



NATIONAL AEROSPACE STANDARD

© COPYRIGHT 2013 AEROSPACE INDUSTRIES ASSOCIATION OF AMERICA, INC. ALL RIGHTS RESERVED



FED. SUPPLY CLASS

NONE

CYBER SECURITY BASELINE

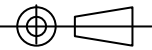
STANDARD PRACTICE



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 12-01

THIRD ANGLE PROJECTION		CUSTODIAN ELECTRONIC ENTERPRISE INTEGRATION COMMITTEE	REVISION 1
PROCUREMENT SPECIFICATION		TITLE CYBER SECURITY BASELINE	CLASSIFICATION STANDARD PRACTICE
NONE			NAS9924 SHEET 1 OF 8



Documents

Document Sharing Hub

REVISION DATE: FEBRUARY 28, 2013

ISSUE DATE: JANUARY 31, 2013

TABLE OF CONTENTS

1.	INTRODUCTION	3
1.1	Who should use this document?	3
2.	TIER 1	4
3.	TIER 2	4
4.	TIER 3	5
4.1	Policy	5
4.2	Technical Controls.....	6

TABLE

TABLE I – Examples of Cyber Threat Risk Mitigations	3
---	---

REVISION

NEW

NAS9924

SHEET 2



Document Sharing Hub

1. INTRODUCTION

Supply chain companies are important to the aerospace and defense industrial base. Suppliers may have unique capabilities that are vital to aerospace and defense programs.

Aerospace and defense companies have been dealing with the threat of cyber intrusion for the past several years. As companies have increased the security of their IT network defenses, the attackers are now being driven to softer targets where they may find some of the same type of data that they previously had sought from these companies. The adversary is also using the collaborative relationships between the aerospace and defense companies and their suppliers as a "back door" as the defenses get better. Companies further down the supply chain may not have had the opportunity or expertise necessary to fully prepare to defend their systems from these attackers, but the result of the increased defenses in the major suppliers is that the attacker may target their suppliers based on their vulnerabilities. This document was designed to be a supplier baseline so that suppliers know what kind of security they need to have if they want to do business with aerospace and defense companies.

1.1 Who should use this document?

This standard practice is written to be used by the aerospace and defense supply chain. It provides basic information that a supplier can use to:

- assess themselves on their information technology security practices;
- determine their preparedness for cyber threat risk management for their customer; and
- assess the risks presented by their own suppliers.

Through the process of self-assessment suppliers can determine where their strengths and weaknesses exist.

This document should be used by any supplier that is interested in protecting their data from disruption or exfiltration. There are three distinct tiers of supplier that could benefit from this standard practice. These tiers are defined as:

Tier 1: Suppliers that operate without a dedicated Information Technology professional on staff nor do they have a dedicated Information Technology Security professional. (Questions 1-5)

Tier 2: Suppliers with a dedicated Information Technology professional on staff, but have no dedicated Information Technology Security professional. (Questions 1-17)

Tier 3: Suppliers that have both dedicated Information Technology professionals and dedicated Information Technology Security professionals on staff. (Questions 1-72)

Table I provides examples of what would be considered an inadequate (bad) statement and what would be considered an adequate (good) statement in response to the questions raised in the document. It illustrates the level of detail that would be expected to clearly show that a specific requirement is being addressed, and to what extent, in order to provide confidence to the company and its customers.

TABLE I – EXAMPLES OF CYBER THREAT RISK MITIGATIONS

Bad:	Good:
"We have hardened our hosts against attack."	"We have applied all security patches for Windows as of 3/31/20xx to our servers. Our Administrator is tasked with keeping up to date on current vulnerabilities that may affect our environment, and our policy is to apply new patches during our maintenance period (2300hrs, Saturday) every week. Critical updates are implemented within 24 hours. A complete list of applied patches is available to you."
"We use encryption."	"All communications between our site and our partner will be protected by IPsec ESP Tunnel mode using 168-bit TripleDES encryption, SHA-1 authentication. We exchange authentication material via either out-of-band shared secret or PKI certificates."

REVISION

NEW

NAS9924

SHEET 3

Document Sharing Hub

