Mission is Possible

Episode 9: Adapting to Changing Supply Chain Risk Management Threats

SASHA: Welcome back to Mission is Possible, a joint project between the National Security Sector at Guidehouse and the School of Public Affairs at American University. I am Sasha O'Connell and I'm excited to introduce this timely episode focused on supply chain risk management.

In this episode, we welcome a guest host, Jason Dury. Jason is a director in Guidehouse's Open Source Solution's team, and he has more than 25 years of experience in the U.S. Intelligence Community and commercial sectors as a multidisciplinary global security professional. Jason is joined by Matt Halvorsen from the National Intelligence and Security Center, and Lisa Barr from CISA.

Thank you for tuning in - I hope you enjoy the discussion.

JASON:

Hello and good morning, good afternoon or good evening to those of you listening, depending on where you are joining us from. My name is Jason Dury and I am excited to be your guest host and moderator for this edition of the Mission is Possible podcast during Supply Chain Integrity Month. I'm thrilled to introduce to everyone today our two knowledgeable and respected guests who have graciously joined us, Lisa Barr and Matt Halvorsen.

Lisa is a program lead for federal cyber security supply chain within the DHS Cybersecurity and Infrastructure Security Agency, or CISA. Lisa has over 18 years experience in the public and private sector, leading projects in cybersecurity, IT strategic planning, and risk management. Within CISA Lisa leads federal cybersecurity supply chain efforts in support of the Federal Acquisition Security Council. Lisa served as a senior advisor to the FASC, from November, 2019 to November, 2020. She spearheaded federal supply chain efforts under the FASC. This included finalizing a FASC strategic plan, charter and the release of FASC's interim final rule in September, 2020, that describes the operation of the FASC. Within CISA'S cybersecurity division, she has led federal cybersecurity governance efforts in support of broader federal cybersecurity risk management.

Matt is a supervisory special agent with the Federal Bureau of Investigation. Matt currently serves as the strategic program manager for the supply chain and cyber director of the National Counter-Intelligence and Security Center. In this role, Matt participates in inter-agency strategic programs initiatives to bolster supply chain security across national security enterprise. Prior to joining NCSC, he served as a field supervisor within the FBI's Washington field office.

He's an expert in human's operations and a certified counter-intelligence investigator. As a field supervisor, he developed a one of a kind national initiative training program, as well as advanced and led the most prolific intelligence operation in the FBI. And with that, I'd like to turn to our discussion today.

I'd like you both to speak to President Biden's February, 2021 executive order, which launches a comprehensive review of the U.S. supply chains and directs federal departments and agencies to identify ways to secure against a wide range of risks and vulnerabilities. With the ultimate goal, of protecting the United States from facing shortages of critical products. I'd appreciate

you both starting within the government's role in building resilient supply chains and some of the other legislative and executive actions that clarify the roles of your agencies. Our listeners would also be interested in details on items such as who is leading the efforts, high-level objectives, information on both the Hundred-Day and year-long studies that are taking place. Who wants to start?

MATT:

Thanks for the question Jason. So the executive or that you're speaking on here, 14017 also kind of goes hand in hand with the executive order from last year on the ICT supply chain which was 13873.

All of these executive orders and additional legislation on supply chain security are not occurring in a vacuum. This is based on a trend of reporting from the Intelligence Community that goes back five or six years, in some of the events that the U.S. government discovered in our supply chain. We'd like to think of it as the seed that grew this tree, started with the intelligence from the Intelligence Community and how it's grown from there.

It's real focus has been on the security of the supply chain, but as we went into the pandemic, a little more than a year ago, we really saw our growth in this concept of resiliency in supply chains and how that can affect security. So that's a big part of these studies that are coming out of this executive order. It's a signature piece for the White House and we're really happy to be a part of it at NCSC. The, the plan and the intent of these studies is really to identify what policy or what legislation can be implemented or changed to strengthen national security and bolster that economic growth. That's really the overarching goals. It'll be interesting to see the final products that come out of these. The intent is to have a single report that speaks with one voice.

I look really forward to seeing them. From the Intelligence Community perspective there's no direct, and I would say that's because the Intelligence Community's tasking is implicit. Our job is to provide intelligence to the policy makers and the legislators.

JASON:

Great. Thank you, Matt. I know for the Hundred-Day reviews and for the year-long studies, that there are different agencies involved in the process; commerce, energy, defense, transportation, health and human services and others they've called out very specific topics to be covered.

Will there potentially also be other areas that are covered as those studies are completed and might uncover different areas within that might need to be a focus?

MATT:

Yes. Good question. I don't think that the study limits broadening the targets. So as you said, the first Hundred-Day studies are very specific. It's semiconductors batteries, critical minerals, strategic materials, APIs, the pharmaceuticals. Those are very specific. The one-year studies are broader and those look at sectors; the defense sector, public health, preparedness sector, the ICT sector and a couple others. There is a possibility out of those longer studies to get more specific, I don't think you'll see any changes in the Hundred-Day studies because they're well on their way and I don't think there would be anywhere near time to change those. It could be at the end of the one year they add a category or they merge categories. That'll really be determined by the White House and National Security Council and the National Economic Council.

