Security Strategies for Global Supply Chains: Addressing Risk, Seizing Opportunity

Potomac Institute for Policy Studies

Cover courtesy of Shutterstock.com

October 2018

NOTICE: These assessments are a product of the Potomac Institute for Policy Studies.

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 and technology issues facing our society. From these discussions and forums, we develop meaningful science and technology policy options and ensure their implementation at the intersection of business and government.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. STUART STREET, SUITE 1200
ARLINGTON, VA 22203
703-525-0770
www.potomacinstitute.org

Contents

Image: Shutterstock.com

Executive Summary

The world's economies are highly interconnected today through global supply chains — networks of companies distributed all over the world designing, producing, and distributing goods and services. Customers, including the public, industry, U.S. government and Department of Defense rely on these supply chains for critical infrastructure and national security systems. This decentralized structure means that the U.S. does not have complete control or jurisdiction over the entire supply chain, meaning threats and disruptions to global supply chain security threaten U.S. national security and the U.S. economy.

The Potomac Institute for Policy Studies' Vital Infrastructure, Technology and Logistics (VITAL) Center was formed in 2017 to examine these critical issues by bringing together a stakeholder community engaged in them. The Potomac Institute has also partnered with Venable, LLP, a globally renowned law firm with deep expertise in government and security issues to hold interdisciplinary forums on supply chain issues. Since its inception, the VITAL Center has held three major workshops and hosted numerous technical lectures in the "Hardware Security Seminars" series, with similar events in the works for the future. These activities have taken a broad view of critical infrastructure and national security, and have examined other industries (such as finance, energy, and pharmaceuticals) in which supply chain security is critical, to form a stakeholder community, compare notes, and draw lessons learned. This report represents a summary of the Center's findings and recommendations to date.

The Potomac Institute thanks all the participants in these discussions for their contributions, and thanks Venable LLP for their partnership. The views contained in this report are those of the Potomac Institute for Policy Studies, and do not necessarily represent the views of symposium participants or affiliated sponsors. Key finding and recommendations from VITAL Center workshops in the year of 2018 are summarized below.

Summary of Findings:

- Vulnerabilities in supply chains for commercial products and critical infrastructure are a national security issue.
- Threats to supply chains are highly varied, complex, and are not unique to international organizations.
- Threats are "baked in" to many critical infrastructure systems, commercial products, and government systems, via both software and hardware supply chains.
- Risk assessment efforts in both government and industry are improving, but still fall short of what is needed.
- Current supply chain risk management and mitigation efforts are insufficient to meet today's known threats, much less prepare for future vulnerabilities.

- The U.S. financial sector faces critical threats due to its central role in international commerce, and the industry has been proactive in addressing cybersecurity and supply chain threats.

- There is an increasing willingness in the private market to identify and understand risk, but gaps remain in companies' ability to address cybersecurity and supply chain security issues on their own.
  Commercial companies value time-to-market over security; defense industry values schedule, cost and performance over security; neither are incentivized to improve supply chain security.

Summary of Recommendations:

- Hold the private sector accountable for failures in product performance and supply chain security breaches that could have been prevented by prioritizing security.

- A comprehensive, holistic approach to supply chain security is needed, and must be clearly articulated across all steps in the supply chain.

- The U.S. Government and industry should work together to establish minimum standards for supply chain security.

- The U.S. Government should require a supply chain security plan as part of the contracting process.

- Conduct more extensive red-teaming efforts, both in the private and public sector, to address supply chain security challenges.

- Improve information-sharing regarding supply chain threats and vulnerabilities between the U.S. Government and Industry.


Image: Shutterstock.com

Introduction

National and economic security depend on the integrity of the global supply chain for public, commercial, government, defense, and critical infrastructure systems. The U.S. government (USG) and U.S. private industry must work in tandem to ensure that supply chains are secure and resilient against a host of threats, malicious and otherwise, that target inherent and emerging vulnerabilities. Disruptions or deliberate attacks on these supply chains can have serious downstream consequences to the U.S. economy, critical infrastructures, military capabilities, and the health and safety of U.S. citizens. Moreover, the increasing use of digital solutions in supply chain management adds both increased capabilities and an entirely new class of vulnerabilities that bad actors can exploit for financial, political, and even military gain. The USG will need to find and implement new tools to identify, monitor, and neutralize threats to the supply chain, and will need to eliminate or mitigate the effects of supply chain vulnerabilities. This will involve the enactment of policies and standards for supply chain stages that are located domestically, as well as the creation of tools to ensure resiliency in the face of vulnerabilities originating overseas.

The U.S. government has begun to address supply chain security with efforts ranging from counterfeit interdiction efforts, to technical solutions, to high level strategic investments in the domestic industrial base. Agencies with relevant efforts in supply chain security include Department of Defense (DoD), the Intelligence Community (in particular Office of the Director of National Intelligence, National Counterintelligence and Security Center (NCSC)), Department of Homeland Security (DHS), Department of Commerce (DoC), and Department of State (DoS), and others such as Agriculture. However, the problem continues to grow, and new approaches are needed. The private sector has been dealing with supply chain vulnerabilities for years and some industries have developed best practices that the government can leverage to inform its efforts. In addition, commercial industry will be an essential partner in implementation of any standards and strategies the U.S. government develops, making their expertise and input important to this discussion.

To begin to address these topics, and to facilitate exchange between and among business and government, the Potomac Institute for Policy Studies founded the Vital Infrastructure, Technology, and Logistics (VITAL) Center in 2017. In its first full year, the VITAL Center hosted a number of events where the security of US national critical infrastructures and supply chains were discussed by panels of national security and supply chain experts. These events covered a large swath of domestic and foreign industries and their supply chains, building a comprehensive picture of supply chain threats to national security, along with best practices and policies for mitigating risks. A summary of these findings, conclusions, and recommendations can be found in the following sections.

On September 13, 2017, the VITAL Center and Venable LLP cohosted an event called "A National Strategy for a Secure Microelectronics Supply Chain," held at Venable LLP's Washington DC office. This event outlined a national strategy for ensuring hardware and software security along the government microelectronics supply chain. It was widely attended by notable industry professionals and government officials in the field and sparked a lively and productive question and answer session after the initial presentations. The event was moderated by Rear Admiral Jaime Barnett (ret.) of Venable LLP, and introductory remarks were made by Michael Swetnam of the Potomac Institute for Policy Studies.

Panelists included:

- Mr. Ari Schwartz, Venable's Managing Director of Cybersecurity Services.
- Mr. J. Michael Daniel, President of the Cyber Threat Alliance
- Terry Halvorsen, Chief Information Officer and Executive Vice President IT and Mobile Business to Business Group at Samsung Electronics

Microelectronics are indispensable components in our defense systems. Assuring that they are both trusted and secure is critical for US national security. In today's global electronics supply chain, hardware and software vulnerabilities are increasingly prevalent, and a whole-of-government and industry solution is needed to ensure a long-term, assured supply of microelectronics enabling our domestic defense capabilities. Security solutions must exist at every stage of the supply chain to include research and design; production; supply, stock, and store; and deployment. Speaker remarks are summarized on pg. 13

On May 1, 2018, the VITAL Center and Venable LLP cohosted a seminar focusing on current cyber threats to key sectors' supply chain security, using the financial and telecommunications sector as case studies. These case studies highlighted the kinds of security risks and mitigation tactics in the financial services and telecommunications industries. They provided context to the threat facing not only the US public sector, but its private sector as well. The seminar, held at Venable LLP's headquarters downtown Washington D.C., featured speakers with broad experience in cybersecurity, supply chain monitoring, financial services security, and telecommunications. The event was moderated by Mr. Ari Schwartz of Venable LLP, and introductory remarks were made by Dr. Michael Fritze, Director of the VITAL Center at the Potomac Institute for Policy Studies.

Panelists included:

- Ms. Joyce Corell of the Office of the Director of National Intelligence, National Counterintelligence and Security Center (NCSC), who framed the discussion in a keynote address;
- The Honorable Melissa Hathaway, President, Hathaway Global Strategies, Senior Fellow and Member of the Board of Regents, Potomac Institute for Policy Studies;
- Mr. Charlie Miller of the Santa Fe Group; and
- Mr. D.E. (Ed) Wilson, Jr. of Venable LLP.

Attendees represented a mix of government and industry stakeholders, who actively engaged with the panelists in a discussion at the conclusion of the panel. The speakers' remarks are summarized in Appendix 1, and their biographies are included in "Supply Chain and Cybersecurity" beginning on page 19 .

On September 19th, 2018, the VITAL Center hosted a second supply chain security-focused seminar, entitled "Security Strategies for Global Supply Chains." This event, held at the Potomac Institute in Arlington, Virginia, sought to build upon the themes of the first seminar. This event included perspectives from the energy sector and pharmaceutical industry and encouraged dialogue between stakeholders in both the public and private sector. The event was moderated by Dr. Michael Fritze, Director

of the VITAL Center at the Potomac Institute for Policy Studies. Mr. Michael Swetnam, Chairman of the Board and CEO of the Potomac Institute provided introductory remarks to the Potomac Institute's mission. He also spoke to the mission of the VITAL Center and the role it plays in bringing together a community of supply chain security experts and stakeholders across business and government.

The seminar speakers included:

- Dr. Joye Purser of the Office of the Secretary of Defense, Cost Assessment and Program Analysis (OSD CAPE), who provided a keynote address, followed by panelists:
- Mr. Chris Nissen of the MITRE Corporation;
- Dr. Tushar Misra, Vice President and Global Head, Oncology and Biologics Operations, Takeda Pharmaceuticals International, Co.;
- General Al Gray, USMC (ret.), Potomac Institute Chairman of the Board of Regents, Member of the Board of Directors, and Senior Fellow of the Potomac Institute of Policy Studies.

The discussion following the panel, moderated by Dr. Michael Fritze, included input from the audience. The speakers' remarks are included in "Security Strategies for Global Supply Chains" beginning on page 25.

Image: Shutterstock.com

Image: Shutterstock.com

Findings

Vulnerabilities in supply chains for commercial products and critical infrastructures pose significant threats to national security.

The public, industry and government all depend on the reliability of commercial products and critical infrastructure systems. Cyberattacks are often treated only as isolated IT incidents, but in the case of large-scale attacks on the financial sector, telecommunications, or another critical infrastructure, when the IT capability goes down, so does the whole business or network. Companies still bring bad product to market, and bad product fixes to market, because it makes money, but this business model is becoming an overall safety issue. No matter the end-product, the most important aspect of any supply chain is its ability to deliver a safe, uncorrupted product to the end user, whether that person is a warfighter, medical patient, or commercial consumer.

There are inherent vulnerabilities everywhere, because the core backbone operating systems for many critical infrastructures and supply chains contain flawed products. The full supply chain can be manipulated in any number of ways, with a low barrier to entry for attackers.

Threats to supply chains are highly varied, complex, and are not solely attributable to foreign actors.

Stakeholders need to think through supply chain threats to each of their business transactions.

With increasingly globalized supply chains, it is more difficult to understand specific actors' motivations for a transaction or partnership. However, foreign companies are not the only source of threats. There are many insider threats to US-domestic supply chains and critical infrastructure.

There are many possible impediments to an uncorrupted product being delivered on time to the correct location. These may include poor law enforcement, lacking trade regulations, low standards of governance, and corruption in the public and private sectors. All these aspects can play a crucial role in the diversion, counterfeiting, or direct theft of previously unadulterated products.

The solution to managing risk abroad isn't to simply avoid buying foreign, since most production of complex systems now occurs in a globalized environment.

Threats are already "baked in" to many critical infrastructure systems, commercial products, and government systems, via both software and hardware supply chains.

Security is often discussed in a very tactical way. But there is another problem looming on the horizon, with companies like Cisco, Microsoft, and other largescale system backbone providers and their security loopholes in their software, enabling all sorts of cyberattacks to supply chains and operating systems. From an information-communication-technology perspective, the US has embedded poorly designed, flawed devices into its critical infrastructure. The economic opportunities that these flawed devices bring by being bought to market too early without proper security measures leave them vulnerable. These devices and the infrastructure they support are inherently exposed to hacktivism, fraud, crime, and espionage, all because the underlying infrastructure backbone is flawed. New problems due to an unsecured cyber backbone become apparent every day, many of which are targeting core products. Not a day goes by that people's systems aren't being penetrated by cyberattacks. The government is not in a position to relax with the status quo of standards and security. It has lost classified information and billion-dollar intelligence capabilities.

The private sector is not in a position to become lax with its security standards either. Many firms

say that they can provide security services, but they also want to provide fixes to the first bad services that necessitated specific security software. This highlights how companies foster unhealthy markets, by bringing a flawed, unsecured product to market, and then by bringing a bad product "fix" to market.

Risk assessment efforts in both government and industry are improving, but still fall short of what is needed.

Because government is less robustly funded, it will not always do the complete due diligence required to assure security because of budget constraints, despite its best intentions.
Risk assessment is moving away from point-in-time benchmarking that is static towards continuous monitoring. There are certain areas from a risk perspective that should be monitored non-stop.
For this purpose, third party risk assessment and management is becoming an increasingly valued service. While much of the valuable data on supply chain security is not available for free, there are companies that monitor security of supply chains in a comprehensive fashion, and they should be used more than they are to aide in information gathering.

Current supply chain risk management and mitigation efforts are insufficient to meet today's known threats, much less prepare for future vulnerabilities.

