MIS 4596

Risk Controls

Unit #21

Agenda

- Equifax Case Discussion
- Risk Assessment
  - Risk evaluation
  - Collect data
  - Analyze risk
  - Risk management techniques
  - Select a risk control baseline
- Next class… onto Milestone 4

Breakout Group Questions

Work together to discuss and answer the following questions:

1. What was the cause of the Equifax breach?
2. How long were attackers within Equifax's network before their access was removed?
3. What problems do you see with Equifax's detection and response to the breach?
4. How could Equifax have better notified and assisted people affected by the breach?

What is Equifax’s business model?

What is Equifax's business model?

- One of 3 main U.S. credit reporting companies along with Experian and TransUnion
- Collects consumer and business credit information and conducts data analysis on income and consumer creditworthiness for financial service providers
- Equifax is provided its key information resource (i.e. consumer data) free of charge
- Equifax adds value using proprietary analytical models to produce credit scores and profiles of individual people for commercial purposes

What is the consumer in this business model?

What is the consumer in this business model?

- Equifax managed data on >820 million consumer and >91 million businesses around the world
- Consumers' banks, employers, lenders, and public records are suppliers of consumers' personal information to Equifax which it turns into products and sells back to financial service providers
- Consumers rely on Equifax to provide good data on their creditworthiness to lenders and to protect their data
- Consumers cannot opt out of having their data collected an analyzed by Equifax
- Consumers do not have an explicit contract with Equifax and lack a good recourse in the event something goes wrong

What information system vulnerabilities were identified at Equifax

- Equifax left consumer information exposed on a website accessible to any internet user (12/2016 through 6/2017)
- Equifax was careless in patching systems
- Difficult to get management to understand the problems
- No prepared to respond to a data breach
- Issues with data hygiene
  - Expired certificates, errors in the certificate chain, other web security issues
  - No audits of security policies and systems

What information system vulnerabilities were identified at Equifax

- Apache Struts Vulnerability
  - Open source Java software for building web applications
  - Equifax used this software for its web portal that enabled customers to dispute items in their credit reports
  - Security flaw discovered and Equifax security team notified on March 8, 2017; installed updated intrusion detection system signatures on March 14; certificates for identifying/authenticating web access source IP addresses not updated/fixed until July 29th (these used to identify hackers accessing Equifax's systems)
    - Hacker's vulnerability scans able to detect the security flaw on March 10 and installed backdoors which they began using to access and exfiltrate PII on May 13th onward…
    - Accessible through 2 publicly available exploits
      - » Hackers able to insert malware and their own code in website pages, disable firewalls, and mask the origins of their data packets

Was Equifax careless or unlucky?

Was Equifax careless or unlucky?

- Data are core to their business, anything that compromises the data or harms Equifax's ability to collect it is an existential threat to the company
  - Yet they did not secure customer data

- They ignored numerous warnings:
  - Company notified in early March of the vulnerability exploited by the attacker
    - *Data breach began 2 months later in May and continued through July 29th when breach was discovered by Equifax*
  - MSCI ESG report from April 2017 gave Equifax a 0 rating for privacy & data – lowest in its peer group
  - Ignored Mandiant as they were investigating issue at the time of the breach

- Did not seem to understand cybersecurity
  - Basic cybersecurity vulnerabilities in its website were not mitigated
    - Expired certificates, vulnerable outdated plug-ins…
  - CTO and key cybersecurity employees left the firm
  - At risk of dangers from unpatched open-source software

What was the Board of Director’s responsibility for the breach?

