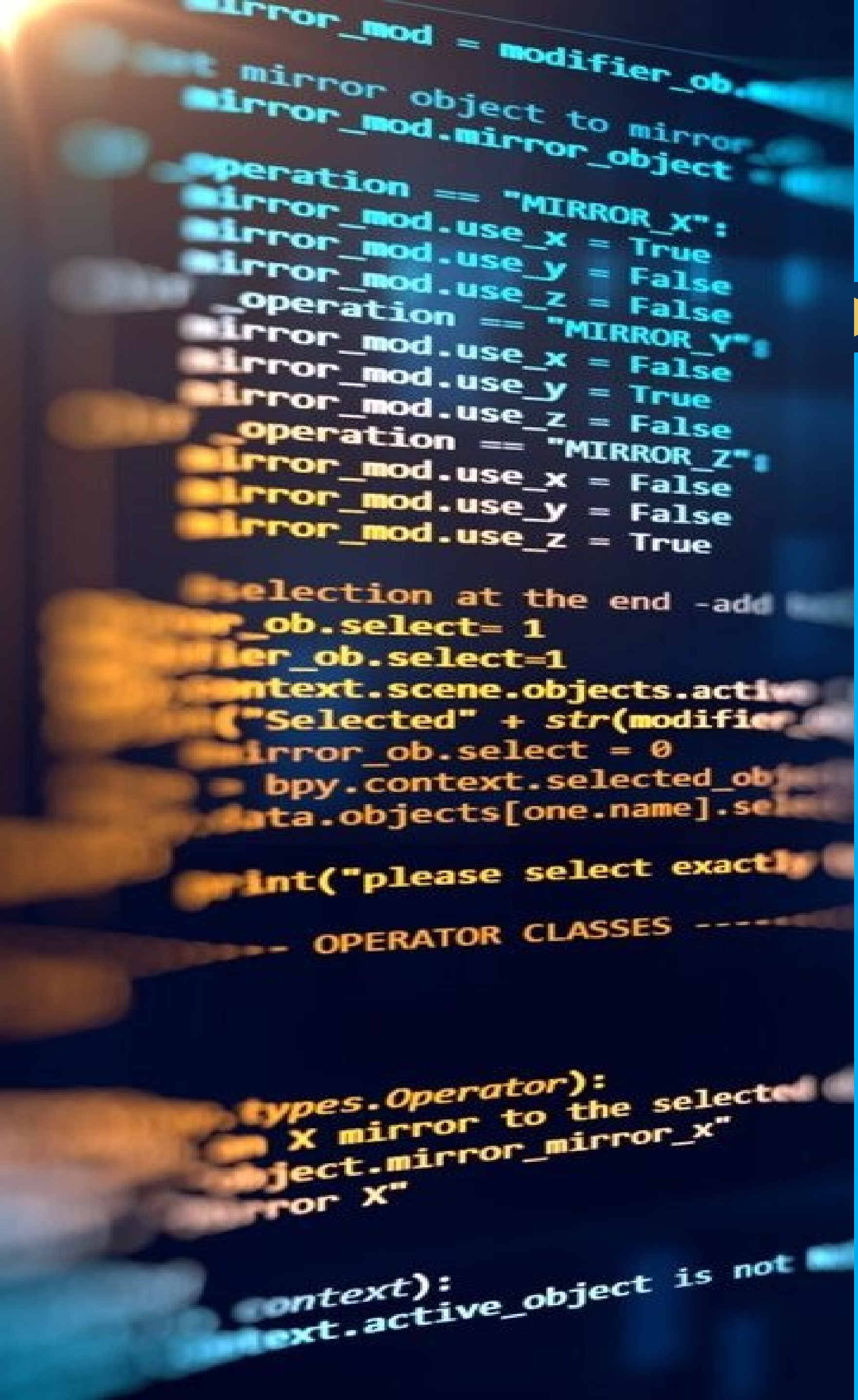


```
irror_mod = modifier_ob
 mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
 _operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
 _operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

selection at the end -add
 _ob.select= 1
ier_ob.select=1
ntext.scene.objects.active
("Selected" + str(modifier
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].se

int("please select exactly

-- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
ror X"

ontext):
ext.active_object is not
```