Risk management is becoming increasingly complex. For example, the supplier network for the F35 is multi-faceted, multi-national, and complex. Threats in this example can come from many vectors, both inherent and introduced. This makes them difficult to address, especially against adversaries whose attack vectors are also equally varied. "Integrated risk reduction" is a term coined by Joyce Corell – and it involves using all information available to assess the risk in any particular supply chain. Critical infrastructure protection work will not work unless the private sector gets into the game, and does a much better job of talking to each other to establish standards for security.
If the US can regulate energy, food, medicine, then it needs to have a minimum standard of care for IT companies and products writ large. The private sector has a responsibility to fix the core backbone of critical infrastructure IT products, which represent a major vulnerability.

The U.S. financial sector faces heightened threats due to its central role in international commerce, which has spurred the industry to be proactive in addressing cybersecurity and supply chain threats.

The dollar is the reserve currency, which means that 98% of all international transactions are routed through the US, making its financial services sector a large target. Subsequently, the financial sector has realized this and responded with innovation in security measures to counteract the high level of threats. Because the dollar is the reserve currency, it lends itself to a number of critical uses. It can be used to impose economic sanctions, for example shutting down the South African government. The dollar can also be used to follow drug money traffic, trace terrorist funding, and trace illicit funds like money laundering coming out of 3rd world countries.
The reason we need to protect this financial infrastructure, and remain the reserve currency, is because we must hold onto all these abilities, hence the financial services sector's offensive strategy in addressing cyber threats and flawed operating backbones.

There is an increasing willingness in the private market to identify and understand risk, but gaps remain in companies' abilities to address cybersecurity and supply chain security issues on their own.

Companies tend to only fix problems when they have a clear economic impact. In many sectors, companies are more willing to improve security but corporate boards are not bringing on the expertise needed to address the problems identified. More red-teaming efforts in both the public and private sector would aide with response time when a supply chain has been compromised, and encourages innovative thinking in terms of predicting threats and devising creative solutions to address them.

Commercial companies value time-to-market over security, and the defense industry values schedule, cost and performance over security. Neither are incentivized to improve supply chain security.

Rapid tech development creates unintended vulnerabilities, so systems need to be designed with security in mind. There is no "one-and-done" decision making solution on when trying to select partnerships with the highest levels of supply chain security. Business partnerships are not "one-and-done" in terms of security of the product, and require monitoring and benchmarking. An ongoing conversation is needed to facilitate the highest levels product security. In software development side, companies need to fully develop their products' security protections instead of rushing products to market to increase their profit margins at the expense of the customer's security. The security in a part or system's supply chain must be prioritized as equivalent to or even more important than cost, schedule, and performance when executing the acquisitions process for defense and intelligence applications, expanding to all of government.

Image: Shutterstock.com

Image: Shutterstock.com

Recommendations

Hold the private sector accountable for failures in product performance and supply chain security breaches that could have been prevented by prioritizing security.

Administrative, legal, and technological controls on digital business are not treated in the same way as financial controls. The CEO should have sign off on these cyber security controls, or they are considered negligent. S/he must be legally responsible to sign off on risk controls of his or her enterprise, because all businesses are digital in some capacity now and require security measures of one kind or another.

A comprehensive, holistic approach to supply chain security is needed, and must be clearly articulated across all steps in the supply chain.
A team with diverse abilities across every point of the supply chain is needed to collectively manage risk.

The U.S. Government and industry should work together to establish minimum standards for supply chain security.

Regulate the digital product coming into the market, and then have minimum standard of care, and then a light touch. If the US government keeps pushing on the middle, we're going to strangle the economy and not fix the problem.

The U.S. Government should require a supply chain security plan as part of the contracting process.

Any company wanting to do business with the United States Government must have a supply chain security plan to assure, monitor and verify the provenance of its product from beginning to end of design, production, and distribution. If a company does not have this kind of plan, it should not get the government's business.

Conduct more extensive red-teaming efforts, both in the private and public sector, to address supply chain security challenges.

Backup communications, data storage, and other vital systems to prevent outright failure if attacked. Develop a new system of incentives for industry to facilitate this process.

Improve information-sharing regarding supply chain threats and vulnerabilities between the U.S. Government and Industry.

Neither the government nor industry can solve supply chain security issues on their own. Public-private partnerships, information-sharing exchanges, and improved cooperation are needed to close the supply chain security gap.

Image: Shutterstock.com

Event Summary: A National Strategy for a Secure Microelectronics Supply Chain (Cosponsored by Venable LLP)

September 13, 2017

This event outlined a national strategy for ensuring hardware and software security along the government microelectronics supply chain. It was cosponsored by the Potomac Institute for Policy Studies and Venable LLP at Venable's DC office. It was widely attended by notable industry professionals and government officials in the field and sparked a lively and productive question and answer session after the initial presentations.

Key findings from this event included the fact that there is undoubtedly a critical need for a secure national supply line for microelectronics. This need is both expensive and persistent. After some delay, policymakers have taken notice of this issue and directed the DoD to develop a plan to secure their supply chain. The current administration has also expanded the goal of hardware security to include all critical sectors of the national infrastructure.

When taking action to ensure security, bot software and hardware must be addressed. In both cases, there are different tiers of threats at each stage of the supply chain that require unique security strategies. They range from threats posed by teenagers with a laptop, to nation states funding world-class computer scientists. When addressing each, spending should match the severity of the threat.

The highest tier of trusted assurance is not necessary for all systems. The US does not need to manufacture every chip domestically that is used in the US for the purpose of combating low tier threats. Guaranteed trust in each stage of the supply chain should only be utilized for most sensitive technologies. On that note, there are security solutions for DoD at each stage of the supply chain. At the R&D phase, DoD can work with commercial companies to establish Trust. At production, DMEA can provide chips for critical systems. Stock, store, and supply is the mission of JFAC, and DoD is well-prepared for protecting critical components during deployment. While this strategy is an answer for DoD, it is not a direct match when expanding to other critical systems. As a nation state problem, this will require a nation state solution.

In identifying risk for both industry and government, there is a need for standards and metrics to quantify security. This will allow utilization of more traditional cost benefit analysis. There is a problem with incentivizing security in industry. To solve this, quantify the value of security to transform it into a tangible asset to industry, as is often done in cybersecurity for financial services. On the point of trade, ITAR is an impediment to State-of-the-Art technology access. It is harming U.S. business and security interests. The U.S. should move to a classification system instead.

It was concluded that there is an ongoing need for joint classes between industry and government officials on their respective business models to increase understanding between the two sectors.

Michael Swetnam

Chairman of the Board and CEO, Potomac Institute for Policy Studies

Mr. Michael Swetnam is the Potomac Institute for Policy Studies' Chief Executive Officer. As the lead speaker of the event, Mr. Swetnam outlined the purpose of the meeting: to highlight the need from a trusted national supply line for microelectronics. He noted that the formal policy for regulating security in microelectronics is ten years old and it created what would eventually become Cyber Command. The process of investigating and addressing cyber threats is expensive, costing billions of dollars in these ten years, and must continue to be addressed. The need for continued investment will not go away.

After providing this context, Mr. Swetnam highlighted the need to focus on hardware security in addition to software security. Threats that are "baked in" security flaws, like kill switches and backdoors, that can be activated at will is a daunting prospect that must be addressed. To better understand the wide range of threats, he described the Defense Science Board's Tiers of Threats starting with software threats.

Tiers of Threat scale from Tier I to Tier VI. In terms of software, the lowest threat levels exist on everyday people's laptops and mobile devices. They are created by high schoolers and are inexpensive to handle. The next step up the scale introduces professional criminals. These are more expensive threats with real consequences like identity theft, intellectual property theft, and credit card scams, that can have large economic costs, into the billions of dollars nationwide. Higher up the scale, the types of attacks that qualify for that classification are limited to nations states. They require the world's best minds with substantial funding, are involve cyberattacks that are beyond the scope of the public imagination. Dealing with attacks of this magnitude requires substantial investment and is the job of Cyber Command, and the reason we spend billions on that problem. It is critical that we match spending to the level of threat.

After describing the tiers for software threats, Mr. Swetnam addressed the corresponding tiers for hardware. The threat spectrum is similar in principle, but fewer threats exist on the lower level. These involve practices like counterfeiting, which exist but are a comparatively small problem. The threats in the higher tiers are much more concerning. These stem from nation state actors with access to foundries who can input backdoors and kill switches into processors. There are a very limited number of countries that fit this description, and there is a very real possibility that this could happen.

After describing the purpose of the meeting and the Tiers of Threats, Mr. Swetnam posed the question: How do we address the full spectrum of threats, while allocating our resources in the correct way? The problem extends along the entire supply chain and deals with more than just software; there are vulnerabilities and room for improvement all along the supply chain, with spectrums of threat at each stage for software and hardware. The full spectrum must be addressed, which includes: R&D, Production Supply, Stock, and Store, and Deployment.

Mr. Swetnam touched on recent efforts to secure this supply chain. Policymakers have been slow to understand the reality of the threat, but FY 2017 NDAA Sec. 231 outlines objectives for a year-long plan for the DoD to develop a plan to secure their supply chain. Building from that objective, the current administration expanded the goal of hardware security to include all critical sectors of the national infrastructure.

In answer, he said that we do not need to manufacture every chip that is used in the US just to make sure that we don't have counterfeit. Furthermore, guaranteeing trust in each stage of the supply chain is not something that you should do for all your chips. Only the chips in the most sensitive technologies, such as those in F-35s, in the command and control systems on Air Force One, or in nuclear weapons, merit this expensive process. These critical systems must be comprised entirely of trusted components, so that they work when and how they are supposed to work

Mr. Swetnam noted that DoD has been thinking about the trusted supply chain problem for a very long time. There are people working on each of the four steps of the supply chain, and there are people working in the non-profit realm with them. What DoD hasn't done is wire together into a cohesive plan that makes the individual parts run correctly together and used appropriately. The majority of the systems in DoD do not need to worry about this, they can get their chips commercially, but if it is a specially designed chip, you want it to be developed in the US. In answer to the US Congress and the administration, there needs to be a plan that puts together the billion-dollar efforts of DoD, rationalizing and integrating it. That integrated plan should be the national strategy moving forward.

When speaking of this national strategy, he said that we do not need to manufacture every chip that is used in the US just to make sure that we don't have counterfeit. Furthermore, guaranteeing trust in each stage of the supply chain is not something that you should do for all your chips. Only the chips in the most sensitive technologies, such as those in F-35's, in the command and control systems on Air Force One, or in nuclear weapons, merit this expensive process. In these critical systems, they must be comprised entirely trusted component, so that they work when and how they are supposed to work

He also outlined an effective strategy for the microelectronics at each stage of the supply chain. At the R&D phase, commercial companies will work with the USG to establish Trust. However, at the production phase they are less likely to share information. To fill this gap, DMEA in Sacramento currently is optimized produce state of the practice chips when necessary for these critical systems, and currently makes about 1.5 billion dollars per year in chip production already. It is well situated for expanded trusted production, and it is one of the few places in DoD that has the acquisition authority to do this. JFAC will then handle the stock, store, and supply with some guidance in the future. On the deployment side, DoD is already well prepared for protecting its critical chips, as long as they are properly identified.

Mr. Swetnam noted that for DoD, the above outlined strategy is an answer. However, if the mission is expanded to other critical systems like the electrical grid, the answer must be tailored to be an answer for those as well. When doing so, it is important to remember that this is a nation state problem with a nation state solution. On the electrical grid, for example, there is no need to make it cost five time as much, just to make sure all subcomponents come from the same source. There are better methods. Most chips that are produced overseas are perfectly serviceable. However, there are some critical components that should be trusted, and those need to be identified.

Ari Schwartz

Managing Director of Cybersecurity Services, Venable LLP

Ari Schwartz is a leading voice in national cybersecurity policy with over two decades of government and nonprofit sector experience, Ari Schwartz is Venable's Managing Director of Cybersecurity Services. He began his speech by declaring the need to decipher ways to make this process work for more than just the top layer of chips.

He posited that the way to do that is by promoting trust by standardizing the process of securing chips. This means testing against gold standards throughout the supply chain, from design to production to test to end use. The different pieces must flow together so that you know what it is supposed to look like during design and what it looks like when it comes out of production. It must look the same when it is received by the user, and it must still look the same when being deployed. This process cannot be restrictively cost prohibitive in order to apply solution across critical infrastructure and allow wide range of players to use tools.

Mr. Schwartz also brought up the need to move away from having these supply chain security conversations on a country-to-country level, because solutions are not country-based. So many components in systems come from so many different places, so many devices are part of the internet of things and are attached to critical networks, that it becomes very difficult to develop Trust in those systems. In order to develop that Trust, we need to move into a discussion that doesn't rely only on US-produced chips.

He ended by saying that whatever comes out of the DoD strategies security standards will drive the rest of discussion across critical infrastructure.

J. Michael Daniel

President, Cyber Threat Alliance, and Former White House Cybersecurity Coordinator

Michael Daniel currently serves as the President of the Cyber Threat Alliance and was previously the Special Assistant to the President and Cybersecurity Coordinator on the National Security Council Staff. Mr. Daniel began by outlining a number of trends in cybersecurity that are making the goal of security harder and more diverse every day. They are:

- At the conservative end, ten million new devices are added to the internet of things every day.
- While the physical world has a finite amount of room to secure, the realm of cyberspace is constantly expanding the real estate that needs to be secured.
- More and more people are pursuing their goals through the medium of cyberspace, be they malicious actors or otherwise.
- With this shift to more threats being carried out online. Ten years ago, there was serious concern about attacks such as website defacement, but there is now a willingness to move up the threat

spectrum to stage larger and more impactful attacks. Malicious actors are willing to take higher risks than ever before.