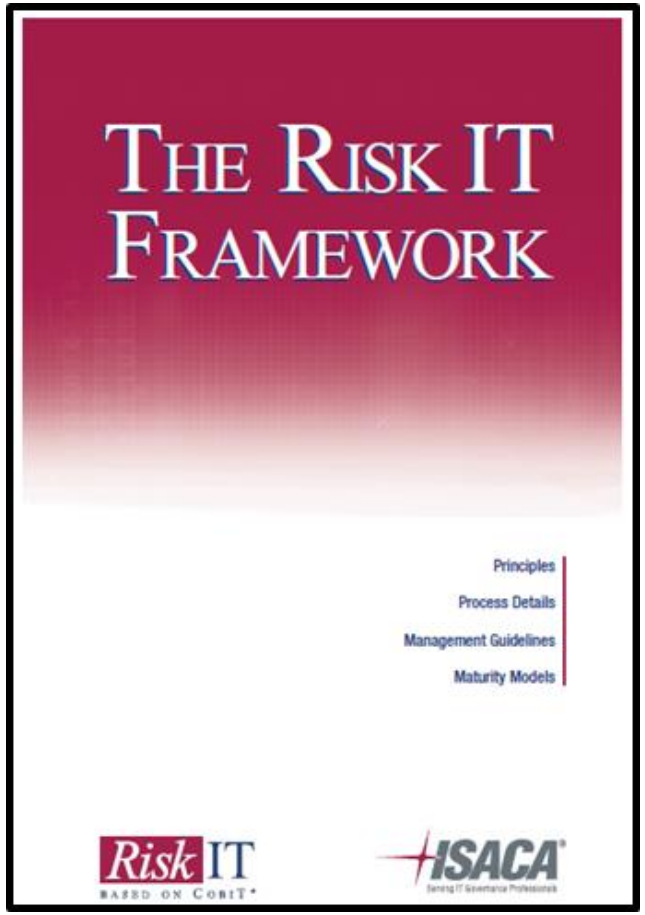
- Board should have identified data breaches as a potential existential threat to the company, and hold management accountable for how it was addressing the threat
- Technology Committee were completely unprepared and lacked expertise

What questions should the Board have asked of management?

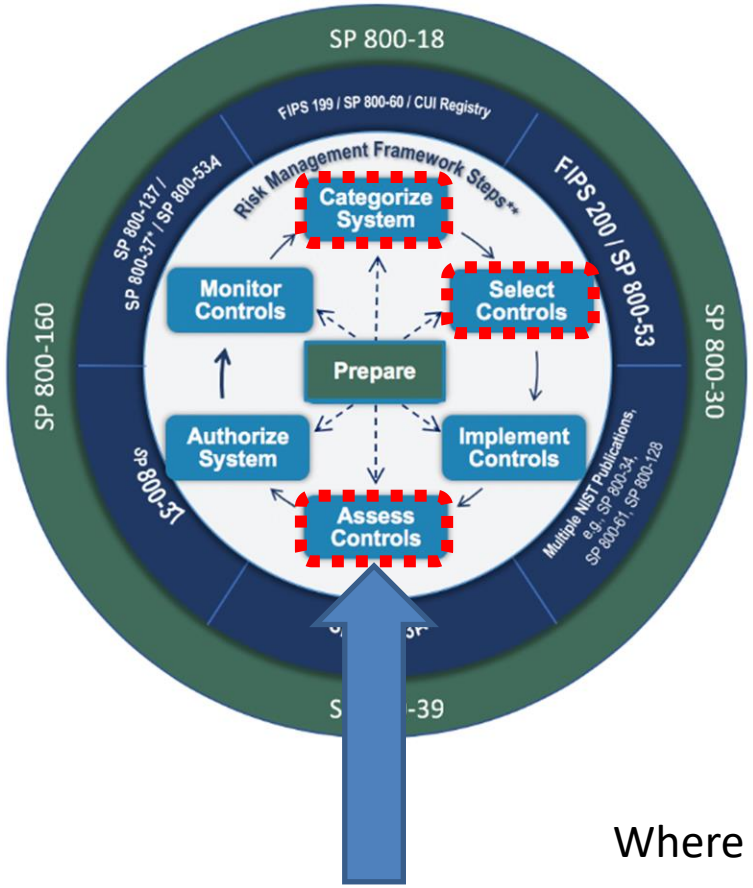
What questions should the Board have asked of management?

