AEROSPACE INDUSTRIES ASSOCIATION

April 8, 2013

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Subject: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Reference:
Document Citation: 78 FR 13024
Page: 13024 -13028 (5 pages)
Agency/Docket Number: Docket Number 130208119-3119-01
Document Number: 2013-04413

Dear Ms. Honeycutt:

The Aerospace Industries Association (AIA) was founded in 1919. AIA is the premier United States based trade association representing over 370 aerospace and defense manufacturers and suppliers and approximately 844,000 aerospace and defense workers. Our members represent the United States of America's leading manufacturers and suppliers of civil, military, and business aircraft, helicopters, unmanned aerial systems, missiles, space systems, aircraft engines, materiel, and related components, equipment services, and information technology.

We are pleased on behalf of our membership to provide you the following information in response to your Request For Information (RFI). AIA supports the role of NIST and their lead role to develop in partnership a cybersecurity framework to protect the Nation's Critical Infrastructure. Within the Industry today, AIA member companies support the implementation of risk management and cybersecurity best practices. Cybersecurity is a critical part of our Industry Business Model and is enlisted as one element of an Enterprise Risk Management Framework. When examined, the NIST Cybersecurity Framework for Critical Infrastructure should be actionable, technology neutral, and commensurate with the sensitivity/criticality of the data being protected (data categorization). In parallel, activities should incorporate existing Industry Risk Management & Assessment methodologies and toolkits as to applicability of approach on situational awareness and overall risk mitigation. The risk management scope needs to be consistent throughout implementation with an emphasis on regulation (e.g. FAR/DFARS, FAA), not voluntary participation alone. Audit and Compliance should also be aligned and conducted based on risk, not systematic checklists, which time and again have proven that compliance does not necessarily mean secure.

Industry believes that organizations that choose not to participate in the Voluntary Critical Infrastructure Cybersecurity Framework based on their risk assessment and/or contract requirements should not be restricted from providing products and services to the Government. For example, a company following NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information System implements network security with a focus on continuous monitoring based on their assessed risk to their network. Their actions would likely meet or exceed the security controls identified in a future Critical Infrastructure Cybersecurity Framework, ensuring that data that is directly relevant to the nation's security is protected.

When developing a Critical Infrastructure Cybersecurity Framework, AIA recommends considering the following Frameworks, Standards, Guidelines, & Best Practices currently in use by our members:

Aerospace Industries Association of America, Inc.
1000 Wilson Blvd., Suite 1700, Arlington, Virginia 22209-3901
Ph. (703) 358-1000 / Fax (703) 358-1011 www.aia-aerospace.org

- ISO/IEC 27000-Series, Information Security Standards
- NIST Special Publication 800 Series, Information Security
- Australian Government, Defence Signals Directorate, Strategies to Mitigate Targeted Cyber Intrusions
- National Aerospace Standard 9924, Standard Practice for Cybersecurity Baseline
- Center for Strategic & International Studies' 20 Critical Security Controls
- ISO/IEC 15026, System and Software Assurance

Due to the complexity of most standards, their implementation difficulty, and cost, some companies have not systematically implemented standards. Affordable, risk-based standards have to be scalable across Industry and the Critical Infrastructure; blind compliance with a set of standards alone does not prevent malicious activity. Incentives, Tax Credits, and Liability Protections should be considered in combination with enhanced cybersecurity instead of solely relying on the regulation and voluntary standards approaches.

Risk assessments do not identify which standards to implement. The effectiveness of a standard is in the overall implementation and operation based on the design, controls, and process around data, systems, and networks. Deterrence and resiliency in recovery and mission assurance is also a critical ability. Any discontinuity either directly to the Critical Infrastructure, Aerospace Industry, Enterprise, and/or from a critical vendor or partner within the supply chain could impact operation and delivery of products. A singular focus on cybersecurity best practices, certifications, and compliance is unlikely to provide defenses against a sophisticated cyber threat/event. Any Critical Infrastructure Cybersecurity Framework needs to ensure that the security controls protecting sensitive/critical systems actually provide the expected defenses against a determined attacker.

Aerospace and Defense companies are seeking to ensure a clear definition of the extent to which the aerospace industry is considered critical infrastructure, noting that it may be categorised as such as part of the DoD supply chain, or through performance-based logistics contracts. This could lead to a large overhead if the entire supply chain is forced to take precautions, or awkward discontinuities could arise between and within companies if only the primes and upper tiers are so categorised. Conversely, if the aerospace industry is not categorised as critical, then the extent to which companies are being targeted by APT would not be adequately recognised.

AIA supports improved security posture across the Critical Infrastructure (Domestic and International) aligned with a Legislative process to minimize the number of Government oversight authorities (non-duplication , agency confliction), enhance existing public/private information sharing forums (unclassified and classified), and enable situational awareness (intelligence, protection, & mitigation). On behalf of the AIA members, we appreciate the opportunity in partnership to share information and our Industry perspective with NIST. AIA remains available to support NIST's cybersecurity framework development efforts and will gladly support as requested.

Sincerely,

James 'Rusty' Rentsch
AVP Technical Operations