- Society is becoming increasingly dependent on our network, including our internet of things. This high level of digital dependence leaves us open to threats.

Mr. Daniel then went on to say that as the cyber community tries to address the growing number of software, network, and hardware vulnerabilities, the question of how to anchor trust arises. The answer is to anchor trust in hardware. If that is the root, then malicious actors will have to work to attack it. This then begs the question of how to ensure security in this root of trust.

When answering this, he noted that geography does not equal security. That is to say that simply making the product here does not guarantee that everyone touching the hardware is reliable. Furthermore, the supply chain is, and will remain, global. This means that it is foolish to assume that there is a geographic solution.

Mr. Daniel then said that the solution is to manage risk with hardware just as we manage risk with software. This includes using a multi-faceted approach with alternative paths to recovery to mitigate any threats. We should also flip the problem around by anticipating the objective of attractive and address their intended end goal and corresponding mode of attack to secure those vulnerabilities. This will allow us to focus on our efforts instead of advocating security in general, a benefit because of the expense of securing every part of the manufacturing process.

Terry Halvorsen

Former DoD Chief Information Officer and Chief Information Officer at Samsung Worldwide

Mr. Terry Halvorsen is the Chief Information Officer and Executive Vice President IT and Mobile Business to Business group at Samsung Electronics. Prior to Joining Samsung Electronics, he served as the Department of Defense Chief Information Officer.

Mr. Halvorsen began by stressing the importance of not losing focus on software security while trying to increase focus on hardware security. He also acknowledged the huge economic interest that his company has in the subject.

While noting the benefit of talking extensively about hardware, Mr. Halvorsen also emphasized that this is a complete supply chain problem across all of the parts of the system, and that it is also an economics problem. The reason we are so focused on this today, is because many of the foundries in the US are closed. It is no longer an economic reality for businesses to stay in the foundry business. In order to fix that problem, the economics of the situation must be restructured.

He noted that trying to define which systems are critical, and where they share components with non-critical systems, is impossible. The integration of components across systems will continue to be more common and will enlarge that problem. Furthermore, many of these problems are less about cybersecurity and more about a risk-assessment decision that must be made. We've made good ones and bad ones in the past both in the private and public sector, since it is no longer just a government problem. It continues to be a big problem in many of the largest corporations.

Mr. Halvorsen then summarized by saying that there needs to be a restructuring of the economics side of the problem, that we need to look at entire supply chain including people (because the certification and accreditation processes are too slow), systems, and all stages of production, and we need a systems approach that not only looks at best risk level but also what is economically viable to scale.

Image: Shutterstock.com

Event Summary: Supply Chain and Cybersecurity in the Financial Sector (Cosponsored by Venable LLP)

May 1, 2018

This event sought to bring together officials from government and industry to discuss cyber threats to supply chains, the nature of supply chain and cyber vulnerabilities, and how these vulnerabilities are being addressed in case studies of private industries in the United States like the financial services and telecommunications sectors.

Several key insights resulted from this seminar. The nature of vulnerabilities stem partially from rapid tech development, and need to be addressed at all points along the supply chain by a diverse team. This practice is called "integrated risk reduction" and it involves using all information available to a producer to counter both inherent and introduced threats, from both malicious actors and accidentally included via the process of rapid technological development.

Panelists went on to further discuss cyber threats in almost all industries, given that many operations have gone online. From an information, communication, and technological perspective, we have poorly designed, flawed, and vulnerable devices embedded in our critical infrastructures. The economic opportunities brought on by new technologies and digital infrastructures are inherently exposed to hacktivism, covert surveillance, fraud, crime, and espionage. New technologies must be designed with security at the forefront of the design process.

Given that currently deployed technologies and digital infrastructures are already inherently flawed, more must be done to do real-time threat assessment and risk reduction. The current state of risk assessment shows a move away from point-in-time assessment at the beginning of an interaction, with periodic review based on criticality of supplier towards continuous monitoring. There are certain areas from a risk perspective that can be monitored non-stop, and we will begin to see continuous monitoring in real time at an increasing rate.

A good case study for how to manage risk is found in the financial services sector. A robust risk management environment has sprung up in the financial services sector, more so than in other industries, given the heightened risk and possibility for loss. Because the American dollar is a reserve currency, 98% of all international transactions flow through the United States, making its financial services sector a prime target for bad actors. The dollar's status as a reserve currency allows the United States to impose effective economic sanctions, trace drug and trafficking money to aid in deterring criminals, as well as trace money laundering operations the world over. Again, the U.S.'s capability to monitor transactions makes it a target for cyberattacks to the financial infrastructure as much as the volume of money flowing through our financial services industry provides a prime target. This unique quality of the U.S. dollar is another reason why it is important to monitor, assess, and mitigate threats in the financial services.

A root driver of increasing security is more recognition at the board level that cyber vulnerabilities are

a form of extreme exposure to possible losses. There should be some level of expertise on the board to evaluate responses to cyber threats, and to conceptualize third-party risk. However, in most industries it is a struggle to get people on-boarded and operational in a business unit who have this kind of understanding.

In conclusion, this seminar highlighted that despite popular opinion, almost every business and industry is digital, meaning that with current cyber threats no business, supply chain, or infrastructure is secure. More needs to be done to promote security as a primary concern in business transactions and systems design for all types of transactions.

Please see page 40 to view The Santa Fe Group's slides, presented at this event by Mr. Charlie Miller.

Ari Schwartz

Managing Director of Cybersecurity Services, Venable LLP

Mr. Schwartz provided introductory remarks for this session, stressing the shifting nature of cyber challenges and security in the financial services sector and telecommunication. He spoke to the work that Venable does in these areas, representing clients at the highest levels of the private sector. After providing his introductory remark, Mr. Schwartz co-moderated the panel proceedings with Dr. Michael Fritze of the Potomac Institute for Policy Studies.

Joyce Corell

Assistant Director, Supply Chain and Cyber Directorate, National Counterintelligence and Security Center, Office of the Director of National Intelligence

In her keynote address, Ms. Corell discussed the framework for how stakeholders should be thinking about the security of their supply chains, touching on the importance of cybersecurity, a framework for assessing risk, third-party risk assessment, integrated risk reduction, and common oversights when attempting to oversee comprehensive supply chain risk management.

Ms. Corell stressed the importance of thinking about risk within the context of understanding threat, vulnerability and consequence. This is a framework for thinking these supply chain security issues through. When an entity thinks about threats, it categorizes them through an understanding of an adversary's intentions and an adversary's capabilities. Some adversaries may have a lot of intentions but no actual capability. Therefore, threats are overall a mix of intentions and capabilities.
Vulnerabilities are either inherent or introduced. Through the rapid pace of technology development, sometimes vulnerabilities are introduced not for malicious or malign purposes, but by the nature of rapid and diverse technology development. Looking at different tech sectors like energy and electricity delivery, there is a lot of excitement and increasing demand for cutting edge technology that puts more tools in the hands of the consumer. The risks associated with doing so are part of the nature of the evolution of technology, and these technologies sometimes lead to more vulnerabilities that add or exacerbate those originally inherent in a system.

Thinking through the framework for assessing risk, Ms. Corell asked the group how a company understand how it manages its risk. Any threat will be realized when an adversary can apply their capabilities against an inherent or introduced vulnerability. If there's no opportunity to do so, then risk is managed. That's the concern, when a capability can be applied against an inherent or introduced vulnerability. Theoretically, anywhere along the supply chain presents an opportunity for vulnerability exploitation.

To cut down on the number of risks, Ms. Corell discussed how intentions to exploit inherent and introduced vulnerabilities get deterred. She discussed mechanisms for deterrence of intentions. Having guns, gates, and guards is a way to think about deterrence in a physical sense. Physical deterrence serves a purpose by causing someone to think twice about taking some type of precipitous action, but in a fight for security increasingly being found in the digital domain, physical deterrence is not enough to manage risk.
A malicious actor's capabilities enable them to realize attacks and exploit vulnerabilities in a system or supply chain. From a risk management perspective, understanding an adversary's capabilities allows their disruption. If you have inherent or introduced vulnerabilities, you obviously want to detect and defend against capabilities that would exploit these. From a consequence perspective, you need to think through as follows: Are these consequences fixable? Are they fatal? If a system has been compromised, do you restore or discard it?

Another challenge in this particular domain is how one thinks through business transactions and the decisions that businesses make and how can one understand what one is getting in to with different types of partnerships. Are deals engaging with foreign entities to be perceived as legitimate business practices, or something worthy of concern? Just because companies get into joint ventures does not necessarily mean something illicit is going on.

Concern over foreign theft of intellectual property and other threats has increasingly turned toward China. As more Western firms do business in China, the theft of intellectual property has been meticulously documented by U.S. stakeholders. Subsequently, much time and effort has been spent over the past five to six years working with the Chinese government to strengthen intellectual property protections. Hesitation in pursuing joint ventures lingers, given that doing so can be confusing and complicated when working with companies in countries with documented histories of IP theft. In her mind, the better way to assess supply chain risk is to take a "country-agnostic approach" to risk, and to assess the risks that look across all relevant business relationships through the supply chain, including looking at all the organizations that have a third-party relationships, and understand what the associated risks are in in those relationships.

Ms. Corell encouraged implementing "integrated risk reduction" as a template to think risk through. Integrated risk reduction attempts to make the distinction between operational and financial risks. She argued dynamic risks have to be considered from multiple angles. When considering who to do business with, corporations and governments must be scrupulous in judging risk. Often times there is no way to fully quantify risk. Financial analysts and data aggregators can assist in this process by focusing on operational risk instead of financial risk almost exclusively.

Ms. Corell recommended that having good relationships across different lines of business in your supply chain, to have an integrated team approach, is one of the most important strategies for handling risk. Ms. Corell ended by positing that mutual trust along the supply chain is possibly the most important factor in building a resilient industry.

Melissa Hathaway

President, Hathaway Global Strategies, LLC, Member, Potomac Institute Board of Regents, Former cybersecurity advisor to President George W. Bush and President Barack H. Obama, Former Senior Director (Acting) for Cyberspace on the National Security Counsel

In her talk, Melissa Hathaway described the lack of real security on digital platforms and the scale of the threat and risk posed to every business and government entity without a rock-solid cybersecurity risk management strategy. She highlighted the fact that at present, essentially no business or government's supply chain or overarching online platform is safe from exploitation or direct attack.

Ms. Hathaway encouraged different thinking on the topic of supply chains. Ms. Hathaway describes global economic growth is increasingly dependent on the digital information communications technologies that are being embedded in the marketplace. Digital integration represents enormous economic and social opportunities by connecting emerging markets to the global network. Ms. Hathaway cautions that the rush to capture this new economic opportunity is coming at the cost of overlooking serous structural security risks. Crime, fraud, espionage, disruption of service, and now destruction of property are all proliferating digitally because the underlying infrastructure is seeded with vulnerable code. Ms. Hathaway cited Microsoft as a particularly vulnerable private corporation to malicious digital actors.

Ms. Hathaway also noted that the government has been penetrated due to lapses in digital security. State secrets and classified information have been stolen. If the government continues to digitally integrate without putting proper security measures in place, more damaging digital disruptions are inevitable. Ms. Hathaway noted that that digital attacks are comparatively easy and cheap to conduct, making the government and industry vulnerable to a wider range of adversaries.

Ms. Hathaway cited the WannaCry? cyberattack as an example of the growing extent of our vulnerabilities. The tools used in the attack were originally stolen from the government itself and then turned on Microsoft products. Miscommunication and an unwillingness to take blame on either side led the WannaCry? malware to spread globally, causing billions in damages in an extremely short period of time. Ms. Hathaway argued that the damages from such extensive attacks cost lives, with hospitals and clinics losing functionality. State actors are using digital attacks to devastate adversaries' infrastructure. She advocated for holding manufacturers and software developers accountable for securing their systems. She recommended implementing an inspections regime for all foreign code to ensure its security, establishing international standards for software security, and creating a new comprehensive cybersecurity initiative. Ms. Hathaway concluded by advocating that the current level of risk in the digital industry is only rising and unless corrective action is taken, will cause increasingly negative effects to the growing industry.

Charlie Miller

Senior Vice President, The Santa Fe Group

Mr. Charlie Miller built off of Ms. Hathaway's discussion of cybersecurity threats and vulnerabilities, taking up the point of assessing vendor and third part risk using continuous monitoring and other emerging practices to continuously assess vendors' cybersecurity, IT, privacy, data security, and business resiliency controls. His presentation then discussed program tools used by the Santa Fe Group that allow for trust, verification, and benchmarking via continuous monitoring to identify and mitigate third party risk in real time.

Miller spoke on the issue of risk within the supply chains of companies. Through his company, Miller has promoted the method of risk handling known as trust-but-verify. He noted that this method became a viable option for countering risks within the supply chain. This trust-but-verify method consists of two key steps to be taken in order to alleviate the risks. The first part of the process, trust, takes the form of a questionnaire that had approximately two thousand questions and currently has one thousand three hundred questions. These questions were created to verify and validate that procedures are operational and controls are working. The second part of the trust-but-verify method is to verify across multiple organizations within the company, looking into their outsourcing options to search for any potential risk. This process works well however it is often a lengthy method for risk sensing. For a business that relies on speed and getting products to consumers quickly, stepping between due diligence and this necessary speed can place much scrutiny on the decision makers, and cause them to prioritize schedule over security.