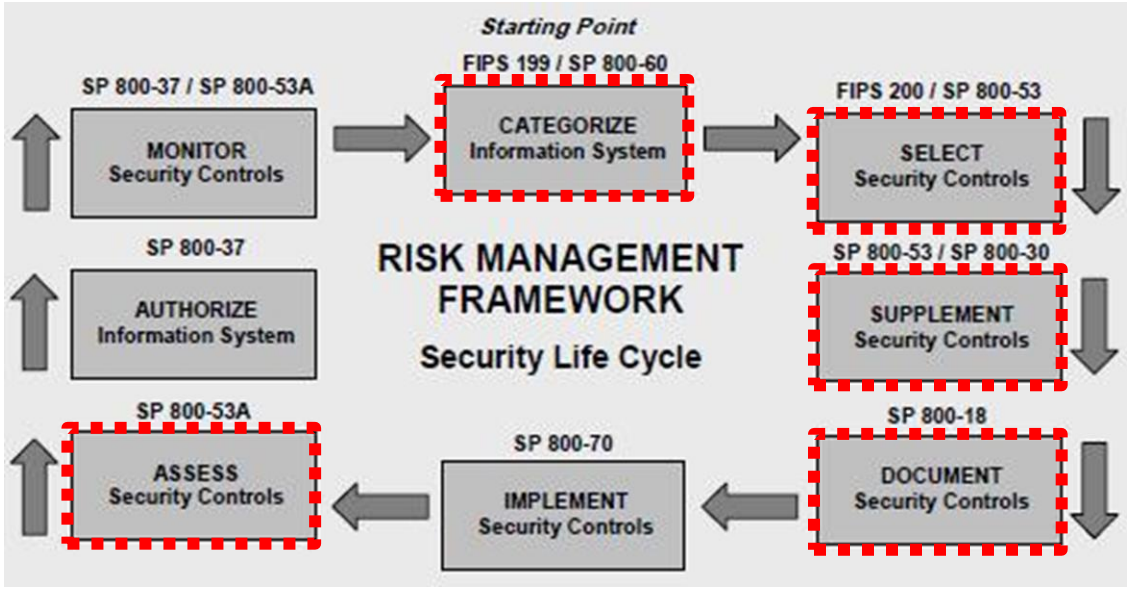
- What assets, tangible and intangible, are the most important to us and at risk from cyber-attack?
- How are we quantifying cyber-risk?
- When was the last time we updated our response plan and processes?
- How much is the company spending on cybersecurity?
- Does our cybersecurity team and reporting structure make sense?
- What are our industry standards, do we need to go above and beyond these?
- Who is in charge of cybersecurity on the Board?

Risk Evaluation and Control



NIST Risk Management Framework…



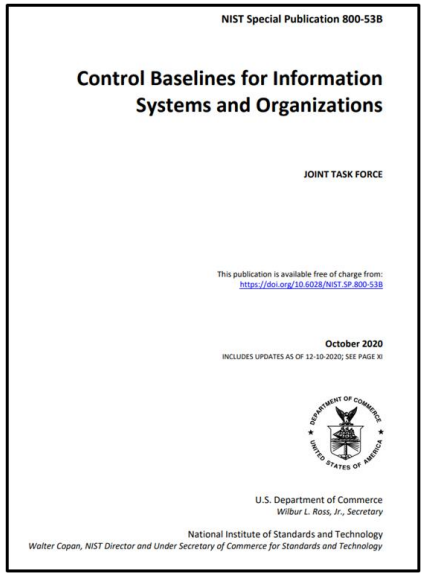


Where does your Milestone 3 penetration testing report fit?

After assessing controls…

Milestone 4 recommends improvements to the security controls to mitigate the vulnerabilities you found in the information system

- Where do you find security controls to recommend the organization add to improve the protection to their information system?


NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

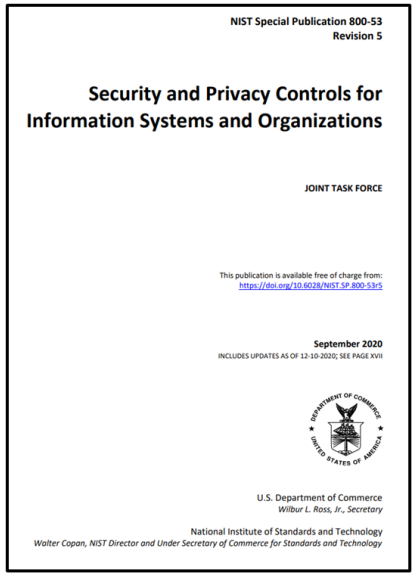
This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53B

