

National Aerospace Standard 9933

Critical Security Controls for Effective Capability in Cyber Defense



National Aerospace Standard (NAS9933)

The aerospace and defense industry is committed to staying ahead of cyber threats and ensuring resilience in today’s complex cybersecurity ecosystem. We must have dynamic, risk-based solutions to counter cyber threats. Static, “checklist” compliance is not enough.

In June 2015, the National Institute for Standards and Technology (NIST) released NIST Special Publication (SP) 800-171, which currently consists of 110 “controls” (conditions or actions) that the government determined are the benchmarks for minimum cyber security. If some of its 110 controls are not satisfied, a company can still be awarded a contract so long as it has a system security plan and a plan of action and milestones that details which controls have been implemented, and how it plans to implement the rest.

To better address cyber threats, AIA has adopted the dynamic nature of the Exostar Cyber Security Questionnaire as the baseline for our cybersecurity standard. This new standard 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 for compliance, 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 (beyond the compliance-based FAR, DFAR, and NIST SP 800-171 controls), as a way to measure a company’s cybersecurity risk.
- > To align the fragmented and conflicting requirements that the Department of Defense (DOD) contracting process imposes on industry. Rather than different DOD organizations using different tools to assess a company’s security across different contracts, this standard is designed to apply common and universal elements of cybersecurity across each enterprise.

AIA’s cybersecurity standard will mark an important step forward in driving our industry toward true risk- and threat-based cybersecurity. Our goal is to provide companies with a methodology to evaluate their systems and processes, and to enable reciprocity, so that a company’s level of security is accepted by all prime contractors, systems integrators, and DOD. We intend for this standard to establish the cybersecurity baseline in the aerospace and defense industry, and that it will support government leaders’ efforts to align with industry and move beyond minimal compliance toward greater risk- or threat-based security.

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

NATIONAL AEROSPACE STANDARD
© COPYRIGHT 2015 AEROSPACE INDUSTRIES ASSOCIATION OF AMERICA, INC. ALL RIGHTS RESERVED.

