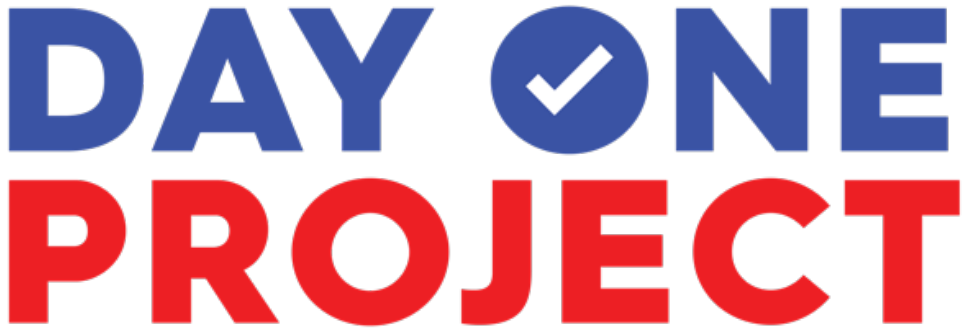

A National Secure Electronics Initiative

Eric Breckenfeld

October 2020

The Day One Project offers a platform for ideas that represent a broad range of perspectives across S&T disciplines. The views and opinions expressed in this proposal are those of the author(s) and do not reflect the views and opinions of the Day One Project or its S&T Leadership Council.

Summary

Semiconductor integrated circuits (ICs) will continue to play an increasingly significant role in society as smart phones, internet-of-things (IoT) devices, artificial intelligence, autonomous vehicles, 5G communications, and other vastly interconnected technologies redefine many facets of daily life in the United States. The interconnectedness of these technologies presents novel opportunities for adversaries to exploit these systems for financial or strategic gain. The present geopolitical difficulties between China and the US, coupled with supply chain interruptions associated with the COVID-19 pandemic have made concerns about the robustness of the IC supply chain especially germane. In particular, China's enormous investment[1] in expanding its production capacity of advanced ICs is of grave concern. Against this landscape, there is an exciting opportunity for the next administration to develop a sophisticated American IC security infrastructure by launching a National Secure Electronics Initiative (NSEI). The NSEI will set a goal of achieving levels of security for electronic hardware in defense and commercial sectors at the design, manufacturing, and deployment stages with quantifiable strength comparable to the protections available at the software and data level, such as the Advanced Encryption Standards (AES).[2]

Through NSEI, the next administration will ensure that not only defense, but also municipal and commercial supply chain processes, data, toolsets, key personnel, and facilities are secured against penetration by external threats or subversion by internal threats. The NSEI will integrate defense efforts and advancements with the commercial and municipal sectors by developing a more robust innovation pipeline through investments in early stage research, working across industry, government, and academia to develop a comprehensive set of security metrics, and fully leveraging the resources and expertise of other government agencies beyond those tied to defense. Making the United States a pioneer of such efforts would also represent a significant value add for domestic design and manufacture of electronic devices.

To reach these goals, the federal government should undertake a comprehensive agenda, led by the White House via the NSEI, to greatly expand existing efforts in the secure microelectronics space, such as the DoD Trusted and Assured Microelectronics (T&AM) program, and extend those efforts to better include the commercial and municipal sectors in addition to defense. The NSEI should complement but not depend upon other potential parallel efforts in this space. For example, two pieces of legislation, the CHIPS for America

[1] Josh Horwitz, Samuel Shen, "Sino-U.S. Tech Race Turbo-Charges China Chip Investment, Triggering Bubble Fear", Reuters, 2020, www.reuters.com.

[2] National Institute of Standards and Measurements, "Announcing Development of a Federal Information Processing Standard for Advanced Encryption Standard" , Federal Register, Vol 62, 1997.

Act[3] and American Foundries Act of 2020[4], have recommended the expansion of onshore capacity in advanced node ICs. The Semiconductor Industry Association has made similar recommendations and provided estimates for the potential impact of either $20B or $50B worth of federal investment in this space.[5] The technologies developed under the NSEI would improve electronic security regardless of where the devices were manufactured, but would benefit from an expansion in domestic capacity. This is critical because although an increase in US manufacturing of advanced ICs is desirable on its own merits, the security of defense, consumer, and municipal electronics should not hinge on such developments.