Miller continued to note the history and current state of risk assessment. He noted that in the past, risk assessment was easier because there was usually only one outsourcing relationship, which made the process easier. Today, however, there can be multiple relationships, bringing in third and fourth party risk. These two types of risk are respectively the risks associated with your supplier and your supplier's suppliers. Each supplier has vulnerabilities and the more that are involved, the more they bring their risks together to form a collectively large risk profile.

The techniques brought forth by the Santa Fe Group can be applied at the beginning of the outsourcing relationship or throughout the relationship in one of two year intervals. Miller noted that there are areas that you can monitor on a continual basis and understand the risks that are raising or lowering or if there is additional work that would need to be done. These techniques work well in combating risk, however, he noted that the techniques can be expensive and therefore only bigger players in industry can afford them. One solution to this common issue is the information sharing concerning certain suppliers that can holistically aid in the processes of all companies.

There are three major takeaways noted by Miller at the conclusion of his speech. He emphasized that governments and companies must participate in the development of standards. Without this participation, standards will be set by other countries and American companies will be closed out of the standard making process. Secondly, there must be opportunities to collaborate to create a network of risk assessment. Miller only mentioned his third takeaway slightly, however, he mentioned the need to improve the efficiency and effectiveness of risk assessment and the process to combat the threats. Miller proposed these methods of risk management to protect companies from third and fourth party risk on the world stage.

D.E. (Ed) Wilson, Jr.

Attorney, Venable LLP

Mr. Ed Wilson of Venable LLP closed the panel by discussing supply chain security risks in the financial industry, which served as a "best practices" benchmark for how entire industries conceptualize supply chain risk and mitigation.

Mr. Wilson detailed his observation of the financial infrastructure and how the system will change going forward. He stated that electronics are the infrastructure of the financial system. Wilson noted that the typical flow of payments goes from business-to-business or business-to-consumer, however these payments are increasingly becoming consumer-to-consumer and consumer-to-business.

Because much of the world uses the dollar as its reserve currency, Wilson noted that the United States government is able to track the flow of money with 98% of transactions being routed through the United States. Previously this flow was unattached to the name of the individual or entity sending funds. As noted by Wilson, someone could send money from one bank to another and no individual's name would be attached to that transaction. Today, however, names, account numbers, and banks are attached to the transaction. This enables someone to enter into these and change any of the fields in the transaction. This opens up the possibility of cheating within the system.

Wilson further noted the rapidly changing environment of payments. Moving from credit and debit cards to purely online money transfers again opens up bank information to be used by someone other than the owner.

Wilson continued by referencing the issues Joyce Corell and Charlie Miller raised, that the number of contractors working with any central company is a larger number than in the past, which leaves room for vulnerabilities. Wilson noted that in the recent past, it was possible to know each participant in a transaction. Now, however, due to the large number of contractors and vulnerabilities created through a diverse network of service providers and affiliated parties, the identity of participants and the location of a payment issue is difficult to know.

A further concern raised by Wilson was the loss of personal space due to the diminishing role of cash money in the financial system. He posited that society is losing the ability to disconnect the personal from the financial system all together.

Wilson concluded his statements with warnings that the financial system could fall under its own weight should banks continue to make contracts with a growing number of different service providers, increasing both the number and breadth of avenues for threats and vulnerabilities to affect the system as a whole.

Event Summary: Security Strategies for Global Supply Chains

September 19, 2018

At the September 19th seminar, subject matter experts and stakeholders in the field of supply chain risk management came together to discuss challenges and risk management strategies in addressing supply chain vulnerabilities across industries. Representatives of the energy sector, the pharmaceutical industry, and the defense and intelligence communities all shared their insights.

Key findings from this forum spanned several topics. It was determined that the solution to managing risk abroad isn't to simply avoid buying foreign, since most production of complex systems now occurs in a globalized environment. Critical infrastructure protection work will not work unless the private sector starts prioritizing and marketing security as a feature. In addition, the private sector must do a better job of talking across sectors to establish standards for security. On the software development side, companies need to fully develop their products' security protections instead of rushing products to market to increase their profit margins at the expense of the customer's security.

The role of the government in establishing standards for security was also discussed. If the US can regulate energy, food and medicine, then it needs to have a minimum standard of care for IT companies and products writ large. The security in a part or system's supply chain must be prioritized as equivalent to or even more important than cost, schedule, and performance when executing the acquisitions process for defense and intelligence applications, expanding to all of government. Over all, more red-teaming efforts in both the public and private sector would aide with response time when a supply chain has been compromised, and encouraged innovative thinking in terms of predicting threats and devising creative solutions to address them.

From a government acquisitions perspective, it was suggested that any company wanting to do business with the United States Government must have a supply chain security plan to assure, monitor and verify the provenance of its product from beginning to end of design, production, and distribution. If a company does not have this kind of plan, it does not get the government's business.

The seminar was successful in initiating dialogue between government and industry leaders in supply chain risk management, with information sharing and a lively discussion period at the conclusion of the panel.

Michael Fritze, Ph.D.

Vice President, Potomac Institute for Policy Studies

Dr. Fritze moderated this session and facilitated the period of discussion at the conclusion of the panel that contributed to the findings, conclusions, and recommendations of this report.

Michael S. Swetnam

Chairman of the Board and CEO, Potomac Institute for Policy Studies

Mr. Swetnam provided introductory remarks to this session, highlighting how supply chain security has always been an issue, but that in an increasingly connected world, the security of those supply chains is more complicated than ever. He referenced an example of a salad dressing company with no physical employees as an idea of an unconventional company and supply chain. After framing the discussion, Mr. Swetnam introduced Dr. Joye Purser and her keynote address.

Joye E. Purser, Ph.D.

Deputy Director/Joint Data Support, Analysis and Innovation Division, Office of the Secretary of Defense, Cost Assessment and Program Evaluation

Dr. Joye Purser provided the keynote speech at the September 19th seminar on global supply chains, lending a government perspective to the discussion of the need for comprehensive supply chain security in all US critical systems. She opened by illustrating the impact a secure supply chain has on the lethality and interoperability of US military materiel. Dr. Purser stressed that producers of government technology and equipment should maintain close awareness of product design and development, along all aspects of the supply chain so that military operators in the armed forces can do their work with confidence.

Globalized supply networks not only affect government systems and lives, but those of civilians as well. Dr. Purser highlighted the ever-expanding and more complex nature of how goods are financed, designed, developed, produced, sold, and used. She pointed out a panelist in the pharmaceutical sector, and stated that the banking-, energy-, and health care sectors had money and lives at stake. She cited that tracking parts, let alone full systems, is an ever-more complicated task since there are so many locations and personnel involved in making the materials for components, and components for full systems.

Dr. Purser relayed that the good news was that defense supply chain and industrial base issues had captured the attention of decision makers in the White House and Congress. She pointed to a recent GAO report assessing government supplier and supply chain risks in the defense industrial base, with recommendations on how to address looming concerns around trust and security in critical supply chains. Delving deeper into the risk factors affecting supply chain, Dr. Purser discussed a litany of potential threats, including single source, foreign dependence, obsolete items, capacity limitations, and special-

ized equipment. Microelectronics components in critical systems were a frequent example; and in her keynote Dr. Purser highlighted how vulnerable integrated circuits are to corruption in an unsecured supply chain. Dr. Purser asserted that the US government cannot take chances when it comes to the parts that it purchases for military equipment. She made the case that certain industrial sectors should also take no risk, when it comes to a vulnerable supply chain.

According to Dr. Purser, the US government has acknowledged this matter and has begun to act, to strengthen and bolster the defense materiel supply chain. The National Defense Authorization Act (NDAA) for Fiscal Year 2019, signed into law August 13, 2018, contains several key provisions for supply chain security and supporting the defense industrial base. One such provision is NDAA Section 321, authorizing the use of working capital funds to do small scale construction for the defense industrial base, which would help to secure some of the physical threats to the defense supply chain and mitigate issues surrounding single sourcing. The second key inclusion in the NDAA that Dr. Purser referenced is Subtitle E Sections 841-847, called Industrial Base matters. This section contains eight items ranging from support of defense manufacturing communities to protecting the defense industrial base, to further reports on limited sources of critical components, to another report on the defense electronics industrial base, to limitations of certain procurements application process. This policy focus on defense industrial base issues signals congressional and executive branch intent to continue with bold action in the near future.

With the nature of global commerce generating complex second order effects, the Department of Defense and the US government can take no risks in acquiring equipment critical to national security, and critical to warfighters' safety. Dr. Purser ended her remarks optimistically, citing that there are many dedicated people, both public servants and commercial sector leaders, all working together toward possible solutions. She concluded by observing the precise dilemma faced by supply chain security stakeholders: "Isn't it a paradox that some of our government's biggest challenges, rely on systems that are very, very small?"

Tushar Misra, Ph.D.

Vice President and Global Head, Oncology and Biologics Operations, Takeda Pharmaceuticals International, Co.

Dr. Misra's talks on at the September 19th VITAL supply chain seminar centered on the pharmaceutical industry's supply chain, both on challenges in securing it as well as methods used by pharmaceutical companies to combat threats to the supply chain. While he began his discussion by distinguishing two impacts of a less-than-secure supply chain, economic and safety, Dr. Misra mainly discussed impacts on safety. He noted that a successful supply chain strategy would ensure that the medication reaching each patient is uncorrupted and safe to use. The most important aspect of this secure supply chain is actually having the vial of medicine at the site when a patient shows up and needs the medication.

There are many possible impediments to the correct vial being at the precise location when a patient requires it. Some of the possibilities Dr. Misra noted were poor law enforcement, lacking trade regulations, low standard of governance, and corruption in the public and private sectors. All these aspects can play a crucial role in the diversion, counterfeiting, or direct theft of medications. These problems plague poorer areas of the world at a higher rate than more developed areas overall. That is not to say that the problem does not exist in more developed nations and states, however. According to Dr. Misra,

with around 20% of drugs in poorer regions classified as adulterated in some manner, illegal trade and drug counterfeiting costs world economies 10 to 20 billion dollars annually. Along with the impact on the economy, Dr. Misra reiterated how the lack of a secure supply chain impacts the industry's ability to combat deadly diseases. The issue with substandard medication is not only that the patient is receiving substandard care, but this low-quality care can actually aid the disease in developing an immunity to the medication as it is being administered. In the United States (US), patients are not invulnerable to the issue at hand. The biggest medications that are found to be falsified are the drugs that provide the greatest possibility for pay out.

Antibiotics, painkillers, in addition to cancer, diabetes, and heart disease medications are among the costliest in the US and therefore the most likely to be counterfeited, diluted, diverted, or otherwise adulterated. These medications and others are often designed differently for different regions of the world due to regional genetic make-up. This leads to another problem for pharmaceutical companies. Certain drug types, amounts or concentrations are designed, for example, for someone in Japan may not be correct for a person in Brazil. Therefore the dilution, rerouting, or illegal trade of drugs sometimes means that specific medications are found in countries that have yet to even approve the drug for distribution within its borders.

Dr. Misra proposed a plan for pharmaceutical companies to combat the illegal trade of medication and secure their supply chains. Firstly, he proposed Gap Analysis to look for holes within the supply chain as opportunities for falsification. Secondly, select partners very carefully to ensure proper trade and conduct. Thirdly, simplify the process of production. The more moving parts there are in any given supply chain, the easier it is for something to go wrong. Dr. Misra's penultimate recommendation was to write contracts to have enforceable rules that gives the contracting authority the ability to issue punitive responses to those that break conditions. Furthering this point, he advocated conducting regular audits of the supply chain to ensure all practices and processes are in compliance with the contract. Lastly, Dr. Misra advocated the introduction of brand protection methods. He recommended the further development of technologies for consumers to personally confirm that the medication they are receiving is legitimate and unadulterated. According to Dr. Misra, if all these steps are properly taken, pharmaceutical companies should see a rapid drop in adulterated medications and other supply chain security-related losses.

Christopher Nissen

Director, Asymmetric Threat Response, Special Concepts Group, The MITRE Corporation

Serving on September 19th VITAL seminar panel, Chris Nissen provided lively input from the perspective of someone who has worked extensively on supply chain issues with industry, specifically as the Director of Asymmetric Threat Response at the MITRE Corporation. His talk focused on supply chain security challenges and solutions, using the energy sector as a touchstone case study. In his talk, Mr. Nissen described the future of warfare as a "home game as much as an away game" due to the increasing proliferation of asymmetric threats. Mr. Nissen highlighted that American dominance in the ability to engage in conventional kinetic warfare has led our adversaries to seek to disrupt us by other means. These 'asymmetric attacks' commonly take the form of cyberattacks on both US civilian and government infrastructure. Mr. Nissen argued the need for the United States to develop comprehen-

sive deterrence to asymmetric action. He stressed that the process of developing a policy of deterrence requires the commitment of both government and private industry, because both are likely targets for asymmetric attacks.

Mr. Nissen described asymmetric cyberattacks as "blended operations" where the highest-level access points in a system are all attacked coordinately. The first access point is the supply chain, which consists of hardware, software, and services elements. The second point is cyber operations technology and systems and cyber IT. The final point in the blended operation is the human element. All three primary access points must be secure and watching each other in order to have a fully secure system.

