fissea

Federal Information Systems Security Educators' Association

AWARENESS • TRAINING • EDUCATION

Meaningful Training? Federal or a Private Sector approach?

Dr. Luis O. Noguerol

President & CEO Advanced Division of Informatics & Technology, Inc.

ISSO NOAA Fisheries, USA DC South-East Region

ADiT USA Advanced Division of Informatics & Technology

HACKING21.com

Why Cybersecurity training is relevant in Federal Government?

“Federal information is an asset of the Nation, not of a particular federal agency or its subordinate organizations” NIST 800-37, Rev. 1, Page D-3

Why Cybersecurity training is relevant in the Private Sector?

- **New business opportunities and market trends – “Users on mind’” approach.**
- **Multiple regulations on place (PCI, HIPPA, SOX) and flexibility to adopt the most convenient framework**
- **Strong competition**
- **Sense of ownership**
- **Flexibility to allocate funds for cybersecurity training**
- **Willing to pay more for a better qualified work force**

Revision of Existing Controls **SP 800s - Computer Security** (NIST 800-53, Rev. 4)

Control Family: Awareness and Training (4 Controls and 6 Controls Enhancements)

AT-01 - Security Awareness and Training Policy and Procedures

The organization develops and formally documents security awareness and training policy (SATP); SATP consider purpose; scope; roles and responsibilities; disseminates formal documented SATP including contractors/sub-contractors; defines the frequency of the SATP.

AT-02 - Security Awareness

- All new employees are required to attend the New Employee Orientation Briefing on IT Security. In addition, they are required to complete the web-based security training course **within 3 days of entrance on duty**.
- IT security training **above** the awareness level shall be provided to personnel who manage, design, implement or maintain systems.
- Management shall ensure that all network and **system administrators** having responsibility for performing installation, configuration and maintenance of systems and networks are identified and receive **appropriate training in systems security**. **Because of time and resources**, levels and type of **training in systems security will be determined by each System Owner.**

Revision of Existing Controls (NIST 800-53, Rev. 4) - 2

AT-02(1) - Security Awareness

Practical exercises in security awareness training that simulate actual cyber attacks.

AT-02(2) - Insider Threat

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

AT-03 - Security Training

- **The organization provides role-based security-related training before authorizing access to the system or performing assigned duties, and when required by system changes.**
- **The organization defines the frequency of refresher role-based security-related training.**
- **The organization provides refresher role-based security-related training in accordance with the organization-defined frequency.**

Revision of Existing Controls (NIST 800-53, Rev. 4) - 3

AT-03(1) - Security Training (Environmental Control)

- The organization provides employees with initial training in the employment and **operation of environment controls**.
- The organization defines the frequency of refresher training in the employment and operation of **environmental controls**.
- The organization provides refresher training in the employment and operation of **environmental controls** in accordance with the organization-defined frequency.

AT-03(2) - Security Training (Physical security controls)

- The organization provides employees with initial training in the employment and operation of **physical security controls**.
- The organization defines the frequency of refresher training in the employment and operation of **physical security controls**.
- The organization provides refresher training in the employment and operation of **physical security controls** in accordance with the organization-defined frequency

Revision of Existing Controls (NIST 800-53, Rev. 4) - 4

AT-03(3) - Practical Exercises, (Scenarios' Based)

- The organization includes practical exercises in security training that reinforce training objectives.

AT-03(4) - Suspicious Communications And Anomalous System Behavior

- The organization defines indicators of malicious code.
- The organization provides training to its personnel on organization-defined indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems.

AT-04 - Security Training Records (a)

- The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

Revision of Existing Controls (NIST 800-53, Rev. 4) - 5

AT-04 - Security Training Records (b)

- The organization defines the time period for retaining individual training records.
- The organization retains individual training records in accordance with the organization-defined time period.