Accomplishing the goals outlined below will secure the nation's place at the forefront of global microelectronics security. The consequences of inaction may lead to more powerful cyber-attacks (e.g. rising attacks on health[6] or financial[7] infrastructure, military hardware subversion[8] by adversarial states) on personal data, infrastructure, or vulnerable defense targets.

Challenge and Opportunity

ICs provide the foundation of all computing and information systems. Significant effort at the federal level has been dedicated to the development of security standards, metrics, and protocols for data and software over the past 30 years. However, given the global nature of the IC supply chain, the threat surface for potential cyberattacks has grown to encompass not only software, but firmware and hardware as well. These potential threats are present throughout the hardware manufacturing life cycle, beginning with conception and design, through manufacturing and assembly, and finally deployment and operation across a system's operating lifetime. Specific threats include intellectual property (IP) theft, counterfeiting and overproduction by manufacturers, unauthorized reverse-engineering, and malicious design modifications/insertions, sometimes referred to as "hardware trojans". The reality of such attacks has already potentially damaged dozens of U.S. companies (and also potentially U.S. federal agencies), when a widespread package-level attack was supposedly discovered and reported on in 2018.[9] The White House's Council of Economic Advisers has estimated up to $109B worth of economic damage to the US in 2016 alone[10] as a result of malicious cyber activity, in which electronic hardware attacks will play an increasingly important role. Additionally, a survey conducted in 2019 indicated that over 60% of companies in the US faced

[3] U.S. Congress, House, CHIPS for America Act of 2020, H.R.7178, 116th Congress, Introduced to House June 11th 2020, https://www.congress.gov/bill/116th-congress/house-bill/7178?s=1&r=5.
[4] U.S. Congress, Senate, American Foundries Act of 2020, S.4130, 116th Congress, Introduced to Senate July 1, 2020, https://www.congress.gov/bill/116th-congress/senate-bill/4130.
[5] Antonio Varas et al., "Government Incentives and US Competitiveness in Semiconductor Manufacturing", SIA, 2020.
[6] David Winder, "Cyber Attacks Against Hospitals Have 'Significantly Increased' As Hackers Seek To Maximize Profit", Forbes, 2020.
[7] Maggie Miller, "Financial Firms Facing Serious Hacking Threat In COVID-19 Era", The Hill, 2020, www.thehill.com.
[8] Brad Lendon, "Iran Says It Built Copy Of Captured U.S. Drone", CNN, 2014, www.cnn.com.
[9] Jordan Robertso and Michael Riley, "The Big Hack", Bloomberg Businessweek, 2018, www.bloomberg.com.
[10] The Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy", The White House, 2018, www.whitehouse.gov.

data loss over the previous 12 months as a direct result of hardware level security breaches.[11]

There are a number of consequences that could arise from attacks on the hardware supply chain.

- IP theft can occur at many stages of the design and manufacturing cycle. For defense applications, this can result in the inadvertent leakage of specialized military designs. For commercial entities, this can represent the loss of competitive edge between individual firms, or between the firms of one nation and those of another if the attack is carried out by a nation state. The full damage of such an attack depends on many complex factors potentially unique to the specific designs, their intended use, and the firms in question.
- Counterfeiting and overproduction represent purely economic threats, but adversely affect the competitiveness of US commercial entities. Both are a direct result of the globe-spanning nature of the electronics hardware manufacturing supply chain. Counterfeiting occurs when component manufacturers deliver products that underperform their stated specifications. They may be recycled versions of the original commercial product or less expensive look-alikes. Overproduction is similar to IP theft, and is the result of skyrocketing design costs for complex ICs and the contract foundry business model, where many companies will send their proprietary designs to a single, independent foundry. An unscrupulous foundry with access to a firm's IP has the capability to produce parts in excess of the amount agreed upon in the contract. Such excess parts can then be sold on the open market, undercutting the value of the part.
- Malicious insertion of hardware into the design of a circuit or packaging is the most serious threat for the hardware supply chain. Although the insertion itself does not necessarily do any specific damage to the operation of the component or device in question, it opens the door for additional attacks enabled by the compromised hardware. Depending on the nature of the inserted "hardware trojan", the additional attacks include theft of data, tracking and surveillance of clandestine military system, and "kill switches" that can completely disable a component or system. Weaknesses can also be built into the hardware that can later be exploited by software to achieve the aforementioned results.