Mr. Nissen cautioned that the current systems that have been so beneficial to American industry and government are all inherently vulnerable and could be exploited if an armed conflict broke out. This is where Mr. Nissen drew upon the energy industry as a case study example. He noted that the electrical grid has become bigger and more interdependent, all the while growing without proper inherent redundancy measures to fall back on if attacked. He identified technology, policy, and legislation as the three key factors for hardening US systems against asymmetric attacks. Mr. Nissen recommended that private industry invest now in securing their systems in order to mitigate the effects of future and unknown current attacks. His primary recommendation is to backup communications, data storage, and other vital systems to prevent outright failure if attacked. He also recommends that legislators develop a new system of incentives for industry to facilitate this process. Overall, Mr. Nissen's most encompassing idea was that of prioritizing security in a part or system's supply chain as equivalent to or even more important than cost, schedule, and performance when executing the acquisitions process for defense and intelligence applications, expanding to all of government.

General Al Gray, USMC (ret.)

Chairman of the Board of Regents; Member of the Board of Directors; and Senior Fellow of the Potomac Institute of Policy Studies

General Al Gray provided several key recommendations wrapping up the panel discussion period during the discussion following the panel. Firstly, General Gray synthesized much of the day's commentary into a single thought: If a company want to do any business with the United States Government, it must have a supply chain security plan to assure, monitor and verify the provenance of its product from beginning to end of design, production, and distribution. If a company does not have this kind of plan, it does not get the government's business.

Secondly, General Gray advocated the execution of more red-teaming efforts, both in the private and public sector. This aides with response time when a supply chain has been compromised, and encourages innovative thinking in terms of predicting threats and devising creative solutions to address them.

Appendix 1: Speaker Biographies

Jamie Barnett

Rear Admiral (Ret.), Partner, Telecommunications Group Chair, Venable LLP

Admiral Barnett is Chair of Venable's Telecommunications Group and a partner in the firm's Cybersecurity Practice. He has a rare combination of experience in public safety communications, emergency communications, 9-1-1, alerting, cybersecurity, Universal Service Fund (USF), Telecommunications Consumer Protection Act (TCPA), FirstNet, national defense, homeland security. This experience is invaluable to clients in telecommunications, defense and utilities industries as well as other critical infrastructures.

He was named a Top Lawyer in DC for Cybersecurity by Washingtonian Magazine for 2015.

Admiral Barnett has had a distinguished career in the public and private sector. A surface warfare officer, he has over 30 years of experience in the United States Navy and Navy Reserve, rising to the rank of Rear Admiral and serving as Deputy Commander, Navy Expeditionary Combat Command and Director of Naval Education and Training in the Pentagon. Among other personal awards, he has received four Legion of Merit medals.

In addition to his military service, Admiral Barnett served as the Chief of the Public Safety and Homeland Security Bureau of the Federal Communications Commission where he executed major cybersecurity initiatives. As Chief of the Bureau, Admiral Barnett also led major rulemakings and projects in public safety broadband, emergency alerting and Next Generation 9-1-1, working closely with industry and government stakeholders. He has also testified before Congress and is a noted speaker on cybersecurity.

Joyce Corell

Assistant Director, Supply Chain and Cyber Directorate, National Counterintelligence and Security Center, Office of the Director of National Intelligence

Ms. Corell is the Assistant Director of the Supply Chain Directorate of the Office of the National Counterintelligence and Security Center (NCSC). Prior to this posting she was the Assistant Director for the Strategic Capabilities Directorate.

Ms. Corell served at the National Security Agency (NSA) for 23 years. Her most recent job was the Chief of Technology Policy in the NSA Commercial Solutions Center. Ms. Corell spent a significant portion of her career focused on various aspects of defensive and offensive computer network operations, from capability development to the development of national policy and legislation. Complementing these roles, Ms. Corell also led various activities surrounding partnerships with the private sector ranging from technology transfer, export licensing, and the development of strategic alliances, both domestic and international.

Ms. Corell graduated from William & Mary with a BA in Political Science. She received an MS in National Security Strategy from the National War College and is currently completing an MBA at the Robert H. Smith School of Business at the University of Maryland.

J. Michael Daniel

President, Cyber Threat Alliance, and Former White House Cybersecurity Coordinator

Michael Daniel currently serves as the President of the Cyber Threat Alliance (CTA). CTA works to improve the cybersecurity of our global digital ecosystem by enabling real- me, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field. Its members currently include nine of the largest cybersecurity firms in the world. Michael has been with CTA since February 2017.

Prior to CTA, Michael served as Special Assistant to the President and Cybersecurity Coordinator on the National Security Council Staff. He held this position from June 2012 to January 2017. In this role, Michael led the development of national cybersecurity strategy and policy, and he oversaw implementation of those policies. Michael also ensured that the federal government effectively partnered with the private sector, non-governmental organizations, other branches and levels of government, and other nations.

In this role, Michael focused on executing a three-part cyber strategy: raising the level of our cyber defenses in the public and private sectors over both the short and the long-term; deterring and disrupting malicious cyber activity aimed at the U.S. or its allies; and, improving our ability to respond to and recover from cyber incidents when they occur. During his me in this position, Michael helped develop over half a dozen Presidential guidance documents and worked with Congressional members and staff to pass cybersecurity legislation. He chaired three interagency policy groups, such as the Cyber Response Group. Michael regularly interacted with private industry across multiple sectors and state and local governments in order to convey White House priorities, receive feedback, and promote public- private cooperation and collaboration. Michael played a lead role in creating the government's response to cyber incidents, such the attack on Sony Pictures Entertainment, the intrusion into the Office of Personnel Management, and the Russian efforts to meddle in our electoral process. He played an integral role in driving the integration of cyber capabilities into the broader set of capabilities that can be brought to bear to achieve our strategic interests. Michael also had extensive international engagement in this role, helping to negotiate the cyber commitments with China and implementing the cyber confidence building measures with Russia; he also met with allies and partners on a regular basis, both in DC and abroad, in order to drive greater coordination on cybersecurity policy and operations.

Prior to coming to the National Security Council Staff, Michael served for 17 years with the Office of Management and Budget (OMB). From September 2001 to June 2012, he served as the Chief of the Intelligence Branch, National Security Division, in a career Senior Executive Service position. This branch oversees the Intelligence Community (IC) and other classified Department of Defense programs. In this position, Michael played a key role in shaping intelligence budgets, improving the management of the IC, and resolving major IC policy issues. Within OMB, Michael also served as an examiner in the National Security Division's Front Office supporting the Deputy Associate Director
and in the Operations branch reviewing Navy and Marine Corps operational activities and overseas military operations such as Bosnia and Kosovo.

Michael Fritze, Ph.D.

Vice President, Potomac Institute for Policy Studies

Dr. Fritze is a Vice President at the Potomac Institute for Policy Studies responsible for the Microelectronics Policy portfolio. His current interests and activities include USG trusted access strategies, support of needed legacy technologies, DoD innovation policy and outreach to Industry and strengthening the US Microelectronics Industrial Base. He is also the Director of the VITAL Center (Vital Infrastructure Technology And Logistics) at Potomac.

Dr. Fritze was the Director of the Disruptive Electronics Division at the USC Information Sciences Institute. (2010-2015). He also held a Research Professor appointment in the USC Ming Hsieh Department of Electrical Engineering (Electrophysics). His research interests at ISI included Trusted Electronics, CMOS Reliability & Robustness, Low power 3DIC enabled electronics and Rad-hard electronics. He was a Program Manager at the DARPA Microsystems Technology Office (MTO) from 2006-2010. While at DARPA, Dr. Fritze was responsible for Programs in the areas of 3D Integrated Circuits (3DIC), Steep-Subthreshold-slope Transistors (STEEP), Radiation Hardening by Design (RHBD), Carbon Electronics for RF Applications (CERA), Silicon-based RF (TEAM), Ultra-low power Digital (ESE), Highly regular designs (GRATE) and Leading-edge foundry access (LEAP).

Prior to joining DARPA, Dr. Fritze was a staff member from 1995-2006 at MIT Lincoln Laboratory in Lexington, Massachusetts, where he worked on fully-depleted silicon on insulator (FDSOI) technology development with an emphasis on novel devices. Particular interests included highly scaled, tunneling-based, and ultra-low power devices. Dr. Fritze also worked in the area of silicon-based integrated optics. Another research interest at Lincoln Laboratory was in the area of resolution-enhanced optical lithography and nanofabrication with particular emphasis on low volume technological solutions.
Dr. Fritze received a Ph.D. in Physics from Brown University in 1994, working in the area of compound semiconductor quantum well physics. He received a B.S. in Physics in 1984 from Lehigh University. Dr. Fritze is an elected member of Tau Beta Pi and Sigma Xi. He is a recipient of the Office of the Secretary of Defense Medal for Exceptional Public Service awarded in 2010. He is a Senior Member of the IEEE and is active on the GOMAC Conference Program Committee as well as the NDIA Electronics Division Policy Group. Dr. Fritze has published over 75 papers and articles in professional journals and holds several U.S. Patents.

General Al Gray, USMC (ret.)

Chairman of the Board of Regents; Member of the Board of Directors; and Senior Fellow of the Potomac Institute of Policy Studies

General Al Gray serves as Chairman of the Board of Regents; Member of the Board of Directors; and Senior Fellow of the Potomac Institute of Policy Studies (PIPS). The PIPS serves as a non-partisan, not-for-profit policy research institute that provides an academic forum for the study of key national security, science and technology, and related policy issues.

General Gray has served as Board Chairman and CEO for several public and private companies and has consulted to United States and international industry and government. General Gray's other duties have included service on the Defense Science Board; the Defense Special Operations Advisory Group; the National Security Agency Science Advisory Board; the National Reconnaissance Office Gold Team; the Defense Operations Support Office Advisory Team; and as Director of the Advanced Concept Demonstration Technology for Combat in the Littorals. Consistent with his interest in education and helping servicemen and women, he is trustee Emeritus of Norwich University, past trustee on Monmouth University, past member of the National Defense University Board of Visitors and is Chairman Emeritus of American Military University. He is Chairman Emeritus of The Injured Marine Semper Fi Fund and the America Fund, having served over ten years, to help take care of wounded veterans and their families.

General Gray currently serves as Chancellor of The Marine Military Academy, Chairman of the US Marine Youth Foundation, and as a Trustee of the American Public University System.

In 1991, Al Gray retired after 41 years of service to the United States Marine Corps. From 1987-1991, General Gray served as a member of the Joint Chiefs of Staff, was the 29th Commandant of the Marine Corps, and was advisor to both Presidents Reagan and George H. W. Bush. As Commandant, he instituted and published a Warfighting Philosophy for Marines based on the Maneuver Warfare Thought Process. General Gray developed and implemented a new long-range strategic planning process for the Marine Corps, established the Marine Corps University, and implemented other longstanding changes, such as ensuring that every Marine is a rifleman first and that the Marine Corps was Special Operations Capable.

General Gray enlisted in the Marine Corps in 1950 and achieved the rank of Sergeant while serving in amphibious reconnaissance with Fleet Marine Force, Pacific aboard the submarine USS Perch (ASSP-313). He was commissioned a Second Lieutenant in 1952. In the early years, he held extensive assignments overseas in the Far East and Southeast Asia in infantry, artillery, intelligence, communications and special operations. He has held every infantry command assignment from platoon commander through Division Commander and has commanded every Marine Air Ground Task Force from Marine Corps Expeditionary Unit to Marine Expedition Force. Among his awards are two Defense Distinguished Service Medals, two Navy Distinguished Service Medals, Distinguished Service Medals from the US Army, the US Air Force and the US Coast Guard, the Silver Star Medal, two Legion of Merits with Combat "V", four Bronze Star Medals with Combat "V", thee Purple Hearts, three Joint Commendation Medals, the Meritorious Service Medal, the Navy Commendation Medal, the Vietnamese Cross of Gallantry with Palm and Star, as well as foreign awards from Argentina, Brazil, Chile, Columbia, Korea and The Netherlands.
General Gray holds a B.S. from the University of the State of New York. He also attended Lafayette

College, the Marine Corps Command and Staff College and the Army War College. General Gray is the recipient of two honorary Doctor of Law degrees, one from Lafayette College and the other from Monmouth University, and was awarded a Doctor of Military Science from Norwich University. He was the first awardee of an Honorary Doctorate of Strategic Intelligence degree from the Defense Intelligence College (now the Joint Military Intelligence College), and also was awarded an Honorary Doctorate for Leadership from the Franklin University, and an Honorary Doctorate from the American Public University System.

Terry Halvorsen

Former DoD Chief Information Officer and Chief Information Officer at Samsung Worldwide

Mr. Terry Halvorsen started with Samsung electronics on April first of this year as an Advisor to the CEO and Executive Vice President in the Business to Business group. He has since been appointed as the Chief Information Officer and Executive Vice President IT and Mobile Business to Business group Samsung Electronics.

Prior to Joining Samsung Electronics, Mr. Halvorsen Served as the Department of Defense Chief Information Officer from March 8, 2015 to February 28 2017. He previously served as the Acting Department of Defense Chief Information Officer from June of 2014 until March of 2015. He was the Department of the Navy Chief Information Officer from November 2010 until May of 2014.

As DoD CIO, Mr. Halvorsen was the principal advisor to the Secretary of Defense for information Management / Information Technology and Information Assurance as well as non-intelligence space systems; critical satellite communications, navigation, and timing programs; spectrum; and telecommunications. He provided strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology-based capabilities required to support the broad set of Department missions. As the Department of Navy CIO, Mr. Halvorsen was the principal Information Technology, Information Assurance and privacy policy advisor to the Secretary of the Navy.

