Sneak Peak at CIS Critical Security Controls V 7

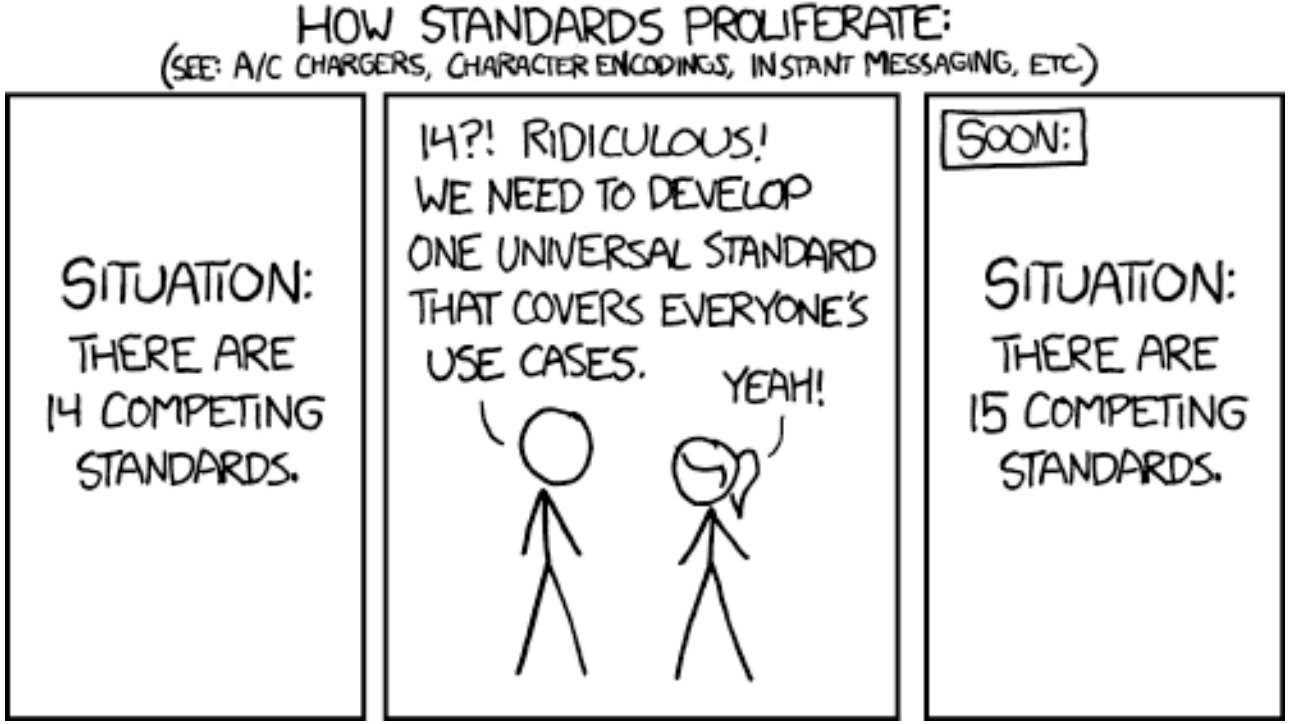
Release Date: March 2018

Presented by **Kelli Tarala**

Principal Consultant Enclave Security

AuditScripts

2 Standards and Frameworks



Information Assurance Frameworks

- There are a number of industry groups trying to address the issues
- Numerous frameworks have been established, such as:
  - NIST 800-53
  - NIST Cybersecurity Framework
  - ISO 27000 Series
  - CoBIT
  - IT Assurance Framework (ITAF)
  - IT Baseline Protection Manual
  - Consensus Audit Guidelines / Critical Security Controls
  - Many, many others

Enter the CIS Critical Security Controls

- Official home of the Critical Security Controls
- Not for Profit group responsible for managing the Critical Security Controls
- Utilizes a volunteer army of contributors for each of their projects
- Responsible for maintaining community efforts such as:
  - Security benchmarks
  - Security metrics
  - Critical Security Controls
  - Managing the MS-ISAC

5 Document Contributors

International Contributors Include:

- UK Government Communications Headquarters (GCHQ)
- UK Centre for the Protection of National Infrastructure (CPNI)
- Australian Defence Signals Directorate (DSD)
- Japanese Security Researchers
- Scandinavian Security Researchers
- GCC Security Researchers
- Turkish Security Researchers
- Canadian Security Researchers
- Many other international researchers

US Contributors Include:

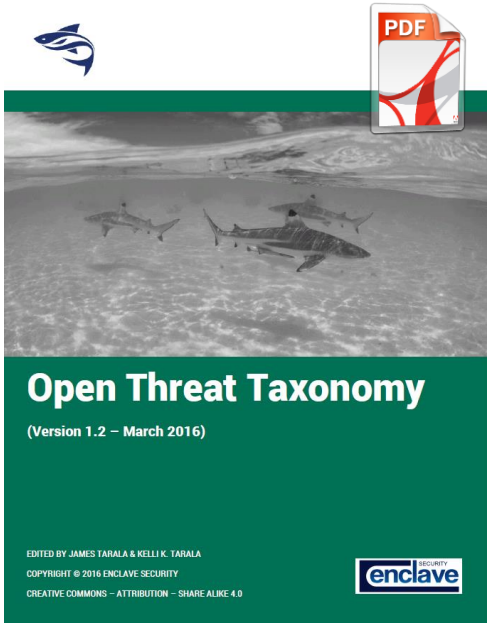
- Department of Homeland Security (DHS)
- National Security Agency (NSA)
- Department of Energy (DoE) Laboratories
- Department of State (DoS)
- US-CERT and other incident response teams
- DoD Cyber Crime Center (DC3)
- The Federal Reserve
- The SANS Institute
- Civilian penetration testers
- Numerous other Federal CIOs and CISOs
- Hundreds of other private sector researchers

CSCs are Based on Known Threats

- The CSCs are based on current, observable threats to information systems, not theories
- Hundreds of organizations have contributed

- One of the latest efforts is the release of a community threat model, the Open Threat Taxonomy (v1.1), which will be used to document and prioritize threats

- OTT will be used to define threats to define controls
- Will help standardize risk assessments, make one less paperwork step for organizations to complete



Project Guiding Principles

1. Defenses should focus on addressing the attack activities occurring today,
2. Enterprise must ensure consistent controls across to effectively negate attacks
3. Defenses should be automated where possible
4. Specific technical activities should be undertaken to produce a more consistent defense
5. Root cause problems must be fixed in order to ensure the prevention or timely detection of attacks
6. Metrics should be established that facilitate common ground for measuring the effectiveness of security measures

Key Principles for Version 7

1. Improve the consistency and simplify the wording of each sub-control
2. Implement “one ask” per sub-control
3. Bring more focus on authentication, encryption and application whitelisting
4. Account for improvements in security technology, and emerging security problems
5. Better alignment with other frameworks (e.g., the NIST CSF)
6. Support for the development of related products (e.g. measurements/metrics, implementation guides)

9 The Critical Security Controls (v6.1)

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training To Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

10 The Critical Security Controls (v7)

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Controlled Use of Administrative Privileges
4. Continuous Vulnerability Assessment and Remediation
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs
7. Email and Web Browser Protections

Malware Defenses

8. Limitation and Control of Network Ports, Protocols, and Services
9. Data Recovery Capabilities

AuditScripts

11 The Critical Security Controls 11- 16 (v 7)

11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training To Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training To Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Critical Security Control #1
Inventory of Authorized and Unauthorized Devices

1.1 Maintain Detailed Asset Inventory

1.2 Asset Inventory Information

1.3 Active Discovery Tool

1.4 Passive Asset Discovery

1.5 DHCP Logging

1.6 Address unauthorized assets

1.7 Deploy network level authentication

1.8 Client certificates

Critical Security Control #2
Inventory of Authorized and Unauthorized Software

2.1 Inventory of Authorized Software
2.2 Software Inventory Information
2.3 Software Inventory tools
2.4 Software inventory integration
2.5 Software Supported by Vendor
2.6 Address unapproved software
2.7 Application Whitelisting
2.8 Application Whitelisting of Libraries
2.9 Application Whitelisting of Scripts
2.10 Air gap high risk applications

Critical Security Control #2: Inventory of Authorized and Unauthorized Software

2.8 Application Whitelisting of Libraries

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.