AT-05 - Contacts with Security Groups and Associations (withdrawn from AT)

The organization establishes and ***institutionalizes*** contact with selected groups and associations within the security community to:

a) facilitate ongoing security education and training for organizational personnel

b) stay up to date with the latest recommended security practices, techniques, and technologies

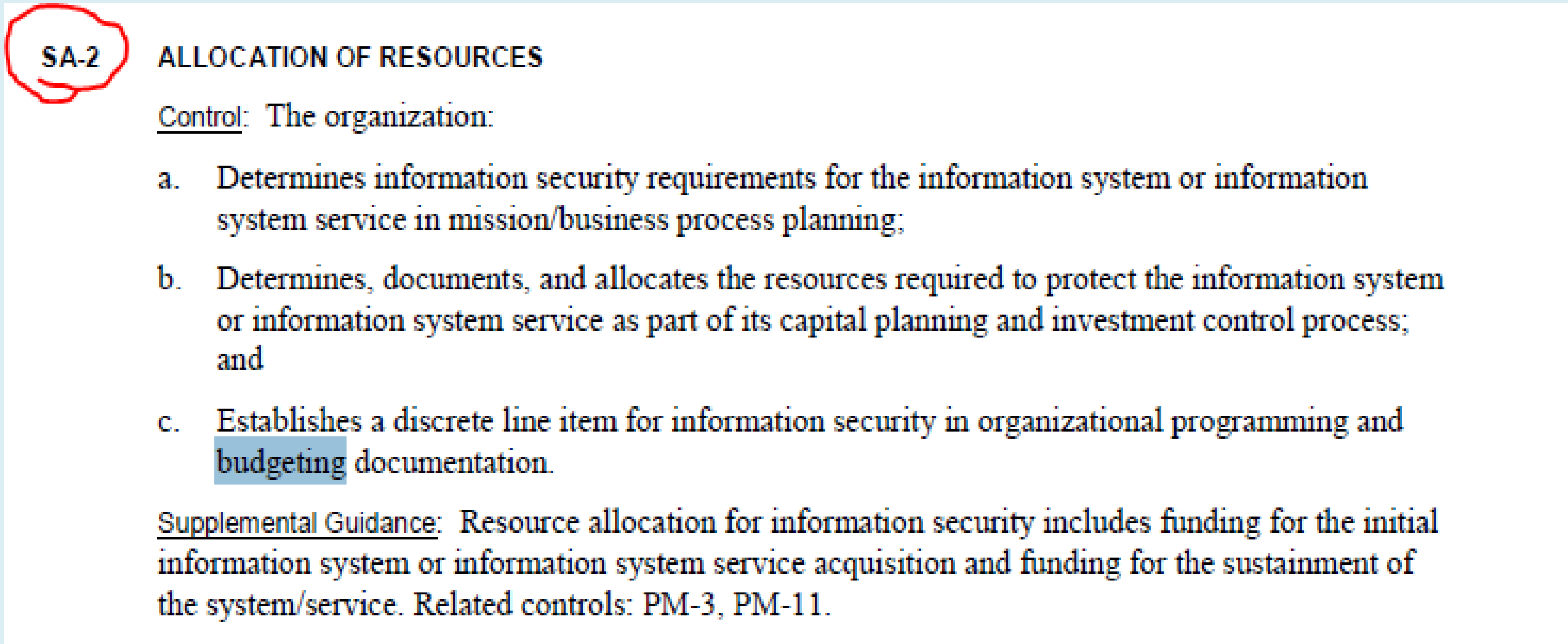
c) share current security-related information including threats, vulnerabilities, and incidents.

Disputable considerations in Federal approach - 1

- Redundant Controls – AT-02(**1**); AT-02(**2**)...
- Reactive approach – “...**within 3 days** of entrance on duty”
- Confusing language – “...**above** the awareness level shall be provided to personnel who manage...”
- Unclear definitions – “... system administrators ... receive **appropriate** training in systems security...”
- Subliminal suggestions – “***Because of time and resources***, levels and type of training in systems security **will be determined by each System Owner**
- “Unique,” complex, and unpractical security Framework
- Minimum consequences – personnel’ “pampering”
- Lack of incentives and professional growth
- **Budget** – **never** used in this control

