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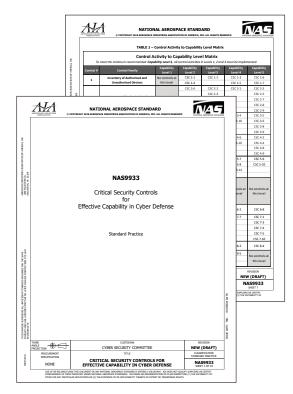## Critical Security Controls for
Effective Capability in Cyber Defense

AIA
AEROSPACE INDUSTRIES
ASSOCIATION

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 global ecosystem. As industry and government continue to partner on dynamic, risk-managed solutions to counter cyber threats, we've designed this standard to complement the government's efforts embodied in the Federal Acquisition Regulation, the Defense Federal Acquisition Regulation Supplement, and non-federal standards developed by the National Institute for Standards and Technology (NIST).

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