Before serving as the Department of the Navy CIO, Mr. Halvorsen was the Deputy Commander, Navy Cyber Forces. He began serving in that position in January 2010 as part of the Navy Cyber reorganization. Previous to that, Mr. Halvorsen served as the Deputy Commander, Naval Network Warfare Command. He was responsible for providing leadership for over 16,000 military and civilian personnel and supporting over 300 ships and approximately 800,000 globally dispersed computer network users. In this position he was responsible for the business performance of Navy network operations, space operations, information operations and knowledge management.

Mr. Halvorsen served as an Army intelligence officer active and reserve in a variety of assignments, including Operations Just Cause and Desert Storm. He holds a bachelor's degree in history from Widener University and a master's degree in educational technology from the University of West Florida. He is a Rotary International Paul Harris Fellow and an Excellence in Government Leadership Fellow.

Melissa Hathaway

President, Hathaway Global Strategies, LLC, Member, Potomac Institute Board of Regents, Former cybersecurity advisor to President George W. Bush and President Barack H. Obama, Former Senior Director (Acting) for Cyberspace on the National Security Counsel

Melissa Hathaway is a leading expert in cyberspace policy and cybersecurity. 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. She is President of Hathaway Global Strategies LLC and she is also a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs, a Senior Fellow and member of the Board of Regents at Potomac Institute for Policy Studies, a Distinguished Fellow at the Centre for International Governance Innovation in Canada, and a non-resident Research Fellow at the Kosciuszko Institute in Poland. 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, Melissa brings a unique combination of policy and technical expertise, as well as board room experience to help others 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. She publishes regularly on cybersecurity matters affecting companies and countries. Most of her articles can be found at the following website: http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html

Charlie Miller

Senior Vice President, The Santa Fe Group

Charlie's key responsibilities include expanding the Shared Assessments Third Party Risk Management membership driven program and facilitates thought leadership, research studies, regulatory, partner and association relationships. Charlie has vast industry experience, having led vendor risk management and financial services initiatives for several global companies. Charlie was previously the Director of Vendor and Business Partner Risk Management at AIG, and implemented third party risk management programs at Bank of Tokyo Mitsubishi (BTMU). He held multiple leadership roles at Merrill Lynch & Co., Inc. where he oversaw the company's global vendor management program, designed and implemented major global initiatives including: financial systems standardization; privacy; acquisition/divestiture due diligence; information leakage and data protection. He was a consulting partner at Deloitte and lead a financial services practice unit focused on technology outsourcing, risk management and cost control. He is a frequent speaker on third party risk and began his journey at IBM as a systems engineer.

Charlie is a distinguished Fellow of the Ponemon Institute, Certified International Privacy Professional and Certified Third Party Risk Professional.

Tushar Misra, Ph.D.

Vice President and Global Head, Oncology and Biologics Operations, Takeda Pharmaceuticals International, Co.

Tushar Misra has over 30 years of industrial experience and has worked in the pharmaceutical industry in both R&D and Commercial areas. He is currently leading the Oncology & Biologics manufacturing and supply chain functions for Takeda Pharmaceuticals. This job involves the manufacture of high-value oncology medications and supplying them to over 80 countries. These products require cold chain distribution and are critical in saving patients' lives.

Christopher Nissen

Director, Asymmetric Threat Response, Special Concepts Group, The MITRE Corporation

Christopher Nissen is currently Director of Asymmetric Threat Response at the MITRE Corporation, a not-for-profit which operates and manages seven Federally-Funded R&D Centers (FFRDCs) serving in the National Interest. He has 30 years of experience in developing solutions for extremely complex national security challenges. In his current role, he works across the corporation developing essential strategic elements to address non-kinetic, full-spectrum asymmetric threats to national security both in the public and private sectors. Two of the primary attack vectors utilized by these threats are supply chains and ICS cyber-physical. Chris has developed extensive work programs in these and other domains across the technology, policy, and legislative solution spaces. Chris has also served as Director of the Communications and Networking Technical Center, leading a division of over 230 engineers in a diverse portfolio of programs and technology development spanning microelectronics to satellite communications. Some of his accomplishments include putting forth an original vision for the development of an anti-jam capability for the nation's Global Positioning Satellite system, and the development and implementation of several special communications techniques. He holds BSEE and MSEE degrees and has also has a background in structured analytical techniques.

Most recently, Chris led a senior study team that produced the report "Deliver Uncompromised, A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War" which is available at: https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security/

Joye E. Purser, Ph.D.

Deputy Director/Joint Data Support, Analysis and Innovation Division, Office of the Secretary of Defense, Cost Assessment and Program Evaluation

Dr. Joye Purser serves as Deputy Director for Joint Data Support, within the Analysis and Innovation Directorate at Cost Assessment and Program Evaluation (CAPE), within the Office of the Secretary of Defense. In this role, she leads in the development of quality analytical products for the Joint Staff. She previously was on-detail as the Defense Science and Technology Examiner within the National Security Division at the Office of Management and Budget in the White House. There, she managed all technology-related budget proposals from the Department of Defense; and she advised both OMB as well as the National Security Council on how new and developing legislation, policies, world events, or industry activities affect the technological superiority of the American warfighter.

Prior to her White House detail, Dr. Purser served within CAPE as a senior program analyst and adviser to the Secretary of Defense: leading and directing evaluations of science, space, health IT, and C4 programs, as well as chemical/ biological defense, counter-terrorism, and homeland defense programs. She came to the Pentagon in 2011 as the special assistant to the Director of CAPE. Before that, she worked for multiple Members of Congress as a seven-year Capitol Hill staffer for health, science, and energy policy. Additionally, she has worked for a nonprofit advocacy organization, Research America, that teaches scientists and engineers how to effectively advocate and message to Congress and other decision makers. She founded and owns a consultancy as a scientific writer.

Dr. Purser earned a PhD in molecular microbiology from the University of Texas and a BS degree from Georgia Tech. Her life's mission is to do good for scientists. She lives in the Washington, DC, area with her husband and two children.

Ari Schwartz

Managing Director of Cybersecurity Services, Venable LLP

A leading voice in national cybersecurity policy with over two decades of government and nonprofit sector experience, Ari Schwartz is the Managing Director of Cybersecurity Services for Venable's Cybersecurity Risk Management Group. In his role, Mr. Schwartz directs the establishment of cybersecurity consulting services for Venable, assisting organizations with understanding and development of risk management strategies, including implementation of the Cybersecurity Framework and other planning tools to help minimize risk. Mr. Schwartz also coordinates the Coalition for Cybersecurity Policy and Law, a group of leading cybersecurity companies dedicated to educating policymakers on cybersecurity issues and promoting a vibrant marketplace for cybersecurity technology solutions.

Prior to joining Venable, Mr. Schwartz was a member of the White House National Security Council, where he served as Special Assistant to the President and Senior Director for Cybersecurity. As Director, Mr. Schwartz coordinated all network defense cybersecurity policy, including critical infrastructure protection, federal network protection, supply-chain efforts, cybersecurity standards promotion, and information sharing. He led the White House's legislative and policy outreach to businesses, trade

groups, academics, and civil liberties groups on cybersecurity and developed new policies and legislation, including development of the Executive Orders on the Security of Consumer Financial Protection, Cybersecurity Information Sharing, and Sanctions Against Individuals Engaging in Malicious Cyber-Enabled Activities. Additionally, Mr. Schwartz led the successful White House rollout of the Cybersecurity Framework and the White House Cybersecurity Summit held at Stanford University.

Mr. Schwartz also served in the Department of Commerce, where he advised the Secretary on technology policy matters related to the National Institute of Standards and Technology (NIST), the National Telecommunications and Information Administration (NTIA), and the U.S. Patent and Trademark Office (USPTO). He led the Department's Internet Policy Task Force and represented the Obama Administrations on major Internet policy issues on privacy and security before Congress, at public events, and before the media.

Mr. Schwartz began his career in Washington at OMB Watch. For twelve years, he worked at the Center for Democracy and Technology, including serving as Vice President and Chief Operating Officer, developing legislation and policy related to privacy, cybersecurity, and open government.

Michael S. Swetnam

Chairman of the Board and CEO, Potomac Institute for Policy Studies

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 Pro-

cessing 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.

D.E. (Ed) Wilson, Jr.

Attorney, Venable LLP

Mr. Wilson's practice focuses on assisting private and governmental parties negotiate the laws and policies regulating payments, money, business, investment and political activity. His primary emphasis is on solving Washington-related business and regulatory matters.

Issues include cross-border business and financial transactions; government contracts; payments; anti-money laundering (AML/CFT) rules for traditional and non-traditional financial institutions; anti-corruption standards applicable in home, host and residence countries; nomination and confirmation issues in the U.S.; political activities – by U.S. and non-U.S. persons – in the U.S.; and policy and regulatory matters related to the U.S. Treasury, State and Commerce (BIS/EAR) Departments, multilateral development banks, and international organizations.

Mr. Wilson represents public officials, private individuals, and private and public entities (including embassies and sovereigns) in situations requiring the resolution of an immediate legal issue, and a longer-term, strategic solution.

These representations involve anti-corruption issues (FCPA and its international counterparts), the Bank Secrecy Act (FinCEN), the Foreign Agents Registration Act (FARA), the International Trafficking in Arms Regulations (DDTC/ITAR), the Committee on Foreign Investment in the United States (CFIUS); economic sanctions matters (OFAC); the Ethics in Government Act; and product safety issues.

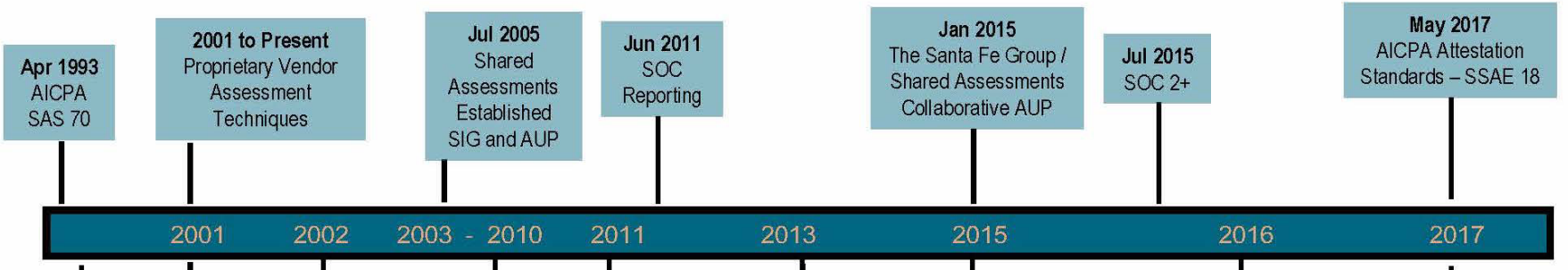
In addition to these regulatory matters, Mr. Wilson is active in domestic and international payments (card processing, prepaid cards, card issuing, financial institutions, remittances, EFT, ACH, SWIFT), and business transactions as well as homeland security, fiscal issues and government contracts.

Appendix 2: Sante Fe Group Slides Presented by Charlie Miller

Environmental Analysis – Third Party Risk Impact

- **Shared Assessments environmental analysis- focuses on these areas:**
  - Economic, Technology, Regulatory, Legal, Demographic and Risk Assessments
- **Risk Assessments – Third (N^{th}) Party**
  - Complexity – supply chain - EcoSystem
  - Point in time → continuous monitoring
  - Collaboration - assessment repositories
  - Economic pressures – need for efficiency and cost savings
- **Technology - Risk and Threat Landscape**
  - Exponential demand for innovation
    - Fintech, Artificial Intelligence, Machine Learning, Internet of Everything
  - Increased move to the Cloud
  - Advanced cyber attack techniques
- **Regulatory - Data Protection / Resiliency**
  - Accountability of board of directors and individual board members
  - Regulatory focus on cyber/third party risk (local, national and international)
  - Global privacy regulations (EU, China)
  - Oversight of critical infrastructure

Evolving Regulatory Landscape of TPRM



Aug 1996
Health Insurance Portability and Accountability Act (HIPAA)

Jul 2001
Graham-Leach Bliley Act (GLBA)

Nov 2001
OCC 2001-47 Third Party Relationships

May 2002
OCC 2002-16 Foreign Third Party Service Providers

2003 – 2010
Privacy Breach Notification Laws – Various States

Jun 2008
FDIC FIL 44-2008 Guidance for Managing Third Party Risk

Jan 2011
PCI-DSS V2.0 Payment Card Industry – Data Security Standards

Jan 2012
FDIC FIL 3-2012 Payment Processor Relationships Revised Guidelines

Oct 2013
OCC 2013-29 Third Party Relationships: Risk Management Guidance

Dec 2013
FRB SR 13-19 Guidance on Managing Outsourcing Risk

Feb 2015
SEC OCIE and FINRA Report on Cyber Security

Feb 2015
FFIEC Information Technology Examination Handbook: New Appendix for Business Continuity Planning Booklet

May 2015
PCI-DSS V3.0 Payment Card Industry – Data Security Standards

Jun 2015
FFIEC – Cybersecurity Assessment Tool

Nov 2015
FFIEC Information Tech Handbook: Revised Management Booklet

May 2016
Global Data Protection Regulation (GDPR) Compliance May 2018

Jun 2016
OCC 2016-18 Cybersecurity of Interbank Messaging and Wholesale Payment Networks: FFIEC Statement

Jun 2016
FDIC FIL 43-2016 - Info Tech Risk Examination (InTREx) Program

Sep 2016
FFIEC – Press Release Revised Info Sec Booklet

Feb 2017
OCC 2017-07 Third Party Relationships: Supplemental Examination Procedures

Mar 2017
NYS DFS – 23 NYCRR 500 Cybersecurity Requirements for Financial Services Companies

Jun 2017
OCC 2017-21 Frequently Asked Questions to Supplement OCC-2013-29

The Office of the Comptroller of the Currency (OCC) defines a third party relationship as any business arrangement between a bank and another entity, by contract or otherwise; and it expects a bank to practice effective risk management, regardless of whether the bank performs the activity internally or through a third party.