Disputable considerations in Federal approach - 2

SA- System and Services Acquisition – **Budget**



SA-2 **ALLOCATION OF RESOURCES**

Control: The organization:

a. Determines information security requirements for the information system or information system service in mission/business process planning;

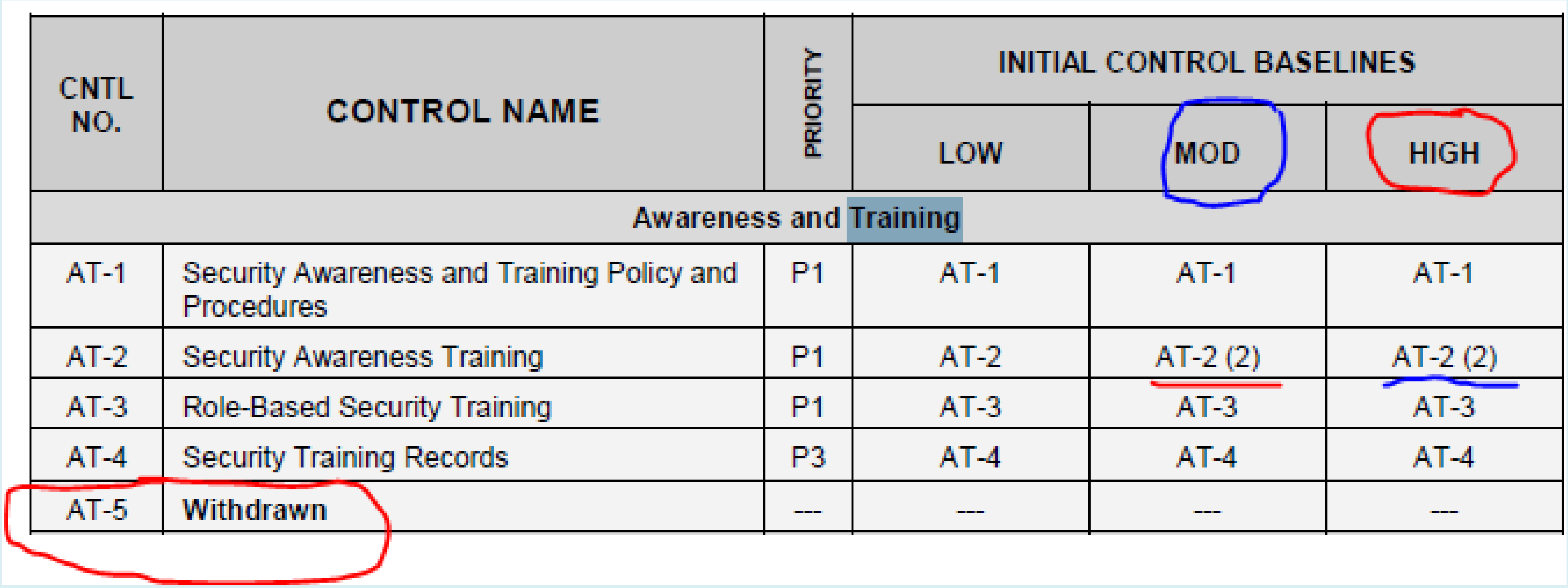
b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Supplemental Guidance: Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service. Related controls: PM-3, PM-11.

Disputable considerations in Federal approach - 3

Differentiated training - depending of Information System Classification – **cost factor/administrative burden**?



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	**Withdrawn**	---	---	---	---

From: NIST SP 800-53 Revision 4, Page D-3

Disputable considerations in Federal approach - 4

Lack of enforcement – only other 3 controls “enforced”