These concerns have prompted several actions by the Department of Defense (DoD) over the last 20 years, such as the Trusted Foundry Program (TFP) in 2003, which established a series of requirements that a foundry facility would need to meet in order to be considered "trusted". Among other responsibilities, these facilities would provide an assured chain of custody for ICs, ensure against reasonable threats related to supply disruption, prevent modification or tampering, and protect the ICs from unauthorized reverse engineering attempts. Although this trust model did prove valuable, the relative growth of offshore vs. onshore capabilities made it increasingly difficult or impossible to accredit advanced node foundries. More recent efforts, such as the 2017 launching of the Microelectronics Innovation for National Security and

[11] Sheye Daniels, "BIOS Security – The Next Frontier for Endpoint Protection", Forrester Consulting, 2019.

Economic Competitiveness (MINSEC)[12] effort, and broader T&AM efforts at Naval Surface Warfare Center (NSWC) Crane, Air Force Research Laboratories (AFRL), DARPA, Defense Microelectronics Activity (DMEA), and other parts of the defense sector have attempted to address the gaps in the TFP model of protection. While these DoD-led efforts have yielded promising results, four major gaps remain in the implementation and eventual success of a broader secure electronics strategy in the commercial and municipal sectors:

- Narrow focus on defense-critical systems
  The research, development, and demonstration (RD&D) efforts funded by the DoD thus far have focused on technologies of unique value to national defense, such as military GPS communications platforms. Historically, these technology platforms were most likely to be attacked by an adversary. However, the increasing interconnectedness of municipal, financial, and health systems makes the foundational hardware for those systems similarly attractive to such adversarial attacks. Furthermore, solutions tenable to the DoD, which depend on the military's unique ability to purchase or produce low volumes of custom parts with enormous cost overhead, may not be tenable to those civilian sectors at the highest risk of attack. These issues, taken together, prevent the developed protections from being easily generalized to other sectors, which could greatly benefit from enhanced electronic security, such as smart and interconnected municipal systems or commercial autonomous vehicles.

- Underdeveloped early stage research
  The DoD's current efforts have overwhelmingly focused on solutions that will have a near-term impact on the identified issues. To use DoD terminology, these solutions have been developed at the *Demonstration and Validation* maturity level or higher, bypassing efforts at the *Basic Research*, *Applied Research*, and *Advanced Technology Development* levels. As such, there is a missing stage of the pipeline for novel groundbreaking technologies to reach maturation. Specifically, early research and development in this area is underdeveloped. The absence of a comprehensive pipeline which could rapidly mature promising technologies from basic research up through development and deployment is a significant gap in the innovation cycle for electronics hardware protection.

- Insufficient development of standards, metrics, and protocols for hardware security
  Due to the DoD's focus on near-term solutions, those technologies currently under development tend to target known threat models for current vulnerabilities. A key success of the development of the AES encryption scheme was the creation of a robust set of standards, metrics, and protocols to assign quantitative values to security, which have remained valid since the adoption of AES in 2002. Likewise, hardware security will need to develop standards, metrics, and protocols so that (1) threat models can be

[12] Jeremy Muldavin, "DoD Trusted and Assured Microelectronics Summary", Invited Talk, NDIA Electronics Division Meeting, Arlington, VA, Feb. 2019.

scaled appropriately as attacks become more advanced; and (2) the benefits and tradeoffs between different methods of technology protection can be compared against one another. The current lack of robust metrics is another impediment to the continued development of electronics hardware protection, and government has the opportunity to serve as a convening authority on the development of these standards, metrics, and protocols alongside industry.

- Inability to leverage full capabilities of federal agencies
  Given the focus on defense-relevant technology platforms, the federal agencies that have participated in the development of electronics hardware security have primarily been connected to the Joint Federated Assurance Center (JFAC), and thus extensively DoD-focused, with the exception of the DOE-affiliated Sandia National Laboratories. There are some DOE-led efforts, such as the Cybersecurity Institute for Energy Efficient Manufacturing,[13] which has been announced in 2019 and funded by the Advanced Manufacturing Office, though its full role is presently unclear. The absence of collaboration with other agencies inserts speed bumps into the implementation of novel technological solutions. The present lack of a coordinated effort across relevant federal agencies is a great opportunity for leadership at the administration level to coordinate efforts among other potentially relevant federal groups (National Science Foundation, Department of Energy, Department of Commerce, the Manufacturing Institutes, and others) in the development of a comprehensive electronics hardware protection strategy.

