Shaping the Future of Aerospace

AEROSPACE CYBERSECURITY AND SAFETY

Background: As the world's largest aerospace professional society, serving a diverse range of more than 30,000 individual members from 88 countries, and 95 corporate members, the American Institute of Aeronautics and Astronautics (AIAA) urges Congress to enact policies that will address the growing threat, costs, and potential shortcomings relative to cybersecurity at various federal agencies, and within the aerospace and defense (A&D) industry in general.

The full scope of cybersecurity threats is difficult to grasp and quantify. Vulnerabilities run the gambit from compromised Personally Identifiable Information (PII) to Distributed Denial of Service (DDoS) attacks on critical infrastructure all the way to economic espionage and the subversion of critical national security and public safety systems. Agencies and companies are facing significant and ongoing cybersecurity and safety threats, while at the same time confronting nontechnical issues including budget uncertainty, an evolving national strategy, and how, when, where, and if information can be shared among impacted agencies and industries. While key agencies within the Federal Government are currently dealing with these challenges, this ambiguity on strategy and information sharing is impacting the private sector.

Budget constraints forced upon the Federal Government as a result of sequestration and the Budget Control Act have resulted in the consideration of tough tradeoffs as agencies focus their limited dollars on the areas vital to the overall safety and security of the systems and assets they oversee on the "franchise" programs (i.e., Next Generation Air Traffic Control System, International Space Station, etc.). Alternatively, an agency could choose to spread fewer dollars over all areas equally. Regardless, critical systems and programs are put in jeopardy. Developing and implementing a robust cybersecurity strategy will require barriers to be identified and addressed—not the least of which are technology challenges—and sustained and adequately funding, as well as overall coordination and collaboration.

Most federal agencies struggle to stay current with the rapidly changing threats of cybersecurity, let alone anticipate new developments. Government Accountability Office (GAO) reports continue to highlight shortcomings and gaps in agencies' efforts to address both physical and network cyber challenges. Additionally, the Office of Inspector General (OIG) at both NASA and the FAA have highlighted information technology (IT) infrastructure as key areas of concern among top management challenges at both agencies. The FAA IG specifically called for developing a strategic vision to better manage current technologies, plan for future systems, and maximize cost savings.

These reports, as well as recent cyber and physical intrusion events, highlight vulnerabilities in the safety, reliability, and redundancy of key federally managed systems. The A&D private sector faces similar cybersecurity challenges related to industrial espionage, loss of technology, and cyber attacks that have national security and safety implications as well. Relationships between federal and private entities can leave both systems vulnerable to attack. With today's commercial aircraft network flying more than ever before, commercial aircraft are becoming targets for cyber attacks. Understanding the nature of the threat and breaking down barriers to information sharing will be key aspects of developing a robust and viable national cybersecurity strategy.

Issue: Open Sharing of Information. Sharing of current threats, recent breaches, and evolving intelligence is paramount to addressing future threats. The Director of the National Security Agency (NSA) said, “It’s only matter of the ‘when,’ not the ‘if,’ that we are going to see something dramatic.” Methods of successful cyber attacks are frequently copied. If agencies and companies know what current attack methods have been used and what vulnerabilities were exploited, additional attacks can be minimized or mitigated, if not thwarted. Information Sharing and Analysis Centers (ISAC) were established to facilitate the exchange of information. Subsequent actions (PPD-21, etc.) were done to strengthen that sharing. Congress should conduct a review of the current sharing protocols and direct the Department of Homeland Security (DHS) to report on shortcomings and proposed changes.

Issue: Cybersecurity Framework and Roadmap. The number of public and private sector players in the cybersecurity realm is extensive. A framework that leads to a roadmap and an implementable strategy are essential to organize the stakeholders and build consensus. In 2013, AIAA released a framework to address commercial aviation. Frameworks for tackling cyber challenges in the space and defense sectors need to be established. Participation by key government agencies (DHS, DoD, DoT, etc.) will be critical to developing a unified and actionable framework from which a roadmap and strategy can evolve. Congress should direct all relevant federal agencies to participate in and support the development of a unified framework for cybersecurity in the space and defense sectors and support the advancement of the 2013 commercial aviation framework to an accepted national level strategy.

Issue: A&D Industry Assessment. After the 2008 financial crisis, the Federal Reserve began conducting periodic “stress tests” on financial institutions to determine their ability to cope with certain hypothetical scenarios. Currently there is no similar government-wide, standard approach for conducting a cybersecurity stress test. Before directed action to address vulnerabilities can be taken, the current state of the system must be established. Recent GAO reviews have been of limited scope with regard to agencies and infrastructure (GAO-15-6). A comprehensive review is necessary. Congress should direct that a plan be developed for a government-wide stress test that will incorporate the relevant aspects of the DHS National Infrastructure Protection Plan (DHS NIPP), called for in the National Institute of Standards and Technology (NIST) document “Framework for Improving Critical Infrastructure Cybersecurity” (Feb. 2014), and AIAA’s “A Framework for Aviation Cybersecurity” (Aug. 2013).

AIAA Recommendations:

GAO conduct review of barriers to open sharing of information regarding cyber threats

Direct the responsible agencies to participate in public-private partnerships in the development of Cybersecurity Roadmaps for Defense and Space comparable to the AIAA “Framework for Aviation Cybersecurity

GAO conduct federal agency stress test that will incorporate the relevant aspects of the DHS NIPP, NIST document, and AIAA’s “Framework for Aviation Cybersecurity”