

NAS9933

Critical Security Controls for Effective Capability in Cyber Defense

Standard Practice

THIRD ANGLE PROJECTION	CUSTODIAN CYBER SECURITY COMMITTEE	REVISION NEW
PROCUREMENT SPECIFICATION NONE	TITLE CRITICAL SECURITY CONTROLS FOR EFFECTIVE CAPABILITY IN CYBER DEFENSE	CLASSIFICATION STANDARD PRACTICE NAS9933 SHEET 1 OF 34

USE OF OR RELIANCE UPON THIS DOCUMENT OR ANY NATIONAL AEROSPACE STANDARD IS ENTIRELY VOLUNTARY. AIA DOES NOT QUALIFY SUPPLIERS OR CERTIFY CONFORMANCE OF ITEMS PRODUCED UNDER NATIONAL AEROSPACE STANDARDS. AIA MAKES NO REPRESENTATION OR CLAIM RESPECTING (1) THE SUITABILITY OF ITEMS FOR ANY PARTICULAR APPLICATION OR (2) THE EXISTENCE OF OR APPLICABILITY THERETO OF PATENT OR TRADEMARKS RIGHTS.

TABLE OF CONTENTS

1	DEVICE INVENTORY.....	10
1.1	Guidance.....	10
2	SOFTWARE INVENTORY	11
2.1	Guidance.....	12
3	SECURE CONFIGURATIONS	12
3.1	Guidance.....	13
4	ASSESS/REMEDIATION.....	13
4.1	Guidance.....	15
5	MALWARE DEFENSES.....	15
5.1	Guidance.....	16
6	IN-HOUSE SW SECURITY.....	16
6.1	Guidance.....	17
6.2	6a. PURCHASED SW SECURITY	17
6.3	Guidance.....	18
7	WIRELESS ACCESS.....	18
7.1	Guidance.....	19
8	DATA RECOVERY	19
8.1	Guidance.....	20
9	SKILLS/TRAINING	20
9.1	Guidance.....	21
10	NETWORK DEVICES	21
10.1	Guidance.....	22
11	NETWORK CONTROLS.....	22
11.1	Guidance.....	22
12	ADMINISTRATIVE PRIVILEGES.....	23
12.1	Guidance.....	24
13	BOUNDARY DEFENSE	24
13.1	Guidance.....	25
14	AUDIT LOGS.....	26
14.1	Guidance.....	27
15	CONTROLLED ACCESS.....	27
15.1	Guidance.....	27
16	ACCOUNT MONITORING and CONTROL.....	28
16.1	Guidance.....	29
17	DATA PROTECTION.....	29
17.1	Guidance.....	30
18	INCIDENT MANAGEMENT	30

REVISION

NEW

NAS9933
SHEET 2



Document Sharing Hub

USE OF OR RELIANCE UPON THIS DOCUMENT OR ANY NATIONAL AEROSPACE STANDARD IS ENTIRELY VOLUNTARY. AIA DOES NOT QUALIFY SUPPLIERS OR CERTIFY CONFORMANCE OF ITEMS PRODUCED UNDER NATIONAL AEROSPACE STANDARDS. AIA MAKES NO REPRESENTATION OR CLAIM RESPECTING (1) THE SUITABILITY OF ITEMS FOR ANY PARTICULAR APPLICATION OR (2) THE EXISTENCE OF OR APPLICABILITY THERETO OF PATENT OR TRADEMARKS RIGHTS.

18.1	Guidance.....	31
19	SECURE NETWORK ENGINEERING	31
19.1	Guidance.....	32
20	PENETRATION TESTS.....	32
20.1	Guidance.....	33
21	GOVERNANCE.....	33
21.1	Guidance.....	33
22	MOBILE DEVICE.....	34
22.1	Guidance.....	34

TABLES

TABLE 1 – Control Activity to Capability Level Matrix	7
---	---

REVISION

NEW

NAS9933

SHEET 3



Document Sharing Hub

FOREWORD

CIS Critical Security Controls, v. 5.1. is the property of Center for Internet Security, Inc. ("CIS") and is licensed under a Creative Commons Attribution-No Derivatives 4.0 International Public License (<https://creativecommons.org/licenses/by-nd/4.0/legalcode>).

