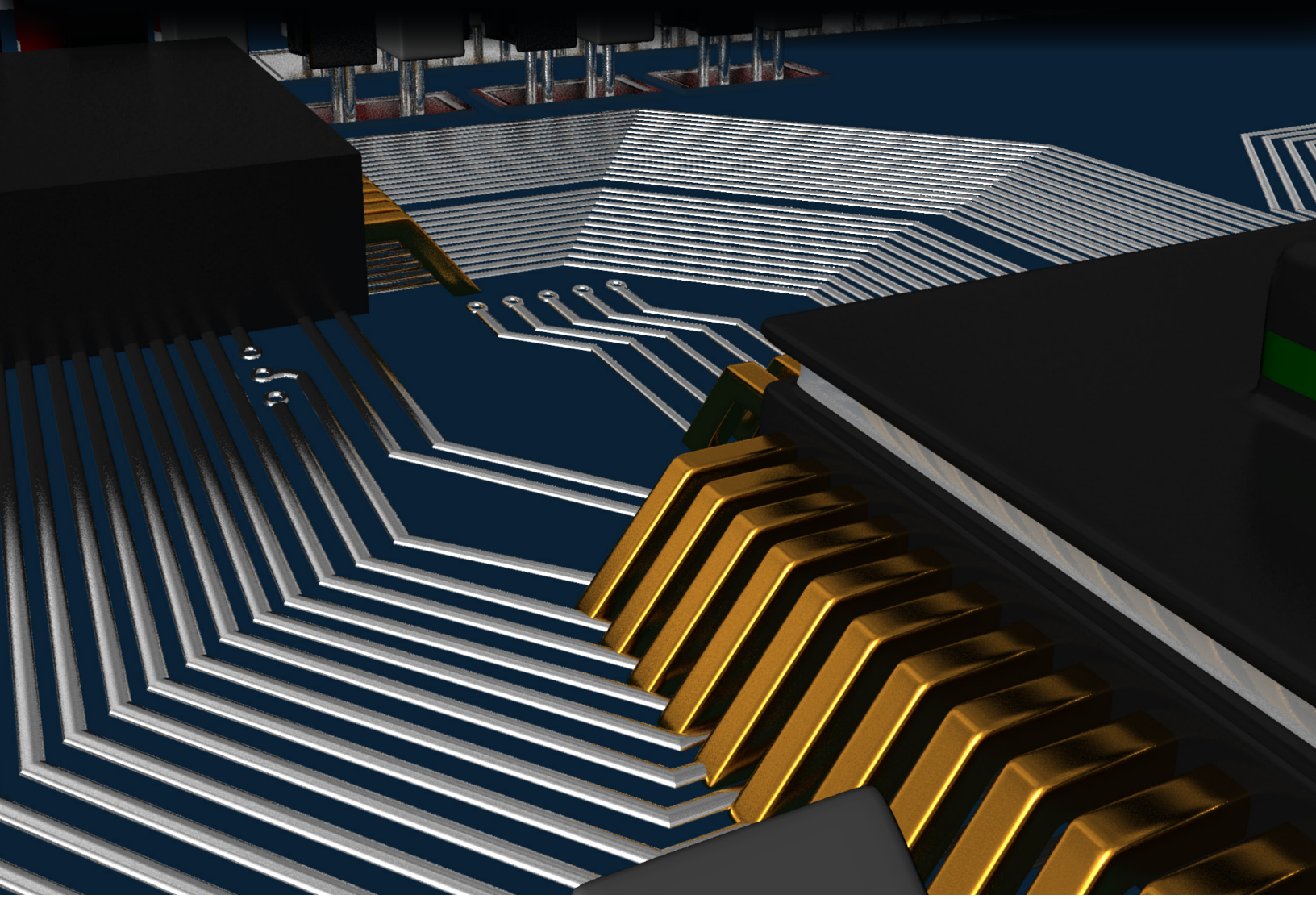
A POTOMAC INSTITUTE FOR POLICY STUDIES REPORT

ENSURING ACCESS TO TRUSTED STATE-OF-THE-ART MICROELECTRONICS



CONGRESSIONAL SEMINAR REPORT

MAY 20, 2016

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200
Arlington, VA 22203

Copyright © 2016
Potomac Institute for Policy Studies

901 N. Stuart St, Suite 1200
Arlington, VA, 22203
www.potomacinstitute.org
Telephone: 703.525.0770; Fax: 703.525.0299
Email: webmaster@potomacinstitute.org

NOTICE: This report is a product of the Potomac Institute for Policy Studies. The conclusions of this study are our own and do not necessarily represent the views of the sponsors or participants.

Please note that the transcript has been edited for publication.

The Potomac Institute for Policy Studies is an independent, 501(c)(3), not-for-profit public policy research institute. The Institute identifies and aggressively shepherds discussion on key science, technology, and national security issues facing our society. From these discussions and forums, we develop meaningful policy options and ensure their implementation at the intersection of business and government.

All images, credit: Alex Taliesen.

Potomac Institute Press

TABLE OF CONTENTS

Executive Summary 4

Background 6

Event Transcript. 9

Speaker Bios 29

Additional Information 34

EXECUTIVE SUMMARY

The United States requires secure and reliable microelectronics to accomplish its national security missions. Our ability to prevent malicious tampering or counterfeiting of these components is of vital importance to the US Government (USG). The highly international nature of the commercial industry today, and the increasing complexity of chips, makes achieving that goal more difficult than ever before. The USG needs a set of options across the entire supply chain to guarantee assured access to secure and Trusted microelectronics. The sale of IBM Microelectronics to GlobalFoundries in 2015 jeopardized trusted access for the USG. In response, a policy to guarantee continued access to Trusted microelectronics now and into the future has been created. The immediate and long-term parts of this solution were funded, yet the crucial steps to guarantee trusted access within the next three to 10 years also needs the necessary budgetary support. The global semiconductor market is rapidly changing, and the USG must adapt its microelectronics strategy to these global market changes. This includes not only reaching agreements with companies for components that have been manufactured in a completely trusted supply chain, but also having back-up plans to ensure that the confidentiality and functionality of components can be trusted, even when the front-end-of-the-line manufacturing comes from an untrusted source.

The Potomac Institute held a Congressional Seminar on May 20, 2016 in order to provide a briefing on major issues in trusted microelectronics and make experts in this area available for discussion. The seminar was attended by Congressional staff and members of government, industry, and think tanks. The speakers included Michael Swetnam, The Honorable John Young, Jr., Mr. Ken Colucci, and Ms. Melissa Hathaway.

The speakers identified major issues in hardware security and discussed the importance of maintaining access to trusted microelectronics for defense systems. Major issues addressed included:

- Electronics are key components in our defense systems, and assuring that their hardware components are trusted is critical for US national security. Today the United States spends billions of dollars on software in cybersecurity but very little to secure the hardware our systems depend on. As the Honorable John Young pointed out, DoD will spend nearly $1 Trillion to build essential defense systems over the next decade, and insecure hardware could compromise this

investment. Investment in trusted hardware capabilities are comparatively small and will ensure that secure, Trusted hardware is available for these systems.

- With the sale of IBM Microelectronics to GlobalFoundries, long-term US government access to Trusted State-of-the-Art (SOTA) microelectronics remains uncertain, although there is a current trusted supplier contract in place between DMEA and GlobalFoundries. The Potomac Institute's analysis of market forces and historical Trusted Foundry models indicates that DoD should work to establish a capability to ensure continuity of operations and reduce DoD dependence on a single source for advanced microelectronics, in the event that GlobalFoundries decides to exit this business area.

- There are currently many US suppliers that have been accredited by DMEA to manufacture trusted microelectronics for DoD systems, and that are willing and able to provide increased capability to DoD. Increased funding and more stringent policy requirements for trust would likely drive increased use of their capabilities. However, an "insurance policy" capability is still needed for technologies that commercial companies are no longer willing or able to produce but that are still needed for DoD systems.

- To successfully meet current and future operational needs, the USG must invest in alternative fabrication solutions that solve both trust and access issues, and can be implemented in the near-term. Secure and assured microelectronics are essential to our national security systems, and a solution that ensures long-term viability is needed.

- Speakers reviewed current efforts to ensure US government access to Trusted SOTA microelectronics and argued that more investment is needed in mid- and long-term solutions. DoD's FY17 budget request does not provide an "insurance policy" for trusted and assured production of essential microelectronics parts in the event that a US source is unable or unwilling to provide them for DoD.

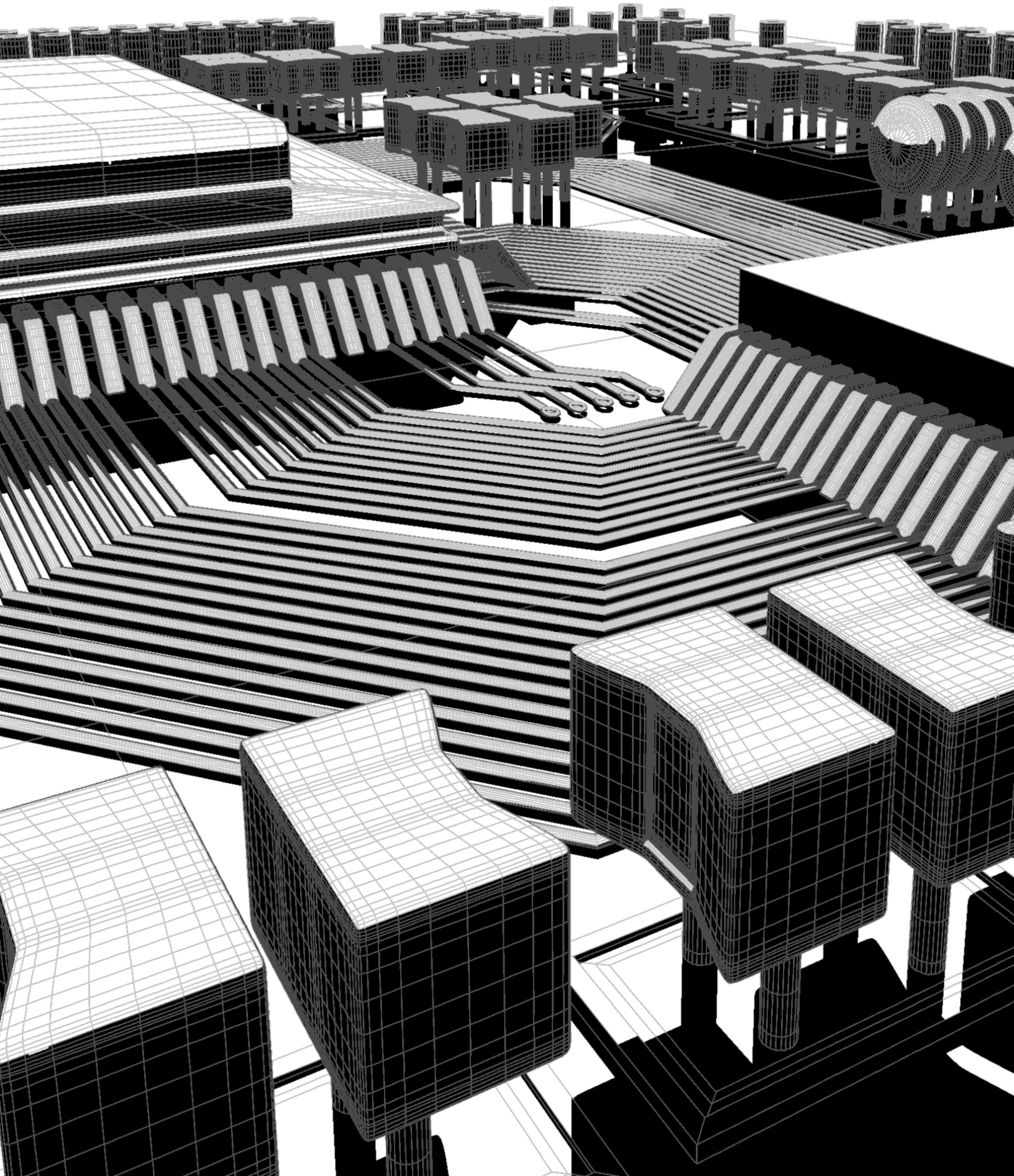
The Potomac Institute will be holding additional workshops and studies in this area. For more information or to participate, please contact Dr. Mike Fritze, mfritze@potomacinstitute.org.

