Adopting a Robust and Integrated Cybersecurity Policy
as One of Our Top National Security Priorities
An AIAA Information Paper

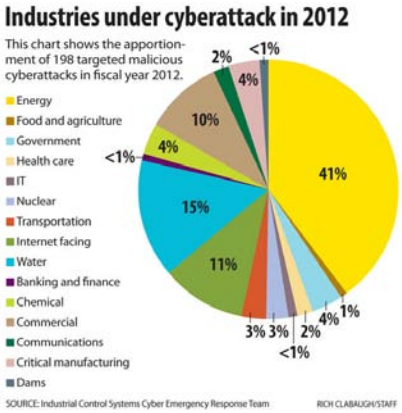
Abstract

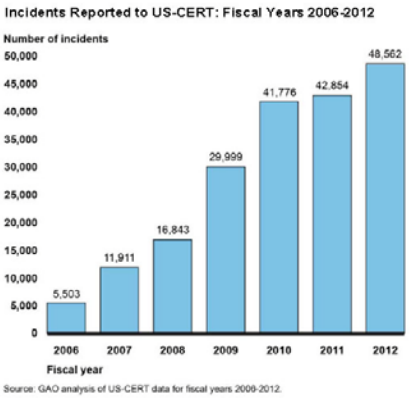
The American Institute of Aeronautics and Astronautics (AIAA) recognizes that the area of cybersecurity is profoundly important to not only the aerospace and defense industry, but also to those deemed to be part of the "critical infrastructure." The level of connectivity within medical, financial, and utility sites, and certainly within U.S. government functions, has never been higher. While this connectivity provides efficiency and advancement, it also offers numerous – and ever growing – points of intrusion for individuals and state-sponsored organizations seeking to exploit vulnerabilities. And as the services and data accessible through the cloud and the web continue to increase, so too does the potential threat and level of severity to companies that rely on networks. With today's level of interconnectivity surely to increase, the growing threat to aerospace, defense, and all segments of our critical infrastructure, requires making a robust and integrated cybersecurity policy one of our top national security priorities.

Issue Background

Recent headlines of sophisticated and sustained attacks against financial institutions and media outlets highlight how prevalent cyber attacks are, across many industries. The importance of cybersecurity is reflected in recent comments President Obama made in this year's State of the Union address. Regarding cybersecurity, he said "America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."

Most people's frame of reference regarding cybersecurity comes from the loss of Personally Identifiable Information, or PII. But as Secretary of Defense Panetta indicated in an October 2012 speech to business executives, "the even greater danger – the greater danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation."





General Accounting Office (GAO) reviews continue to note significant shortcomings in terms of the preparedness level of federal agencies with respect to cybersecurity (GAO-12-666T). In

addition to vulnerabilities within the federal networks, the Department of Homeland Security (DHS) saw a 52% increase in the number of cyberattacks against critical infrastructure within the U.S., with the energy sector being the primary target. While defense related secrets are certainly at risk from the prolific number of cyberattacks being launched, Secretary Panetta noted that "The collective result of these kinds of attacks could be a cyber Pearl Harbor: an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability."

President Obama recently issued an Executive Order (EO) intended to increase information sharing and develop standards to protect our national security. This EO was meant to partially address stalled cybersecurity legislation. However, its impact is limited by the fact that it does not have the same effect as law. Meanwhile, the United States still faces a myriad of issues related to the growing cybersecurity threat: State-sponsored organizations that train thousands of computers and users directly at U.S. networks; A shortage of properly trained cybersecurity personnel; Evolving threats that outpace our ability to adapt; Existing or recently developed systems (NextGen) that may or may not be cyber secure but are extensively network dependent.