Control families 21 & 22 along with the *Control Activity to Capability Level Matrix* at Table 1 are used with permission from Exostar, Copyright 2018, All Rights Reserved.

AEROSPACE INDUSTRIES ASSOCIATION OF AMERICA, INC.
1000 WILSON BLVD.
ARLINGTON, VA 22209

THIS DRAWING SUPERSEDES ALL ANTECEDENT STANDARD DRAWINGS FOR THE SAME
PRODUCT AND SHALL BECOME EFFECTIVE NO LATER THAN SIX MONTHS FROM THE LAST
REVISION DATE.

FORM 09-01

REVISION

NEW

NAS9933

SHEET 4



Document Sharing Hub

USE OF OR RELIANCE UPON THIS DOCUMENT OR ANY NATIONAL AEROSPACE STANDARD IS ENTIRELY VOLUNTARY. AIA DOES NOT QUALIFY SUPPLIERS OR CERTIFY CONFORMANCE OF ITEMS PRODUCED UNDER NATIONAL AEROSPACE STANDARDS. AIA MAKES NO REPRESENTATION OR CLAIM RESPECTING (1) THE SUITABILITY OF ITEMS FOR ANY PARTICULAR APPLICATION OR (2) THE EXISTENCE OF OR APPLICABILITY THERETO OF PATENT OR TRADEMARKS RIGHTS.

Introduction

The Aerospace and Defense industry shares concerns raised by senior DOD leaders about threats to the security of DOD and industry's data and networks. The American Aerospace and Defense industry is fully committed to partnering with the U.S. government to stay ahead of cyber threats and ensure resilience in the increasingly complex cybersecurity ecosystem. To counter this dynamic cyber threat, dynamic, risk-based solutions are required rather than static, 'checklist' compliance requirements.

To this end, AIA proposes this standard which is based on levels of security with an eye toward constant growth in cyber-defense capabilities. As industry continues to work toward greater security, it is anticipated that this standard will baseline the aerospace and defense industry towards a single goal as well as assist the DOD in aligning with industry toward greater risk/threat-based security.

OBJECTIVE

To align the Aerospace and Defense industry in viewing Cybersecurity through a single focus, this National Aerospace Standard (NAS) on Cybersecurity has been developed for measuring a company's cybersecurity capability. There are two primary goals for this standard:

- To provide industry partners an idea of where a company is on the path to security beyond the compliance-based FAR, DFAR, and NIST SP 800-171 controls and a way to measure a company's cybersecurity risk.
- To align the additional requirements industry is experiencing through the DoD contracting process. Rather than different DoD organizations using different tools in the contracting process to assess a company's security across different contracts, this standard is designed with cybersecurity in mind first and foremost.

While this standard is designed to cover a company's entire Enterprise IT infrastructure for all elements that are governed by the same security policies, if multiple networks are governed by differing security policies, separate standards may be tracked. Additionally, industry partners may require the use of the information in this standard for risk assessment and management purposes, including the assessment of control implementations and/or solutions with alternative or equally effective security measures (e.g. configuration settings, boundary protection, internet isolation, behavior management).

The information contained in this standard makes use of the CIS Controls™ as described by the Center for Internet Security (CIS) and outlines a recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks. This standard uses version 5.1 of the CIS Controls.

Within each Control family, there are several Control Activities designed to give a company an idea as to where it stands from a Capability Level standpoint. Capability Levels are defined as follows:

- **Level 0** - Indicates no or minimal cyber risk management program; significant cyber protections are lacking; additional risk mitigations must be implemented (not specifically addressed in this standard)
- **Level 1** - Indicates a basic level cyber risk management program; some protections in place but additional risk mitigations must be implemented
- **Level 2** - Indicates a moderate level cyber risk management program; good protections in place but additional risk mitigations are required to protect sensitive information
- **Level 3** - Indicates a solid performing cyber risk management program; strong protections have been implemented; Advanced threats are understood and taking steps to address with specific controls; Additional risk mitigations are likely needed to protect against advanced attacks
- **Level 4** - Indicates a cyber risk management program that can detect, protect against, and respond to advanced threats; Specific advanced controls are implemented
- **Level 5** - Indicates a cyber risk management program that can detect, protect against, and respond to advanced threats; Specific advanced controls are implemented and optimized on an ongoing basis

A company must have implemented all control activities contained within a capability level to attain that capability level and prior to being able to meet the next capability level. Refer to the Control Activity to Capability Level Matrix in the following section which lists each control within each Control family. The controls in the matrix appear, at times, out of numerical order and were ordered this way to help guide implementation. The premise is that if a company has only 1 more control they could implement then they should implement the next control listed in the control matrix.