BACKGROUND

The most capable military in the world requires secure and reliable electronic components in order to accomplish its missions. Virtually all United States national security systems (from the Joint Strike Fighter to satellites to encryption systems) have microelectronics as core components. Cyber dominance is a large part of the "third offset" strategy for the US Department of Defense (DoD). The overriding need for security in these components presents an enticing threat vector for our adversaries. Microelectronics (or integrated circuits, ICs) are susceptible to hardware exploits that could change their intended function or cause them to fail. While the USG has spent billions of dollars on software security, hardware security is an under-funded and under-prioritized part of our cybersecurity strategy. The Trusted Foundry model relied on a single commercial company (IBM) to provide both Trust and Access to the USG, through a secure production line at IBM. However, this model does not seem sustainable over the long term. Past strategies and dedicated government programs have attempted to enable the acquisition of secure chips, but these attempts have not been sustainable due to high costs and commercial industry business drivers. Further, the USG must embrace the fact that the semiconductor industry is global, meaning the US government has little ability to control the supply chain or impose security requirements. Going forward, the USG must be able to acquire trusted microelectronics from assured sources. Spurred by the IBM sale, DoD chartered the "Trusted State-of-the-art Microelectronics Strategy Study" that put forth six long-term recommendations for the USG, as shown in the table on page 7.

The Trusted State-of-the-art Microelectronics Strategy (TSMS) study acknowledged the need for achieving Trusted access affordably by partnering with commercial industry and included recommendations such as utilizing Trusted photomasks and split fabrication in order to achieve Trust. This study's findings emphasized the need for the USG to develop multiple pathways to assure access and trust, rather than relying on a single, highly secure foundry. In the past year, some of the recommendations from the study have been adopted, resulting in additional funding requests in the DoD budget request for FY17. However, the recommendations have not been fully adopted. The USG will leave a gaping hole in its strategy to maintain access to trusted microelectronics if it continues to rely on a single source for its SOTA trusted microelectronics and does not begin to implement mid-to-long term solutions.

IBM Capability Lost	Recommendation	Comments
State-of-the-art	**#1**. Establish an alternate state-of-the-art (≤45nm) trusted supply chain using trusted masks, design for security, and mask authentication.	Addresses access to state-of-the-art integrated circuits
State-of–the-practice	**#2**. Establish advanced technology solutions, e.g., split manufacturing, for unique state-of-the-practice capabilities.	Addresses access to state-of-the-practice integrated circuits
Unique technologies	**#3**. Establish production for Silicon Germanium (SiGe) processes.	Addresses access to this unique technology used by some critical applications
Future technologies	**#4**. Establish robust, cross-organization Research and Development (R&D), Productivity and Quality (P&Q), and Capacity Expansion (CAPEX) programs to develop alternative fabrication sources for low volume secure manufacturing, leverage advanced microelectronics technologies, design for security and trust in untrusted environments, and support the maturation and transition of R&D to the user community.	Risk reduction and advanced technology needed to reduce dependence on any one foundry or technology
	#5. Maintain and evolve DoD Trusted Supplier network.	Continues to mature existing network
	#6. Alter policy and technical implementation approach as required to support redefined approach to trust and verification.	Evolves policy and technical implementation approaches to match state of technology
White Paper Recommendations by TSMS study team.		



Mike Swetnam

Chairman & CEO, Potomac Institute for Policy Studies; Member, Technical Advisory Group, Senate Select Committee on Intelligence

Ladies and gentlemen, thank you all for coming today. We will try and make this as concise and to the point as possible, because it's a beautiful day outside, and probably the first beautiful day this spring here in Washington DC. Welcome one and all. I'm Mike Swetnam, CEO of the Potomac Institute for Policy Studies. We're here sponsoring this informational session, which is hosted by Congressmen Dutch Ruppersberger. We would like to thank him very much for being our host, giving us a place to present this seminar, the purpose of which is to provide some information about a critical national security need we've identified out there threatening the United States.

The Potomac Institute for Policy Studies is 21 years old, and we'd like to think of ourselves as rising out of the ashes of something called the Office of Technology Assessment (OTA), which actually originated in this building 44 years ago and was abolished 21 years ago for a variety of reasons. The Potomac Institute is a nonpartisan, not-for-profit, public service organization that sees as its mission the pursuit of science and technology studies for the purpose of policy, examining how science and technology can drive policy. For the last 21 years, the Potomac Institute has been fulfilling that mission of studying the effects of science and technology on policy and to a large degree, whenever possible, providing information to the United States Congress. We have, to a large extent, been working for Congress on a variety of issues and a number of studies, year-in and year-out.

Over the past 10 years, the Institute was engaged by the Office of the Secretary of Defense to look at the issues of hardware vulnerability. For a long time people thought of the vulnerability of our hardware to foreign threats and cyber as two separate things. Today we want to correct that a little bit and help people understand that cyber, i.e., those attacking our information, is more than software, it's hardware too. People can put viruses not just in the programs running on a computer, but also in the hardware itself. That's what we're here to talk about. Most of you have heard about addressing the software vulnerability inherent in our systems and it's only recently that we're starting to discover that our enemies have been putting things in the chips themselves. This is not just a threat you can eliminate by cleaning out your software — flushing your systems. What do you do when you find backdoors are hardwired on the microprocessor itself or even worse, a killswitch that allows someone to turn your system off right in the heart of the battle. We are finding more and more of these things in our systems, and it's threatening our capability and what we have available to us in the United States to deal with it. We have a small advertisement to summarize this issue, so let's start with that.

(Video shown)

This is a short clip to try to highlight the problem that we're facing. We have often found our enemy locked inside of the microelectronics that are controlling the systems that we depend on for our military and our communications. How we deal with that is really hard. It's not as simple as turning the computer off, flushing the software, and putting in a new program. It often entails reworking the system, finding another source of microelectronics, finding a source you can trust — and asking what it means to say you trust that source. It's becoming harder and harder to do this when we find that the key manufacturers of microelectronics have been, for the last couple decades, leaving the United States and going to China and other places that we know we'll never be able to trust.

When the sole remaining trusted high security fabrication facility for state-of-the-art microelectronics that was partnered with the federal government sold its core capability to a company out of the Middle East, the Department of Defense (DoD) went on high alert, asking how they could fix this. They employed the Potomac Institute to put together a senior review group under the Under Secretary of Defense for AT&L, Frank Kendall. This senior review group is a group of former undersecretary level acquisition officials who provided him with an independent assessment of how to go forward. A representative sample of that group is here with us today, to talk to you about this problem and answer your questions.

I'd like to introduce them to you now, have them say a few words about this problem, what can be done about it, and entertain your questions. First is the former Undersecretary of Defense for Acquisition, former DDR&E, former Assistant Secretary of the Navy for Acquisition, who has spent 20 years up here on the Hill on these acquisition issues, Mr. John Young.

We also have with us one of the most experienced acquisition officials to serve in the administration in and out for a number of years. First for a number of years with the NRO, then as an Executive Director of the Overhead NRO Commission that Rumsfeld commissioned, and as special assistant to him later on, then Chief Scientist and special adviser at MIT Lincoln Labs, and finally Senior Fellow at the Potomac Institute, Mr. Ken Colucci.

Finally, I mentioned cyber a little bit ago. Almost a decade ago, the Director of National Intelligence identified cyber as the largest threat the country had, that needed to be identified and worked on immediately. He formed something called the Consolidated National Cyber Initiative (CNCI), and put Melissa Hathaway in charge. She put together an inter-agency group, and formed a multibillion-dollar effort in the government to address our cybersecurity problems. She later became the first Special Assistant to the President on cyber issues — the cyber Czar, if you will — and served in that role under two presidents, Ms. Melissa Hathaway.

The Honorable John Young, Jr.

Former Under Secretary of Defense for Acquisition, Technology and Logistics, Former Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN(RDA)); Former Director, Defense Research and Engineering (DDR&E), Member of the Board of Regents, Potomac Institute for Policy Studies

I would like to start off by thanking the Potomac Institute for their analysis in this area. It's a complex area and it's a more important area than people realize. I think the Potomac Institute has done some excellent technical and bipartisan work here to try and help the Department, Congress, and major acquisition programs.

I'm going to approach the issue but scope it, if you will. Major acquisition programs have evolved over time, as all of you know, to be more software intensive, or rather more computing intensive. There were issues already when I was in the Navy acquisition job with the Aegis Combat System. It was an exquisite capability in its time, and still is today. That capability was delivered by an intimate coupling of the hardware and software. That made it very difficult to upgrade, and created proprietary issues. To help itself, the Navy embarked on a campaign that I helped lead to open up that architecture so it would be more easy to upgrade the software and add capability and try to keep pace with advancements in computing. I would like to highlight that it was a multimillion dollar effort to do that.

At about the same timeframe, there were issues with the F-22 and diminished manufacturing resources. That was a several hundred-million dollar effort to identify alternatives or recover the ability to produce old chips, which is not optimal, when you have the chance to put more capabilities in systems. Re-engineering the diminished manufacturing resources was a big effort on the F-22 and the program eventually embarked on an Aegis-like journey towards open architecture.

We also found ourselves at AT&L with a space-based infrared system that had a similar issue on SBIRS. Because of the allocation, it was almost like the Aegis issue; functionality of the software had been allocated between different software processors on the satellite. It was discovered there were issues with the clock speeds and the ability of the two processors to process and harmonize and synchronize the results. That led to a re-engineering of SBIRS.

A program that didn't come to fruition but died, which really highlighted some of these issues was TSAT, the transformational satellite capabilities. I went out and talked with industry, and what they were going to do on the program was use current generation computing chips and seek waivers from some of the requirements for the trust and rad-hard demands in that system for computing power. The situation was such that they needed that generation of chips, because relying on older generation chips would have added three or four hundred pounds to the satellite. That's a huge issue for what was already a big and complex satellite.

One issue I want to bring to your attention are the common threads here of the constant escalation in the amount of code that needs to be processed in these systems, the intense and growing importance of clock time and synchronization in process or speeds for completing the results and fusing those results together, and DoD's demand on current technology for space, weight, and power. These are issues that are important for all DoD systems and particularly space systems. Relying on older generations of computing systems inevitably means more weight, more power usage, and more space on the platform.

