Securing Production of America's Information and Computer Technology

AUI White Paper on the need for a public-private partnership dedicated to microelectronics supply chain assurance and R&D.

The U.S. government's national security posture relies on information and communications technology (ICT) and thus relies on the integrity of installed microchips. For the broader microchip marketplace, the main goals are cheaper, faster, and more powerful, which means that aspects of the chips that are critical to the U.S. government (such as robust, secure, and resilient) are no longer driving the semiconductor industry. ICT must be trustworthy and reliable to perform as and only as designed and when and only when needed. In addition to repatriating ICT hardware and software, ensuring that security and robustness again become prime attributes of the design, fabrication, installation and operations will require independent mission assurance functions to be implemented. Further, research and development (R&D) must be an integral component of the effort if we are to regain technological superiority in a world where the threat continues to evolve at an increasing rate.

AUI proposes establishing a new leadership entity focused exclusively on securing the ICT supply chain from design through operations, ensuring management control to drive culture change, re-writing the code of conduct governing ICT design, and providing the needed focus on security and resiliency as major qualities for integrated circuits for national security needs. This entity could take the form of a new Federally Funded Research and Development Center (FFRDC) or a consortium of industry, academic, and government experts through other contracting mechanisms. This capability would evolve and align with the needs of the Department of Defense (DOD) and industry. This leadership entity would not compete with industry and would fill niche needs distinct from any particular foundry approaches.

BACKGROUND:

Microelectronics underpin every military platform, intelligence apparatus, and critical infrastructure network and provide secure communications, electronic warfare capabilities, and cryptographic applications, among others. Important national security technologies have size, weight, power, and performance goals that can only be met through the use of the most sophisticated semiconductor devices. However, in today's marketplace, U.S. national security is precariously dependent on the integrity of commercial suppliers for those microchips.

Although the U.S. government was once the driving force behind semiconductor technology, consumer demand for products and services has driven the technology and the marketplace in a different direction. The global marketplace for personal computing devices, smart phones, and other devices has impelled the microelectronic industry to restructure itself to serve this new demand. The industry operates using a global supply chain that supports continuous foundry operations and the volumes are such that national security needs amount to less than 1% market share. National security technologies now have minimal influence over the semiconductor industry. Further, potential adversaries not only have access to the most

sophisticated technology, in some instances they have become the very suppliers of the components the U.S. requires to regain technological superiority.

Meanwhile, increased attention is being paid to the threat China poses to U.S. industrial might through its covert and overt methods to steal or buy U.S.-developed technologies, threatening our nation's economic primacy. Russia has demonstrated similar persistent, advanced, and ever-improving capabilities, including through automated means, the penetration of industrial control systems. Other countries exploit the weakness of the microelectronics we use, and continue to exhibit advanced hacking capabilities, to conduct espionage, and to destroy information held by U.S. organizations and industry. In addition, malefactors have demonstrated the ability to create great wealth through cyber-crimes and threaten the stability of weak nations, which provides incentive for DOD to continually look for and mitigate vulnerabilities. Finally, there have been examples in the past few years (e.g., Meltdown or the Fitbit GPS tracking issues) of a different type of threat to our national ICT – results of design optimization that ignore attributes critical to our national and economic security.

Policymakers have begun to awaken and respond to these threats, and Congress has shown growing bipartisan concern over this issue as evidenced by language in legislation over the past few years. Further, White House administrations continue to catalog the ever-increasing severity of cyber threats confronting the nation and are acting through existing mechanisms, such as through the Committee on Foreign Investment in the United States (CIFIUS) and targeted, albeit uncoordinated, R&D efforts. However, there is not a strategic, holistic approach aimed at solving a multi-layered issue with impacts on regulatory frameworks, acquisition policies, R&D investments, and government standards.

