From Preparation to Practice Workshop
Randy Marchany, Virginia Tech
From Preparation to Practice: Using the CIS Critical Security Controls to Implement NIST 800-171 Security Compliance

Randy Marchany, Virginia Tech *with Special Guests*

Joanna Grama, EDUCAUSE
Jarret Cummings, EDUCAUSE
Agenda

1. Preparation
   a. What is CUI and NIST 800-171 and why do we care?
   b. FSA update

2. Practice
Handouts for Today

Materials from today’s session:

Part I. Preparation
Higher Education Data Context

- Data is Valuable!
- User credentials/passwords
- Personally identifiable information
  - Financial information
  - Health information
- Student data
- Proprietary information/trade secrets
- Research data
- Information about how networks and IT resources work
- Confidential information that could cause personal embarrassment
The Struggle to Protect is Real

- Multiple “enterprise” systems with differing types of data
  - And “shadow systems”
- “Access anywhere” paradigm
- Different audiences (students, faculty, staff) with vastly different data needs
- Institutions are not homogenous—different institutions have different levels of protected data
Controlled Unclassified Information

- CUI is essentially any data that should be safeguarded that is not classified
- Data that are concerning for higher ed: research data, controlled technical information, export control research data, student records and personally identifiable information
Legal Basis for CUI Protection

• Executive Order 13556 to establish a government wide program (Nov. 2010)
• NIST Special Publication 800-171 to define security requirements for protecting CUI in non-federal information systems and organizations (June 2015)
• Federal CUI rule (32 CFR Part 2002) to establish the required controls and markings for CUI government wide (Sept. 2016)
Legal Basis for CUI Protection

• *For Defense Contracts*: Defense Federal Acquisition Regulation Supplement (DFARS) 252.204.7012 establishes NIST 800-171 as the minimum security standard for protecting both CUI and CDI. (Dec. 2015)

• *For Civilian Contracts*: Federal Acquisition Regulation (FAR) clause to apply the requirements of the federal CUI rule and NIST SP 800-171 to contractors (*expected any day now*)
I'm too NIST-y, and too much in love*

*Sincere apologies to Ella Fitzgerald

- National Institute of Standards and Technology (part of Dept. of Commerce)
- Computer Security Division has a resource center of cybersecurity standards
- OMB states that federal agencies must follow NIST standards and guidelines for non-national security systems
NIST 800-171 Requirements

• Protect **federal** data in **non-federal** information systems
  – State, local, and tribal governments; colleges and universities are examples of non-federal organizations
• Only applies to the components of non-federal systems that process, store, or transmit CUI
• Goal is to make sure that requirements for the protection of CUI are consistent, whether such CUI is in federal or non-federal information systems
<table>
<thead>
<tr>
<th>NIST 800-171 Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
</tr>
<tr>
<td>Awareness &amp; Training</td>
</tr>
<tr>
<td>Audit &amp; Accountability</td>
</tr>
<tr>
<td>Configuration Management</td>
</tr>
<tr>
<td>Identification &amp; Authentication</td>
</tr>
<tr>
<td>Incident Response</td>
</tr>
<tr>
<td>Maintenance</td>
</tr>
</tbody>
</table>
Dear Colleague Letter Gen 16-12

- Issued July 1, 2016
- Reminds institutions that student financial aid information is subject to the security requirements of the Gramm-Leach-Bliley Act ("GLBA") (15 U.S.C. §6801)
- "Strongly encourages" institutions to review and understand the security standards of NIST SP 800-171
- Notes that the Department is beginning to incorporate GLBA requirements into its annual audit guide.

https://ifap.ed.gov/dpcletters/GEN1612.html
What is GLBA?

• Enacted 1999
• Applies to financial institutions handling a customer’s nonpublic personal information
• Includes a privacy rule and safeguards rule
  – Higher ed falls under FTC regulatory authority for GLBA
  – For higher ed, FERPA compliance is deemed compliance for GLBA Privacy Rule
  – FTC issued their safeguards rule in 2002
GLBA Safeguards Rule (16 CFR §314)

Institutions must:
• Maintain a written information security program;
• Designate a information security program coordinator;
• Perform a risk assessment;
• Design and implement an information safeguards program;
• Select and manage service providers and require them to implement appropriate safeguards; and
• Periodically evaluate and update their security program.
The Plot Thickens

- First we had GLBA
- Then, CUI standardization
- And then NIST 800-171
- And then DCL GEN 16-12
- Now GLBA Auditing
- Next: ???
And Speaking of Plot Twists...