ISO - Risk Control Areas and More…

- Risk Assessment and Treatment
- Security Policy
- Organizational Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems, Acquisition, Development and Maintenance
- Incident Event and Communications Management
- Business Resilience
- Compliance
- Mobile
- Privacy
- Software Application Security
- Cloud Security

Third Party Risk Management Process

Establish Third Party/Contract Risk	Ensure Use and Completion of Templates and Control Assessments	Standard Contract Language	Formalize Oversight and Monitoring	Exit Strategy and Asset Return
Third Party/Contract • New/existing • RFx/sole source/renewals • Relationship owner is key **Risk Criteria** • Simple, clear and consistent • Applied at contract level • Due diligence requirements **Control Assessments** • Areas to include: security, information, personnel, site, business continuity, regulatory requirements, etc. • Leverage industry standards • Capture appropriate documentation **Remediation/Issue Closure**	**Clauses (Legal Approved)** • Right to audit • Information security • Physical security • Background checks • Business resiliency/disaster recovery • Fourth parties • Encryption requirements as appropriate • Termination and exit **Authorized Negotiators/Signers** • Goods and services • Specialized services (real estate, benefits, legal, etc.) **Exceptions and Approval**	**Leverage** • Assigned risk ranking • Assessments and prior reviews **Ongoing Monitoring** • Periodic validation of risk ranking • Frequency based on risk and service provided • Agree on scope and type of review to be performed • Perform onsite reviews • Point in time assessment move toward continuous monitoring **Ensure Issue Remediation/Closure** **Third Party Performance** • Scorecard program • Reporting **Software and License Compliance**	**Termination** • Normal • Cause • Convenience • Breach **Asset Return** • Return and/or confirmation of destruction of confidential data **Exit Strategies** • Developed internally, not with third party • Outlines approach to be followed if critical third party prematurely terminates • Outlines various options to ensure continued service availability

SFG SHARED ASSESSMENTS

Program Tools

- **Member-Developed**
- **Mapped to Regulations, Guidelines/Industry Standards as they Evolve**
- **Members Incorporate Program Tools into their TPRM programs**
- **Continuous Monitoring and Other Emerging Practices Guidance**
- **Including Assessments for Cybersecurity, IT, Privacy, Data Security and Business Resiliency Controls:**
  - **SIG**: Standardized Information Gathering questionnaire – procurement and risk management assessments
  - **AUP**: Agreed Upon Procedures – performing standardized onsite risk management assessments
  - **VRMMM**: Vendor Risk Management Maturity Model – evaluating maturity of third party risk programs

SFG SHARED ASSESSMENTS

Regulatory and Industry Mappings - In Scope

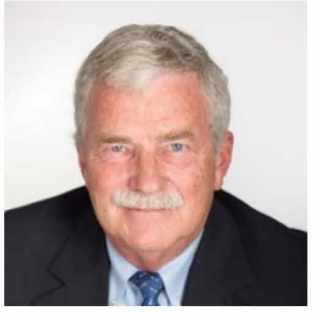
- **Industry Standards, Regulations and Guidance:**
  - OCC Bulletin 2013-29 Guidance on Third Party Relationships, 2013
  - US Cyber Consequences Unit (CCU) Cybersecurity Matrix Tool, 2009
  - HIPAA Final Rule Modifications, 2013
  - NIST Cybersecurity Framework (CSF), 2014
  - Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) V.3.0.1, 2014
  - ISO Standards 27001 & 27002, 2013
  - Payment Card Industry (PCI) PCI DSS v.3.2, 2016
  - FFIEC Cybersecurity Assessment Tool (CAT), 2015
  - FFIEC IT, IS & Outsourcing Examination Management Handbooks, 2015
  - FFIEC Information Technology Examination Handbook – Appendix J, 2015
  - Global Data Protection Regulation (GDPR) Compliance, May 2018
  - NY State Cybersecurity Regulation (23 NYCRR 500), 2017
  - NIST Special Publication 800-53, Revision 4, Security and Privacy Controls, 2015
  - NIST Special Publication 800-184, Guidance for Cybersecurity Event Recovery, 2016
  - Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) V3.1

Research and Publications

Published – Available on *www.sharedassessments.org:*

- *"Vendor Risk Rating for Third Party Management"*
- "*2016 Tone at the Top and Third Party Risk"* Ponemon Research
- "*2016 Vendor Risk Management Benchmark Study"* Protiviti Research
- *"2017 The Internet of Things (IoT): A New Era of Third-Party Risk*" Ponemon Research
- "*Evaluating Cloud Risk for the Enterprise*"
- "*Public Cloud Provider Assessment Best Practices*"
- "*Continuous Monitoring of Third Party Vendors: Building Best* Practices"
- "*Fourth Party Risk Management Issues and Best* Practices"
- "*Building Best Practices in Third Party Risk Management: Involving Procurement*"
- *"A Guided Assessment - Providing Advancements in Building Best Practices for Vendor Onsite Assessments"*
- *"2017 Vendor Risk Management Benchmark Study"* Protiviti Research
- "*2018 The Internet of Things (IoT): A New Era of Third-Party Risk*" Ponemon Research

Presenter



Charlie Miller, CIPP, CTPRP, Senior Vice President, The Santa Fe Group, Shared Assessments Program – Evangelist

- Charlie's key responsibilities include expanding the Shared Assessments Program and facilitating regulatory, partner and association relationships. Charlie has vast industry experience, having led vendor risk management and financial services initiatives for several global companies. Charlie was previously the Director of Vendor and Business Partner Risk Management at AIG, and implemented third party risk management programs at Bank of Tokyo Mitsubishi (BTMU) and Merrill Lynch & Co., Inc.

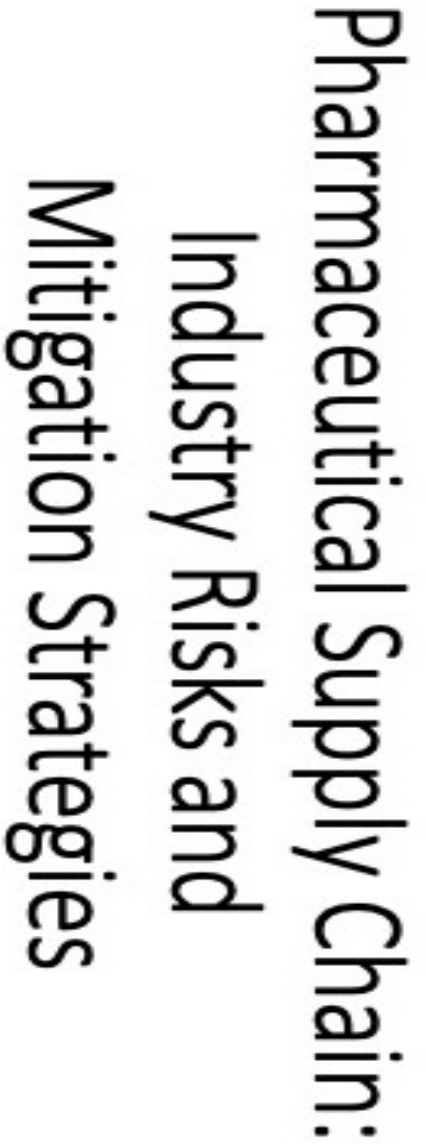
SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

www.sharedassessments.org

1-917-279-2229 charlie@santa-fe-group.com

follow us on

Appendix 3: Takeda Pharmaceuticals International, Co. Slides Presented by Tushar Misra



Contents

Common Risk Factors

External Challenges

- Weak regulatory oversight and enforcement, low penalties, illicit trade via the internet across borders
- Access to affordable, quality, safe and effective medical products is constrained
- Standards of governance are low, ranging from poor ethical practices through to corruption in both the public and private sectors
- The tools and technical capacity to ensure good practices in manufacturing, quality control and distribution are limited.

Internal Challenges

- Complexity of supply chains
- Lack of policies, procedures, and technologies used to provide visibility and traceability of products within the supply chain
- Mergers and consolidations expand global footprint resulting in increased exposure
- Expansion into emerging markets

3

2 World Health Organization (2017) WHO Global Surveillance and Monitoring System for Substandard and Falsified Medical Products: Executive Summary, p. 4

Common Definitions

Counterfeit

Medicine which was deliberately and fraudulently produced and/or mislabelled with respect to identity and/or source to make it appear to be a genuine product. The definition applies to both branded and generic products.

Diversion

Legitimate pharmaceutical product is approved and intended for sale in one market, but is then illegally intercepted and sold in another market. Many times, drug regulators in the second market have not formally approved the use of the diverted drugs. In some cases, the drug may be legal, but is smuggled into the second market through false declarations as to its nature and identity

Theft

The criminal stealing of products, often during a burglary or robbery.

Key Global Industry Trends

Counterfeit

- The Pharmaceutical Security Institute in 2016 recorded 3,509 pharmaceutical crimes, including counterfeiting, diversion and major theft, impacting 134 countries. This accounted for a 60% increase in new incidents in the past five years. [1]
- Asia continues to lead the world in counterfeit production and export of counterfeit medicines.
- The effects of counterfeit medicines range from untreated conditions, increased disease resistance, adverse side effects and the support of criminal and terrorist organizations to the death of patients.
- Widespread sale of counterfeits, substandard and expired medicines continues to threaten patients in Africa with 42% of reports of substandard or falsified medicines to the WHO between 2013 and 2017 came from the region. [2]

Diversion

- Illegal diversion of medicines has steadily increased globally, creating patient safety risks
- These products traded outside of the legitimate supply chain may be improperly stored and transported, impacting the efficacy of the products and their sterility.
- Stolen or expired products may be sold through diversion.
- Diversion is prevalent in the Middle East with products from Turkey being particularly susceptible.
- Illicit online selling of pharmaceuticals through illegal online pharmacies, business-to-business trading forums, business-to-consumer sites and consumer-to-consumer platforms, as well as via social media and the dark web have increased the volume of diverted products and counterfeits, impacting both developed and developing countries.
- The United States is the largest market for illegal online pharmacies, followed by Japan.

Theft

- Pharmaceutical Security Institute recorded 128 incidents of major theft (over $100,000) in 20 countries in 2017.
- Over half of these incidents occurred in Brazil which has a severe risk of cargo theft and where pharmaceuticals are specifically targeted.
- In a recent case in the EU, organized, large-scale theft of at least 25 different cancer medicines occurred from hospitals and clinics in Greece and Italy between 2013 and 2017

[1] *Pharmaceutical Security Institute*
[2] World Health Organization (2017) *WHO Global Surveillance and Monitoring System for Substandard and Falsified Medical Products*, p. 11

Focus on Counterfeits

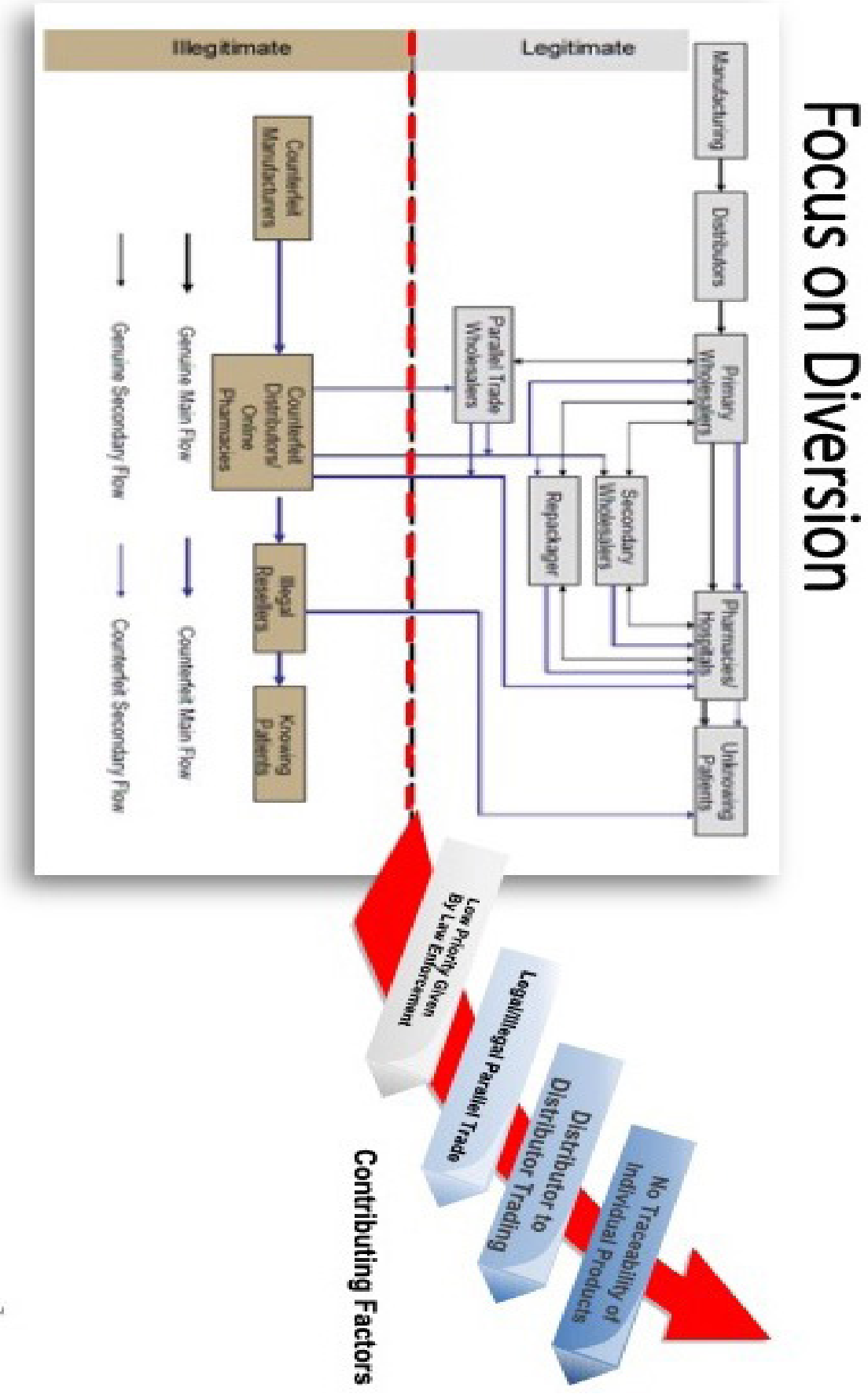
- All therapeutic areas have been effected by counterfeiting.
- While lifestyle products such as erectile dysfunction drugs have been traditionally targeted, life-saving medicines have been increasingly victimized.
- PSI reports that the three most counterfeited therapeutic categories continue to be Genito-urinary, Anti-infective and Central Nervous System.
- Injectable medicines accounted for 17% of counterfeit incidents recorded by PSI in 2017.
- Cardiovascular medicines experienced the highest increase of counterfeiting with 106% more reported incidents in 2017 than in 2016.
- Incidents of counterfeit cytostatic (oncology) medicines increased by 25% in 2017.