AN OFFERING IN THE BLUE CYBER SERIES

DCMA DIBCAC Cybersecurity Audit Common Deficiencies

VERSION: 15 November 2022

#29 IN THE BLUE CYBER EDUCATION SERIES

PURDUE
UNIVERSITY

Manufacturing
Extension Partnership

CYBERSECURITY AUDIT COMMON DEFICIENCIES

Sponsored by Purdue MEP and Purdue cyberTAP

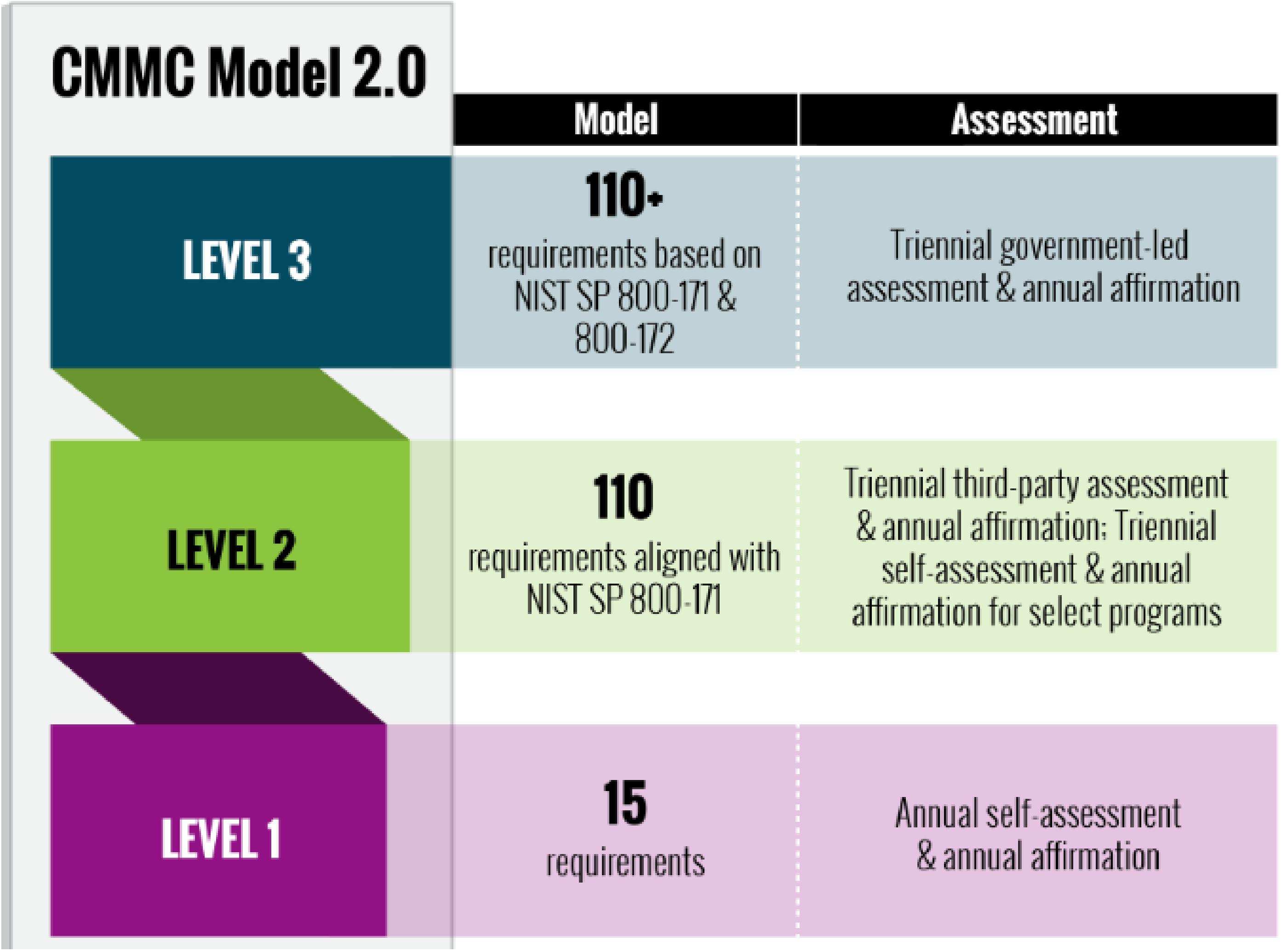
Purdue Manufacturing Extension Partnership
(800) 877-5182
www.mep.purdue.edu

PART OF THE MEP National Network™

Agenda

- DCMA DIBCAC has identified a list of “Top 10 Other Than Satisfied (OTS)” Requirements in the 100+ audits that they have conducted based upon NIST 800-171.
- In this session, review the Top 3 cybersecurity controls that have resulted in an OTS result to date:
  - FIPS-validated cryptography (3.13.11)
  - Multifactor authentication (3.5.3)
  - Documentation of system flaws (3.14.1)