Although these challenges are daunting, never before has there been a more opportune time to take action at the administration level. The DoD is in the process of re-evaluating its strategy for microelectronic manufacturing security[14] for the next generation of electronic hardware. The economic impacts of the global COVID crisis have helped expose certain supply chain vulnerabilities in the defense and consumer sectors.[15] Members of Congress have expressed support for the changes that the DoD is pursuing.[16] This past year, Congress has introduced bi-partisan legislation, such as the American Foundries Act,[17] aimed at targeting portions of this issue, with the goal of including similar language in the NDAA. There is an enormous opportunity for these efforts, coupled with a strong vision of leadership from the administration, to have a deeply transformative impact at a critical time for the field of microelectronics manufacturing and security.

[13] Department of Energy News Media, "DOE Announces $70 Million for Cybersecurity Institute for Energy Efficient Manufacturing", Department of Energy, 2019, www.energy.gov.
[14] C. Todd Lopez, "DoD Adopts 'Zero Trust' Approach to Buying Microelectronics", DoD News, 2020, www.defense.gov.
[15] David Vergun, "Pandemic Revealed Supply Chain Vulnerability, Pentagon Official Says", DoD News, 2020, www.defense.gov.
[16] Amy H. Peterson, "Grassley Letter Sheds Light on Microelectronics", , Estherville News, 2020, www.esthervillenews.net.
[17] Office of Senators Charles E. Schumer, "With the Support of new York's Semiconductor Industry, Schumer Announces Bipartisan American Foundries Act…", Schumer Newsroom, 2020, www.schumer.senate.gov.

Plan of Action

The next administration, building on the DoD's MINSEC and T&AM efforts, as well as those efforts ongoing in Congress, should establish a National Secure Electronics Initiative (NSEI) focused on addressing the four previously identified major gaps.

Engage in public-private partnerships with commercial and municipal sectors

Although efforts from the DoD have traditionally targeted defense applications and sought to leverage the specific strengths of the DoD supply chain, there is a mutually advantageous opportunity to integrate these efforts with the commercial sector. The first opportunity lies in the development of technologies that allow the defense industry to manufacture DoD-critical products with access to the full range of global manufacturing capabilities, not just those facilities which are captive to the DoD or wholly contained within the US. Despite its advantages, the strategy of manufacturing defense-critical electronics only in the most secure fabrication facilities limits the DoD's ability to access state-of-the-art electronics. Since 2017, T&AM and related efforts have begun to develop technologies that hinder or prevent the primary security concerns that would arise at a potentially adversarial manufacturing facility (IP theft, counterfeiting, reverse-engineering, malicious insertions), which would allow the defense sector full access to the global semiconductor supply chain, and thus ensure state-of-the-art electronics access. The administration should use Title III of the Defense Production Act to fund the scaling up of these technologies once they have matured through research and development.

The second key opportunity lies in accelerating the security of commercial and municipal electronics hardware using the hardware protection capabilities that are under development at the DoD and commercial defense companies. This could include GPS or inertial navigation systems for autonomous vehicles, any number of sensors for smart cities applications, server infrastructure for financial or healthcare databases, or any smart devices for power/water distribution. Each of the aforementioned cases not only has significant overlap with DoD hardware deployment logistics, but also is a potentially attractive target of attack for a hostile nation state. There is also value in providing hardware protection for those cases which are not similar to defense electronics. Many commercial products, such as smart phones, have very short deployment lifetimes and thus do not present an attractive target for malicious insertion. However, there is still a risk of IP theft, counterfeiting, and overproduction. Thus, although it may take some redevelopment, there is enormous value in transitioning many of the DoD efforts in the area of hardware protection to the commercial sector. The NSEI can accomplish this by coordinating collaborative efforts between defense and commercial research groups in order to share the results of successful programs and potentially pursue follow-on efforts funded via SBIR or similar vehicles.