a) **Contingency Planning,** (CP-3): Contingency Training

a) **Incident Response,** (IR-2): Incident Response Training

a) **System and Services Acquisition,** (SA-16): Developer-Provided Training

Disputable considerations in Federal approach - 5

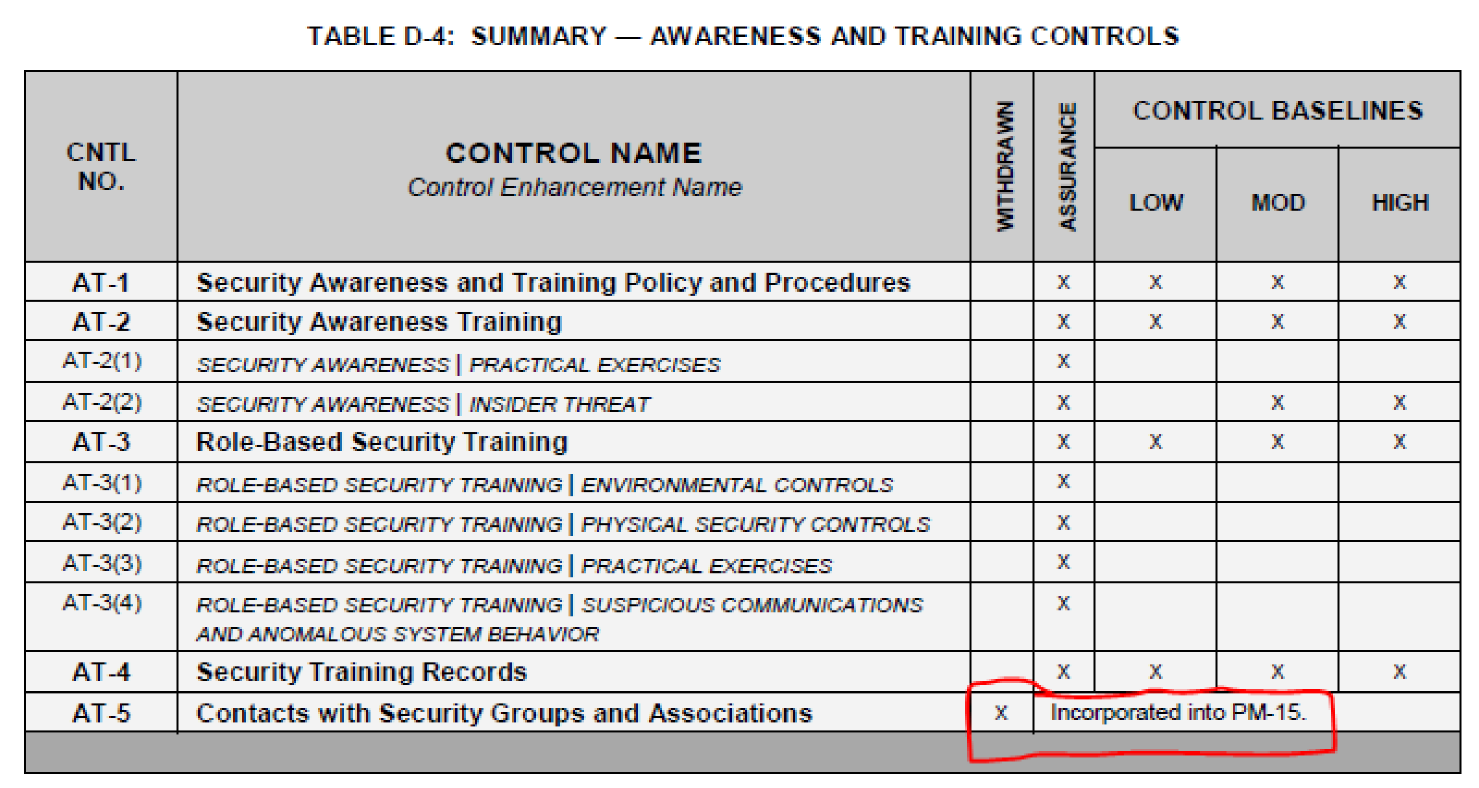


TABLE D-4: SUMMARY — AWARENESS AND TRAINING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AT-1	**Security Awareness and Training Policy and Procedures**		x	x	x	x
AT-2	**Security Awareness Training**		x	x	x	x
AT-2(1)	*SECURITY AWARENESS | PRACTICAL EXERCISES*		x			
AT-2(2)	*SECURITY AWARENESS | INSIDER THREAT*		x		x	x
AT-3	**Role-Based Security Training**		x	x	x	x
AT-3(1)	*ROLE-BASED SECURITY TRAINING | ENVIRONMENTAL CONTROLS*		x			
AT-3(2)	*ROLE-BASED SECURITY TRAINING | PHYSICAL SECURITY CONTROLS*		x			
AT-3(3)	*ROLE-BASED SECURITY TRAINING | PRACTICAL EXERCISES*		x			
AT-3(4)	*ROLE-BASED SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR*		x			
AT-4	**Security Training Records**		x	x	x	x
AT-5	**Contacts with Security Groups and Associations**	x	Incorporated into PM-15.			

From: NIST SP 800-53 Revision 4, Page D-14

PM Family – Program Management **“hanging”**

Advanced Division of Informatics & Technology HACKING21.com

Electronic “Pearl Harbor”

- OBM Circular A-76 (Revised on May 29, 2003), recognized that federal agencies may be as or more efficient and effective as private sector organizations.
- From 2009 – 2013, the number of data breaches in the Federal Government went from 26,942 to 46,605 (only published)
- **21% all federal information security breaches in 2013 were traced to government workers who lacks of appropriate training**
- $10 billion was spent by the Federal Government in 2014 as effort to protect “privilege” information, but the Associated Press publish a report in which assert at least **50% of federal data breaches this year were caused by federal personnel**
- The Global Information Security Workforce estimated an increase of 13% each year, (after 2017), for highly qualified personnel in Cybersecurity.
- McKinsey forecast over 150,000 untaken positions in Cybersecurity by 2018 because lack preparation and specialization
-
- TrendMicro consider that Cybersecurity professions will be growing 12 times faster than the whole job market by 2018.
- 70 percent of the professional workforce will conduct their work on personal smart devices by 2018