Be it the loss of advanced defense weapons technology, the compromise of critical infrastructure, the loss and manipulation of personally identifiable information, or the realization that all avenues (hardware/software) are riven with unrepairable penetration points, the time has long past when reliability could be achieved through oversight and management alone. *Until and unless the United States reestablishes sovereignty over the design, production and distribution of ICT hardware, and software embeds resiliency into all such devices and systems from the outset, these liabilities to national security will continue unabated.*

As a result, regaining control over ICT cybersecurity threats requires a multi-pronged approach that results in the design, manufacture, delivery, and maintenance of increasingly secure products. Mission assurance must independently validate security standards and implementation in all steps of the supply chain. Finally, a program that supports and maintains leading-edge research in semiconductor manufacturing, enhanced robustness and resilience, system-on-chip design, and supply chain security must be established to analyze emerging cyber threats and derive methods to counter them.

THE PROPOSED MODEL FOR MISSION ASSURANCE AND ACCESS:

To most effectively address the current and growing risk, a green-field, dedicated research, development, test and evaluation (RDT&E) effort is needed. The time for a new trust approach is urgent, but precedents for substantially changing the paradigm in national security do exist. For example, within a decade - from the late 1940s to the early 1950s - Admiral Rickover took the nascent technology of nuclear power and used it to transform not only the Navy's submarine force but the entire American military strategy. Rickover recognized that to be successful in developing and exploiting nuclear power, he needed to exercise an extraordinary level of management control both within his command and in the contractors and laboratories that supported the effort. He clearly recognized that there needed to be a reliance on management control, strategic thinking, and questioning attitude in the design and implementation aimed at instilling a new culture and creating training paradigms that formed the foundation of the nuclear power we use today. For microelectronics, a comparable strategy could be used to fundamentally shift the culture and focus efforts on improving security.

A new organization could best provide independent testing of ICT technology to assure its security, aid manufacturers to repatriate production and incorporate secure technologies into their products, and coordinate and conduct leading-edge research. The green-field efforts of this organization would help prevent the mistake of relying on accepted wisdom and embedding existing flaws (both physical and attitudinal) into national infrastructure and security processes. It also would provide the Department and other government agencies a critical trust and assurance mechanism that is vital in an environment with only a handful of global suppliers.

This organization must work in a classified environment with national security experts on emerging cyber threats while simultaneously working in open environments with industry and academic researchers to identify new technologies and promulgate security standards for trust and assurance. This can best be done through a new Federally Funded Research and Development Center (FFRDC), acting as a neutral provider for the benefit of the U.S. federal government agencies, although other models could certainly be considered as well. For convenience, this paper continues to refer to the entity as an FFRDC.

In general, FFRDCs are a trusted and objective agent and extension of the government that has the balanced flexibility of hiring, procurement and operations, and brings an R&D perspective that can be aligned with DOD. Further, an FFRDC is well-positioned to interact with industry, academia and other stakeholders in developing industry-wide standards and promoting repatriation of manufacturing. The envisioned FFRDC would be sponsored by Office of the Secretary of Defense or another defense organization in order to effectively coordinate any national strategy around a trusted foundry or efforts that seek to incorporate and verify current non-trusted components developed by broader market demand (i.e. autonomous vehicles, internet of things, etc.). The FFRDC would collaborate with other FFRDCs and research institutions, as well as leverage their unique facilities and capabilities, such as those sponsored by the DOD and the Department of Energy (DOE). In addition, the FFRDC would be separate

from but would interact with the semiconductor industry and, as appropriate, help push forward on R&D relevant to their vision and interests. A model that leverages existing FFRDCs to conduct research in this domain and designated as "work for others" is not sustainable given the growing importance of ICT security, the speed of evolving threats, and the projected increase in government-wide requirements.

Other efforts to support this goal could include a government-sponsored consortium using the Other Transaction Authority (OTA) through the Naval Surface Warfare Center (NSWC) Crane or the Office of the Secretary of Defense. The consortium would bring together government, industry, and academia experts led by an experienced management organization to support multiple areas of government interest.