Another thing I would like to highlight for you is that these are billion-dollar class problems, when issues arise with hardware failures, hardware obsolescence, or loss of manufacturing sources. The Defense Microelectronics Activity (DMEA) has been remarkably helpful in helping to moderate the cost of these issues, when the DoD has been confronted with chips moving offshore, or when the technology moves forward, meaning the DoD unfortunately is left behind. This can happen for a number of reasons. There is a business case for taking them out of production or other obsolescence issues, where they're not long supported. Sometimes support is as big an issue as manufacturing. DMEA has, in many cases, been able to go to a company, before it will retire a process and get access to that process, because it's no longer of significant value in the commercial space, and they can license that process at a low cost and in some cases, buy the equipment to execute that process to produce chips, which is a better way for the DoD to deal with these issues, rather than the more costly things of going up the future food chain. When you go up the food chain, you'll find that you have these multi-hundred billion dollar bills to re-host the software, and make sure it's functional on the processor and upgrade equipment and balance the power and cooling loads in something like an aircraft to function and go through the test process. Testing in major weapons systems these days can easily be 25% or so of the cost. These are really big bills and resolving these issues is important. The DoD has worked its way through these issues in parallel with studies that have been done at the Potomac Institute. None of the solutions have been successful and that is why we are here today.

During my tenure, one of the decisions was to allocate an enterprise bill to each of the Military Services. It was a bill shared amongst the services to try and pay for foundry capability and rad-hard chip capacity. What was discomforting about those solutions is, as you all know, they were not going to be enduring solutions. In general, we were paying to be able to afford a generation or two behind commercial industry in chip capability, paying a substantial amount of money because we were the only users, so we had no base across which to distribute demand. There is already concern about the long development timelines for DoD electronics systems. When you start that long timeline by reaching behind you several years to get your computing technology, that means you have less capable and sometimes obsolete weapons. That does not work well for us.

I think the foundries have been inadequate with the commercial companies. The next generation was the trusted foundry approach at IBM that Mike introduced you to a minute ago. Now our trusted process is foreign owned and, not only that, we paid people to take it, which is frightening to me. The review group at the Potomac Institute and other independent studies have struggled with these issues regarding a problem that has only gotten worse. The worst aspect of it is — set aside obsolescence, bugs, cost to fix software, re-host software, and trying to stay current — there's now an unquestionably higher level of risk that there will be malicious hardware back doors put into our current generation of microelectronics.

This is all complicated by the fact that microelectronics systems, based on some of the research by Potomac Institute, are made primarily overseas. Over 75% of the manufacturing of microelectronics is in Asia. That's where the markets are. That's where many of the new fabs have been put in. It has clearly become an easier path for our adversaries. It's an asymmetric approach to attack us in the cyber domain with software and other tools, because not many people are going to have the same inventory that we have, so this is an affordable way for them to attack us.

The risk is there in the software space, but the hardware space is just as vulnerable. Our system designs and technology are being stolen every day. I'm sure you all hear this and are aware of it. It's not just the DoD. Businesses are being attacked through malware and ransomware. We know that the most sophisticated threats have an ability to get to us through software and they have an equally great ability to get to us through hardware. It is naïve to think that those threats are not exploiting those opportunities.

At a recent event, CIA Director Brennan spoke, and said our supply chain is so vulnerable to adversaries and cyber attacks. He also noted that "defense always lags offense." He is concerned that resources in the scientific community are strained in their ability to deal with these changes. That's a concern, when the CIA Director is talking about issues in that way. The extreme complexity of today's chips makes it virtually impossible to detect minor changes in features hidden in a billion gates by adversaries, which can be activated at critical operational times. Frankly, it would be effective to activate them once we have declared operational capability because it would cause a situation where we would release a system for use, discover the bug, have to go back and pull the system out, find the bug, and re-engineer the parts, which is a multi-hundred million dollar project. Then, of course, there would be the bill for testing on top of that.

This is a hard problem. If it were easy we would not be here. The study led by The Potomac Institute looked at a comprehensive set of solutions spaces and I believe it came to some very productive, pragmatic, and affordable solutions. The Institute continues to sponsor a hardware symposium series to look at all of the things that can be done here, such as methods that can automate validation

and verification of new chips, so we can get to a process making use of the most current chips from any source. The study recommendation opens a path to doing those kinds of things. One of the fundamental recommendations of the study is the split fabrication process, which offers the potential for the DoD to use current technology chips from multiple fabs and then install custom capabilities and final processing of those chips at a secure location. The DMEA is building the capabilities to do that.

Throughout my experience in the DoD, the large fabs like Intel have always refused to vary their processes for custom chips or small batches for any customer, including the DoD. Split fab offers a solution which can offer current generation chips from multiple fabs, which answers our space, weight and power issue that I started with. We can begin to better match the technology appetite of the weapons systems with the chips that we can put in those systems. The challenge is to get split fab funded. It will take four to five years I believe to buy the equipment, install the equipment at the site, validate the processes, and begin to produce chips.

Other recommendations were adopted that allow us to continue to access for an interim the former IBM fabs through Global Foundries with protection measures, but the split fab was not funded in the budget. It is my understanding this was in the budget, because DMEA, to its credit, recognized the severity of the problem, but in January money got shuffled to third offset, the Pacific pivot, etc. These are things that made a major splash in the press, rather than a split fab process that makes trusted systems. This decision has to be reviewed because this solution provides a long-term solution. The senior review group's review highlighted these interim steps, such as continuing to use the fab and investing in validation and verification processes, but the anchor that provides the long term solution is the split fab solution.

To drive home the financial point, because that's been my experience in acquisition, the FY 17 budget asks for $112 billion in procurement and $71 billion dollars in R&D. These levels have been steadily creeping up. Doing the math, it becomes clear that over 10 years we invest $1 trillion in hardware. If that hardware has bugs and flaws in it, and it costs $100 million each time to fix, then it's clear you should find the resources to create a secure solution to sourcing that hardware you're going to be using over the next 10 years. I think the study recommendations are sound and, more importantly, I think they represent the minimum necessary set of actions that need to be taken by the DoD to protect a trillion dollars in future weapons systems and platforms. It is a complex and technical subject, and with that I will stop and turn over to my colleagues. I want to thank each one of you for investing the time to understand these issues.

Mr. Ken Colucci

Former Head of Strategic Initiatives for MIT Lincoln Laboratory, Former Chief of Staff of the National Commission for the Review of the National Reconnaissance Office (NRO), Former VP for Business Development & Strategic Planning, Pacific Sierra Research Corporation (PSR)

Thank you John. I'd like to highlight one of the key issues that John just addressed, specifically the long-term approach to solutions for the challenges that we face. These trusted supplier studies have gone on for over a decade, and the recommendations have been fairly consistent. What concerns me, as John mentioned, is that while the recommendations for long-term solutions have been endorsed by the USD (AT&L) and sent forward as part of the DoD budget request, they then are swept up in the budget crisis of the day, whether it's Third Offset, Sequestration, or something else. This has consistently happened over the years and we end up back in the same situation we are in today. It is an all too common and frustrating outcome in the budget process. One of the primary reasons I agreed to participate was to see what we could do to garner support of DoD senior leaders and members of the Congress and their staffs.

Counterfeit and failed microelectronics are billion dollar issues. We see them all too frequently. I've dealt with them in the national security space world where, quite often, you don't find out there are problems until the system is about to be launched or is on orbit. If we do nothing else today, I hope we can impart to the audience that these are critical issues for the Department of Defense and for the national security community in general, and they jeopardize the ability of the US to maintain technological superiority.

The study and the report touch on a number of things DMEA does, particularly dealing with issues in our legacy systems. Some of these systems have been in development for 10 years or so, and as John mentioned, by the time they're ready to launch or be fielded, many of the critical parts are no longer in production. For that reason we have DMEA, which is able to leverage its microelectronics engineering expertise, proprietary commercial technologies, and flexible manufacturing capabilities to develop solutions which allow systems to remain operational well beyond their expected useful life.

Quite often we don't hear about these issues as they get overshadowed by cyber threats and breaches. When these failed parts surface during a development program the result often is that millions of dollars must be diverted from the development of next generation systems to fund the replacement or repair of counterfeit or failed parts. The bottom line is we end up leveraging future capabilities to pay for our current and past mistakes. I frequently saw this occur at MIT Lincoln Laboratory as I had insight into hundreds of different programs across

all services, the intelligence community, and other agencies. It was a consistent problem during my tenure there and also during the three decades working in the national security space sector. Counterfeit and failed components often made their way into a critical system component because test and validation protocols were often bypassed to save time and costs. Also, during the era of Total System Performance Responsibility (TSPR), rolling integration and IV&V were curtailed, and testing was performed after system integration had occurred.

Looking at the entire gamut of the issues that we've reviewed over the course of the study, I believe there is consensus concerning what the issues are. The challenge for us in the Department of Defense is that we no longer drive the pace of technology development. The commercial marketplace is the driving force and the DoD has very little influence.

The question now is what we do in that environment to support DoD requirements. Do we set up a government fabrication capability? Are there partnerships and arrangements we can do with industry? The Potomac Institute has looked very hard at this and, though there are competing interests at times, when you put it all together everybody agrees that trusted and secure access is a critical issue that requires a long term strategy. Now it's a question of how we address the problem.

The issue is challenging, and it certainly does not get sufficient press because it's not in the news on a daily basis, compared to the cyber challenges that exist. When major network systems go down, or are hacked and sensitive national security information and data is compromised, attention is diverted away from these types of issues. Additionally, DMEA has been successful in providing solutions that allow us to believe that things are not as dire as some of us indicate. That, coupled with the fact that government program managers are hesitant to make public any failures or missteps that might jeopardize their programs.

A frustration for those of us in the business is the fact that we continue to rely on a single trusted foundry supplier. We have watched over time as it became apparent that IBM likely was going to be acquired at some point. It was clear from their business model that it was not in their long-term financial interests to continue to sustain US based fabrication facilities. They cost billions of dollars to recapitalize and to upgrade their production to the next generation, and it's just no longer worth it to them. We've seen this, we've known this, and we've continued to go down that path.

However, we were fortunate this time. Six or eight months ago, we believed we were going to lose access to IBM's trusted foundry. It wasn't clear if the US government was going to be able to use that foundry following the acquisition by Global Foundries. Fortunately, the government was able to negotiate a two-year contract with options to renew every year after for 10 years, but in my opinion that's very

tenuous. We need to continue to advocate for other sources. As you are aware, there is very limited capability on US soil and there only are two companies here in United States to count towards our US-based assets. We need to explore and develop alternative options.

I'd like to take a few minutes to speak on the split fab process. I was not a fan in the beginning, because I was not familiar with that process and how far it has come. It is a limited risk issue for us, at this point. The fact that we can reach out to the commercial side of the house without having them interrupt their production line or having to do anything special for us other than developing the chips that we need, and then bring them to a trusted location where we do the back end, the packaging, and put in the pieces that we need, provides a viable alternative that should aggressively be pursued.

There are the questions of having a government owned, government operated facility, or government owned, contractor operated facility, and the study makes recommendations with regards to those options.

Looking at the options, at places that have the expertise to do this well, DMEA stands apart. MIT Lincoln laboratory has, for example, small R&D capabilities, but when you examine who has the physical space, infrastructure, technology, and the requisite engineering expertise, DMEA is the most logical and qualified entity.

Split fab did not get funded in this budget process. It was in the Department's initial budget, but then was dropped due to other budget priorities. This is a four to five year process, and many of the R&D initiatives that we have are 10 to 12 years down the line. If we don't start immediately, we could find ourselves in a similar situation again and subject to marketplace constraints and priorities. For me, that's very discouraging and I believe the folks on the Hill who are here need to understand how serious this problem is. A number of representatives in the industry have come forward over the course of this study and offered solutions, and it's going to take a combined effort to go forth to make them happen and to provide the US government with a viable, trusted supplier network to meet its future needs.