2.9 Application Whitelisting of Scripts

The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.

Critical Security Control #3 (5)
Secure Configurations for Hardware and Software

3.1 Establish secure configurations

3.2 Implement automated configuration monitoring systems

3.3 Maintain secure images

3.4 Securely store master images

3.5 Deploy system configuration management tools

Critical Security Control #4
Continuous Vulnerability Assessment and Remediation

4.1 Run automated vulnerability scanning tools

4.2 Perform Authenticated Vulnerability Scanning

4.3 Protect dedicated assessment accounts

4.4 Compare back-to-back vulnerability scans

4.5 Utilize a risk-rating process

4.6 Deploy Automated Operating System Patch Management Tools

4.7 Deploy Automated Software Patch Management Tools

Critical Security Control #5 (3)
Controlled Use of Administrative Privileges

5.1 Inventory Administrative Accounts

5.2 Ensure the Use of Dedicated Administrative Accounts

5.3 Change Default Passwords

5.4 Use unique passwords

5.5 Log and Alert on Changes to Administrative Group Membership

5.6 Log and Alert on Unsuccessful Administrative Account Login

5.7 Use multifactor authentication for all administrative access

5.8 Use of dedicated machines for all administrative tasks

Critical Security Control #6
Maintenance, Monitoring, and Analysis of Audit Logs

6.1 Utilize two synchronized time sources

6.2 Activate audit logging

6.3 Enable Detailed Logging

6.4 Central Log Management

6.5 Ensure adequate storage for logs

6.6 Regularly Review Logs

6.7 Deploy a SIEM

6.8 Regularly Tune SIEM

Critical Security Control #7
Email and Browser Protections

7.1 Ensure Use of Only Full Supported Browsers and Email Clients

7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins

7.3 Limit use of scripting languages in web browsers and email clients

7.4 Deploy separate browser configurations to each system

7.5 Implement DMARC and Enable Receiver-Side Verification

7.6 Maintain and Enforce Network-Based URL Filters

7.7 Subscribe to URL-Categorization service

7.8 Log all URL requests

7.9 Block Unnecessary File Types

7.10 Sandbox All Email Attachments

Critical Security Control #8
Malware Defenses

8.1 Centrally managed anti-malware

8.2 Ensure Anti-Malware Software and Signatures are Updated

8.3 Centralize Anti-malware Logging

8.4 Configure Devices Not To Auto-run Content

8.5 Configure Anti-Malware Scanning of Removable Devices

8.6 Enable Operating System Anti-Exploitation Features

8.7 Enable DNS query logging

8.8 Ensure the use of the latest version of Windows PowerShell

Critical Security Control #9
Limitation and Control of Network Ports, Protocols, and Services

9.1 Associate Active Ports, Services and Protocols to Asset Inventory

9.2 Ensure only approved ports, protocols and services are running

9.3 Apply host-based firewalls or port filtering

9.4 Perform automated port scans on a regular basis

9.5 Operate critical services on separate hosts

9.6 Place Application Firewalls

Critical Security Control #10
Data Recovery Capability

10.1 Ensure regular automated backups

10.2 Perform complete system backups

10.3 Test data on backup media

10.4 Ensure protection of backups

10.5 Ensure Backups Have At least One Non-Continuously Addressable Destination

Critical Security Control #11
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

11.1 Install the latest stable version of any security-related updates on all network devices

11.2 Maintain standard security configurations for network devices

11.3 Document traffic configuration rules

11.4 Use automated tools to verify standard device configurations and detect changes

11.5 Manage network devices using Multi-Factor Authentication and encrypted Sessions

11.6 Use dedicated Machines for all network administrative tasks

11.7 Manage network infrastructure through separate network from business

Critical Security Control #12
Boundary Defense

12.1	Maintain an Inventory of Network Boundaries
12.2	Scan For Unauthorized Network Boundaries
12.3	Configure Monitoring Systems to Record Network Packets
12.4	Deploy NetFlow Collection on Networking Boundary Devices
12.5	Deploy Network-based IDS Sensor
12.6	Deny communications with known malicious IP addresses
12.7	Deny Communication over unauthorized ports
12.8	Deploy Network-Based Intrusion Prevention Systems
12.9	Deploy application layer filtering proxy server
12.10	Decrypt Network Traffic at Proxy
12.11	Require all remote login to use multi-factor authentication
12.12	Manage all devices remotely logging into internal network