CMMC Maturity Levels

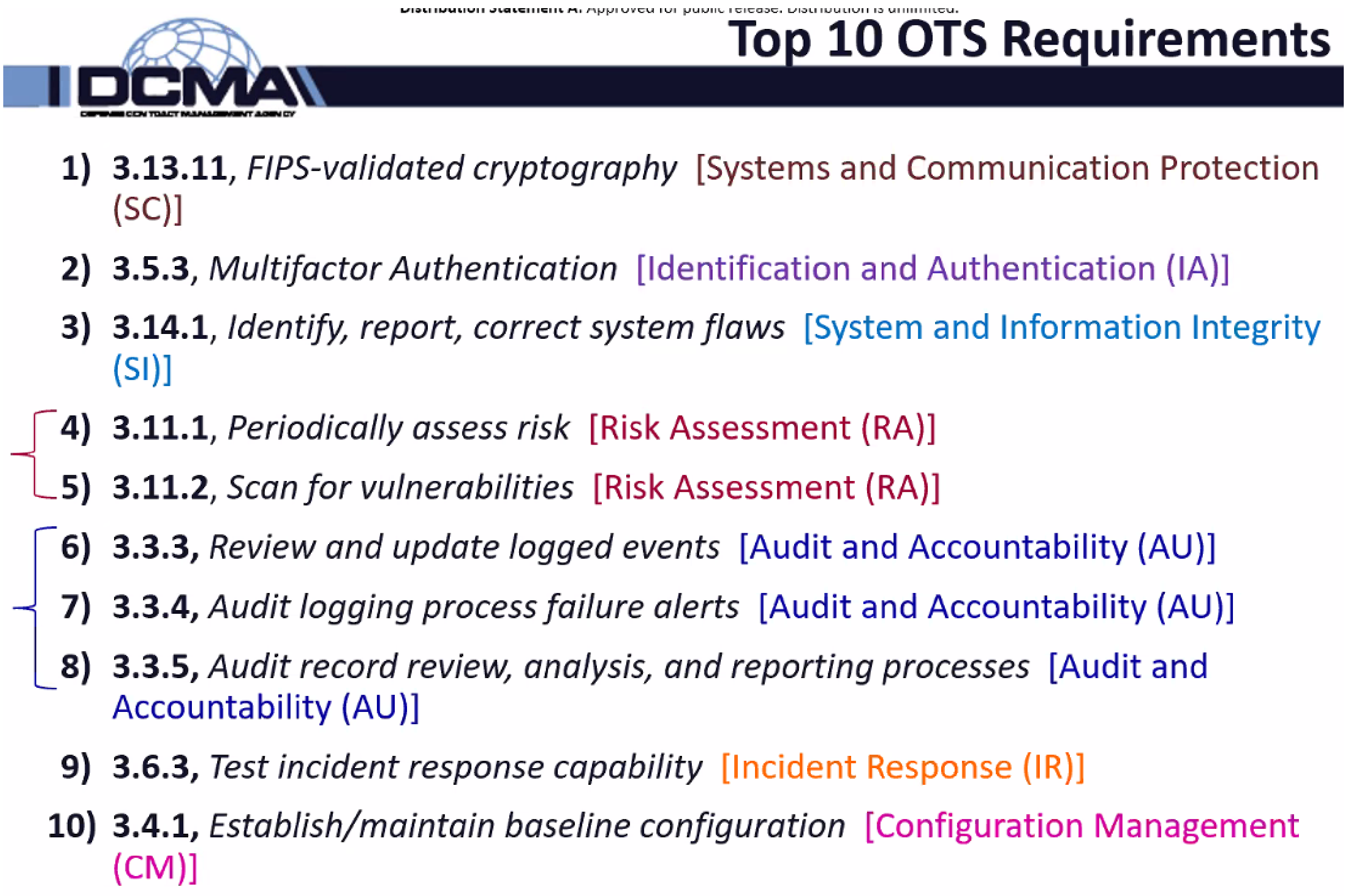


CMMC Model 2.0

	Model	Assessment
LEVEL 3	**110+** requirements based on NIST SP 800-171 & 800-172	Triennial government-led assessment & annual affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171	Triennial third-party assessment & annual affirmation; Triennial self-assessment & annual affirmation for select programs
LEVEL 1	**15** requirements	Annual self-assessment & annual affirmation

Current estimated timeline

- Voluntary audits Aug 2022
  - Followed CMMC assessment process guide (CAP) release
- Interagency review Nov 22 to Feb 23
- 90-day public comment period Feb to May 23
- Interim rule released May 23