There also were a couple of short-term recommendations in the study. One was to continue to work with IBM and Global Foundries. In the past that translated to sustaining a sizable cadre of cleared personnel. There has to be a better way. While Global Foundries has agreed to continue to serve as a trusted foundry with renewable options, the US government needs pursue viable alternative options.

I understand IBM has been very generous, working with DMEA to provide IP and equipment that is no longer commercially viable. DMEA has been able to acquire it at a relatively inexpensive price. While encouraging, implementation takes a long time, even when funding is available. It's a very challenging process to go through and to make happen in a timely manner.

The other issue we haven't talked about is the FPGA world and finding a trusted supplier for those parts. As we say in the study, we believe that's the future. When it comes to FPGAs, we need to keep up with those demands and find a trusted supplier for those technologies. I'd like to see us do more in that world and be proactive in that process.

The last piece is the R&D strategy. The report outlines the details for a long term R&D strategy. I believe we can make copies of the report available to folks here. I understand that some of that was funded in the JFAC, which is a joint effort to bring together the different branches of the military to collaborate and work more efficiently. JFAC was fully funded, which is a key step in the right direction and a sign of forward progress.

I would leave you with one final point. The budget process is painful for all concerned and makes proper planning and execution a challenge. We will continue to face budget hurdles going forward. Our challenge is to continue to advocate for a sustained, long-term trusted microelectronics strategy that will enable the US to maintain a decisive technological advantage.

With that, I'll turn it over to Melissa.

Ms. Melissa Hathaway

Spearheaded the Cyberspace Policy Review for President Barack Obama; Led the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush; Senior Advisor, Harvard Kennedy School's Belfer Center for Science and International Affairs; Member of the Board of Regents, Potomac Institute for Policy Studies

Thank you very much. It's hard to follow my esteemed colleagues here, who are much more technical than I am in this particular area, but I definitely know the threat. The US faces sophisticated cyber threats that overwhelm our defenses due their volume, velocity and variety. In 2008, our principle worry was the extensive targeting of the defense industrial base — illegally copying of intellectual property, weapon system designs, and broad theft of data. Today, we are more worried about the manipulation or destruction of key data.

No nation is cyber ready. Almost 10 years ago, under President Bush, it came to our understanding the amount of compromises that we were seeing in the defense industrial base: the true theft of intellectual property, breaking in, illegally copying designs, compromising weapons systems, and the overall compromising of the architecture of the national security apparatus of the United States. To counter that, I led the Comprehensive National Cybersecurity Initiative (CNCI). It was designed around multiple threat vectors, of which I will talk about a few.

Cyber attacks occur along four main attack vectors: insider access, proximity access, remote access, and supply chain access. The need for ensuring trusted hardware focuses on protecting against supply chain access, but must also include methods that protect against the other three attack vectors. Most notably — the insider threat because it can come from a trusted employee who unknowingly creates or enables a vulnerability in the system. Alternatively, there are insiders who intend to conduct malicious activity. In recent years, the USG has been the victim both types of activities. We've seen vetted personnel, like Edward Snowden, who have introduced exploitable paths, and we've seen spies in our organizations. In the CNCI, we have also looked at threats of proximity and remote access, which means coming in through the Internet or a wireless environment, which are nearly everywhere and exist in homes, businesses, our National Security Agency and soon in the CIA as well, which is remarkable. Adversaries can come in through that spectrum and find a vulnerable path to exploit, which I'm sure we will see happen in the near future, even on classified campuses.

Talking about the supply chain vulnerabilities, whether it is a witting vendor who knowingly built a backdoor into systems or an unwitting vendor that had a product interdicted as it went to market and had some type of tampering done to it. There was an initiative on supply chain risk management as part of the CNCI, and it was multifold. It looked at who the vendors are that we can trust. It also looked at security risk management to include software and hardware. Many of the initiatives we are talking about today under DMEA, such as the trusted supply chain, were results of the initiatives that were started eight years ago.

I'd like to now to talk more broadly about supply chains and supply chain risk management, and how it relates to DMEA and the trusted chip manufacturing that we need. The supply chain risk management lifecycle has seven parts that come into play, with each part containing its own vulnerabilities that must be uniquely handled. Today, we focus on four parts of the supply chain in particular: the design phase, the manufacturing phase, the systems integration phase, and the distribution phase. Threats are not limited to malicious insertion; even acquiring design information poses a threat.

The first is the overall design of the chip What do we want this thing to do? Do we want it to operate a computer, or a cell phone, or a weapons system, or a radar? A chip actually has a wide range of functionality and designing the various parts of that is the most critical phase. The Design stage — determining what function a chip will perform and how it will perform that function — involves a great deal of collaboration between the national security and technical communities. The consequences of inadequate security regarding the design details are the most devastating because if a backdoor is introduced at the design stage, the likelihood of it being found at later phases of the supply chain are low. Therefore it is essential

to ensure data protection schema is in place to manage the risks associated with code insertion, data manipulation and insider access. We need secure design and development practices to be put in place. We generally try to make that happen here on US soil, among US citizens to keep that design secure and un-tampered. You can, in fact, introduce a back door into the design itself, if you're smart enough and are a part of the design team. Insider threat at the design stage is essential and must be dealt with. It's also important for the design to be protected from a data protection perspective. If someone steals that design, they have the ability to develop an immediate countermeasure or interdict at manufacture, because they know what the design scheme is. Insider threat, as well as coming through over the Internet are key parts of overall supply chain risk management. This is where we need to think about both state-of-the-art and state-of-the-practice, which are some of the points that have been discussed as part of the Potomac study.

The second part is the advanced manufacturing stage, which involves the design tools and production machines that transform the raw silicon and metals into an actual chip. This stage is the most global in nature. As it has been mentioned, 75% of the chips in the commercial market are actually manufactured offshore. Even in the trusted foundry program, IBM still had some of their chips produced offshore. We need to recognize that at least 10% of their chips were produced in China, not here in the United States. We took risk mitigation measures against that. Now that we no longer have the trusted foundry, we need to think about advanced manufacturing, and we need to make sure that we have the design tools on station for trusted manufacturing. The trusted manufacturing we have, must consider the design principle that we need those chips to have predictable behavior. DMEA's trusted supplier network and split fabrication production are the most critical to this stage of the supply chain and ensuring that the national security community maintains the ability to ensure that its microelectronics have predictable behavior that matches the design. It is not enough to have 98% of the chips produced function correctly and 2% become compromised because all of those chips will end up in some type of weapons systems or some sensitive system that we need for national security purposes.

This is where we start to talk about trusted suppliers and trusted manufacturing, the importance of validation and verification before it goes to mass production. That's important as the other issues we talked about, such as split fab, where the front end of the line is designed and produced offsite and the back end is brought to a secured sight for the second part of adding special things to obfuscate the design or special packaging to protect the back end of the chip.

I would like to stress that the low volume and long lifetime nature of these components was the most critical issue for this stage. If the Defense community neglects to ensure that it has the ability to reproduce or upgrade these components, which usually are not cost effective for commercial companies to manufacture, then it risks losing the ability to keep those systems in use for their intended lifecycles of 25 to 50 years.

The installation of microelectronics components into systems is the next stage of the supply chain process. Once we have this lot of trusted chips, they are now going to be integrated into systems, i.e. installed in whatever it is they will run, whether it is a weapons system or some other system that needs the chip. As it was mentioned before, these are not high volumes. They are not commercially viable chips. They are not cost effective for commercial companies to produce. This is where we have to actually have the designs on hand and the tools on hand to be able to modify these in the future.

The low volume and long lifetime nature of these components is the most critical issue for this stage. We are integrating them into the weapons systems of Boeing, General Dynamics, pick your weapon system and pick your integrator. Sometimes there are flaws in those chips and they need to be fixed. Sometimes they get damaged in the field and if you want to extend the life of the weapon system, you have to be able to reproduce that chip. If the Defense community neglects to ensure that it has the ability to reproduce or upgrade these components, which usually are not cost effective for commercial companies to manufacture, then it risks losing the ability to keep those systems in use for their intended lifecycles of 25 to 50 years. These are not small capital investments. They are not replaceable every three to five years. They are long life capital investments. Think of this as an industrial capital investment, which will need to be maintained and refreshed over the 25 to 50 years of its life. This is not like your cell phone or your laptop that you'll replace every three to five years. Every one of those manufacturing and integration system parts has its own vulnerabilities that create opportunities for interdiction, malicious insertion and insider threat, depending on what the environment is. To the extent that there are software systems working in there, you can, in fact, manipulate it by coming through the Internet.

The fourth stage of supply chain risk management is the distribution stage. Knowing the chain of custody of component to system and then system to fielding must also be managed. You need to have an assured chain of custody. Measures must be in place to know where every component has been and where it is going. If the chain of custody is not fully secure, adversaries can interdict, manipulate, enhance and/or replace components during distribution. Measures such as silicon security, anti-tamper, anti-counterfeit, and other initiatives are important tools for securing this stage of the supply chain. You could have this problem throughout the chain of manufacturing too, but if I am an effective spy I can actually come in and put something extra into these particular capabilities as they are moving through distribution to market. This is where we need to think about silicon security, anti-tamper, anti-counterfeit, and other things as we look at supply chain risk management.

That is largely a government role and a systems integrator role. Those first four parts of the supply chain. Then the systems are handed off to someone who will operate

that system, handle it, and retire it. Only then will you find out whether or not it works the way it should. If it doesn't work the way it should, you want it to have the ability to recognize that, and destroy itself or beacon itself to let us know that it has been tampered with.

Once a system is in use (operational) and being maintained, there may also be opportunities to interfere with the integrity of the component or weapon system. Field Programmable Gate Arrays (FPGAs) may require software updates to the hardware. Field programmable means I will update the software on the hardware somewhere in the field. Here too, it is essential to ensure secure communications can be established to prevent deliberate manipulation or tampering of the product. That is another interdiction point. If I know what the specific component is, then I can attack over the Internet, interdict the signal in the field and manipulate the component as it's changing the software on the hardware. All hardware is, in fact, software too, and we have to recognize that.

The last stage of supply risk management comes with the retirement of a technology. Finally, it is important that we are thinking about retiring the technology and ensuring that we retire it responsibly. This is where reverse engineering comes into play. Understanding what was really on that chip 25 years ago, and how it can be replicated with today's technology is what is so important about reverse engineering. If systems are not properly retired it is possible that they can be evaluated and reverse engineered to determine unique design components — that could enable third parties to replicate the technology or even worse, develop countermeasures.

If I were to leave you with a couple of things, they would be that there are multiple paths to introducing exploitable components. Our adversaries can do it at the design, manufacturing, packaging, and distribution stages. They can do it as it's operating, they can do it as it is undergoing maintenance, and if you don't retire it properly, they will reverse engineer it and develop a countermeasure. That is supply chain risk management and that is why we need trusted supply chains. We need to think about risk management as we go from design to fielding technologies. Over the past 10 years we've taken trust for granted. We've put explicit trust in the trusted foundry, and we don't have that anymore. I worry that we are going to live from year-to-year wondering if we can trust or not trust that fab. We need to think of that fab as an offshore fab. We need to think now about how we can manage our risk onshore for our most important national security critical systems moving forward. Someone who is really good at cyber is going to gain access to those systems and they are going to manipulate them, so we need to understand how we're going to keep our systems secure, and how we're going to know if and when our systems have been tampered with.