- Cybercriminal underworld is becoming well-organized and the reasons are multiple and details unknown
- USA Federal Government is projected to spend $65 billion on cybersecurity contracts between 2015 and 2020, but the specific amount dedicated to training still under calculation

Considerations

- IT Certs, a college degree, diploma?
- Simplification of existing controls
- Practicality of existing framework (over 110 Controls as part of SP-800).
- NIST 800-**53**, Rev. 4 = 462 pages

  > PCI = 112 pages

References

- Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. NIST SP 800-37, Rev. 1. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html
- Security and Privacy Controls for Federal Information Systems and Organizations. NIST SP 800-53, Rev. 4. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html
- Building an Information Technology Security Awareness and Training Program**.** NIST Special Publications 800-50, (2003), Retrieved from http://csrc.nist.gov/publications/PubsSPs.html
- IT Security and Privacy, retrieved from http://ocio.os.doc.gov/ITPolicyandPrograms/Policy___Standards/DEV01_002681
- Cybersecurity talent shortage matter of economic and national security, retrieved from http://host.madison.com/business/tom-still-cybersecurity-talent-shortage-matter-of-economic-and-national/article_2af553b5-4610-537e-a374-5542f15ff51.html
- The challenges of cyber security education and training in 2015, TrendMicro. Retrieved from http://blog.trendmicro.com/the-challenges-of-cyber-security-education-and-training-in-2015/
- Mobile Devices to Surpass the Number of People on Earth – Infographic. Retrieved from http://aci.info/2014/05/03/mobile-devices-to-surpass-the-number-of-people-on-earth-infographic/
- Taking a more organized approach to cyber security. Retrieved from http://blog.trendmicro.com/taking-a-more-organized-approach-to-cyber-security/
- Cybersecurity trumps terrorism as No. 1 threat; feds struggle to keep up with attacks. Retrieved from http://www.pennlive.com/nation-world/2014/11/cybersecurity_trumps_terrorism.html
- US government increases attention on cyber security. Retrieved from http://blog.trendmicro.com/us-government-increases-attention-cyber-security/
- CIRCULAR NO. A-76 REVISED. Retrieved from https://www.whitehouse.gov/omb/circulars_a076_a76_incl_tech_correction/