Critical Security Control #13
Data Protection

13.1	Identify Sensitive Information
13.2	Perform periodic scans to identify unencrypted sensitive data
13.3	Use host-based DLP
13.4	Deploy approved hard drive encryption software to mobile devices with sensitive information
13.5	Manage system's USB hard drives read/write configurations
13.6	Encrypted data on USB Storage
13.7	Managing USB Devices
13.8	Monitor and block network traffic with sensitive information
13.9	Monitor and detect any unauthorized use of encryption
13.10	Block access to known file transfer and email exfiltration websites

Critical Security Control #14
Controlled Access Based on the Need to Know

14.1	Segment the Network Based on Sensitivity
14.2	Enable Firewall Filtering Between VLANs
14.3	Enable Private Virtual Local Area Networks (VLANs)
14.4	Protect information through specific access control lists
14.5	Encrypt Sensitive Information at Rest and Require Secondary Authentication Mechanism
14.6	Encrypt All Sensitive Information in Transit
14.7	Enforce Detailed Audit Logging for Access to Sensitive Data
14.8	Remove Sensitive Data Sets or Systems Not Regularly Accessed by Organization

Critical Security Control #15
Wireless Access Control

15.1	Maintain an Inventory of Authorized Wireless Access Points
15.2	Detect wireless access points connected to the wired network
15.3	Use a Wireless Intrusion Detection System
15.4	Disable Wireless Access on Devices if Not Required
15.5	Limit wireless access on client devices
15.6	Disable peer-to-peer wireless network capabilities on wireless clients
15.7	Disable Wireless Peripheral Access of Devices
15.8	Use Wireless Authentication Protocols that require Mutual, Multi-Factor Authentication
15.9	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data
15.10	Create Separate Wireless Network for Personal and Untrusted Devices

Critical Security Control #16
Account Monitoring and Control

16.1 Inventory of Authentication Systems
16.2 Configure Centralized Point of Authentication
16.3 Inventory of Accounts
16.4 Disable any unassociated accounts
16.5 Establish process for revoking access
16.6 Ensure all accounts have expiration date that is monitored and enforced
16.7 Require multi-factor authentication
16.8 Encrypted transmittal of username and authentication credentials
16.9 Protect access to authentication files
16.10 Monitor attempts to access deactivated accounts
16.11 Disable Dormant Accounts
16.12 Monitor the use of all accounts
16.13 Profile user's typical account usage
16.14 Enforce long password use for systems not supported by multi-factor authentication
16.15 Configure account lockouts

The Critical Security Controls 17-20 (v 7)

17. Security Skills Assessment and Appropriate Training To Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

More Companion Guide to the Controls

- Governance Controls (v6.0)
- Critical Security Controls Measures and Metrics (v7.0a)
- Many more

Critical Governance Controls

- The Critical Security Controls also define 15 categories of governance controls to complement the technical recommendations

- Version 6.0 is the first publication of these supporting controls (2015)
- Documented in Appendix E of the CSCs

- Even though these controls are not discussed, that does not mean they are not important to your organization

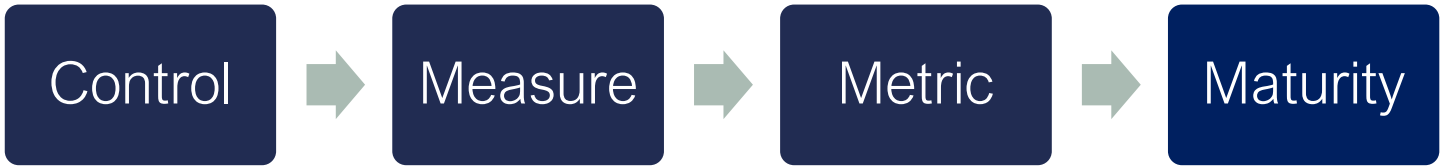
32 Critical Governance Controls (2)