Since ideas are not adopted automatically and are susceptible to the winds of public focus, an ongoing effort must drive the practices to secure our national ICT into the national security consciousness. Additionally, continuity is necessary to prevent apathy or lack of follow through from subverting intended security objectives.

Assurance and Access Model

The AUI approach is to stand up a federally funded research and development center (FFRDC), Other Transaction Authority (OTA), or comparably authorized laboratory that can be a trusted agent for the government and conduct activities to provide assurance in the supply chain. This entity would oversee and promote the following types of assurance and R&D activities:

- Independent testing and analysis of the design efforts (including software used), production, distribution and implementation;
- Development of the methodology for, and in support of, vulnerability testing and potential use of commercial off-the-shelf components;
- Research and development at the request of, and with funding from, the government to develop evolutionary improvements to all steps in the supply chain;
- Collaborative research with academic, industrial and other researchers on new methodologies and technologies building on current developments and based on specific needs of the industry (i.e., "use-inspired research"). Such collaborations will establish links to a community of experts to build the network of independent reviewers and "red team" members as needed. This network and the reviews they would participate in conducting will help to continually assure the USG that the supply chain is providing what is needed, the vulnerabilities are identified, and the suppliers are "certified as trusted;" and
- Development of standards for secure ICT testing and components that can integrate security considerations in the design, resulting product and other steps in the supply chain.

AUI, a global leader in focused scientific research and associated microelectronic RDT&E for the last 50 years, proposes to establish the FFRDC noted above or a similar organization. AUI's capabilities are built on its strong legacy of designing, building, and managing the complex, pioneering facilities for world-class scientific research and experimentation. This includes

creating and managing FFRDCs for over half a century, as well as customizing design and low volume prototyping of specialized mechanical components.

Any successful entity – FFRDC, OTA consortium, or otherwise – will require integrating a wide range of stakeholders operating in both secure, classified, and unclassified environments. AUI is well-positioned as a stand-alone, non-profit, education institution to forge the necessary collaborations. In the classified environment, this new organization will develop and validate new domestic design and production solutions to emergent ICT security threats, vulnerabilities, and weaknesses identified by the national security community. Given the number of critical defense and intelligence applications that rely on communications hardware produced in an unclassified environment, the entity's highest mission is to ensure that the U.S. maintains a robust technological advantage by promoting and enabling domestic production capabilities of U.S. manufacturing and industrial partners. AUI proposes that an FFRDC or other similar mechanisms represent the strongest solution for balancing national security concerns with the need for broad domestic scientific collaborations.

Through the integration of industry in this effort—both as participants and suppliers of the items and process steps to be evaluated, as well as organizations that can license and help transfer any developments that emerge from the research and development efforts—the proposed entity would be able to strengthen the U.S. industrial base and increase its competitive advantage both domestically and globally. In so doing, our proposed model would contribute to long-term mission assurance and R&D throughout the entire procurement chain, including design, distribution, and use of microelectronics and associated software.

The following specific roles and activities are envisioned in the initial phase of work (first 1-2 years) that would be pursued by the FFRDC:

- Engagement with U.S. Manufacturers and Supply Chain Management: AUI will conduct a series of focus groups with providers of secure microelectronics to help identify recommendations for standards or technology that would be useful to share with the broader cleared manufacturing community. AUI will work with approved US-based manufacturers to find ways the entity can assist in promoting U.S. industry, incorporate improved security as a competitive advantage, and encourage the repatriation of manufacturing capacity to the U.S.
- Long-Term Research Plan Development: Stakeholders will identify key areas of research necessary to 1) improve the development, analysis, testing, and validation of hardware; 2) create new and improved standards for enhanced security; and 3) identify automated methods to detect new and emergent cybersecurity threats. AUI will engage the broader research community in debating and advancing these issues through a variety of means, including: presentations at secure industrial conferences; sponsorship of one or more conferences specific to addressing the entity's mission; local forums at existing public and private research organizations; collaboration with appropriate scientific societies; and publication in approved technical and/or scientific journals. Through this process, a long-term research plan will be developed to both encourage independent

research on the topic and create a roadmap for future research.

