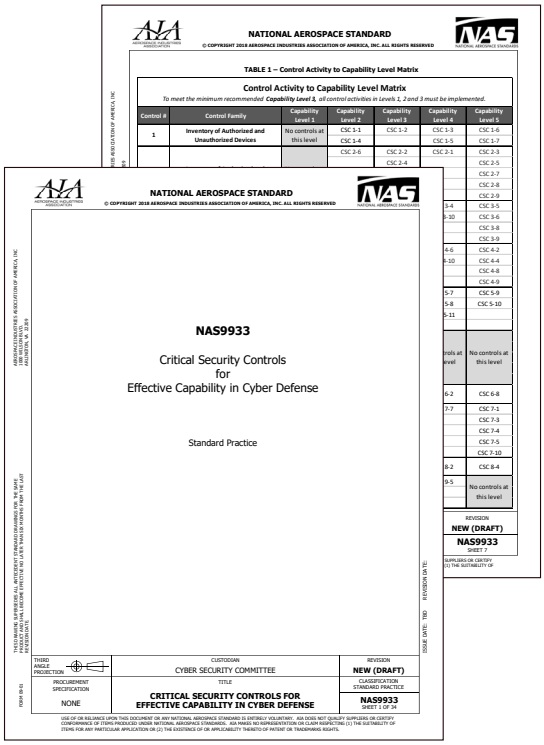
National Aerospace Standard 9933
Critical Security Controls for Effective Capability in Cyber Defense

AIA AEROSPACE INDUSTRIES ASSOCIATION

National Aerospace Standard (NAS9933)


NATIONAL AEROSPACE STANDARD

© COPYRIGHT 2018 AEROSPACE INDUSTRIES ASSOCIATION OF AMERICA, INC. ALL RIGHTS RESERVED

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 1-2	CSC 1-3	CSC 1-6
			CSC 1-4		CSC 1-5	CSC 1-7
			CSC 2-1	CSC 2-2	CSC 2-3	CSC 2-3
				CSC 2-4		CSC 2-5
						CSC 2-7
						CSC 2-8
						CSC 2-9
3-4						CSC 3-5
3-10						CSC 3-6
						CSC 3-8
						CSC 3-9
4-6						CSC 4-2
4-10						CSC 4-4
						CSC 4-8
						CSC 4-9
5-7						CSC 5-9
5-8						CSC 5-10
5-11						
rols at evel		No controls at this level				
6-2						CSC 6-8
7-7						CSC 7-1
						CSC 7-3
						CSC 7-4
						CSC 7-5
						CSC 7-10
8-2						CSC 8-4
9-5						No controls at this level

REVISION NEW (DRAFT)

NAS9933 SHEET 7

SUPPLIERS OR CERTIFY (1) THE SUITABILITY OF

NATIONAL AEROSPACE STANDARD

© COPYRIGHT 2018 AEROSPACE INDUSTRIES ASSOCIATION OF AMERICA, INC. ALL RIGHTS RESERVED

NAS9933

Critical Security Controls
for
Effective Capability in Cyber Defense

Standard Practice

THIRD ANGLE PROJECTION	CUSTODIAN: CYBER SECURITY COMMITTEE	REVISION: NEW (DRAFT)
PROCUREMENT SPECIFICATION: NONE	TITLE: CRITICAL SECURITY CONTROLS FOR EFFECTIVE CAPABILITY IN CYBER DEFENSE	CLASSIFICATION STANDARD PRACTICE; NAS9933 SHEET 1 OF 24

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 TRADEMARK RIGHTS.

In June 2015, NIST released its Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, which the Department of Defense (DOD) adopted as the benchmark for minimum cyber security. NIST's SP 800-171 currently consists of 110 "controls" which require certain conditions or actions. If some of its 110 controls are not satisfied, a company may still be awarded a DOD contract so long as it uses two management documents: 1) a system security plan and 2) a plan of action and milestones. These documents detail which controls have been implemented and how the company plans to implement the remainder.

To assist in addressing the dynamic nature of cyber threats, AIA has adopted the Exostar Cyber Security Questionnaire as the baseline for our cybersecurity standard. This new standard is designed to apply common and universal elements of cybersecurity and consists of 20 control families published by the Center for Internet Security (CIS), and two additional control families we've developed with Exostar. Each control family consists of several sub-controls better known as Critical Security Controls (CSC) and within each family, these CSCs have been categorized into five capability levels. In short, instead of a one-size-fits-all checklist, this format establishes "Capability Level 3" as a minimum performance level, with Levels 4 and 5 as higher-level objectives.

There are two primary goals for this standard:

> To provide industry partners an indication of a company's cybersecurity profile, as a way to measure a company's cybersecurity risk.

> To enable reciprocity across industry and critical infrastructure sectors, so that a company's level of cybersecurity is universally accepted by all whose work supports national interests.

AIA's cybersecurity standard will mark an important step forward in driving industry toward true risk- and threat-based cybersecurity by establishing data protection across diverse enterprises and evolving computing environments. Our goal is to provide companies with a methodology to evaluate their systems and processes. We intend for this standard to establish the cybersecurity baseline in the aerospace and defense industry, and support government leaders' efforts to align with industry on a path toward true security.

Link to AIA NAS Standards Store: https://global.ihs.com/home_page_aia.cfm?&rid=AIA

NAS NATIONAL AEROSPACE STANDARDS