The DoD has taken access to trusted microelectronics for granted; the IBM sale highlighted that there are few options that can meet the demand of our national

security systems and missions. More and more of our national security systems rely on microelectronics and there is a general expectation that key systems will remain in inventory (and operational) for at least 25 or even 50 years. A portion of these systems require trusted microelectronics that cannot be sustained by commercial sourcing. In order to alter the performance or extend the life of a national security or weapon system, we need to be able to replace the chips inside them. We need this flexibility in our arsenal.

Thank you.

Michael Swetnam, Post Panel Comments

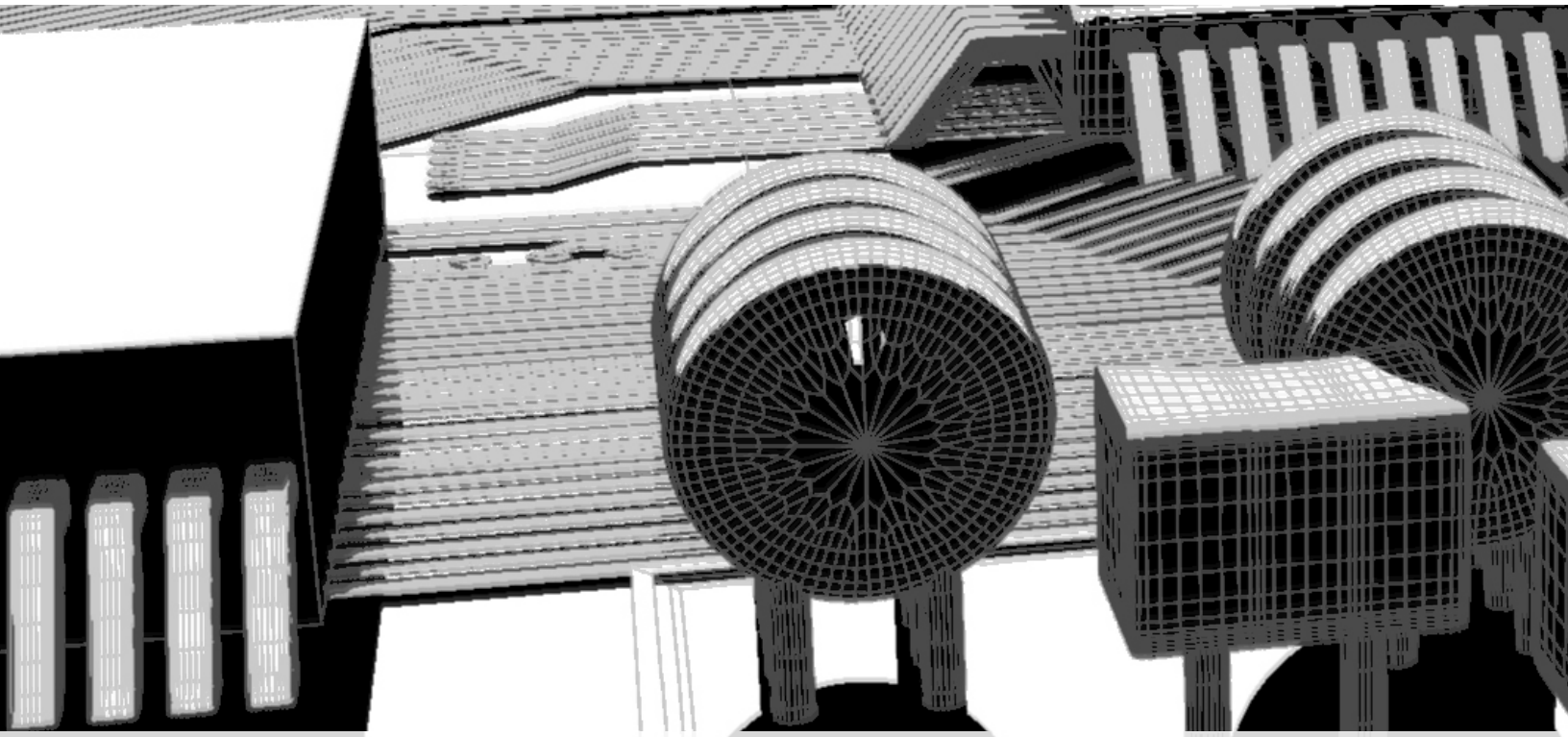
Thank you, again, members of the panel. It occurred to me that I should have put this in a little bit more in context. I will quickly do that now and then turn to questions. This time last year, the Secretary of Defense was concerned about where he's going to get his chips for his most classified, most sensitive systems, since our secure foundry went away. We don't want to just go find another secure foundry. There are lots of options to secure chips: build your own foundry, partner with industry, etc.

The history of microelectronics and the Department of Defense echoes Winston Churchill's famous saying about the Americans. We always get it right after we try every other available option. That's what we've done in microelectronics. We built our own fab at NSA, we built our own fab at DoE, and we built our own fab at NRO, only to have them go obsolete two or three years later. After we spent billions of dollars building them, the technology goes away too quickly. Finally, in the early 2000s, we came up with the concept to partner with one of the commercial guys. We found IBM, and we have spent over the last 12 years almost a billion dollars at IBM making them our source for trusted state-of-the-art microelectronics, only to have them announce last year that they've sold it to a foreign owner. Once again our option didn't work, so the study that we are talking about here and the recommendations we are talking about are all about saying that after having tried all of these options, we can come up with a better long-term answer.

The short-term answer is to get everything out of the fab that we can before it goes away. DoD did that, and they did a wonderful job. They bought everything they could. The mid-term answer was to negotiate with IBM and GlobalFoundries to get them to stay for a year or two and they did that. They secured a new contract. Looking at the long-term, let's do something more enduring. Let's do something better.

The study had three main recommendations. The first of those recommendations is to do research. Fire up DARPA and the research people, go figure out how to give us some more options, go figure out how to do design for trust. Figure out how to break this paradigm where we can't keep up with industry. That is in the President's program, to the tune of about $66 million. DARPA is charging forward to do that in

the future. Let's do that research. Second, let's spend a chunk of money looking at reverse engineering i.e., seeing what's going on. That is what JFAC does; it gives us the ability to check-test and not run blind. That's in the President's budget to the tune of $68 million. That is critical, and we must get that going. The final piece is creating a new foundry model. Let's let industry do the most difficult part, and then we will take it and do the classified part after that. It says let them lay down all the transistors, which is really hard to do, and then we will take that into a classified setting and wire it all up. That arrangement actually works. Industry is doing it for different reasons right now. That's the part that was in the budget and in the President's recommendations, but that fell out and that is the part we are worried about. The concept was, let's stop trial and error and get on a pathway to ensure that 10 years from now we are not having a conversation like this again. Now I will open the floor up to question.

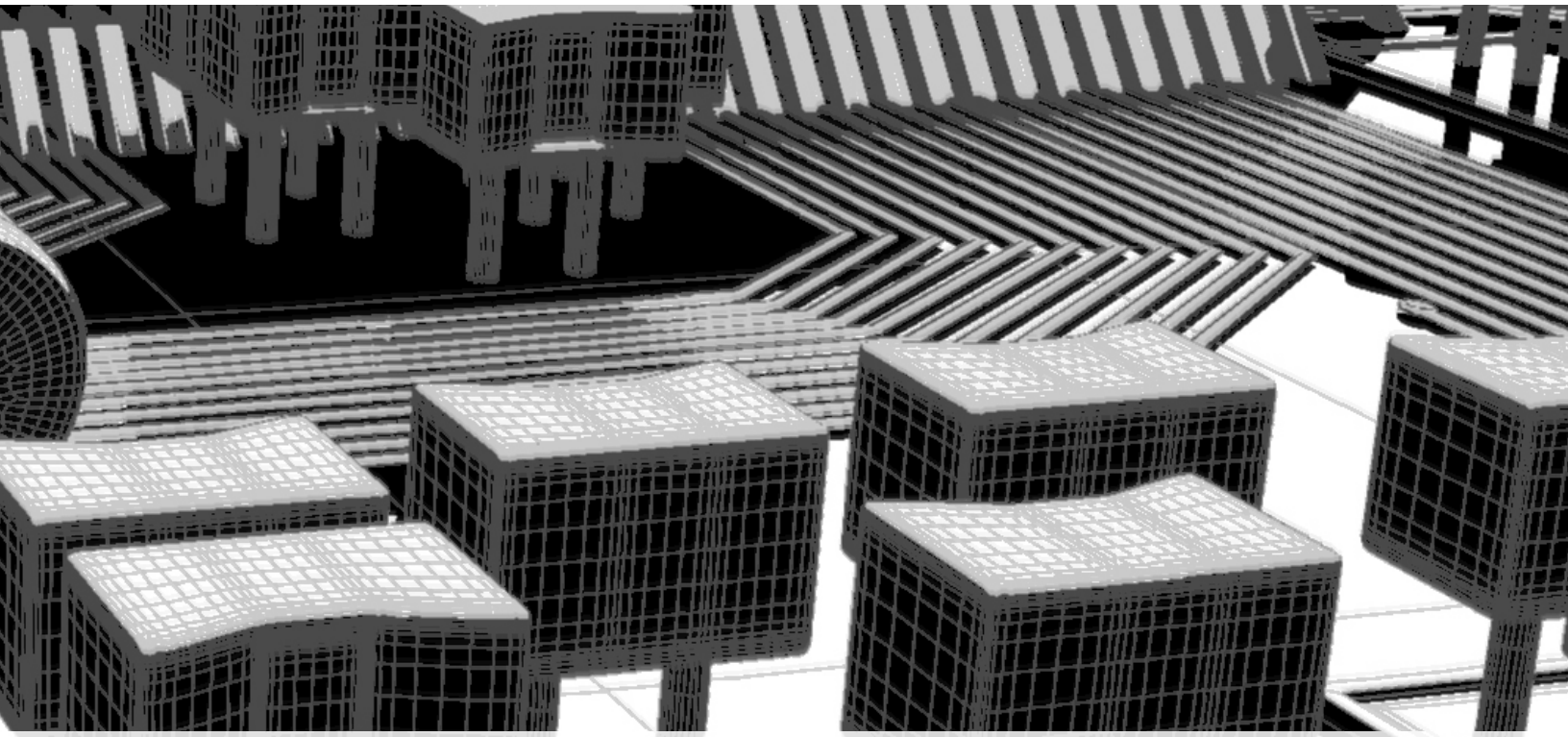


Panel Q&A

Question: Industry is telling us that commercial customers are also increasingly becoming worried about trust. What is the best way for the government to work with other sectors of the economy to amortize the cost of trusted microelectronics beyond government buyers?

Question: We have got to take care of the DoD problem first. We are trying to walk this fine line, finding things that can be done competitively and commercially. This is a space where low-volume means low opportunities. Industry has walked away from it. Big guys don't want to do customization; small guys don't want to do small lots — the unique lots that the DoD needs. It's interesting if commercial has that need. DoD has very unique testing facilities and sometimes people in the commercial sector have come to ask to use those facilities. We have worked with them, in those cases, and there may be a possibility to get split fab in place and to get more support to build on that model. We also want to be careful there, because there are things where government shouldn't intrude into that space.

Ken Colucci: That question brings to mind a model that I've worked with before on network intrusion. There are capabilities that DARPA uses, which allows industry to come in and test and collaborate with the government. It is a challenge to do. I haven't heard industry step up yet and say that they are concerned about it.