REVISION

NEW

NAS9933
SHEET 5



Document Sharing Hub

A minimum Capability Level of 3 is encouraged to ensure a solid performing cyber risk management program is in place. It is recognized that not all companies will be able to immediately attain Capability Level 3. That said, the results should be used to prioritize and implement additional controls that may be needed to improve the health of a company's cybersecurity posture.

Customers may use a company's resulting Capability Level as an indicator to formulate business risk decisions.

It is imperative that a company track updated progress against this standard as additional controls are implemented, and improvements are made to a company's cybersecurity posture.

Notes:

CSC = Critical Security Controls

This standard may be amended without notice.

REVISION

NEW

NAS9933

SHEET 6

TABLE 1 – Control Activity to Capability Level Matrix

Control Activity to Capability Level Matrix						
To meet the minimum recommended Capability Level 3 , all control activities in Levels 1, 2 and 3 must be implemented.						
Control #	Control Family	Capability Level 1	Capability Level 2	Capability Level 3	Capability Level 4	Capability Level 5
1	Inventory of Authorized and Unauthorized Devices	No controls at this level	CSC 1-1 CSC 1-4	CSC 1-2	CSC 1-3 CSC 1-5	CSC 1-6 CSC 1-7
2	Inventory of Authorized and Unauthorized Software	No controls at this level	CSC 2-6	CSC 2-2 CSC 2-4	CSC 2-1	CSC 2-5 CSC 2-8 CSC 2-9 CSC 2-3 CSC 2-7
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	CSC 3-2 CSC 3-3	CSC 3-1	CSC 3-7	CSC 3-4 CSC 3-10	CSC 3-5 CSC 3-6 CSC 3-8 CSC 3-9
4	Continuous Vulnerability Assessment and Remediation	CSC 4-5	CSC 4-1 CSC 4-3	CSC 4-7	CSC 4-6 CSC 4-10	CSC 4-2 CSC 4-4 CSC 4-8 CSC 4-9
5	Malware Defenses	CSC 5-1 CSC 5-2 CSC 5-3 CSC 5-4	CSC 5-5	CSC 5-6	CSC 5-8 CSC 5-11 CSC 5-7	CSC 5-9 CSC 5-10
6	Application Software Security - In-house Developed Software <i>N/A is a choice available for this control family</i>	CSC 6-3 CSC 6-7 CSC 6-9 CSC 6-10 CSC 6-11	CSC 6-4 CSC 6-5 CSC 6-6	CSC 6-2	No controls at this level	No controls at this level
6a	Application Software Security - Purchased Software	CSC 6-1	CSC 6-9	CSC 6-4	CSC 6-2	CSC 6-8
7	Wireless Access Control <i>N/A is a choice available for this control family</i>	CSC 7-6	CSC 7-8 CSC 7-9	CSC 7-2	CSC 7-7	CSC 7-4 CSC 7-5 CSC 7-1 CSC 7-3 CSC 7-10
8	Data Recovery Capability	No controls at this level	CSC 8-3	CSC 8-1	CSC 8-2	CSC 8-4
9	Security Skills Assessment and Appropriate Training	No controls at this level	CSC 9-1 CSC 9-2 CSC 9-3	CSC 9-4	CSC 9-5	No controls at this level