- Development of Standards: AUI will work with stakeholders and the appropriate government agencies to establish common, objective, measurable criteria for assessing the integrity and security of ICT hardware that can be used across multiple critical infrastructure sectors. AUI will also work with relevant industry stakeholder groups to promulgate security standards and remove obstacles to U.S.-based manufacturing.
- Hardware Testing and Validation Pilot: The entity will implement hardware security analysis, testing, and validation services at the core of the organization's mission. Testing and validation will occur on select types of information and communications technology hardware based on new security standards from DOD and the Department of Commerce (DOC). It is anticipated that the Center will leverage existing university test capabilities to rapidly facilitate a startup (e.g., Georgia Tech's secure Cybersecurity, Information Protection, and Hardware Evaluation Research Laboratory, University of Florida's - Florida Institute for Cybersecurity Research, University of Maryland Center for Advanced Lifecycle Engineering (CALCE), Rochester Institute of Technology's National Center in Cybersecurity Research, and University of Alabama's Cyber Institute, etc.). The entity will focus on commissioning specialized equipment and facilities required for complying with security requirements developed in cooperation with DOD and DOC.

In steady-state (years 2 through 10), the organization would provide mission assurance and R&D in throughout the procurement chain, from design through distribution and use of the microelectronics, as well as the software that will be run on them. In the near term, the entity would develop a strategic national security R&D roadmap. The R&D roadmap areas of interest would likely include many of the following topics:

- **Basic Areas**
  - Methods
  - Software
  - Materials
  - Applied Math
- **Testing and Evaluation**
  - Counterfeit Detection of commercial off the shelf technology – how to evaluate to identify and understand risks
  - Reverse Engineering
  - Evaluating Fabricated Units
  - Integration and Assessment
  - Radiation Hardening
- **Other Specific Areas of R&D in Trusted Microsystems**
  - Field-Programmable Gate Array (FPGA)
  - Photonics Microsystems
  - Acoustic Bandgap
  - Advanced Sensors
  - Quantum Information Processing

LAYING THE FOUNDATION:

AUI anticipates that initial first-year funding of $30 million (with a range of $20M-$40M over the first 5 years) will allow for the development of the collaboration network and the capabilities necessary to operate, locate, and equip the initial facilities, and develop long-term operations plans. During the first year, much of the work will be performed at existing facilities (i.e., current FFRDCs and other secure research facilities run for the government). Efforts will also be spent developing a set of siting criteria and identifying potential sites for long-term work of the FFRDC.

The breadth of economic sectors reliant on microelectronics components dictates that a variety of approaches, and funding streams, will be required to create change in industry practices. AUI anticipates that the creation of security standards and validation of hardware to those standards will be borne by national security agencies when the components involved have direct (and likely unique) national security ramifications. Products intended for non-defense or intelligence uses will also be eligible for validation and testing, though the center would look for a broad array of funding sources (such as cost shares with private industry and academia, as appropriate). Additional funds will be available to support new research into security requirements, development of new standards, promulgation of information encouraging companies to purchase and develop components certified by the FFRDC, and expansion of FFRDC efforts to new industries.

BUSINESS CASE FOR SUSTAINING AND ADVANCING PUBLIC-PRIVATE PARTNERSHIPS:
Public-private partnerships that will engage and motivate commercial partners must recognize the important economic and market drivers of the industry (better, cheaper, faster). The FFRDC can take the lead in this partnership through an understanding of the factors impacting corporate decisions of hardware manufacturers, logistic and supply chain partners, software developers, and clients themselves, among other parties. However, while there are many factors in corporate decision-making, the most important is profitability. Commercial partners can reap financial benefits by offering products with security and resiliency as primary differentiating factors. This will not only advance the partnership but allow it to self-sustain as economic benefits accrue to the commercial partners.