Melissa Hathaway: I think that when you start to look out there, with fewer and fewer on-shore, what we would consider US headquartered companies in the chip business is beginning to concern many of our hardware manufacturers and, to some degree, the software manufacturers. Understanding what is worrying our commercial enterprises is important and should probably be part of the DoD's Silicon Valley efforts of understanding where trust is breaking down on multiple fronts.

Furthermore, those same commercial providers are under increasing pressure internationally to hand over their source code and hand over their intellectual property, which again is of concern. To some extent, they are being forced to use a supply chain that is in a foreign sourced area. I'm worried that we have not done a strategic analysis of these companies, in part, to determine how many of these companies are getting ready to be bought by foreign entities. Right now we have DMEA or JFAC, and the ensured trusted supply chain, but some of those supply chains are also at risk as we look at split fab and who can be our commercial provider.

We have to look at who is also an acquisition target and we have to ask ourselves why these acquisitions aren't part of the CFIUS process. We have fought many battles against other foreign countries for their potential technology acquisition in the US. Huawei comes to mind, where we brought a CFIUS case. Why are we not doing a strategic analysis of who's next? I guarantee you there are one or two more companies that are on the block to be sold to a foreign company, which might not be in the best interest of the United States. For maintaining trust in our suppliers, whether that's defense or commercial, it's essential for our national security.

Question: Why is hardware trust not considered at the same level as software trust?

Melissa Hathaway: I personally think that all software is not reliable, because it's not well engineered. We have a belief that we can deal with software updates regularly — every Tuesday, for example — and allow it to be fixed later. In many ways we have held hardware to a higher standard than software and we are now beginning to understand that hardware is more and more an aggregate of multiple software components. If we don't start to address hardware security, because it has underlying software vulnerabilities, then we are actually setting ourselves up for long-term capital vulnerabilities that we cannot afford to have.

John Young: I think we struggle with two issues. In regards to software issues, they have become extremely visible and they have become personal. Most of you have had your data leaked or hacked.

The hardware issue has some visibility when producers discover that some systems have had fake and false parts. In most of those cases it was people cutting corners and finding cheap alternatives, not a direct attack by an adversary. We should be

smart enough though to see that smart adversaries are thinking about it already. You haven't seen as many hardware issues, but we have the ever-present problem in the DoE of not knowing who is going to solve it. Which program is going to decide that it's critical to have trusted chips? I think that's not going to happen. It takes a joint leadership situation, which is why I think it's right that the Potomac study recommendation was to support DASD-AT&L.

Individual services aren't going to want to pay the bill. They're anxious to have the current generation of technology and they're reluctantly taking the risk.

Ken Colucci: Again, I think John's point is that it's not noticeable to most people. It's not in the news. It's often not talked about. I'm not sure if it's an embarrassment to people but it's kept inside the Department. It just comes down to the battle of who's going to pay the bill. I'd like to amplify Melissa's comment a little bit more. Even today it's improved, probably, but I have been to recent DoD forums where it clearly hasn't improved. Companies do not want to divulge how many times and how they've been hacked. It's better to share this knowledge, it's useful. Government is trying to take steps in this space, but there is less of a forum there to talk about hardware attacks. People don't want confidence in their products and programs to be eroded. They don't want to admit that they've been cutting corners. This is the new battleground and it's taking time for everyone to realize it. Traditionally the battlegrounds have been land, sea, and air, and now there's cyber. There are risks in every dimension of it, including software and hardware.

Question: Could it be argued that hardware trust is an aspect of the third offset strategy, that it is an integral part of A2/AD strategies?

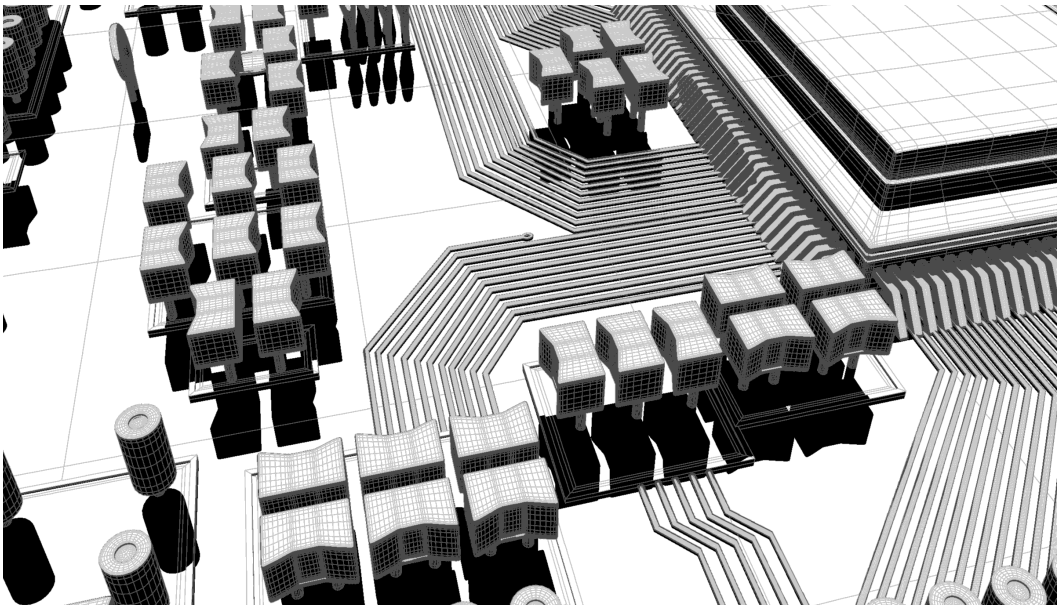
John Young: I'm not going to make that argument. This is part of the core business. There are $117 billion going into systems that people don't view as third offset. If we fail to find a mechanism to make sure that they are trusted and secure, then we have a major failure. This is core — this is not flavor of the month; not an offset — it's the foundation.

Ken Colucci: I agree with John. It is bread and butter. The other folks appear to be more glamorous and are in the sun at the time. What has come to mind as I've looked at these programs is that we have waffled back and forth as to who has responsibility over these programs, between the government and contractors. In order to cut costs, we've decided to waive verification and validation requirements. As a result, we've had things go through the process without being tested along the way. That's part of the equation, determining who is responsible for the issues throughout the process. Individual program managers certainly aren't capable of making that happen without someone setting the standard.

Mike Swetnam: There's a discontinuous point in the curve of understanding of the problem. I think it's true of cyber, writ large. For almost two decades, Melissa and I both lived this, trying to convince people that we are being hacked. They're breaking into all of our stuff. It wasn't until 2006 and early 2007, that the Director of National Intelligence stood up to the President and said there is nothing more important than getting our adversaries out of our computers and out of our mail. Once we woke up to that and said this is a major problem, we said we have to go out and stop this. We don't want a Japan or a China reading our mail and getting into our systems. The same is true whether its software or hardware. People argue about which is more important, or is this sexy or that sexy, but when it's all said and done, there's nothing more important than trusting your systems. There is no higher priority. We have to do this. Just as we have to have cyber command, we have to keep the enemy out of our systems.

Question: I understand the plan A was to give DMEA millions of dollars to stand up a capability that would be ready in four or five years, but could you do a Plan B that utilizes existing suppliers as a base to do split manufacturing? They're doing it on a regular basis now and you wouldn't have to give them nearly as much money, only a fraction of the funds.

Mike Swetnam: The plan was to partner with GlobalFoundries and do this with others that we can find in the industry. Plan A is and has always been partner with industry, but the DMEA part is actually Plan B, because in the past industry has always walked. We need something in place to guarantee access in the event that industry walks. DMEA is our insurance policy. We have to have DMEA anyway for the legacy problem — in 10, 15, 20 years when that technology is not available anymore we have to have the DMEA to step in to be able to make those chips. If we already have DMEA, then we should standup split fab capability with them as an insurance policy, in case private industry doesn't want to do split fab with us. We need this as a backup.



Mike Swetnam

Michael Swetnam assisted in founding the Potomac Institute for Policy Studies in 1994. Since its inception, he has served as Chairman of the Board and currently serves as the Institute's Chief Executive Officer.

He has authored and edited several books and articles including: "Al-Qa'ida: Ten Years After 9/11 and Beyond," co-authored with Yonah Alexander; "Cyber Terrorism and Information Warfare," a four volume set he co-edited; "Usama bin Laden's al-Qaida: Profile of a Terrorist Network," co-authored with Yonah Alexander; "ETA: Profile of a Terrorist Group," co-authored with Yonah Alexander and Herbert M. Levine; and "Best Available Science: Its Evolution, Taxonomy, and Application," co-authored with Dennis K. McBride, A. Alan Moghissi, Betty R. Love and Sorin R. Straja.

Mr. Swetnam is currently a member of the Technical Advisory Group to the United States Senate Select Committee on Intelligence. In this capacity, he provides expert advice to the U.S. Senate on the R&D investment strategy of the U.S. Intelligence Community. He also served on the Defense Science Board (DSB) Task Force on Counterterrorism and the Task Force on Intelligence Support to the War on Terrorism.

From 1990 to 1992, Mr. Swetnam served as a Special Consultant to President Bush's Foreign Intelligence Advisory Board (PFIAB) where he provided expert advice on Intelligence Community issues including budget, community architecture, and major programs. He also assisted in authoring the Board's assessment of Intelligence Community support to Desert Storm/Shield.

Prior to forming the Potomac Institute for Policy Studies, Mr. Swetnam worked in private industry as a Vice President of Engineering at the Pacific-Sierra Research Corporation, Director of Information Processing Systems at GTE, and Manager of Strategic Planning for GTE Government Systems.

Prior to joining GTE, he worked for the Director of Central Intelligence as a Program Monitor on the Intelligence Community Staff (1986-1990). He was responsible for the development and presentation to Congress of the budget of the National Security Agency, and helped develop, monitor and present to Congress the DOE Intelligence Budget. Mr. Swetnam was also assigned as the IC Staff representative to intergovernmental groups that developed the INF and START treaties. He assisted in presenting these treaties to Congress for ratification. Collateral duties included serving as the host to the DCI's Nuclear Intelligence Panel and Co-Chairman of the S&T Requirements Analysis Working Group.

Mr. Swetnam served in the U.S. Navy for 24 years as an active duty and reserve officer, Special Duty Cryptology. He has served in several public and community positions including Northern United Kingdom Scout Master (1984-85); Chairman, Term limits Referendum Committee (1992-93); President (1993) of the Montgomery

County Corporate Volunteer Council, Montgomery County Corporate Partnership for Managerial Excellence (1993); and the Maryland Business Roundtable (1993). He is also on the Board of Directors of Space and Defense Systems Inc., Dragon Hawk Entertainment Inc., and the Governing Board of The Potomac Institute of New Zealand.

The Honorable John Young

The Honorable John Young served as the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)); Director, Defense Research and Engineering (DDR&E); and the Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN(RDA)). Prior to these Presidential appointed, Senate-confirmed positions, John served ten years as a professional staff member of the Senate Defense Appropriations Committee, Subcommittee on Defense.

During his tenure with the US Department of Defense, John led the Mine Resistant Ambush Protected (MRAP) Vehicle Program Task Force at the direction of Defense Secretary Gates. Additional accomplishments include guiding the Biometrics Task Force, establishing the Reliance 21 science and technology oversight process, structuring the SSGN Submarine Conversion program, securing the Virginia Class Submarine multi-year contract, and leading the unprecedented swap of DDG-51 destroyers and LPD-17 amphibious ships between two industry ship yards. John constantly focused on increasing effectiveness and efficiency of the Department of Defense procurement and research programs while controlling costs. Throughout his Pentagon tenure, he worked the details of the Pentagon budget processes to ensure acquisition programs were fully funded to enable successful execution.