October 2020

INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XI

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology


NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

September 2020

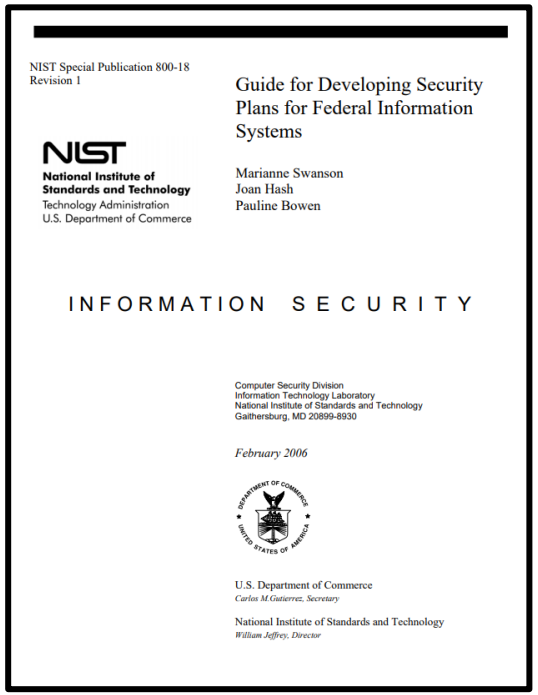
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Security control class designations help clarify controls in preparation of system security plans



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

U.S. Department of Commerce
Carlos M.Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

1. **Management controls** focus on management of the information system and management of risk for a system
2. **Operational controls** address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems) with technical expertise and/or management expertise
3. **Technical controls** focus on automated security controls that the computer system(s) executes

Where can you find information on controls related to improving passwords?

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

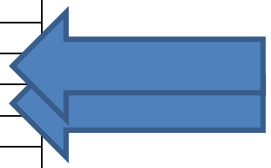
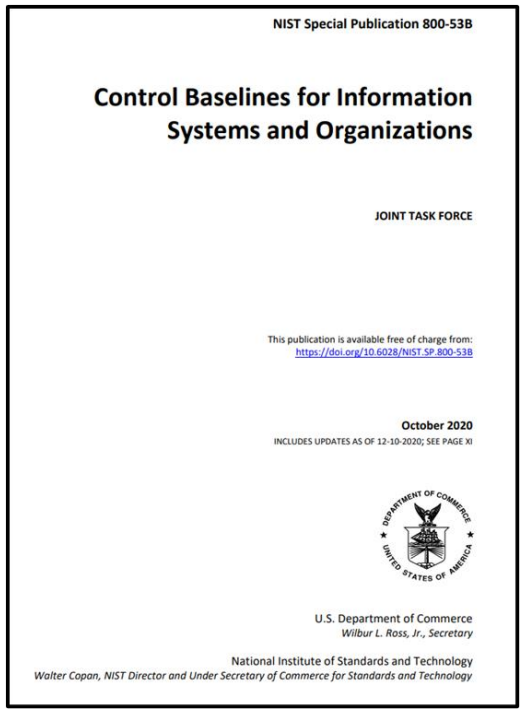


Table 2: Security Control Class, Family, and Identifier

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

Milestone 4: What controls can you recommend for improving password security?



NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53B

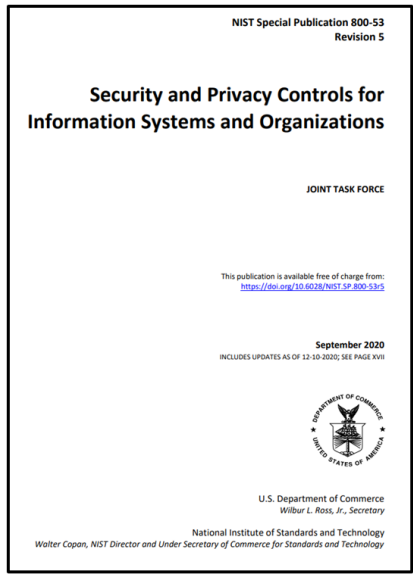
October 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XI