Solutions will require focus on not only the security of individual microelectronic components and the systems they are employed in but the overall resiliency of the national defense and intelligence operations against cyberattack. This is directly complimentary with the dual focus of Critical Infrastructure Security and Resilience as championed and implemented by the Department of Homeland Security (DHS). An added benefit is this broader approach also requires expanding efforts beyond just manufacturers to include the other ICT stakeholders.

As discussed throughout this paper, the proposal's primary tool for ensuring security and resiliency of microelectronics is through the validation and certification of components (and related logistical chains) by an FFRDC or similar entity. By obtaining these certifications, companies can show customers the security of their products and the financial returns of

selecting these products of others non-certified products. However, to push the overall goal of increasing U.S. microelectronic production, AUI will also focus on tracking and certifying the "provenance" of components and logistical train activities. This will provide partners an alternate, less intensive manner of participating while still accruing the Resiliency Dividend. Between 1) certifying U.S. provenance and 2) validating adherence of components to developed standards, the partnership will show benefits to commercial customers such as:

- Certifying manufacturing origin of both first-tier components and final product assembly;
- Reducing the risk of tampering during logistical transport;
- Preventing the use of pirated or fraudulent components (to the benefit of both manufacturers and customers); and
- Protecting the intellectual property of manufacturers and suppliers from interception and inspection at international borders and during transport in foreign countries, among others.

AUI anticipates being able to demonstrate all these benefits to commercial partners from an early stage and that will encourage industry to join the partnership as the entity grows. This will begin with companies doing business directly with U.S. national security agencies but will grow through connections to other industries with high vulnerability to cyberattack and which may realize higher resiliency dividends. These include the firms inside and supplying to the U.S. energy sector, which is vulnerable to attack by foreign government adversaries, and firms in the healthcare device manufacturing sector.

SUSTAINMENT AND ADVANCEMENT OF THE FFRDC

The activities of the proposed entity (e.g., the FFRDC) can be divided into two main buckets: assurance and R&D. The assurance activities would include independent testing of technologies and components from vendors that would aim to supply the USG with trusted microelectronics, including the design methods and software and the distribution and implementation parts of the supply chain. The R&D activities would focus on improving the technologies and methodologies for designing, manufacturing, distributing and implementing microelectronics, including the development of standards for secure ICT that can be implemented by industries designing, manufacturing and delivering trusted microelectronics.

Funding for the assurance efforts at an initial estimated cost of $30M/year would initially be provided by the Department of Defense and other parts of the national security enterprise. During an initial five-year period, the intent would be to develop and implement a model that can recover the costs for the assurance effort through a combination of fixed and variable fees levied on the suppliers to the USG of trusted microelectronics. As currently envisioned, the fixed fee would be related to assuring that a specific design or method has met a set of standards (similar to a "UL" certification but for trusted microelectronics), while the variable would be related to units sold to a USG customer requiring trusted microelectronics. As a result, the quality assurance efforts needed, including the R&D needed to continually improve the testing, would become part of the cost of doing business of supplying trusted

microelectronics to the USG. Transparency would be provided because the entity would be able to independently provide data about costs and activities to the Department of Defense and other parts of the USG.

Funding for the R&D efforts would be provided through competitive grants and contracts from the Department of Defense and the national security enterprise. In addition, funding for R&D would be pursued, including from private companies, other federal agencies, state governments, and foundations. It is expected that the non-Defense support will grow to be between 20-30% of the overall R&D budget, based on experience seen with other FFRDCs. All R&D would be pursued collaboratively with researchers from academia, industry and other research institutions. A significant aim of the R&D pursuits and the partnerships with collaborators and their institutions would be to develop technologies and methodologies that can be transferred to industry, either as published research (either in open literature or through secure distribution channels, as dictated by the research and related constraints) or as intellectual property that is licensed.