Develop a more robust ecosystem of early stage research

The first step of such a pipeline is more funding for basic research in hardware security. Next, it is key to set up government adjudicators, or accredit commercial adjudicators who will help

identify promising technologies which should be accelerated in maturity. DARPA has recently had success in working with the Information Sciences Institute (ISI) and MIT Lincoln Labs to develop a similar process for improving hardware security in a large test circuit based on a military GPS receiver, using the following process: First, empower government adjudicators or program managers to identify promising developments in early stage research from academic and commercial research groups already working within this space. Second, enable early maturation through rigorous testing and collaborative red-teaming in order to work out flaws or vulnerabilities in these promising new technologies. This could be done by assigning funding to red-team competitions at professional conferences or university events. An example of this on a far smaller scale is NYU's Cybersecurity Awareness Worldwide (CSAW)[18] event, where research teams provided circuits that had been protected with a "logic locking" technology to red teams who attempted to attack the protected circuits. Finally, accelerate the ability of a mature technology to scale-up to become relevant to a real technology platform, such as an authentic military GPS receiver. This step of the process will down-select to the most promising technologies identified at the previous stage and engage commercial partners or federal offices who can best assist in scaling up the novel technology to real-world relevance. Having commercial partners help scale these methods is one way to begin transitioning such technologies from a pure defense application to the consumer space, which benefits these companies by improving the products they are able to offer individuals and the DoD. Government and accredited industry adjudicators are most valuable in steps two and three.

In order to assist with the efforts described above, the following supplements to agency research budgets are recommended:

- $2B to Department of Defense for key efforts identified such as T&AM, the Electronics Resurgence Initiative at DARPA, or others. The emphasis on these programs should be towards transitioning technologies to better impact government and commercial applications.
- $1.25B to the National Science Foundation. These efforts should focus on early stage research in the areas identified, and should consider not only the current state of fabrication and design, but also what the industry might look like as advances in automation and machine learning continue to revolutionize manufacturing processes.
- $1.25B to the Department of Energy. These efforts should focus both on early stage research through the Office of Science, and technology testing and transition through key national laboratories.
- $500M to the National Institute of Standards and Technology for early stage research and the development of metrics.

[18] NYU Tandon School of Engineering, "World's Most Comprehensive Student Cybersecurity Games Announce Winners of CSAW 2019", Press Release 2019.

This funding would go specifically towards R&D efforts in the hardware security space targeting near (0-5 year) and medium (5-15 year) term threats. Previous efforts[12] have focused predominantly on the "problems of today", which have sometimes left early stage research out of the equation. This funding would attempt to address the entire innovation process, beginning at the early stage, and would include mitigations against future potential threats.

The ultimate role of the NSEI in this process would be the coordination of efforts. The research offices engaged in microelectronics research can be roughly divided into two distinct categories: those who engage with the subject at the research and development level and those who engage at the implementation or mission level. Since these groups can be spread across multiple agencies with different goals, it is important to have thorough coordination of efforts within each category. It is also critical for the NSEI to identify opportunities for collaboration and cross-pollination between the two groups, where it makes sense. A precedent for this already exists with the coordination offices for the National Nanotechnology Initiative (NNI) and Networking and Information Technology Research and Development (NITRD) program.

Develop robust metrics

Given the difficulties discussed so far, it is clear that a new set of higher resolution metrics need to be developed so that a more comprehensive understanding of risk management can emerge in this sector.

In order to move beyond the "trust" model, new metrics must focus on the classic Risk factors of Threat, Vulnerability, and Consequence[19] in order to better capture the reality of hardware attack risks and mitigations.

These metrics must address:

- What is the likelihood of a successful attack being carried out for a given attack (e.g. malicious insertion)?
- What is the consequence of such an attack (e.g. data theft, damage to infrastructure)?
- What is the probability of the attack going unnoticed long enough for the consequence to bear out?

For attack risks, metrics will need to individually consider the following stages of device lifetime:

- Conception and design
- Manufacturing and assembly
- Deployment and operation

There are very likely additional considerations which will need to be included in the development of these metrics, and the NSEI should rigorously pursue input from the government and commercial sectors. If successful, these metrics will help the government and commercial firms make more informed decisions about what protections are most prudent for given systems based

[19] Roek Van Impe, "Simplifying Risk Management", Security Intelligence, 2017, www.securityintelligence.com.

on their unique risk and cost tolerances. They will also help foster innovation into new mitigation strategies and technologies by clarifying which areas of the risk landscape need additional effort to address.