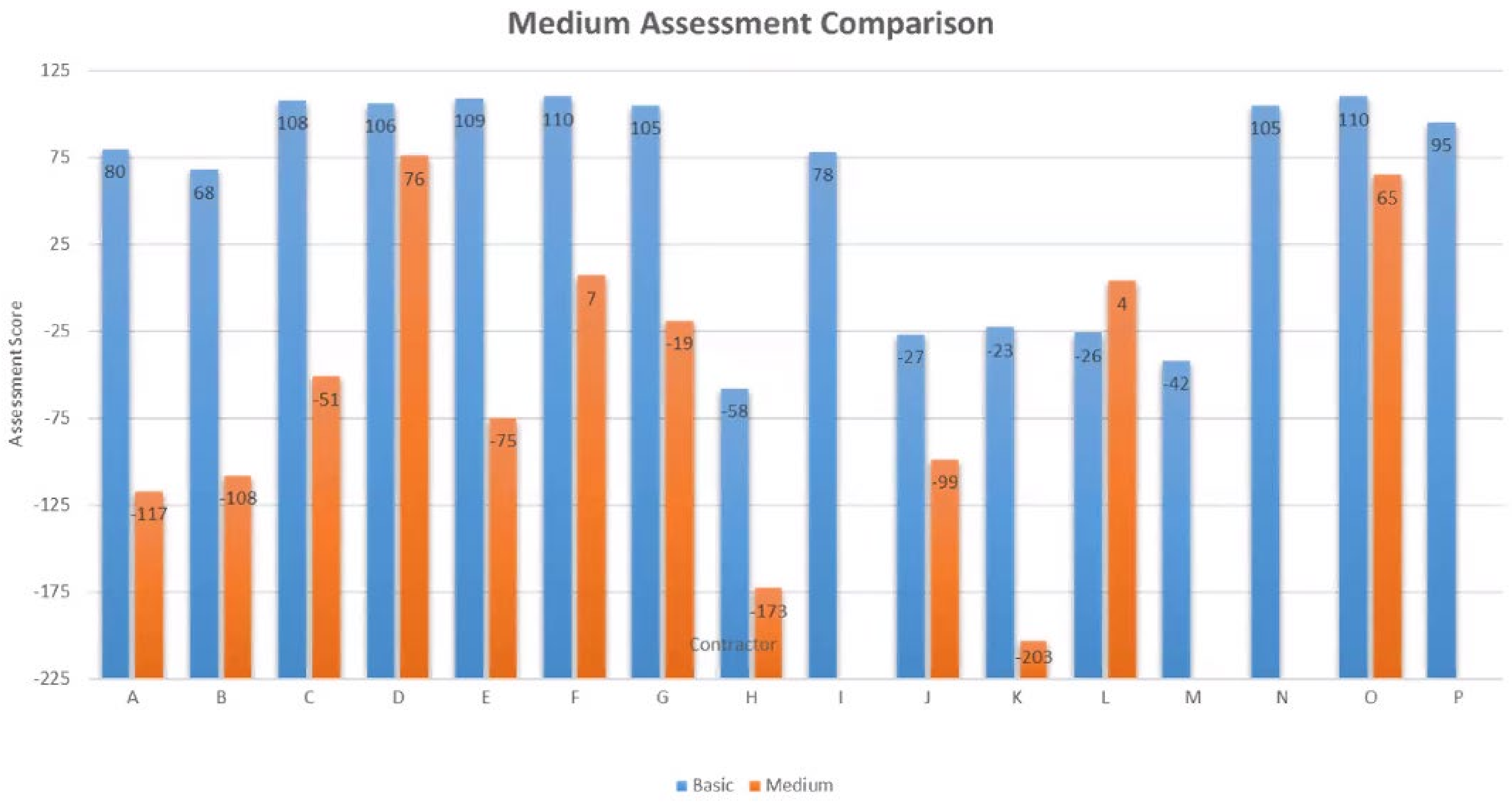
DCMA
DEFENSE CONTRACT MANAGEMENT AGENCY

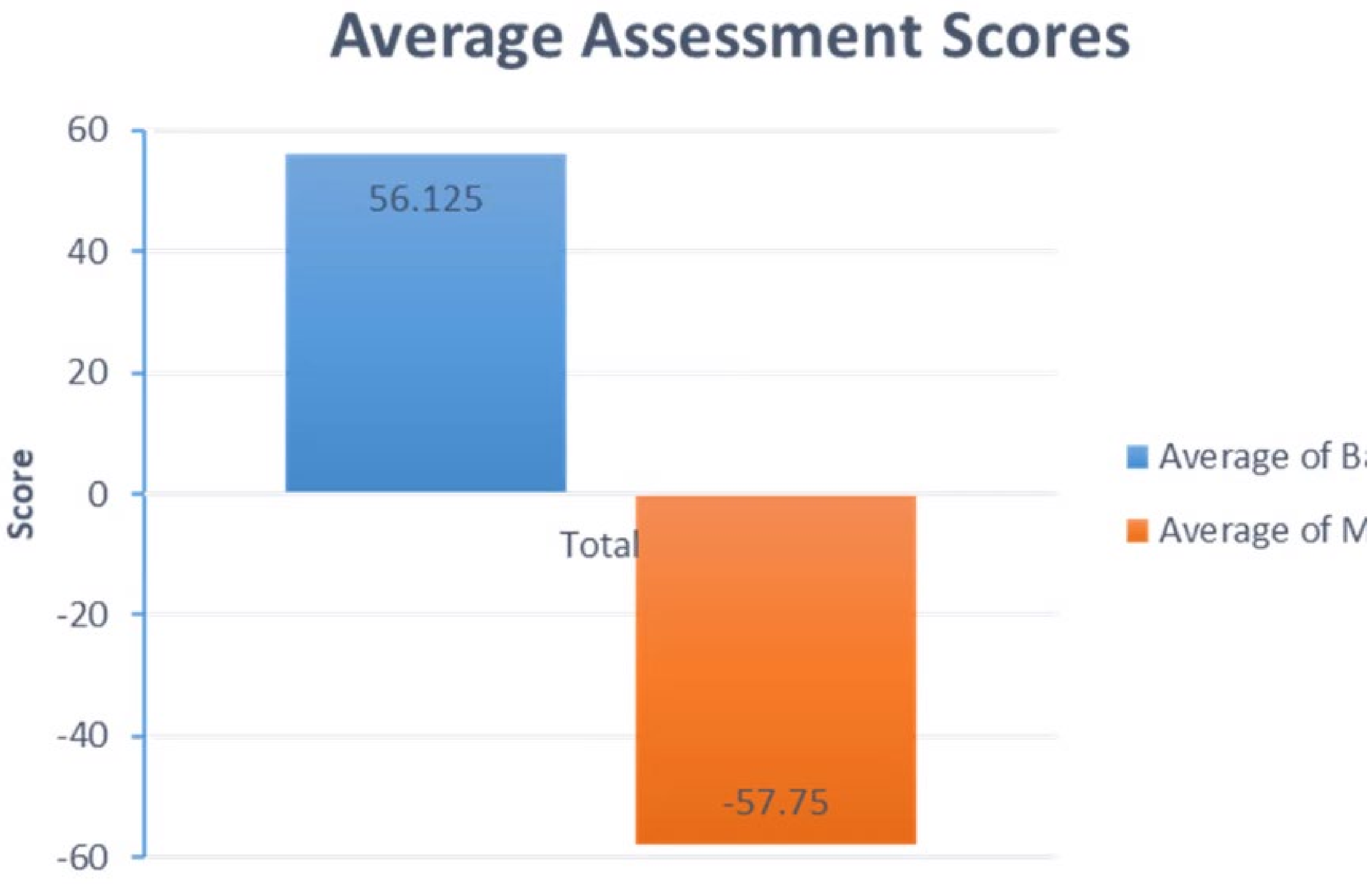
Top 10 OTS Requirements

1) **3.13.11**, *FIPS-validated cryptography* [Systems and Communication Protection (SC)]
2) **3.5.3**, *Multifactor Authentication* [Identification and Authentication (IA)]
3) **3.14.1**, *Identify, report, correct system flaws* [System and Information Integrity (SI)]
4) **3.11.1**, *Periodically assess risk* [Risk Assessment (RA)]
5) **3.11.2**, *Scan for vulnerabilities* [Risk Assessment (RA)]
6) **3.3.3,** *Review and update logged events* [Audit and Accountability (AU)]
7) **3.3.4,** *Audit logging process failure alerts* [Audit and Accountability (AU)]
8) **3.3.5,** *Audit record review, analysis, and reporting processes* [Audit and Accountability (AU)]
9) **3.6.3,** *Test incident response capability* [Incident Response (IR)]
10) **3.4.1,** *Establish/maintain baseline configuration* [Configuration Management (CM)]

Distribution Statement A: Approved for public release. Distribution is unlimited.