Education CIO retires weeks after Capitol Hill confrontation

By Zach Noble | Feb 22, 2016
Timeline: FSA Infosec. Outreach

- Early ‘16: ACE mtg. w/ Dept. of Ed. (ED)
- Fall ‘16: EDUCAUSE/FSA re: 800-171, GLBA
- Early ‘17: EDUCAUSE, NACUBO, et al, negotiate GLBA Safeguards Rule audit objective
- Fall ‘17: Breach/infosec reporting letters
- Early ‘18: EDUCAUSE, ACE letters to FSA
Changing of the FSA Guard

- 01/31: Letter to FSA COO, Dep. COO, cybersecurity senior advisor
- 02/01: COO reassigned (after 6 mos.); acting COO, new dep. COO; lead contact TBD
- Now: Lead contact = exec-level compliance senior advisor, no timetable for response
Changing of the FSA Guard (cont’d)

- Fall ‘16 mtg. (800-171, GLBA): FSA Dep. COO (replaced), CIO (reassigned), dep. CIO (?)
- Acting COO (ops.) and dep. COO (programs, enforcement) dividing responsibilities
- Where will infosec. issues fall? Who will we work with, and when?
Breach/Infosec. Reporting

• What happened?
  • Letters sent to presidents, not official FSA contacts, based on unconfirmed media reports
  • Assert breach notification for anything (not just FSA data; includes “suspected breaches”)
  • Very broad, in-depth infosec. program reporting
Breach/Infosec. Reporting (cont’d)

• What happened?
  • No official, publicly documented authority, policies, processes?
  • No certain, secure reporting mechanisms?
  • No higher ed. stakeholder collaboration?
• Are we now being heard? Definite “maybe”...
Key Points to Note

- No new, official breach/infosec. guidance
- Any new FSA letters? Not that we know...
- Safeguards Rule audit objective? See 2019...
- Check Prog. Participation, Student Aid Internet Gateway Agreements with attorney ([ifap.ed.gov/eannouncements/Cyber.html](ifap.ed.gov/eannouncements/Cyber.html))
Key Points to Note (cont’d)

• Collaborate with business office, institutional auditors on audit objective “dry run”
• Draft OMB/FSA audit objective text: https://er.educause.edu/blogs/2017/8/glba-audit-objective-text-online
• Best basis for testing, but could change
What About CUI Rule (800-171)?

- “Strongly recommended” per DCL 16-12
- FSA can’t implement until ED guidance; ED/FSA churn = still on back burner
- Renewed EDUCAUSE collaboration request
- As w/ audit objective, use this time wisely – will happen, and could happen unexpectedly
“Until Education ensures that information security requirements are considered in program reviews of schools, FSA will lack assurance that schools have effective information security programs.”
Part II. Putting it into Practice
20 CSC Background

• Proven defenses against actual attacks
• Offense informs defense
• Prioritized measures/metrics, continuous diagnostics
• Automation
CSC Alerting/Reporting/Analytics
CSC 1 - Inventory & Control of HW Assets
CSC 2 - Inventory & Control of SW Assets
CSC 3 - Continuous Vulnerability Mgt
CSC 4 - Controlled Use of Admin Privs
CSC 5 - Secure Config for HW, SW
CSC 6 - Maintenance, Monitoring, Analysis of Logs
CSC 12 - Boundary Defense
CSC 16 - Account Monitoring & Control
<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Server Software</th>
<th>Cloud Providers</th>
<th>Mobile Devices</th>
<th>Network Devices</th>
<th>Desktop Software</th>
<th>Multi Function Print Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution Independent Linux</td>
<td>Expand to see related content</td>
<td><a href="#">Download CIS Benchmark</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Server Software</td>
<td>Cloud Providers</td>
<td>Mobile Devices</td>
<td>Network Devices</td>
<td>Desktop Software</td>
<td>Multi Function Print Devices</td>
</tr>
<tr>
<td>Microsoft Windows Desktop</td>
<td>Expand to see related content</td>
<td><a href="#">Download CIS Benchmark</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Server Software</td>
<td>Cloud Providers</td>
<td>Mobile Devices</td>
<td>Network Devices</td>
<td>Desktop Software</td>
<td>Multi Function Print Devices</td>
</tr>
<tr>
<td>Debian Linux</td>
<td>Expand to see related content</td>
<td><a href="#">Download CIS Benchmark</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Server Software</td>
<td>Cloud Providers</td>
<td>Mobile Devices</td>
<td>Network Devices</td>
<td>Desktop Software</td>
<td>Multi Function Print Devices</td>
</tr>
<tr>
<td>Ubuntu Linux</td>
<td>Expand to see related content</td>
<td><a href="#">Download CIS Benchmark</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Server Software</td>
<td>Cloud Providers</td>
<td>Mobile Devices</td>
<td>Network Devices</td>
<td>Desktop Software</td>
<td>Multi Function Print Devices</td>
</tr>
<tr>
<td>Microsoft IIS</td>
<td>Expand to see related content</td>
<td><a href="#">Download CIS Benchmark</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Server Software</td>
<td>Cloud Providers</td>
<td>Mobile Devices</td>
<td>Network Devices</td>
<td>Desktop Software</td>
<td>Multi Function Print Devices</td>
</tr>
<tr>
<td>VMware</td>
<td>Expand to see related content</td>
<td><a href="#">Download CIS Benchmark</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtualisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Server Software</td>
<td>Cloud Providers</td>
<td>Mobile Devices</td>
<td>Network Devices</td>
<td>Desktop Software</td>
<td>Multi Function Print Devices</td>
</tr>
<tr>
<td>Microsoft SharePoint</td>
<td>Expand to see related content</td>
<td><a href="#">Download CIS Benchmark</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collaboration Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Server Software</td>
<td>Cloud Providers</td>
<td>Mobile Devices</td>
<td>Network Devices</td>
<td>Desktop Software</td>
<td>Multi Function Print Devices</td>
</tr>
<tr>
<td>MongoDB</td>
<td>Expand to see related content</td>
<td><a href="#">Download CIS Benchmark</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Server Software</td>
<td>Cloud Providers</td>
<td>Mobile Devices</td>
<td>Network Devices</td>
<td>Desktop Software</td>
<td>Multi Function Print Devices</td>
</tr>
<tr>
<td>IBM DB2</td>
<td>Expand to see related content</td>
<td><a href="#">Download CIS Benchmark</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Exercise 1a: NIST 800-171 to CSC Map