John currently serves on the Board of Directors of SRI International, the Georgia Tech Research Corporation and the Potomac Institute for Policy Studies. John is a member of advisory boards for Cubic Defense Systems, PIXIA Corp and FedBid, Inc. He is a member of the Georgia Tech Aerospace Engineering School Advisory Committee (AESAC) as well as a Trustee for the Georgia Tech Research Corporation. Additionally, John serves as Vice President of Business Development at E6 Partners, LLC.

While at the Defense Department, he received Distinguished Civilian Service awards from the Department of Defense, Joint Chiefs of Staff, and Army. He received a Distinguished Public Service award from the Department of the Navy. He is a Fellow of the American Institute of Aeronautics and Astronautics and member of the Academy of Distinguished Engineering Alumni at the Georgia Institute of Technology as well as being named to the Council of Outstanding Young Engineers at the Georgia Institute of Technology.

John earned a Master's in Aeronautics and Astronautics from Stanford University and a Bachelors of Aerospace Engineering at the Georgia Institute of Technology where he where he participated in the Cooperative Education Program.

Ken Colucci

Mr. Colucci has over thirty years of experience in developing and executing strategic solutions for nationally significant programs. From 2001 to 2008 he was the Head of Strategic Relations for the Massachusetts Institute of Technology's Lincoln Laboratory, a DOD Federally Funded Research & Development Center with $650M of sponsored research and a staff of 3100. In this capacity he served as the primary interface with the senior leadership of DOD, the military services, the Intelligence Community, and also with members of Congress and their staffs concerning technology opportunities, enabling capabilities, and policy-level assessments related to emerging threats and technologies. He also served as a member of the Lincoln Laboratory Senior Management Committee and provided executive oversight of Laboratory intelligence and national security space programs.

Prior to joining Lincoln Laboratory in 2001, Mr. Colucci served as a member of the Secretary of Defense's defense strategy review panel at the beginning of Secretary Rumsfeld's tenure. Previously, he was appointed by the Chairman of the House Permanent Select Committee on Intelligence to serve as the Chief of Staff of the National Commission for the Review of the National Reconnaissance Office (NRO), assessing its future ability to develop and field innovative technologies for space reconnaissance.

From 1988 to 2000 Mr. Colucci held a number of executive positions at Pacific Sierra Research Corporation (PSR). As Vice President for Business Development and Strategic Planning, he was instrumental in negotiating the company's merger with Veridian Corporation and in subsequent acquisitions that helped grow Veridian revenue to $600M. Previously, as Vice President and General Manager of PSR's Intelligence Systems Integration Division, he was the executing authority for multiple DOD, Intelligence, and other government agency contracts. In his prior capacity as Program Manager for Intelligence, Surveillance, and Reconnaissance Programs he fostered the successful development of operational concepts and technologies for integrating national intelligence information for use by tactical commanders during Operations Desert Shield/Desert Storm.

Mr. Colucci is a veteran with over 22 years of service in the U.S. Army, much of which was as a Foreign Area Officer. He has served in political-military assignments in the Office of the Defense Attaché in Bonn, Germany; as a representative of the Joint Chiefs of Staff in Vienna, Austria on the U.S. Delegations to the Mutual and Balanced Force Reductions Negotiations (MBFR) and the Conventional Stability Mandate Talks (CST) between NATO and the Warsaw Pact; and as Chief of the Defense Language Institute's foreign language training program for Defense Attachés, and for presidential translators serving on the Moscow Hotline.

Mr. Colucci currently serves as a member of the Defense Science Board Task Force on Improvised Explosive Devices (IEDs) and as an independent advisor to OSD, the Intelligence Community, the Congress, and to the Massachusetts Port Authority concerning national security and operational intelligence issues.

Mr. Colucci received a BA in Economics and Business Administration from Park University. He has attended graduate studies in Information Systems Management with the University of Southern California and is a graduate of the U.S. Army Command and General Staff College, the Defense Language Institute, and the Harvard University JFK School of Government Program for Senior Executives in National and International Security.

Melissa Hathaway

Melissa Hathaway brings a multi-disciplinary and multi-institutional perspective to strategic consulting and strategy formulation for public and private sector clients. She is a member of the Board of Regents at Potomac Institute for Policy Studies. She is also serves as a Senior Advisor at Harvard Kennedy School's Belfer Center, a Distinguished Fellow at the Centre for International Governance Innovation in Canada, and is the Chair of the Council of Experts for the Global Cyber Security Center in Italy. She served in two U.S. presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush. At the conclusion of her government service she received the National Intelligence Reform Medal in recognition of her achievements.

Previously, Ms. Hathaway was a Principal with Booz Allen & Hamilton, Inc., where she led two primary business units: information operations and long range strategy and policy support, supporting key offices within the Department of Defense and Intelligence Community. Earlier in her career she worked with Evidence Based Research, Inc. and the American Foreign Service Association. Ms. Hathaway is a frequent keynote speaker on cyber security matters, and regularly publishes papers and commentary in this field.

Melissa Hathaway joined Harvard Kennedy School's Belfer Center for Science and International Affairs as a senior advisor to its cybersecurity initiatives in 2009. She is participating and contributing to the joint MIT–Harvard Project on Technology, Security, and Conflict in the Cyber Age (Project Minerva). The primary objective of this project is to generate theoretical, policy, and strategy frameworks to assess threats and identify opportunities in cyberspace for national security, welfare, and influence for international relations in the 21st Century. She is contributing to the interdisciplinary research program by developing methods to measure, model, interpret, and analyze challenges and responses in cyberspace. More recently, Hathaway has been contributing to cybersecurity research initiatives at both the Belfer Center and the Berkman Center for Internet & Society.

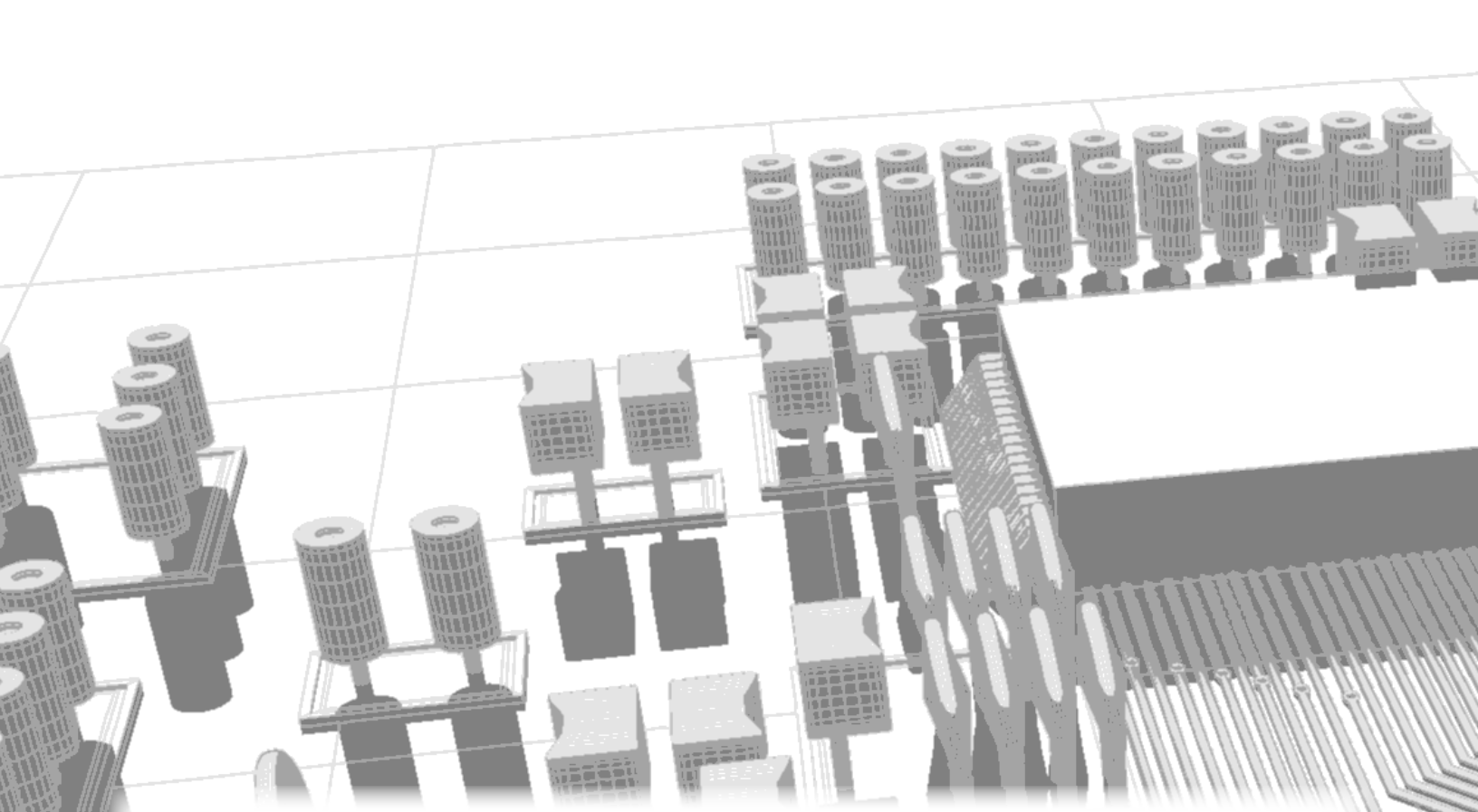
Hathaway is also one of the lead instructors for Harvard's executive program, Cybersecurity: The Intersection of Policy and Technology. Hathaway frequently guest lectures at universities in the Boston area as well as universities overseas.

Hathaway served in two U.S. presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative (CNCI) for President George W.

Bush. She built a broad coalition from within the executive branch and established an unprecedented partnership with Congress to obtain bipartisan support for addressing cybersecurity priorities. She developed and created a unified cross-agency budget submission for FY 2008 and for 2009–2013, assembling disparate funding sources into a coherent, integrated program. Hathaway stood-up the Cybersecurity Office within the National Security Staff and set the expectation and pace to move the United States toward a stronger more resilient information and communications infrastructure. At the conclusion of her government service she received the National Intelligence Reform Medal and the National Intelligence Meritorious Unit Citation Medal in recognition of her achievements.

After her government service, Hathaway established Hathaway Global Strategies, LLC. She is a leading expert in cyberspace policy and cybersecurity and brings a multi-disciplinary and multi-institutional perspective to strategic consulting and strategy formulation for public and private sector clients. Having served on the board of directors for two public companies and three non-profit organizations, and as a strategic advisor to a number of public and private companies, Hathaway brings her clients a unique combination of policy and technical expertise, as well as board room experience that allows her to help clients better understand the intersection of government policy, developing technological and industry trends, and economic drivers that impact acquisition and business development strategy in this field.