Type of product	Number of Member States reporting	Total no. of product reports	Percentage of all products reported to database [a]
Anaesthetics and painkillers	29	126	8.5
Antibiotics	46	244	16.9
Cancer medicines	19	100	6.8
Contraception and fertility treatments	19	29	2.0
Diabetes medicines	7	11	0.8
Heart medicines	22	75	5.1
HIV/hepatitis medicines	9	43	2.9
Lifestyle products [b]	37	124	8.5
Malaria medicines	26	286	19.6
Mental health medicines	19	45	3.1
Vaccines	11	29	2.0

[a] Since only selected products are reported in this table, the percentages in this column do not add up to 100%. A table showing the breakdown of all reports using the anatomical therapeutic chemical classification is provided in the Annex to the main report.

[b] So-called lifestyle products include products for cosmetic use, erectile dysfunction, body-building and dieting.

[1] World Health Organization (2017) WHO Global Surveillance and Monitoring System for Substandard and Falsified Medical Products Executive Summary, p. 3


Focus on Diversion
Illegitimate
Legitimate
Manufacturing
Distributors
Primary Wholesalers
Parallel Trade Wholesalers
Secondary Wholesalers
Repackager
Pharmacies/ Hospitals
Unknowing Patients
Counterfeit Manufacturers
Counterfeit Distributors/ Online Pharmacies
Illegal Resellers
Knowing Patients
Genuine Main Flow
Genuine Secondary Flow
Counterfeit Main Flow
Counterfeit Secondary Flow
Low Priority By Law Enforcement Given
Legal/Illegal Parallel Trade
Distributor to Distributor Trading
No Traceability of Individual Products
Contributing Factors

Maintaining Supply Chain Integrity
Gap Analysis to Detect Risk of Vulnerabilities
*What is value to be gained by illicit traders?
*How would they penetrate the supply chain?
*What are the weak points in the supply chain?
*What measures should be in place?
Careful Selection of Supply Chain Partners
*Due diligence
*History of thefts, losses?
*Effective mitigation strategies?
*Security evaluation
*Ties to organized crime
*Criminal issues with principal parties
Simplification of Supply Chains to Reduce Risk
*Reduce exposure to additional parties
*Reduce the number of touches
*Reduce information outside your control
*Increase oversight resources per segment
Contract Language for Partners
*Physical Security standards
*Background investigations for personnel
*Temporary labor policies
*Audit/investigation rights
*Information Security Standards
*Business Continuity/Disaster Recovery
Auditing to Ensure Partner Compliance
*Quality Audits
*GDP Audits
*Supply Chain Security Audits
*Minimum loss threshold for Security notification
Effective Brand Protection Technologies
*Overt for consumer identification
*Covert for detection of counterfeit attempts and strain analysis
*Flexible to respond to dynamic needs
*Regulatory & serialization requirements vary
*Staying ahead of counterfeiters

Mitigation Strategies for End to End Supply Chain Security

Segment	Mitigation
Up Stream	•Supplier risk assessments •Transportation and logistics assessments •Supplier selection and auditing •Supplier security assessments •Material qualification •Quality agreements •Material inspection and testing •SQM standards •Supplier management database •Commercial supply agreements •Supplier EHS reviews
MANUFACTURING	•Security standards •Supply Chain Security Audits •Anti-counterfeiting packaging solutions •Serialization •GDP •Incident reporting •Packaging technology assessments •Technology management •Packaging strategy development •Waste management guidelines •Conveyance standards •Global transportation service agreements •Equipment/Asset disposition (tooling, printing presses, etc)

Segment	Mitigation
Transportation	•GDP Standards •Threat awareness and training •CTPAT/AEO/PIP compliance •Limits on value of product shipped •Transportation Security standards •Supply Chain Security assessments •Incident management •Transportation conditions •Risk and vulnerability analyses •Carrier assessment and Shipment tracking systems •Selection •Conveyance standards •Certified cargo screening program •Third party LSP assessment and selection process
Warehousing	•CTPAT/AEO/PIP compliance •Conveyance product care requirements •Security standards •Security assessments •Security management •Incident reporting •Risk and vulnerability analysis •Warehousing audits •Third party LSP assessment •Product destruction/waste management •LSP oversight •Sort and segregate policy •Return goods policy •Order processing and inventory control

Segment	Mitigation
Customer/ Trading Partner	•Distributor assessment and selection •Due diligence of warehouse distributors •Terms of sale/trade policies •Supply and pricing •Wholesale model rules •Direct to Pharmacy •Samples management •Free goods (e.g., humanitarian goods) •Reverse logistics
Marketplace	•Complaint handling •Theft response program •Authentication of suspect counterfeits •Forensic testing •Law enforcement/customs collaboration •Illicit trade investigation and response •Internet monitoring •Threat awareness and risk assessment •Market Surveillance •Sales force education •Sales monitoring •Parallel trade monitoring of licenses
Patient	•Internet awareness/education •Counterfeit education/awareness •Public affairs advocacy •Patient authentication programs

Collaboration is Key

Rx 360

To assure the quality and authenticity of the products moving through the supply chain by sharing information and developing processes.

ASOP (Alliance for Safe Online Pharmacies)

To ensure patient access to safe and legitimate online pharmacies in accordance with applicable laws.

PSI (Pharmaceutical Security Institute)

To facilitate the sharing of information on the counterfeiting of pharmaceuticals among its members and initiates enforcement actions through the appropriate authorities.

IFPMA (International Federation of Pharmaceutical Manufacturers & Associations)

To raise awareness about the dangers of fake medicines through the Fight the Fakes campaign.

IACC (International Anti-Counterfeiting Coalition)

To hinder the spread of counterfeits through partnerships, such as with payment processors and online marketplaces, and by the promotion of stronger regulations and legislation.

Conclusions

- Key drivers are lack of enforcement, weak penalties, corruption, profitability, low risk, and ease
- The problem continues to grow
- The Internet is a huge driver and vehicle of sales and distribution
- All products in all therapeutic areas have been counterfeited
- There is need to take a holistic, risk based approach
- It is a shared responsibility, working with internal functions and external agencies, organizations, and supply chain partners

11

About the Sponsors

The Potomac Institute for Policy Studies

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 and technology issues facing our society. From these discussions and forums, we develop meaningful science and technology policy options and ensure their implementation at the intersection of business and government.

The Potomac Institute's Vital Infrastructure, Technology, and Logistics (VITAL) Center is dedicated to fostering and supporting comprehensive supply chain security as an integral part of all major US industries. Secure and resilient critical infrastructures will help the US maintain a strong national defense. As part of this mission, the VITAL Center works to:

- Assess the evolving strengths and weaknesses of our nation's critical infrastructure systems and technologies, and the supply chains they depend on.
- Advance knowledge of critical infrastructure and supply chain security challenges and solutions across the US Government and industry to include policy makers, the Department of Defense, and the manufacturing industrial base.
- Bridge the gap between commercial and defense supply chain security practices.
- Strengthen policy to ensure continued security of our nation's critical infrastructure and supply chains.

The Vital Infrastructure Technology and Logistics Center

The Vital Infrastructure, Technology, and Logistics (VITAL) Center is dedicated to fostering and supporting comprehensive supply chain security as an integral part of all major US industries. Secure and resilient critical infrastructures will help the US maintain a strong national defense. As part of this mission, the VITAL Center works to:

- Assess the evolving strengths and weaknesses of our nation's critical infrastructure systems and technologies, and the supply chains they depend on.
- Advance knowledge of critical infrastructure and supply chain security challenges and solutions across the US Government and industry to include policy makers, the Department of Defense, and the manufacturing industrial base.
- Bridge the gap between commercial and defense supply chain security practices.
- Strengthen policy to ensure continued security of our nation's critical infrastructure and supply chains.

US critical infrastructures encompass highly visible sectors like transportation, water, and agriculture as well as less conspicuous sectors like energy, finance, and information technology (IT). If any of these infrastructures were attacked, whether by hostile nation-states or by non-state actors, it would have major negative impacts on our national security and the economic well-being of our country. Even less nefarious disruptions to the supply chain, caused by inclement weather for example, are increasingly worrisome as the global economy becomes more intertwined and interdependent.

Due to the number, scale, and complexity of these sectors, no one entity can tackle the issue of critical infrastructure vulnerability alone. Both government and industry have a shared interest in the continued stability of domestic infrastructures and their global supply chains and are thus natural allies in the efforts to secure these systems. Through improved communication and strategic planning, industry and government entities can combine and coordinate efforts in comprehensively securing critical infrastructures.

The DCIP defines the following 16 sectors as critical based on their influence on the nation's economic health and security: chemicals, commercial facilities, communications, manufacturing, dams, defense, emergency services, energy, finance, food and agriculture, government facilities, healthcare, information technology (IT), nuclear facilities, transportation, and water. The number of sectors considered vital to the US is simply too great to be managed by one office of the federal government, or even by the federal government alone. Taken together, the 16 critical sectors identified by the DoD account for thousands of companies, millions of jobs, and billions of dollars of revenue changing hands across the country. The only effective way to provide comprehensive critical infrastructure protection is through a coordinated effort, both among government agencies and between government and industry. The VITAL Center aims to bridge the gap between government and industry security efforts by connecting diverse stakeholders from both worlds, creating a community of interest to create more comprehensive mechanisms of action for critical infrastructure protection.

Venable LLP

Venable is an American Lawyer 100 law firm. With nearly 700 attorneys across the country, Venable is strategically positioned to advances its clients' business objectives in the U.S. and abroad. Venable's clients rely on its proven capabilities in all areas of corporate and business law, complex litigation, intellectual property, and regulatory and government affairs.

Venable's communications experience and relationships deliver solutions to communications challenges and goals. The laws, regulations, investigations, and procedures relating to communications, privacy, data breach, and cybersecurity pose a bewildering challenge to the successful execution of communications strategy and business development. Venable retains an experienced, action-oriented team that loves to devise strategies for navigating laws, regulations, and procedures to achieve communications goals in a timely way, executing those strategies in an accountable way. Venable's legal team is comprised of a combination of attorneys who have served in the federal executive branch agencies, as members of Congress, and on congressional staffs. Many if not all have long-term experience shaping policy and rule-making, practicing before federal and state agencies. Venable team members marshal the facts, understand the agency processes, and use their knowledge of the process and relationships with decision-makers to accomplish goals.

Venable has over a century of experience staying on the cutting edge of technology, the lifeblood of the communications industry. Venable is experienced in and understands the technologies that routinely disrupt and revolutionize communications. It understands the communications axiom, New technology defies conventional legal models. Venable's mission has been to find innovative ways for service providers, entrepreneurs, inventors, and communications users to bring new technology on line, a challenge that demands attorneys who have the capacity to synthesize and understand the entire communications playing field.

Venable focuses on legal scholarship, regulatory insight, and advocacy. Venable has inaugurated major rule-makings, leading multifaceted campaigns at the FCC, before other agencies, and on Capitol Hill to have rules and policies adopted or to fend off unwanted regulations.

Venable's work combines advice on broad policy questions and specific solutions to everyday industry problems. It offers both front-edge knowledge of the thinking of legislators and regulators and first-hand experience solving the issues that confront the executives of electronic commerce, financial services and communications companies. Venable's policy work enhances its operational advice, and vice versa.

Venable combines legal theory and practical know-how in an integrated approach to complex privacy and security issues. Venable has had a measurable impact on privacy and information security laws and regimes. You can learn more about Venable's Communications and eCommerce, Privacy, and Cybersecurity areas of practice here.

https://www.venable.com/communications/