Leverage other agency resources

Additionally, this proposal aims to leverage additional government resources, beyond the DoD's capacity. A non-exhaustive list of agencies that would be valuable to include in the NSEI are:

1) National Science Foundation (NSF)

Investment in basic research at the academic level will provide a critical pipeline for new technologies. In order to fully leverage the US innovation ecosystem, it is important to find ways to foster early innovations and identify technologies for rapid maturation. The ability of the NSF to contribute to electronic hardware security will be further enhanced by the increase in research funding recommended above.

2) Department of Energy (DOE)

The DOE Office of Science can provide a very similar role to that of the NSF in fostering early research and development. Certain offices within the DOE Office of Energy Efficiency and Renewable Energy can also contribute domain expertise at a more technical level than the Office of Science. For example, the Advanced Manufacturing Office could make valuable contributions in the area of electronics additive manufacturing for anti-tamper applications. Finally, the role of the DOE National Laboratories, which already participate in the JFAC T&AM efforts, could be expanded.

3) Department of Commerce (DOC)

The National Institute of Standards and Technology (NIST) provides a critical research service to the federal government in many technical areas. The involvement of NIST was a cornerstone of the development, validation, and approval of the AES algorithm. Similar efforts will ultimately need to occur for electronics hardware security metrics.

4) Department of State (DOS)

The International Traffic in Arms Regulations (ITAR) guidelines are under the purview of the DOS. In short, these regulations limit the flow of defense technologies to non-US entities. If technologies developed within the DoD framework are going to be successfully transitioned to the commercial or municipal sector, having stakeholders from the DOS serve in an advisory capacity will be key to ensure full compliance with ITAR guidelines.

5) Intelligence Community

The innovations that occur in the unclassified academic world may have applicability in addressing concerns of the Intelligence Community. As such, their involvement in the NSEI could provide opportunities to transition promising early technologies into a framework that suits their unique requirements.

6) Manufacturing USA Institutes

There are a number of inter-agency efforts which could be leveraged to assist with the success of this proposed initiative. A good set of examples are the Manufacturing USA[20] institutes which convene commercial, business, and academic perspectives for several emerging technology focus areas. The Advanced Functional Fabrics of America (AFFOA) and NextFlex institutes both contain electronics packaging within their portfolios and would be valuable networks for the NSEI to leverage. The aforementioned Cybersecurity Institute for Energy Efficient Manufacturing has been announced by the DOE in 2019 and would ideally emphasize early stage cybersecurity research for vulnerable infrastructure. They would all be ideal partners for the NSEI.

To accomplish these goals, NSEI should RD&D funding to those areas already identified by MINSEC and T&AM, as well as those identified in the 2020 American Foundries Act. Federal resources and leadership, as well as continued engagement with the private industrial and academic sectors, key states and localities, and with Congress are critical for rapid maturation and broad adoption of the key standards, metrics, and technologies developed by this initiative.

In addition to pursuing the above priorities, a comprehensive NSEI should:

1. Bolster domestic workforce development in disciplines and sub-disciplines critical to continued long-term development of these key technologies. This is important because improving the technical competence and competitiveness of US workers in the broad field of circuit design (not only hardware security) will have beneficial downstream effects on electronics security in a holistic sense. This could be accomplished by:
    a. Working with universities and private companies to develop additional curricula aimed at providing more training in physical circuit design for state-of-the-art silicon nodes.
    b. Electronic Design Automation (EDA) companies such as Cadence, Synopsys, and Mentor have historically supported this at some institutions, and these sorts of partnerships should be expanded.
    c. Collaboration with the companies who design and sell chips is critical as well. Carnegie Mellon University (CMU) recently partnered with Apple Inc. to create the Apple Ph.D. Fellowship in Integrated Systems along with a corresponding Masters-level program.[21] This partnership has led to the development of additional curricula at CMU and has helped drive additional students at the undergraduate level to pursue the foundational courses required for these programs. This effort is in the process of being slowly expanded to additional schools, and offers the dual advantage of enriching the curricula for these academic programs and helping educate the type of graduate who can provide