Medium Assessment Study Scores




Average Assessment Scores
60
40
20
0
-20
-40
-60
Score
56.125
Total
-57.75
Average of B
Average of M

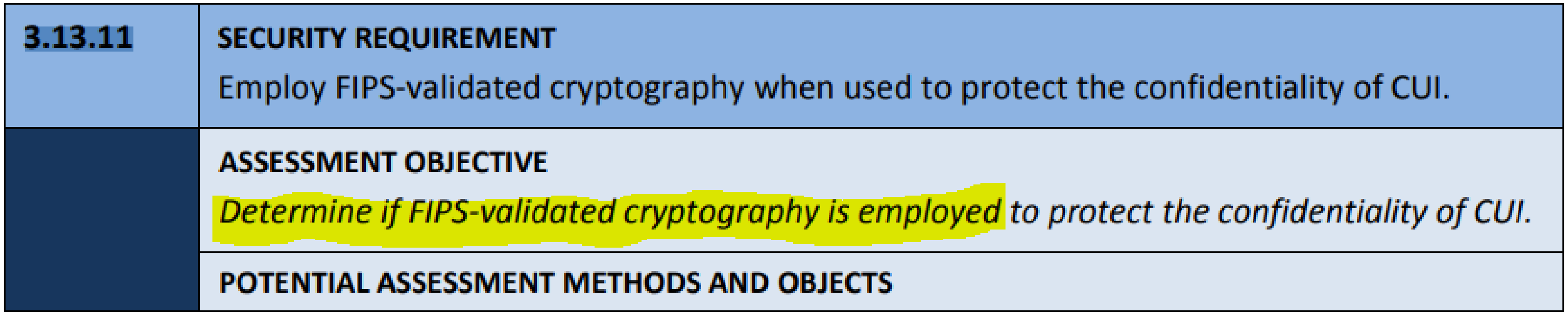
Top 3 audit deficiencies

- Presentation approach
  - Review NIST 800-171 guidance
    - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
  - Review NIST 800-171A guidance
    - Assessing Security Requirements for Controlled Unclassified Information
  - Provide supplemental references
  - Speculate regarding potential reasons for failure/deficiencies
  - Provide practical suggestions for full compliance

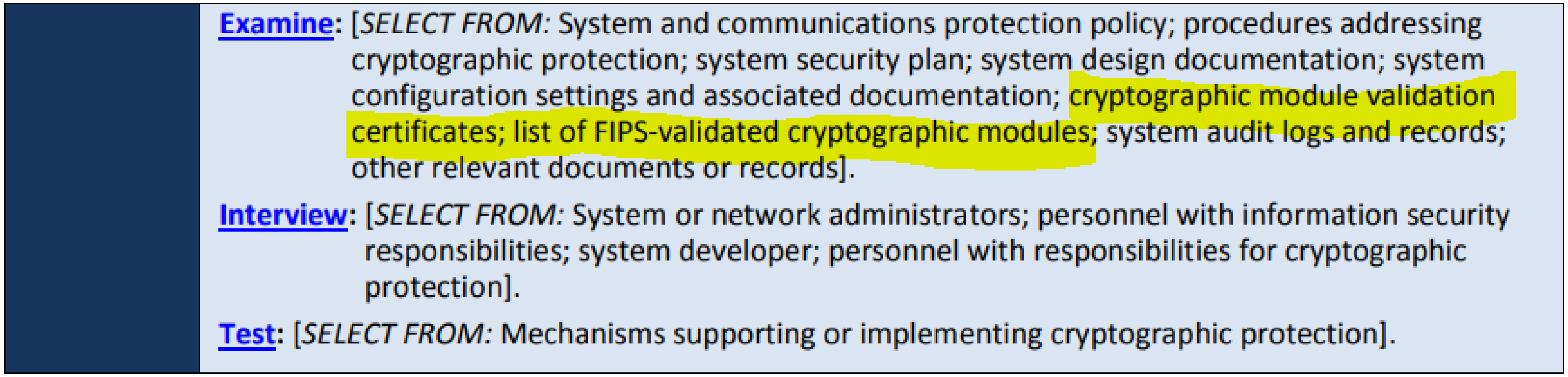
FIPS-validated cryptography (3.13.11)

- Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
- DISCUSSION
  - Cryptography can be employed to support many security solutions including the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Cryptographic standards include FIPS validated cryptography and/or NSA-approved cryptography. See the below:
  - NIST CRYPTO - National Institute of Standards and Technology (2019) Cryptographic Standards and Guidelines. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines
  - NIST CAVP - National Institute of Standards and Technology (2019) Cryptographic Algorithm Validation Program. https://csrc.nist.gov/projects/cavp
  - NIST CMVP - National Institute of Standards and Technology (2019) Cryptographic Module Validation Program. https://csrc.nist.gov/projects/cmvp