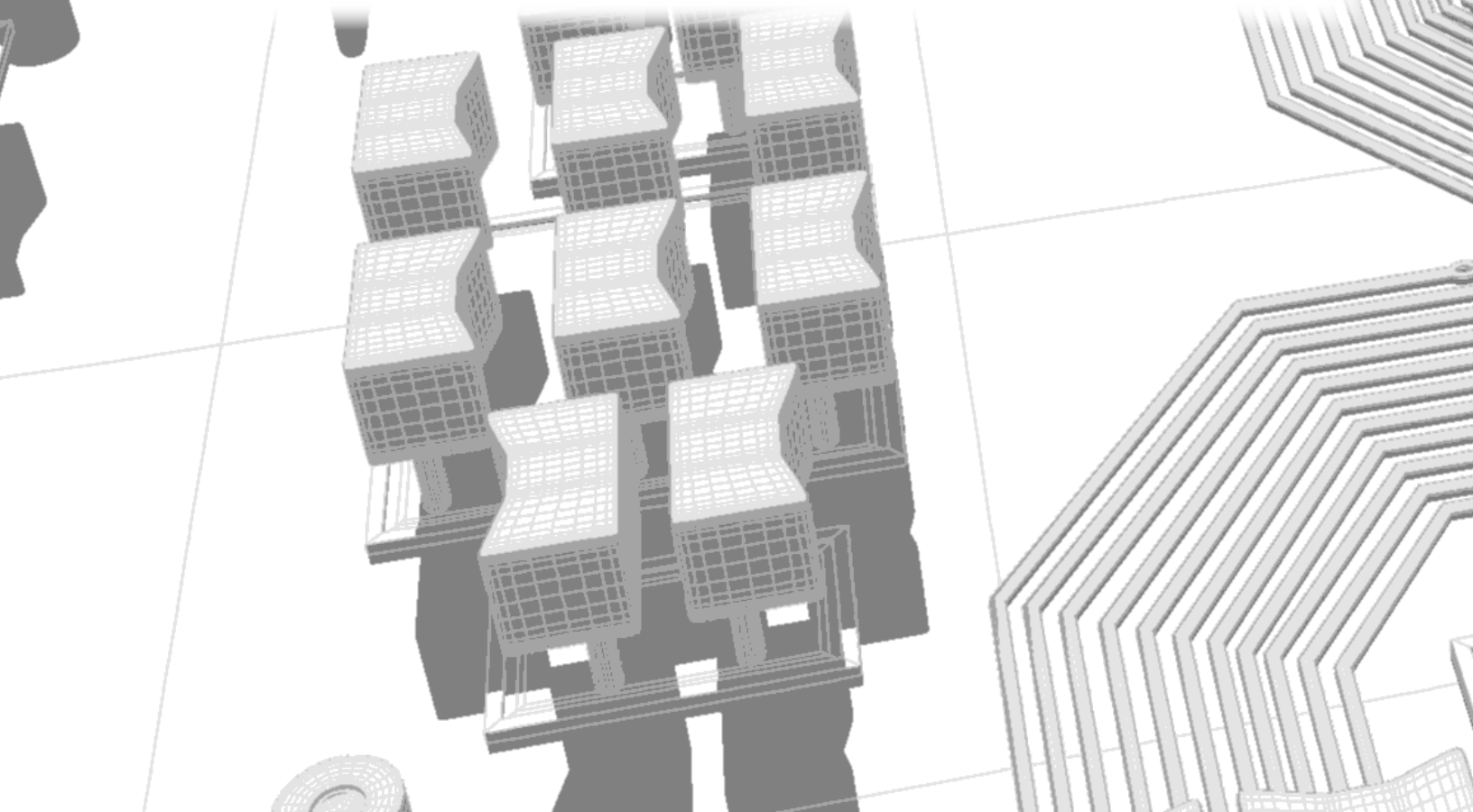
Hathaway has a B.A. degree from The American University in Washington, D.C. She has completed graduate studies in international economics and technology transfer policy and is a graduate of the U.S. Armed Forces Staff College, with a special certificate in Information Operations.

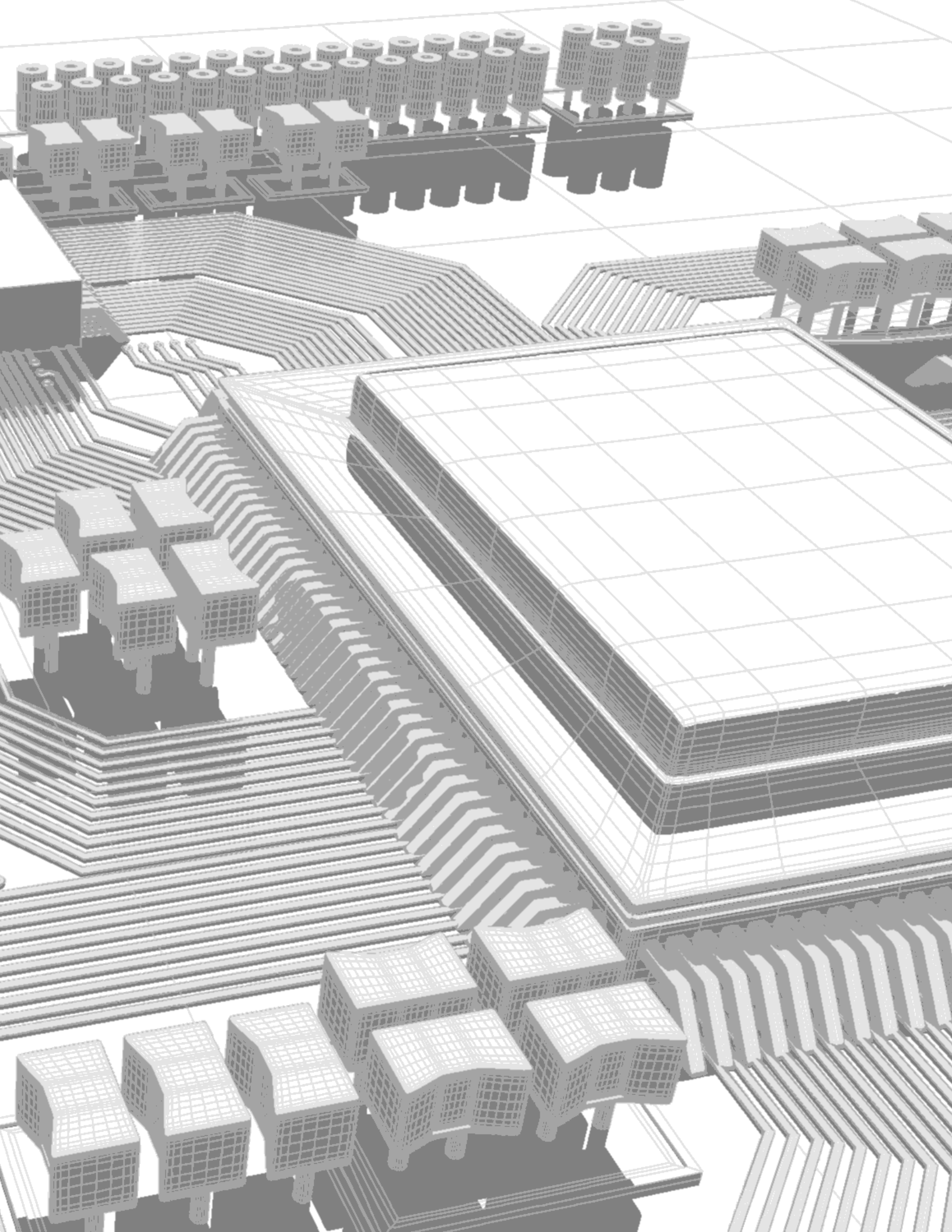


ADDITIONAL INFORMATION

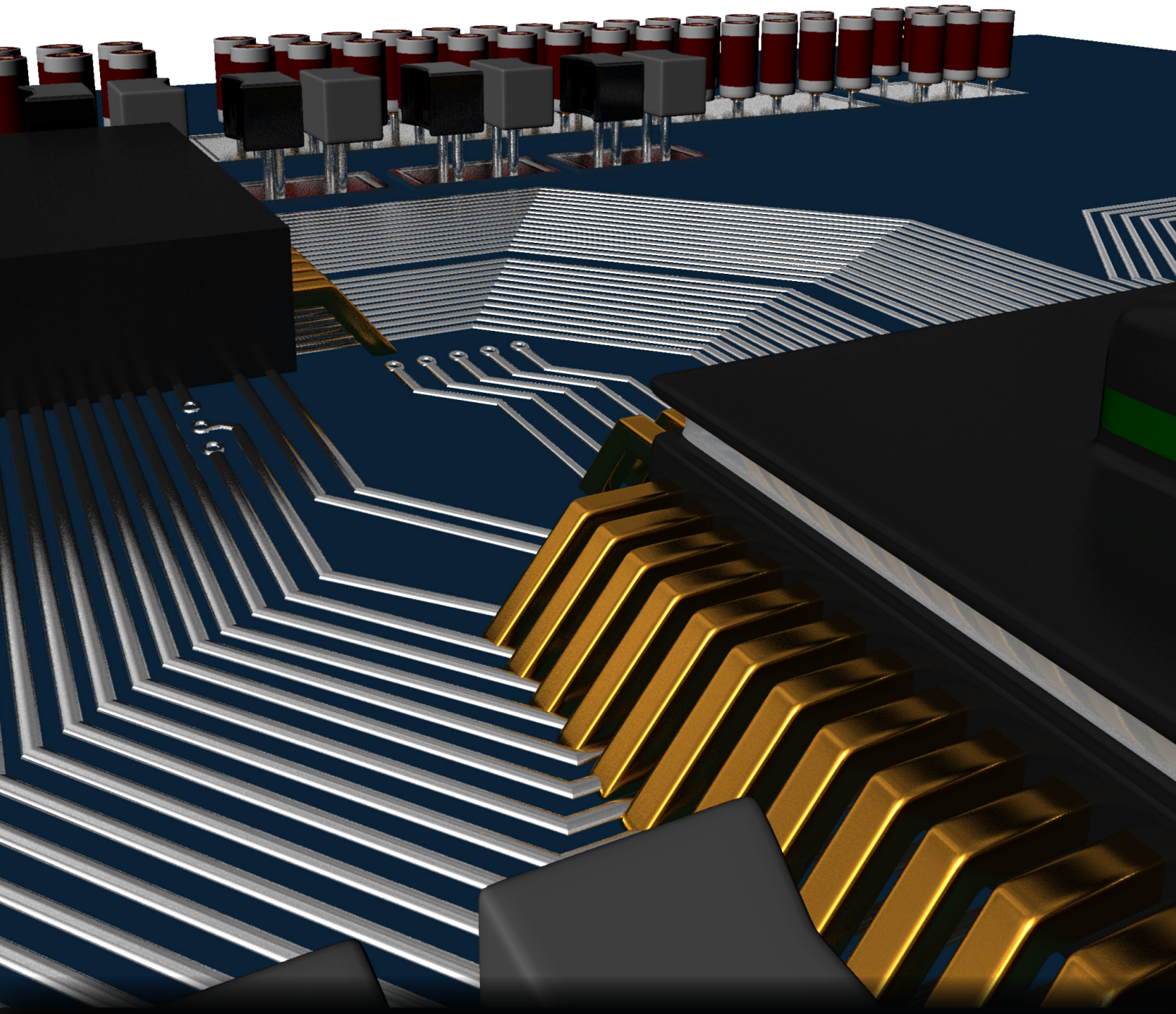
The Potomac Institute will be holding additional workshops and studies in this area.

For more information or to participate, please contact Dr. Mike Fritze, mfritze@potomacinstitute.org.





A POTOMAC INSTITUTE FOR POLICY STUDIES REPORT



POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200
Arlington, VA 22203