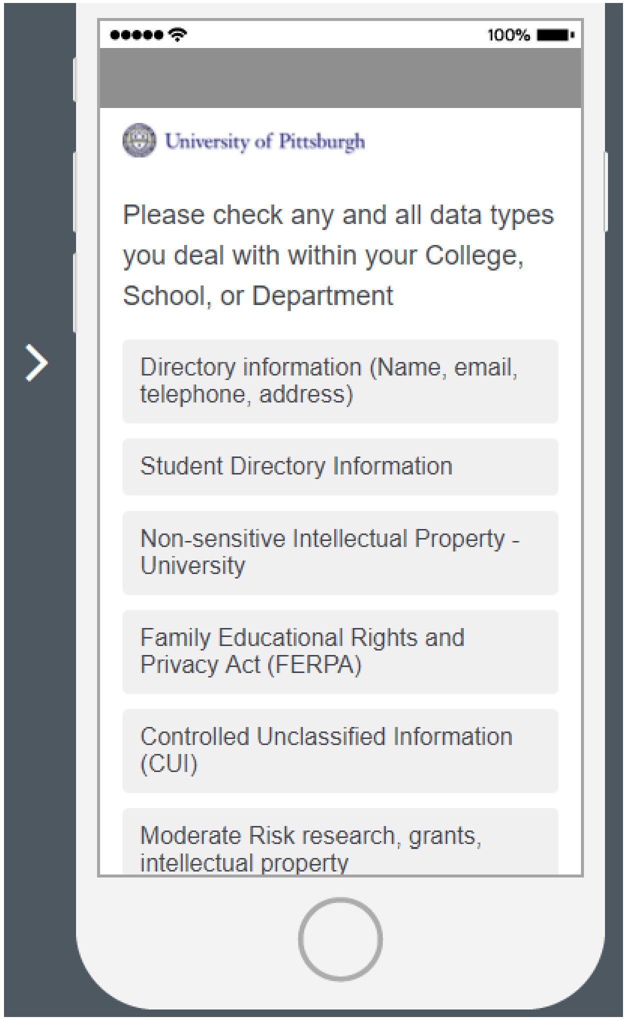
- NIST 800-171
- Initial questionnaire to identify high-risk data
- Basic questionnaire for low/moderate risk
- Detailed questionnaire for high-risk
- Multi-year project

NIST 800-171 sample questionnaire



Please check any and all data types you deal with within your College, School, or Department

- Directory information (Name, email, telephone, address)
- Student Directory Information
- Non-sensitive Intellectual Property - University
- Family Educational Rights and Privacy Act (FERPA)
- Controlled Unclassified Information (CUI)
- Moderate Risk research, grants, intellectual property
- Europian Union citizen information (students, research particpants, etc)
- Human Resource Information
- Payment Card (PCI)



University of Pittsburgh

Please check any and all data types you deal with within your College, School, or Department

- Directory information (Name, email, telephone, address)
- Student Directory Information
- Non-sensitive Intellectual Property - University
- Family Educational Rights and Privacy Act (FERPA)
- Controlled Unclassified Information (CUI)
- Moderate Risk research, grants, intellectual property

Summary

- Many frameworks to choose from
- Compliance may be your driver
- Use other frameworks as references
  - Crosswalks exist
  - Can help with control creation
- Take your time

Questions and Discussion

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
- https://www.nist.gov/cyberframework
- 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
- https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework
- https://youtu.be/J9ToNuwmyF0

Thank You