171A - FIPS-validated cryptography (3.13.11)



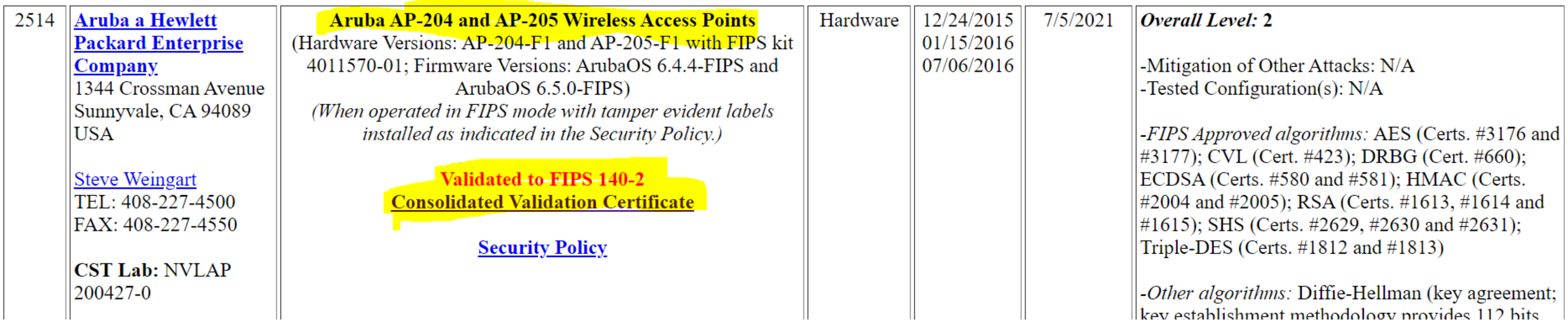
3.13.11	**SECURITY REQUIREMENT** Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
	ASSESSMENT OBJECTIVE *Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS



	Examine: [*SELECT FROM:* System and communications protection policy; procedures addressing cryptographic protection; system security plan; system design documentation; system configuration settings and associated documentation; cryptographic module validation certificates; list of FIPS-validated cryptographic modules; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer; personnel with responsibilities for cryptographic protection]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing cryptographic protection].

- How determined? Where found?

Module Validation Lists



2514	**Aruba a Hewlett Packard Enterprise Company** 1344 Crossman Avenue Sunnyvale, CA 94089 USA Steve Weingart TEL: 408-227-4500 FAX: 408-227-4550 **CST Lab:** NVLAP 200427-0	**Aruba AP-204 and AP-205 Wireless Access Points** (Hardware Versions: AP-204-F1 and AP-205-F1 with FIPS kit 4011570-01; Firmware Versions: ArubaOS 6.4.4-FIPS and ArubaOS 6.5.0-FIPS) *(When operated in FIPS mode with tamper evident labels installed as indicated in the Security Policy.)* **Validated to FIPS 140-2** **Consolidated Validation Certificate** **Security Policy**	Hardware	12/24/2015 01/15/2016 07/06/2016	7/5/2021	***Overall Level: 2*** -Mitigation of Other Attacks: N/A -Tested Configuration(s): N/A -*FIPS Approved algorithms:* AES (Certs. #3176 and #3177); CVL (Cert. #423); DRBG (Cert. #660); ECDSA (Certs. #580 and #581); HMAC (Certs. #2004 and #2005); RSA (Certs. #1613, #1614 and #1615); SHS (Certs. #2629, #2630 and #2631); Triple-DES (Certs. #1812 and #1813) -*Other algorithms:* Diffie-Hellman (key agreement; key establishment methodology provides 112 bits