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IA-1	**Policy and Procedures**		x	x	x
IA-2	**Identification and Authentication (Organizational Users)**		x	x	x
IA-2(1)	MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS		x	x	x
IA-2(2)	MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS		x	x	x
IA-2(3)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(1)(2).			
IA-2(4)	LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(1)(2).			
IA-2(5)	INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION				x
IA-2(6)	ACCESS TO ACCOUNTS — SEPARATE DEVICE				
IA-2(7)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — SEPARATE DEVICE	W: Incorporated into IA-2(6).			
IA-2(8)	ACCESS TO ACCOUNTS — REPLAY RESISTANT		x	x	x
IA-2(9)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — REPLAY RESISTANT	W: Incorporated into IA-2(8).			
IA-2(10)	SINGLE SIGN-ON				
IA-2(11)	REMOTE ACCESS — SEPARATE DEVICE	W: Incorporated into IA-2(6).			
IA-2(12)	ACCEPTANCE OF PIV CREDENTIALS		x	x	x
IA-2(13)	OUT-OF-BAND AUTHENTICATION				
IA-3	**Device Identification and Authentication**			x	x
IA-3(1)	CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION				
IA-3(2)	CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION	W: Incorporated into IA-3(1).			
IA-3(3)	DYNAMIC ADDRESS ALLOCATION				
IA-3(4)	DEVICE ATTESTATION				
IA-4	**Identifier Management**		x	x	x
IA-4(1)	PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS				
IA-4(2)	SUPERVISOR AUTHORIZATION	W: Incorporated into IA-12(1).			
IA-4(3)	MULTIPLE FORMS OF CERTIFICATION	W: Incorporated into IA-12(2).			
IA-4(4)	IDENTIFY USER STATUS			x	x
IA-4(5)	DYNAMIC MANAGEMENT				
IA-4(6)	CROSS-ORGANIZATION MANAGEMENT				
IA-4(7)	IN-PERSON REGISTRATION	W: Incorporated into IA-12(4).			
IA-4(8)	PAIRWISE PSEUDONYMOUS IDENTIFIERS				
IA-4(9)	ATTRIBUTE MAINTENANCE AND PROTECTION				
IA-5	**Authenticator Management**		x	x	x
IA-5(1)	PASSWORD-BASED AUTHENTICATION		x	x	x

What controls can you recommend for improving password security?



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

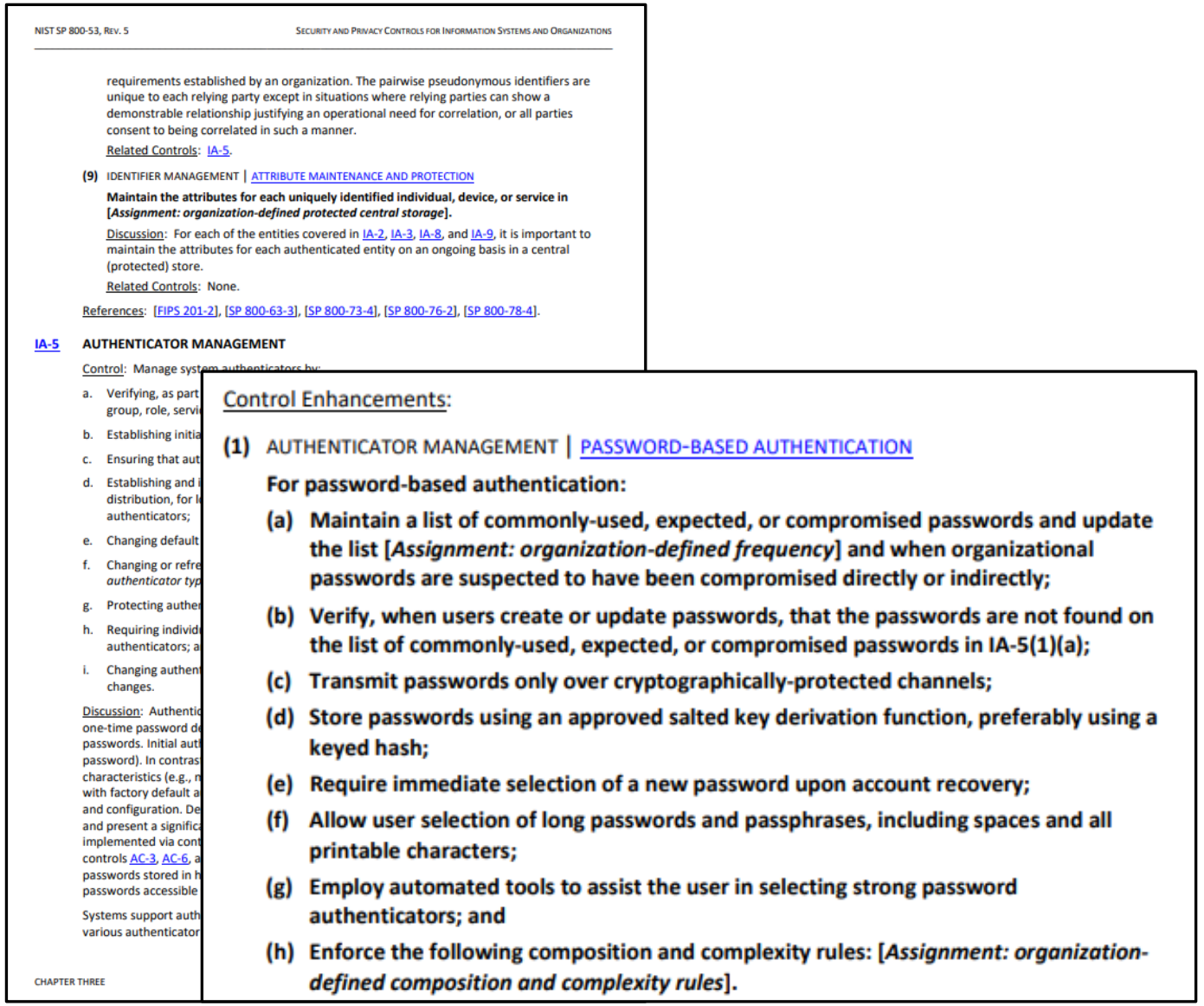
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology



NIST SP 800-53, REV. 5 — SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

requirements established by an organization. The pairwise pseudonymous identifiers are unique to each relying party except in situations where relying parties can show a demonstrable relationship justifying an operational need for correlation, or all parties consent to being correlated in such a manner.

Related Controls: IA-5.

(9) IDENTIFIER MANAGEMENT | ATTRIBUTE MAINTENANCE AND PROTECTION

Maintain the attributes for each uniquely identified individual, device, or service in [*Assignment: organization-defined protected central storage*].

Discussion: For each of the entities covered in IA-2, IA-3, IA-8, and IA-9, it is important to maintain the attributes for each authenticated entity on an ongoing basis in a central (protected) store.

Related Controls: None.

References: [FIPS 201-2], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4].

IA-5 AUTHENTICATOR MANAGEMENT

Control: Manage system authenticators by:

a. Verifying, as part
group, role, servi
b. Establishing initia
c. Ensuring that aut
d. Establishing and
distribution, for
authenticators;
e. Changing default
f. Changing or refre
authenticator typ
g. Protecting authe
h. Requiring individ
authenticators; a
i. Changing authen
changes.

Discussion: Authentic
one-time password d
passwords. Initial aut
password). In contras
characteristics (e.g., n
with factory default a
and configuration. De
and present a signific
implemented via cont
controls AC-3, AC-6, a
passwords stored in h
passwords accessible

Systems support auth
various authenticator

CHAPTER THREE

Control Enhancements:

(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

For password-based authentication:

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [*Assignment: organization-defined frequency*] and when organizational passwords are suspected to have been compromised directly or indirectly;

(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

(c) Transmit passwords only over cryptographically-protected channels;

(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;

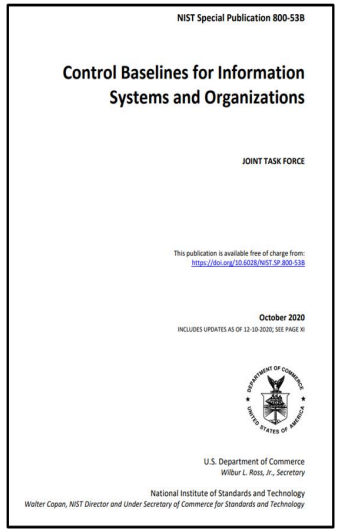
(e) Require immediate selection of a new password upon account recovery;

(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;

(g) Employ automated tools to assist the user in selecting strong password authenticators; and

(h) Enforce the following composition and complexity rules: [*Assignment: organization-defined composition and complexity rules*].

Milestone 4… What other types of controls do you think aught be added or improved?



NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

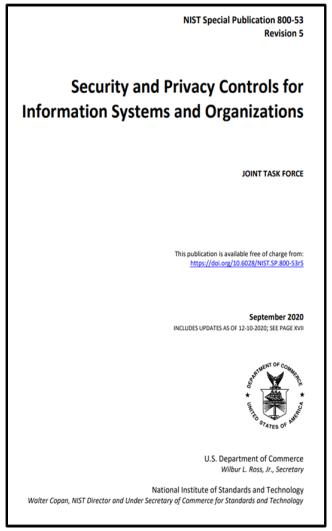
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53B

October 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XI

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management