For both the assurance and R&D activities, it is expected that the facilities needed would come from a combination of new facilities (standard laboratories, clean rooms, equipment, test stands, etc.) and uniquely equipped facilities provided through agreements with partners. The value in having new facilities and equipment is that they can be developed expressly for the purpose of testing leading edge ICT in a trusted environment (i.e., new facilities would not be constrained with existing, built-in flaws or vulnerabilities). The value in relying on partners for unique facilities and equipment that already exist is to reduce overlap and duplication, and thus minimize the costs for standing up, say, a world leading microscope, a one-of-a-kind radiation hardening manufacturing line, or similar unique facility that might be readily available and would only be needed by this entity on a periodic basis.

Specific partners would likely include Lincoln Laboratories, Sandia National Laboratories, other Department of Energy National Laboratories or facilities, various UARCs, and other entities that conduct research in leading edge microelectronics (e.g., IBM). Such collaborations would facilitate robust collaborations with leading researchers and institutions (including industry) in this space, and provide insights to help this entity stay abreast of the breakthroughs and process developments to ensure that the assurance capabilities can accommodate them. Potential collaborations would be subject to careful scrutiny to ensure the trusted agent aspect of our proposed FFRDC. At the same time, such a collaboration would need to be open enough to provide transparency to the manufacturers about expectations, testing and analysis protocols used, and results; engage their staff in the development of the standards; and solicit their involvement in the “red teams” and reviews mentioned above.

Mechanisms for engaging partners to allow for use of unique facilities would be through use agreements, memoranda of agreement/understanding, and contractual arrangements, as needed depending on the partner and the specific need for their facilities. Combined, the facilities associated with the proposed entity supplemented with access to partners’ unique facilities and capabilities would be an incredibly valuable resource for researchers. In addition,

there would be staff researchers at the proposed entity who are well positioned to help solve unique problems. As a result, some of the capacity for the R&D component could be run as a User Facility. A user facility is a research facility available by external researchers, typically under conditions such as:

- The facility is open to all interested potential users, but in this case as currently envisioned, access would be limited to researchers from trusted institutions who themselves have been vetted.
- Allocation of facility resources is determined by merit review of the proposed work, and in this case, the peer reviewers would come from the network mentioned above.
- User fees are not charged for non-proprietary work if the user intends to publish the research results. Full cost recovery is required for proprietary work. This model would apply for the proposed facility, although there would be a review and an imposed waiting period prior to publishing data from the facility to determine if publication in the open literature or some other secure distribution channel is warranted.
- The facility provides resources sufficient for users to conduct work safely and efficiently, and this would be employed in the proposed facility.
- The facility supports a formal user organization to represent the users and facilitate sharing of information, forming collaborations, and organizing research efforts among users, and this would be employed for the proposed facility and would comprise collaborators from the network mentioned above.
- The facility capability does not compete with an available private sector capability, and this would be true for the proposed facility as a key idea would be to supplement existing capabilities and enable the domestic supply chain to substantially improve their products and processes for implementation in the USG (i.e., for trusted ICT applications).

In this latter part, the model would be similar to the Bioenergy Research Centers run by the Department of Energy and comparable to the National Network of Manufacturing Institutes (NNMI) run by various agencies, including the Department of Defense. In these models, the centers generally bring together manufacturers, academia (universities, community colleges), government (federal, state, regional), and non-profits to pursue unique, but often industrially relevant, technologies with broad applications (i.e., real-world use inspired research). The aim is to accelerate the path toward commercial use and reduce the cost and risk of commercializing new technologies, manufacturing methodologies, and related activities, as well as to foster the education, training and innovation. The “users” bring their issues to the center, collaborate with the center to use the facility and tap the knowledge of the researchers, and work to solve the issue. A model similar to this would be applicable to the trusted microelectronics discipline, particularly as many aspects of the supply chain would be improved to enhance the security of the product for the USG.

The business case described above is preliminary but is based on the experience of AUI’s management team, and AUI’s heritage, which involves standing up and managing FFRDC’s for the National Science Foundation and the Department of Energy.