- https://csrc.nist.rip/groups/STM/cmvp/validation.html

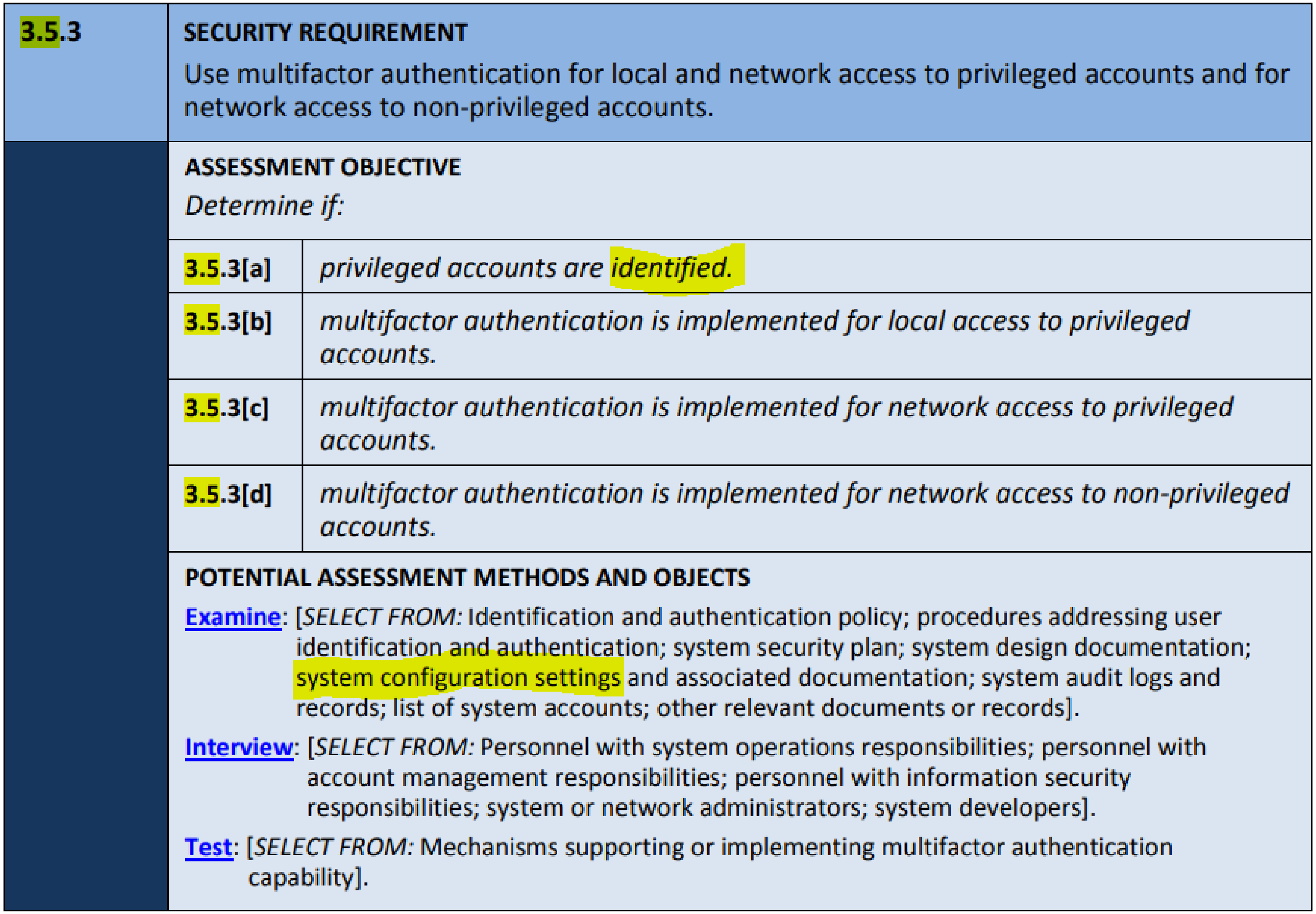
FIPS-validated cryptography (3.13.11)

- Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
- Why is this the top deficiency?
  - ❑ Understanding?
  - ❑ Cost to replace devices/software?
  - ❑ Failure to check the validation list?
  - ❑ Improper CUI scope on the network?
- Practical solutions

Multifactor authentication (3.5.3)

- Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- Discussion
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- Key Words/Concepts:
  - Factors to authenticate
  - Local access vs. network access
  - Privileged vs. non-privileged accounts

171A - Multifactor authentication (3.5.3)



3.5.3	**SECURITY REQUIREMENT** Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.5.3[a]	*privileged accounts are identified.*
	3.5.3[b]	*multifactor authentication is implemented for local access to privileged accounts.*
	3.5.3[c]	*multifactor authentication is implemented for network access to privileged accounts.*
	3.5.3[d]	*multifactor authentication is implemented for network access to non-privileged accounts.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; list of system accounts; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with system operations responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. Test: [*SELECT FROM:* Mechanisms supporting or implementing multifactor authentication capability].	

PURDUE
UNIVERSITY

Manufacturing
Extension Partnership

Multifactor authentication (3.5.3)

- Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- Why is this the 2nd highest deficiency?
  - ❑ Understanding regarding when MFA is required?
  - ❑ Cost to purchase MFA tools?
    - Free trials, focus on most at risk network access
- Practical solutions

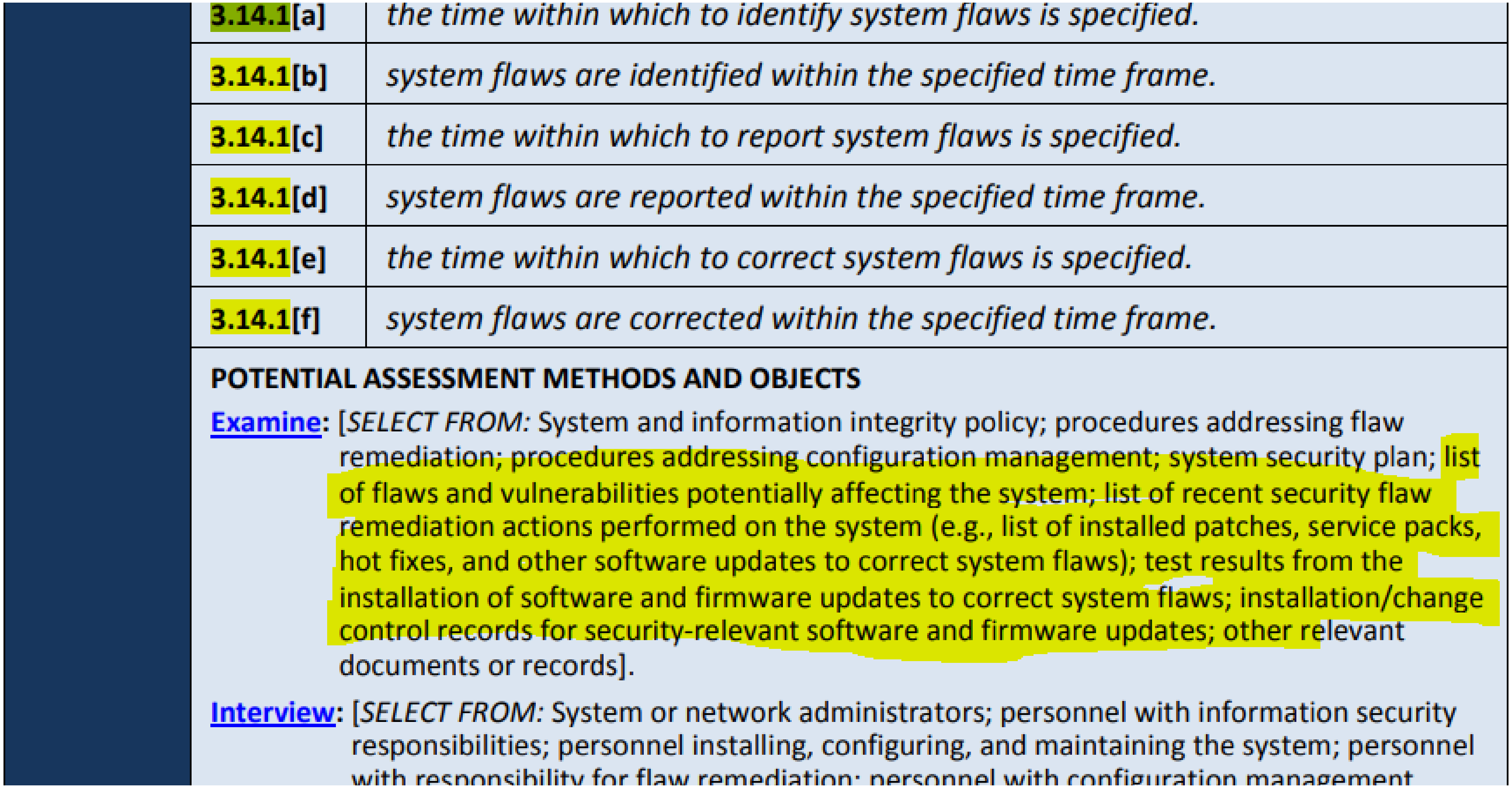
Documentation of system flaws (3.14.1)