• [https://www.auditscripts.com/free-resources/critical-security-controls/](https://www.auditscripts.com/free-resources/critical-security-controls/)
  • Click on Auditscripts Critical Security Controls Master Mapping link to download spreadsheet
  • Open the spreadsheet
Exercise 1b: Standards to CSC Mapping

• Open 800-171-Table 3-to-20Crits spreadsheet
• Discussion
Discussion

- 70% of the 800-171 control numbers map to the 20 Critical controls.
- Which ones have you done already?
- Determine the scope
  - Just the CUI systems or the whole net?
Exercise 2: CSC Map to CIS Benchmarks

- Pick appropriate benchmark (Linux, Windows, Mac)
- Map benchmark sections to each 800-171 CSC
- Cut commands out of benchmark doc, paste into flat file to create NIST 800-171 configuration script file – mods may be needed
4.1.1 Configure Data Retention

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.

4.1.1.1 Ensure audit log storage size is configured (Not Scored)

Profile Applicability:
- Level 2 - Server
- Level 2 - Workstation

Description:
Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.

Rationale:
It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

Audit:
Run the following command and ensure output is in compliance with site policy:

```bash
# grep max_log_file /etc/audit/auditd.conf
max_log_file = <MB>
```

Remediation:
Set the following parameter in `/etc/audit/auditd.conf` in accordance with site policy:

```bash
max_log_file = <MB>
```

5.3.3 Ensure password reuse is limited (Scored)

Profile Applicability:
- Level 1 - Server
- Level 1 - Workstation

Description:
The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

Rationale:
Forcing users not to reuse their past 5 passwords makes it less likely that an attacker will be able to guess the password.

Note that these change only apply to accounts configured on the local system.

Audit:
Run the following commands and ensure the `remember` option is '5' or more and included in all results:

```bash
# egrep "\!password\!required\!*\!pam\!pwhistory\.so\!/etc/pam\!d\!/common\!password\!\!password\!required\!pam\!pwhistory\.so\!\!remember\!5"
```

Remediation:
Edit the `/etc/pam.d/common-password` file to include the `remember` option and conform to site policy as shown:

```bash
password required pam_pwhistory.so remember=5
```

Notes:
Additional module options may be set, recommendation only covers those listed here.

CIS Controls:
16 Account Monitoring and Control
Account Monitoring and Control
Optional: Run script on Cyber Range

- Take the script file you created, copy it to your Google Drive
- Access your drive from the Cyber Range host
- Copy the config script to your Range host
- Run the script.
Summary

• Have a way to move from policy to implementation
  • Methodology extends to other standards
• Living process – modified continuously
• Questions?
Helpful Resources

An Introduction to NIST Special Publication 800-171 for Higher Education Institutions
https://library.educause.edu/resources/2016/4/an-introduction-to-nist-special-publication-800-171-for-higher-education-institutions

NIST SP 800-171 Compliance Template by the Common Solutions Group
https://library.educause.edu/resources/2016/9/nist-sp-800-171-compliance-template

New Federal Data Protection Requirements Impact Higher Education Institutions
https://library.educause.edu/resources/2017/10/new-federal-data-protection-requirements-impact-higher-education-institutions

#Security18
Helpful Resources

CIS Controls & Benchmarks
http://www.cisecurity.org

Critical Security Controls gap analysis spreadsheets
https://www.auditscripts.com/free-resources/critical-security-controls/

Materials from today’s session:

#Security18
Questions?

Randy Marchany
University IT Security Officer
Virginia Tech
marchany@vt.edu

Joanna Grama
Director of Cybersecurity & IT GRC Programs
EDUCAUSE
jgrama@educause.edu

Jarret Cummings
Director of Policy & Government Relations
EDUCAUSE
jcummings@educause.edu

#Security18
Thank you!

Please be sure to complete the evaluation for today’s workshop. Your feedback helps improve both the conference and the presentations.