- Executive Sponsorship
- Information Assurance Program Management
- Information Assurance Policies and Standards Management
- Data Classification
- Risk Management
- Compliance and Legal Management
- Security Awareness and Education
- Audit and Assessment Management
- Personnel and Human Resources Management
- Budgets and Resource Management
- Physical Security
- Incident Response Management
- Business Continuity and Disaster Recovery Management
- Procurement and Vendor Management
- Change and Configuration Management

Metrics, Measures, and Maturity Levels: Companion Guide

CIS Critical Security Controls Measures and Metrics (v7.0a)									
			Sigma Maturity Levels						
Title	Description	Measure	Sigma Level Zero	Sigma Level One	Sigma Level Two	Sigma Level Three	Sigma Level Four	Sigma Level Five	Sigma Level Six
Maintain detailed asset inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory	What percentage of the organization's hardware assets are not presently included in the organization's asset	Greater than 69%	69% or Less	31% or Less	6.7% or Less	0.023% or Less	0.00034% or Less	0.0000019 % or Less

Controls, Measures, Metrics, Maturity



Controls, Measures, Metrics Example

Maintain detailed asset inventory

What percentage of the organization's hardware assets are not presently included in the organization's asset inventory?

Sigma Level Zero	Sigma Level One	Sigma Level Two	Sigma Level Three	Sigma Level Four	Sigma Level Five	Sigma Level Six
Greater than 69%	69% or Less	31% or Less	6.7% or Less	0.023% or Less	0.00034% or Less	0.0000019 % or Less

An “On Ramp” to Maturity

- The primary goal of the Critical Security Controls is defense
- However, by prioritizing these controls, an organization is also making steps towards achieving compliance with other standards & regulations
- Mappings currently exist between the CSCs and:
  - NIST 800-53 rev4
  - ISO 27002 Control Catalog
  - NIST Cybersecurity Framework
  - HIPAA / HITECH Act

Invitation to Comment on the Controls

Public Review is open from **January 22 through February 5.**

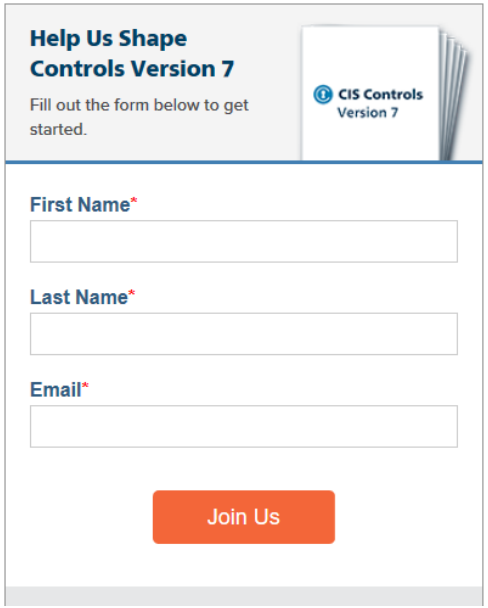
CIS Controls

Call for Feedback: CIS Controls Version 7

Central to CIS' commitment to you is that our cyberdefense best-practices work will remain relevant and effective in an ever-changing landscape of technology, business demands, and attacker tradecraft. Therefore, we have started the process of updating the CIS Controls from Version 6.1 to 7.

Be Part of the Process

The CIS Controls have always been the product of a world-wide community of adopters, vendors, and supporters, and V7 will be no exception. Your challenges, priorities, and feedback are essential to this work.



Launch Date: March 19 2018

Stay Tuned at

https://learn.cisecurity.org/ciscontrols7-cfp

In Summary

- Regardless if you follow the Critical Security Controls, each organization needs a strategy for defense
- Be aware of the changing threat landscape and have a plan for preventing future attacks
- Organizations need to set priorities for system and data defense, this is one good option
- Most importantly, the controls are only useful if they are implemented
- Watch for more changes to come & stay vigilant

Further Questions

- Kelli Tarala
  - E-mail: Kelli.Tarala@enclavesecurity.com
  - Twitter: @KelliTarala
  - Blog: http://www.auditscripts.com/

- Resources for further study:
  - The Critical Security Controls Courses – SEC 440 / 566
  - AuditScripts.com Resources