- Identify, report, and correct system flaws in a timely manner.
- Discussion:
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- Key words/concepts:
  - patches, service packs, hot fixes, and anti-virus signatures

Documentation of System Flaws – Supplemental Information

- Common Weakness Enumeration (CWE) database https://cwe.mitre.org/
- Common Vulnerabilities and Exposures (CVE) database https://www.cve.org/
- SP 800-40 rev 4 provides guidance on patch management technologies.
  - https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

171A - Documentation of system flaws (3.14.1)



3.14.1[a]	*the time within which to identify system flaws is specified.*
3.14.1[b]	*system flaws are identified within the specified time frame.*
3.14.1[c]	*the time within which to report system flaws is specified.*
3.14.1[d]	*system flaws are reported within the specified time frame.*
3.14.1[e]	*the time within which to correct system flaws is specified.*
3.14.1[f]	*system flaws are corrected within the specified time frame.*

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine: [*SELECT FROM:* System and information integrity policy; procedures addressing flaw remediation; procedures addressing configuration management; system security plan; list of flaws and vulnerabilities potentially affecting the system; list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct system flaws); test results from the installation of software and firmware updates to correct system flaws; installation/change control records for security-relevant software and firmware updates; other relevant documents or records].

Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for flaw remediation; personnel with configuration management

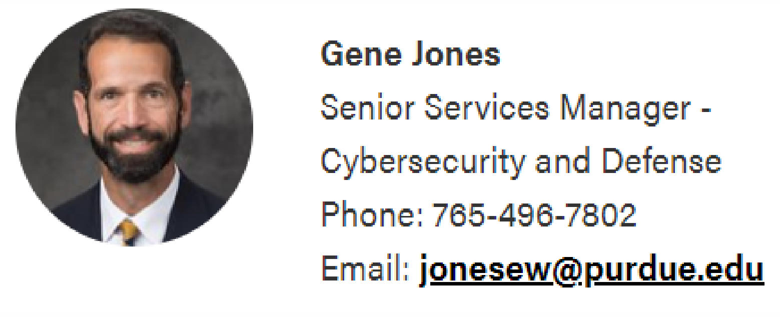
Documentation of system flaws (3.14.1)

- Identify, report, and correct system flaws in a timely manner.
- Why is this the 3rd highest deficiency?
  - Understanding patch management procedures?
  - Cost to purchase a ticketing system?
  - Failure to document the problems and corrections in the ticketing system?
- Practical solutions

Summary

- Be as rigorous as possible in your basic assessments.
- Common characteristics in the top 3 audit deficiencies
- Get the help that you need, sooner rather than later.
- Last reminder –
    - ❑ Your contract/prime contractor requirements can change instantaneously, but your business can't complete all NIST 800-171 requirements as fast.

CONTACT INFORMATION & UPCOMING EVENTS



Gene Jones
Senior Services Manager -
Cybersecurity and Defense
Phone: 765-496-7802
Email: jonesew@purdue.edu

George Bailey
Assistant Director, Cyber Services
765-494-7538
baileyga@purdue.edu

References

- **Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)** https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of
- **Supplier Performance Risk System (SPRS)** https://www.sprs.csd.disa.mil/default.htm https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf
- **NIST SP 800-171 DoD Assessment Methodology, Version 1.2.** DoD Procurement Toolbox
- **Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations** **https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final**
- **Office of the Under Secretary of Defense for Acquisition and Sustainment – CMMC** **https://www.acq.osd.mil/cmmc/index.html**
- **CMMC Accreditation Body** CyberAB > Home
- **DoD CUI Program** https://www.dodcui.mil/