TABLE 1 – 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 1.4 |
| | | | CSC 1.4 | CSC 1.5 | CSC 1.6 | CSC 1.7 |
| | | | CSC 2.1 | CSC 2.2 | CSC 2.3 | CSC 2.4 |
| | | | CSC 2.4 | CSC 2.5 | CSC 2.6 | CSC 2.7 |
| | | | CSC 2.8 | CSC 2.9 | CSC 2.10 | CSC 2.11 |
| | | | CSC 3.1 | CSC 3.2 | CSC 3.3 | CSC 3.4 |
| | | | CSC 3.5 | CSC 3.6 | CSC 3.7 | CSC 3.8 |
| | | | CSC 3.9 | CSC 3.10 | CSC 3.11 | CSC 3.12 |
| | | | CSC 4.1 | CSC 4.2 | CSC 4.3 | CSC 4.4 |
| | | | CSC 4.5 | CSC 4.6 | CSC 4.7 | CSC 4.8 |
| | | | CSC 4.9 | CSC 4.10 | CSC 4.11 | CSC 4.12 |
| | | | CSC 5.1 | CSC 5.2 | CSC 5.3 | CSC 5.4 |
| | | | CSC 5.5 | CSC 5.6 | CSC 5.7 | CSC 5.8 |
| | | | CSC 5.9 | CSC 5.10 | CSC 5.11 | CSC 5.12 |
| | | | CSC 6.1 | CSC 6.2 | CSC 6.3 | CSC 6.4 |
| | | | CSC 6.5 | CSC 6.6 | CSC 6.7 | CSC 6.8 |
| | | | CSC 6.9 | CSC 6.10 | CSC 6.11 | CSC 6.12 |
| | | | CSC 6.13 | CSC 6.14 | CSC 6.15 | CSC 6.16 |
| | | | CSC 6.17 | CSC 6.18 | CSC 6.19 | CSC 6.20 |
| | | | CSC 6.21 | CSC 6.22 | CSC 6.23 | CSC 6.24 |
| | | | CSC 6.25 | CSC 6.26 | CSC 6.27 | CSC 6.28 |
| | | | CSC 6.29 | CSC 6.30 | CSC 6.31 | CSC 6.32 |
| | | | CSC 6.33 | CSC 6.34 | CSC 6.35 | CSC 6.36 |
| | | | CSC 6.37 | CSC 6.38 | CSC 6.39 | CSC 6.40 |
| | | | CSC 6.41 | CSC 6.42 | CSC 6.43 | CSC 6.44 |
| | | | CSC 6.45 | CSC 6.46 | CSC 6.47 | CSC 6.48 |
| | | | CSC 6.49 | CSC 6.50 | CSC 6.51 | CSC 6.52 |
| | | | CSC 6.53 | CSC 6.54 | CSC 6.55 | CSC 6.56 |
| | | | CSC 6.57 | CSC 6.58 | CSC 6.59 | CSC 6.60 |
| | | | CSC 6.61 | CSC 6.62 | CSC 6.63 | CSC 6.64 |
| | | | CSC 6.65 | CSC 6.66 | CSC 6.67 | CSC 6.68 |
| | | | CSC 6.69 | CSC 6.70 | CSC 6.71 | CSC 6.72 |
| | | | CSC 6.73 | CSC 6.74 | CSC 6.75 | CSC 6.76 |
| | | | CSC 6.77 | CSC 6.78 | CSC 6.79 | CSC 6.80 |
| | | | CSC 6.81 | CSC 6.82 | CSC 6.83 | CSC 6.84 |
| | | | CSC 6.85 | CSC 6.86 | CSC 6.87 | CSC 6.88 |
| | | | CSC 6.89 | CSC 6.90 | CSC 6.91 | CSC 6.92 |
| | | | CSC 6.93 | CSC 6.94 | CSC 6.95 | CSC 6.96 |
| | | | CSC 6.97 | CSC 6.98 | CSC 6.99 | CSC 7.00 |
| | | | CSC 7.01 | CSC 7.02 | CSC 7.03 | CSC 7.04 |
| | | | CSC 7.05 | CSC 7.06 | CSC 7.07 | CSC 7.08 |
| | | | CSC 7.09 | CSC 7.10 | CSC 7.11 | CSC 7.12 |
| | | | CSC 7.13 | CSC 7.14 | CSC 7.15 | CSC 7.16 |
| | | | CSC 7.17 | CSC 7.18 | CSC 7.19 | CSC 7.20 |
| | | | CSC 7.21 | CSC 7.22 | CSC 7.23 | CSC 7.24 |
| | | | CSC 7.25 | CSC 7.26 | CSC 7.27 | CSC 7.28 |
| | | | CSC 7.29 | CSC 7.30 | CSC 7.31 | CSC 7.32 |
| | | | CSC 7.33 | CSC 7.34 | CSC 7.35 | CSC 7.36 |
| | | | CSC 7.37 | CSC 7.38 | CSC 7.39 | CSC 7.40 |
| | | | CSC 7.41 | CSC 7.42 | CSC 7.43 | CSC 7.44 |
| | | | CSC 7.45 | CSC 7.46 | CSC 7.47 | CSC 7.48 |
| | | | CSC 7.49 | CSC 7.50 | CSC 7.51 | CSC 7.52 |
| | | | CSC 7.53 | CSC 7.54 | CSC 7.55 | CSC 7.56 |
| | | | CSC 7.57 | CSC 7.58 | CSC 7.59 | CSC 7.60 |
| | | | CSC 7.61 | CSC 7.62 | CSC 7.63 | CSC 7.64 |
| | | | CSC 7.65 | CSC 7.66 | CSC 7.67 | CSC 7.68 |
| | | | CSC 7.69 | CSC 7.70 | CSC 7.71 | CSC 7.72 |
| | | | CSC 7.73 | CSC 7.74 | CSC 7.75 | CSC 7.76 |
| | | | CSC 7.77 | CSC 7.78 | CSC 7.79 | CSC 7.80 |
| | | | CSC 7.81 | CSC 7.82 | CSC 7.83 | CSC 7.84 |
| | | | CSC 7.85 | CSC 7.86 | CSC 7.87 | CSC 7.88 |
| | | | CSC 7.89 | CSC 7.90 | CSC 7.91 | CSC 7.92 |
| | | | CSC 7.93 | CSC 7.94 | CSC 7.95 | CSC 7.96 |
| | | | CSC 7.97 | CSC 7.98 | CSC 7.99 | CSC 8.00 |
| | | | CSC 8.01 | CSC 8.02 | CSC 8.03 | CSC 8.04 |
| | | | CSC 8.05 | CSC 8.06 | CSC 8.07 | CSC 8.08 |
| | | | CSC 8.09 | CSC 8.10 | CSC 8.11 | CSC 8.12 |
| | | | CSC 8.13 | CSC 8.14 | CSC 8.15 | CSC 8.16 |
| | | | CSC 8.17 | CSC 8.18 | CSC 8.19 | CSC 8.20 |
| | | | CSC 8.21 | CSC 8.22 | CSC 8.23 | CSC 8.24 |
| | | | CSC 8.25 | CSC 8.26 | CSC 8.27 | CSC 8.28 |
| | | | CSC 8.29 | CSC 8.30 | CSC 8.31 | CSC 8.32 |
| | | | CSC 8.33 | CSC 8.34 | CSC 8.35 | CSC 8.36 |
| | | | CSC 8.37 | CSC 8.38 | CSC 8.39 | CSC 8.40 |
| | | | CSC 8.41 | CSC 8.42 | CSC 8.43 | CSC 8.44 |
| | | | CSC 8.45 | CSC 8.46 | CSC 8.47 | CSC 8.48 |
| | | | CSC 8.49 | CSC 8.50 | CSC 8.51 | CSC 8.52 |
| | | | CSC 8.53 | CSC 8.54 | CSC 8.55 | CSC 8.56 |
| | | | CSC 8.57 | CSC 8.58 | CSC 8.59 | CSC 8.60 |
| | | | CSC 8.61 | CSC 8.62 | CSC 8.63 | CSC 8.64 |
| | | | CSC 8.65 | CSC 8.66 | CSC 8.67 | CSC 8.68 |
| | | | CSC 8.69 | CSC 8.70 | CSC 8.71 | CSC 8.72 |
| | | | CSC 8.73 | CSC 8.74 | CSC 8.75 | CSC 8.76 |
| | | | CSC 8.77 | CSC 8.78 | CSC 8.79 | CSC 8.80 |
| | | | CSC 8.81 | CSC 8.82 | CSC 8.83 | CSC 8.84 |
| | | | CSC 8.85 | CSC 8.86 | CSC 8.87 | CSC 8.88 |
| | | | CSC 8.89 | CSC 8.90 | CSC 8.91 | CSC 8.92 |
| | | | CSC 8.93 | CSC 8.94 | CSC 8.95 | CSC 8.96 |
| | | | CSC 8.97 | CSC 8.98 | CSC 8.99 | CSC 9.00 |

NAS9933
Critical Security Controls for Effective Capability in Cyber Defense

Standard Practice

CLASSIFICATION: CYBER SECURITY COMMITTEE
REVISION: NEW (DRAFT)

CRITICAL SECURITY CONTROLS FOR EFFECTIVE CAPABILITY IN CYBER DEFENSE
NAS9933 SHEET 1 OF 34

