April 8, 2013

National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
cyberframework@nist.gov

Request for Information - Framework to Improve Critical Infrastructure Cybersecurity

On behalf of the Semiconductor Industry Association (SIA),[1] we appreciate and share the Administration's interest in addressing the cybersecurity challenges facing our country. Semiconductors are a fundamental building block for the modern electronics that drive today's communications, transportation, information technology, energy systems, and many other applications. Accordingly, SIA hopes to play a constructive role in the development of sound and effective public policy by offering our expertise and assistance.

The government can best address cyber security vulnerabilities by partnering with industry to enhance security. We appreciate this RFI as part of the government's effort to reach out to industry and gain our insights and benefit from our expertise. To that end, we have provided the following comments regarding security and authenticity, as well recommended policy principles, that we believe are important for the government to consider as cyber security policies and initiatives are developed and implemented.

Security and Authenticity for Semiconductors

SIA recognizes the government's interest in ensuring the security and authenticity of semiconductors with regard to government purchases of semiconductor products. Ensuring the security and authenticity of semiconductor products is a top priority of the semiconductor industry, and SIA member companies have developed a number of business protocols and safeguards to ensure the security of their operations. These practices include, among others:

- Measures to promote a secure supply chain – companies in the semiconductor industry implement a range of practices to advance the security of their product development and supply chain – from product design and production to distribution. The industry has also

[1] SIA is the voice of the U.S. semiconductor industry, one of America's top export industries and a key driver of America's economic strength, national security and global competitiveness. The semiconductor industry directly employs nearly a quarter of a million people in the US. In 2012, US semiconductor sales totaled more than $145 billion, and semiconductors make the global trillion dollar electronics industry possible. Founded in 1977 by five microelectronics pioneers, SIA unites companies that account for 80 percent of America's semiconductor production. Through this coalition, SIA seeks to strengthen U.S. leadership of semiconductor design and manufacturing by working with Congress, the Administration and other key industry stakeholders to encourage policies and regulations that fuel innovation, propel business and drive international competition.

worked with other elements of the IT supply chain to develop standards and other initiatives that provide product security and authentication.

- Incorporation of security features into semiconductors – semiconductor companies incorporate risk appropriate technologies into their products to help promote security and authentication.
- Authorized distribution channels – semiconductor companies distribute products through authorized distributors that safeguard the authenticity and reliability of semiconductor products.
- Secure personnel policies – semiconductor companies implement rigorous personnel practices to safeguard product design, manufacturing, and distribution operations.
- Developing a research agenda – SIA and members companies have a long history of working in close partnership with the government and universities on research, including efforts to promote product and systems trust and assurance. The Semiconductor Research Corporation (SRC), the industry's collaborative research consortium, is leading an industry initiative to identify and address research priorities aimed at strengthening security and trustworthiness throughout the design and manufacture process.
- Cooperation with law enforcement – SIA and member companies have cooperated with the arrest and prosecution of people who have made, imported, and sold semiconductor counterfeits. These counterfeits were destined for critical applications such as a high speed train braking system, radiation detection instruments used by first responders, and a Navy vessel Friend-or-Foe identification system.
- Partnerships with government – SIA and member companies work closely with governments to promote product security and authenticity. For example, for semiconductors that are used in special military or space applications, the government and industry have established a "trusted supplier" program. The industry also works with government to address the challenge of counterfeit products.

In short, the semiconductor industry is inherently security-sensitive in terms of the design, sourcing, manufacture, and distribution of our products. U.S. semiconductor companies operate under robust and mature security practices and protocols, and the industry has long been subject to strict export control regulations and other legal and regulatory regimes designed to assess, monitor, and control access to semiconductor-related technologies and products. Semiconductor products increasingly have built-in security features that are used to protect system hardware from a cyber-attack, as well enhance the operation of other hardware and software based security features and end-use products.

In many cases, the government can advance its security interests by improving upon existing practices, without the need for new requirements or mandates. For example, the government can protect against the proliferation of counterfeit parts through the use of sound procurement practices. Such practices should include:

- Minimizing risk by purchasing semiconductors only from authorized distributors.
- Making improved counterfeit detection and enforcement efforts a top priority for U.S. Customs and other authorities.
- Improving collaboration between U.S. anti-counterfeiting authorities and industry to identify and stop the flow of counterfeits into our country, as well as pressing U.S.

trading partners to take action against counterfeiters. The government can also play an important role in support of research to enhance product security and authentication.

- Leveraging existing and emerging industry standards and practices that promote innovation, interoperability, and open competition to reduce counterfeiting technologies and overall proliferation.

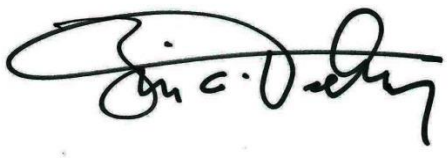
Recommended Policy Principles

SIA recommends that any new requirements to secure IT networks and systems be based on the following principles:

- Flexible policies – solutions should be flexible and avoid "one size fits all" approaches. Rigid, single approaches to security are unlikely to remain adaptive to emerging challenges.
- Non-proprietary, technology neutral requirements – mandates requiring specific technologies, domestically made technologies, or sole source vendors are not effective and should be avoided.
- Consider impact on cost, feasibility, and innovation – potential solutions should take into account feasibility and costs from a manufacturing and supply chain perspectives, and the impact on technology development and innovation.
- Adoption of special requirements for military or space applications – where prescriptive requirements are needed for sensitive applications such as the military, intelligence, or space areas, these requirements should be limited to those special applications; they should not be applied to other government functions or the commercial sector.
- Promote and encourage trade – policies should be harmonized to the greatest extent possible, and should not be based on the country of origin or the nationality of the technology vendor. Solutions should be based on how a product is designed, produced, and distributed, and not by whom or where it is made. Requirements should also avoid the forced transfer of IP.

SIA and member companies will continue to work to advance these principles and continue our efforts to work toward stronger product security and authentication around the world. SIA and our member companies look forward to establishing a dialogue and a partnership as work to establish a framework for addressing any risk in the supply chain continues.

Sincerely,



Brian Toohey
President & CEO
Semiconductor Industry Association