[20] Manufacturing USA, Accessed October 1, 2020, www.manufacturingusa.com.
[21] Carnegie Mellon University Electrical & Computer Engineering "Exploring Integrated Systems", The Circuit Magazine, P.21, 2020.

the most value for the future IC industry. These sorts of collaborations should be incentivized and greatly expanded.

d. Providing financial support for the development of institutional infrastructure to offer professional development opportunities beyond undergraduate or graduate degrees.
    i. With the development of additional circuit design curricula, there is an opportunity to offer these courses outside of the traditional degree structure for later-stage professionals who work at any number of small or large companies who need access to this sort of expertise. The reality of the circuit design field is that training can become outdated after a short period of time as the field advances and it is highly beneficial to have convenient and credible opportunities for continued training in this space.
    ii. During COVID, online learning has provided a tremendous opportunity for working professionals to pursue educational opportunities without taking leave of absence from their career. The administration should capitalize on this opportunity and provide financial support for universities, so that they can formalize the transition to online learning in a post-COVID world and provide highly valuable courses for mid-career training and professional development, such as circuit design.

2. Identify opportunities for adding value to the commercial supply chain and thus incentivizing more rapid adoption of security standards and metrics by the private sector. Such opportunities could include:
    a. Helping provide quantifiable security metrics for commercial products, and therefore provide customers with a better understanding of the cost vs. protection tradeoffs for their data and devices.
    b. Mitigation of supply chain risks, such as the threats of IP theft and overproduction.

A successful NSEI will result in the development of a body of security technologies capable of mitigating threats to electronic hardware for both consumers and manufacturers. Additionally, the NSEI will cultivate a collaborative research and development ecosystem between public and private entities, which will be capable of rapidly developing and scaling novel security technologies as the cyber threat landscape continues to evolve. These technologies may be agnostic towards the expansion or contraction of onshore manufacturing capability, and would represent a value-add in either case. The most important feature is expanding the DoD's ability to mitigate identified risks regardless of access to domestic facilities. The most ideal scenario would include further development of onshore manufacturing capabilities through programs and incentives running in parallel to the NSEI. Full implementation of the NSEI requires comprehensive collaboration across key federal agencies and with the private sector, academia, and states and localities taking into account:

1. White House leadership and coordination: The White House should spearhead the initiative, driving progress throughout the executive branch and mobilizing support in

Congress, industry, science, and the public. Through an Executive Order, the Office of Science and Technology Policy will launch NSEI and catalyze implementation and coordination across agencies.

2. Budget: $459M was assigned to MINSEC and related efforts in 2020. Delivering on the aforementioned goals requires, at a minimum, $5B spending on electronics security RD&D programs for five years, spread out among additional federal agencies as described earlier. This is roughly in line with the recommendation from the American Foundries Act for supplemental R&D funding.
3. Increased agency participation and use of other policy tools: All relevant federal offices (NSF, DOE, DOC, DOS, intelligence community, manufacturing institutes) – not just JFAC Federated Organizations – should pull together to develop and establish mutually agreed-upon security metrics and standards, which can be enforced via regulation, procurement, and other relevant agency tools.
4. Mobilization of non-federal actors: Academia and industry are critical to the success of electronic hardware security RD&D and manufacturing. It is important to establish a robust and continued pipeline for novel technologies in this space and mature these technologies to the point where they can be integrated with market-relevant tools, especially advanced circuit design tools used at commercial EDA vendors.

About the Author

Eric Breckenfeld is a Lead Scientist at Booz Allen Hamilton where he serves as a consultant for predominantly U.S. defense clients, including DARPA and the U.S. Naval Sea Systems Command in the areas of electronic materials/components and hardware supply chain security. Prior to his work at Booz Allen Hamilton, Eric was an AAAS Science and Technology Policy Fellow at the National Nanotechnology Coordination Office where he managed the *Sustainable Nanomanufacturing* and *Nanoelectronics for 2020 and Beyond* Signature Initiatives. Previously, Eric was a National Research Council Fellow at the Naval Research Laboratory where he performed basic and applied research on electronic materials. Eric received his BS in Engineering Physics from the University of Wisconsin-Madison and his Ph.D. in Materials Science and Engineering from the University of Illinois Urbana-Champaign.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of a future presidential term. For more about the Day One Project, visit dayoneproject.org.