Control #	Control Family	Capability Level 1	Capability Level 2	Capability Level 3	Capability Level 4	Capability Level 5
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	CSC 10-1	No controls at this level	CSC 10-3	No controls at this level	CSC 10-6
		CSC 10-2		CSC 10-4		
		CSC 10-5				
11	Limitation and Control of Network Ports, Protocols, and Services	CSC 11-2	CSC 11-4	CSC 11-3	CSC 11-7	No controls at this level
			CSC 11-6			
			CSC 11-5			
			CSC 11-1			
12	Controlled Use of Administrative Privileges	CSC 12-3	CSC 12-1	CSC 12-10	CSC 12-12	CSC 12-2
		CSC 12-7	CSC 12-4	CSC 12-11	CSC 12-13	
			CSC 12-5	CSC 12-6	CSC 12-14	
			CSC 12-9			
			CSC 12-8			
13	Boundary Defense	CSC 13-1	CSC 13-7	CSC 13-11	CSC 13-9	CSC 13-5
			CSC 13-3	CSC 13-8	CSC 13-4	CSC 13-10
			CSC 13-6		CSC 13-2	CSC 13-12
						CSC 13-13
14	Maintenance, Monitoring, and Analysis of Audit Logs	No controls at this level	CSC 14-1	CSC 14-10	CSC 14-6	CSC 14-8
			CSC 14-3	CSC 14-2	CSC 14-7	
			CSC 14-4		CSC 14-9	
			CSC 14-5			
15	Controlled Access Based on the Need to Know	No controls at this level	No controls at this level	No controls at this level	No controls at this level	CSC 15-1
						CSC 15-3
						CSC 15-4
						CSC 15-2
16	Account Monitoring and Control	CSC 16-1	CSC 16-6	CSC 16-15	CSC 16-3	CSC 16-12
		CSC 16-2	CSC 16-5	CSC 16-16		CSC 16-13
		CSC 16-4	CSC 16-11	CSC 16-17		CSC 16-14
		CSC 16-7	CSC 16-9			
		CSC 16-8				
		CSC 16-10				
17	Data Protection	No controls at this level	CSC 17-1	CSC 17-13	CSC 17-7	CSC 17-5
			CSC 17-2		CSC 17-10	CSC 17-6
			CSC 17-3		CSC 17-14	CSC 17-8
			CSC 17-4			CSC 17-9
						CSC 17-11
						CSC 17-12
						CSC 17-15

REVISION

NEW

NAS9933
SHEET 8



Document Sharing Hub

Control #	Control Family	Capability Level 1	Capability Level 2	Capability Level 3	Capability Level 4	Capability Level 5
18	Incident Response and Management	No controls at this level	CSC 18-1	CSC 18-6	CSC 18-4	CSC 18-5
			CSC 18-2			CSC 18-7
			CSC 18-3			
19	Secure Network Engineering	No controls at this level	CSC 19-3	CSC 19-1	No controls at this level	CSC 19-4
						CSC 19-2
20	Penetration Tests and Red Team Exercises	No controls at this level	CSC 20-1	CSC 20-5	CSC 20-4	CSC 20-3
					CSC 20-2	CSC 20-7
					CSC 20-6	CSC 20-8
21	Organization/Governance	CSC 21-1	CSC 21-2	CSC 21-4	CSC 21-5	CSC 21-6
			CSC 21-3			
22	Mobile Device	No controls at this level	CSC 22-1	No controls at this level	No controls at this level	No controls at this level
			CSC 22-2			
			CSC 22-3			

REVISION

NEW



NAS9933
SHEET 9

Document Sharing Hub

USE OF OR RELIANCE UPON THIS DOCUMENT OR ANY NATIONAL AEROSPACE STANDARD IS ENTIRELY VOLUNTARY. AIA DOES NOT QUALIFY SUPPLIERS OR CERTIFY CONFORMANCE OF ITEMS PRODUCED UNDER NATIONAL AEROSPACE STANDARDS. AIA MAKES NO REPRESENTATION OR CLAIM RESPECTING (1) THE SUITABILITY OF ITEMS FOR ANY PARTICULAR APPLICATION OR (2) THE EXISTENCE OF OR APPLICABILITY THERETO OF PATENT OR TRADEMARKS RIGHTS.

1 DEVICE INVENTORY

IN RELATION TO INVENTORY OF AUTHORIZED AND UNAUTHORIZED DEVICES, WHICH OF THE FOLLOWING CAPABILITY LEVEL 1 TO 3 CONTROLS HAS YOUR ORGANIZATION IMPLEMENTED?

CHECK ALL THAT APPLY.

- ☐ Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s). Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed. (CSC 1-1)
- ☐ Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network. (CSC 1-4)
- ☐ Deploy dynamic host configuration protocol (DHCP) server logging and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information. (CSC 1-2)

IN RELATION TO INVENTORY OF AUTHORIZED AND UNAUTHORIZED DEVICES, WHICH OF THE FOLLOWING CAPABILITY LEVEL 4 TO 5 CONTROLS HAS YOUR ORGANIZATION IMPLEMENTED?

CHECK ALL THAT APPLY.

- ☐ Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network. (CSC 1-3)
- ☐ Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems. (CSC 1-5)
- ☐ Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access. (CSC 1-6)
- ☐ Utilize client certificates to validate and authenticate systems prior to connecting to the private network. (CSC 1-7)

1.1 Guidance

Control Objective: Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Control #	Control Family	Capability Level 1	Capability Level 2	Capability Level 3	Capability Level 4	Capability Level 5
1	Inventory of Authorized and Unauthorized Devices	No controls at this level	CSC 1-1	CSC 1-2	CSC 1-3	CSC 1-6
			CSC 1-4		CSC 1-5	CSC 1-7

REVISION

NEW

Documents

SHEET 10

Document Sharing Hub

USE OF OR RELIANCE UPON THIS DOCUMENT OR ANY NATIONAL AEROSPACE STANDARD IS ENTIRELY VOLUNTARY. AIA DOES NOT QUALIFY SUPPLIERS OR CERTIFY CONFORMANCE OF ITEMS PRODUCED UNDER NATIONAL AEROSPACE STANDARDS. AIA MAKES NO REPRESENTATION OR CLAIM RESPECTING (1) THE SUITABILITY OF ITEMS FOR ANY PARTICULAR APPLICATION OR (2) THE EXISTENCE OF OR APPLICABILITY THERETO OF PATENT OR TRADEMARKS RIGHTS.

2 SOFTWARE INVENTORY

IN RELATION TO INVENTORY OF AUTHORIZED AND UNAUTHORIZED SOFTWARE, WHICH OF THE FOLLOWING CAPABILITY LEVEL 2 TO 3 CONTROLS HAS YOUR ORGANIZATION IMPLEMENTED?

CHECK ALL THAT APPLY.

- ☐ Dangerous file types (e.g., .exe, .zip, .msi) should be closely monitored and/or blocked. (CSC 2-6)
- ☐ Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified. (CSC 2-2)
- ☐ Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level. (CSC 2-4)

IN RELATION TO INVENTORY OF AUTHORIZED AND UNAUTHORIZED SOFTWARE, WHICH OF THE FOLLOWING CAPABILITY LEVEL 4 TO 5 CONTROLS HAS YOUR ORGANIZATION IMPLEMENTED?

CHECK ALL THAT APPLY.

- ☐ Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow. When protecting systems with customized software that may be seen as difficult to whitelist, use item 8 below (ref: CSC 2-8) (isolating the custom software in a virtual operating system that does not retain infections). (CSC 2-1)
- ☐ The software inventory systems must be integrated with the hardware asset inventory so that all devices and associated software are tracked from a single location. (CSC 2-5)
- ☐ Configure client workstations with non-persistent, virtualized operating environments that can be quickly and easily restored to a trusted snapshot on a periodic basis. (CSC 2-8)
- ☐ Deploy software that only provides signed software ID tags. A software identification tag is an XML file that is installed alongside software and uniquely identifies the software, providing data for software inventory and asset management. (CSC 2-9)
- ☐ Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network. This includes alerting when unrecognized binaries (executable files, DLL's and other libraries, etc.) are found on a system, even inside of compressed archives. This includes checking for unrecognized or altered versions of software by comparing file hash values (attackers often utilize altered versions of known software to perpetrate attacks, and file hash comparisons will reveal the compromised software components). (CSC 2-3)
- ☐ Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment. (CSC 2-7)

REVISION

NEW

Documents

SHEET 11



Document Sharing Hub