Mission is Possible

JASON:

Great. Thank you, Lisa, did you want to add anything to this?

LISA:

I did want to highlight a couple of things. So, obviously the Department of Homeland Security and Commerce have a role to play with regards to the one-year timeframe. They're responsible for looking at the comms and the IT sector. I think one of the things that would be interesting that comes out of the reports even after a year is while they're geared towards working with the private sector and both DHS and Commerce are going to be engaging with the private sector, leveraging some of CISA's partners through the ICT Supply Chain Risk Management Task Force.

It'll be interesting to see the impact that it will have on the continued need to secure the supply chain from the federal side, because I think that while there are implications certainly for the private sector in terms of the suppliers and vendors that obviously has a secondary impact on the federal community in terms of what they're acquiring.

I would foresee that there will be probably even a stronger need from the federal community to be coming to the Federal Acquisition Security Council and leveraging some of the information that is outlined within the Federal Acquisition Supply Chain Security Act because of the connection between the security of what the federal government's buying, and what comes out of the reports and the studies.

JASON:

Matt, Lisa, thank you very much for that. One of the things that you've both highlighted was the implications and engagement with the private sector as part of the process of helping secure federal agencies. There are many companies and collaboration teams and groups that are looking to understand what the implications of these studies may have on them as they move forward to secure their supply chains in support of contracting with the government.

Included in the areas such as; onshoring, reinvigorating the U.S. supply chain and industrial base, and capacity within the United States and also shoring up the security of university and private research institutions, including those that are working on advanced materials and technology development. I am curious if you could both discuss your perspectives on how the executive order may impact private companies and research institutions in the United States?

MATT:

That's a big question. The short answer is we don't know, because part of it is really going to depend on the engagement of the private sector on these studies. You and I have talked about this, and I think Lisa alluded to it, the U.S. Government doesn't make anything. We don't have any factories, we have to buy everything. From pencils, to bullets, aircraft carriers, we purchase it all.

Private industry is going to be engage to provide its opinions or its perspective, whether it's through mechanisms, such as the ICT SCRM Task Force that Lisa mentioned that CISA is running. Or whether it's through the DIB Infrastructure that DOD has, or whether it's through the FBI where we engage private industry to provide threat reporting and things of that.

Which of those private sector outreach mechanisms is used, will depend on the agency conducting the study and I think that is going to inform the studies such that they're not coming

up with ideas or proposed legislation in a way that is going to affect private industry getting that input.

All of that stuff you talked about I think is, for lack of a better term, on the table. And if there is onshoring is that done with public-private partnerships? Whether it be with semiconductors or microelectronics or rare earth minerals, because the difficulties with trying to do that from a financial perspective in the United States versus overseas, whether that's with working with allies and trying to increase supply chains with allied countries that are more in keeping with the Five Eyes or the Tech Ten. I don't think there's a quick answer to how it's going to affect the industry. Industry's going to have the ability to provide input and opine on the decisions. I don't see the White House or Congress making these decisions in a vacuum.

JASON:

Part of the question is more of those changes to how supply chain risk management will be taking part in the future and increasing public-private partnership and information sharing and that has to continue supply chain risk management and protection of the supply chain.

Lisa with that, I'd love for you to address how you envision changes to supply chain risk management in the years to come from the perspectives of DHS, if there's an ideal state that CISA and the DHS might have that we're aiming towards? Especially as your role across of the different agencies within the government.

LISA:

Thanks Jason, one thing I would probably touch on is building off what Matt said that public-private partnership is key to how we address the whole of government, whole of nation problems in this space. That's why we are engaging with the private sector and why DHS and Commerce are going to be leveraging some of the existing public-private partnerships in order to address the requirements and the asks from the study so that the Administration and the federal government is actually hearing directly from the private sector through these taskings and studies.

An ideal state for supply chain is having a secure and resilient supply chain that the American people know they can rely upon that maintains their way of life. Now striving towards the ideal is the admirable course of action we need to follow. We won't reach the ideal state overnight. There is a very practical, pragmatic approach that we need to take, that's going to require dedicated resources, public-private partnerships and the whole of government approach. It can't be done in silos. In order to have a secure and resilient global supply chain and even an American supply chain, we have to have this united approach.

As the nation's risk advisor, supply chain security is a top priority for the Cybersecurity and Infrastructure Security Agency. As the cyber attacks continue to evolve within the federal government, it's important that the CIO, the CISOs and the chief acquisition officers are looking at making decisions jointly around what they are acquiring.

We have to partner with private industry in order to share relevant supply chain risk information and overcome some of the barriers that we're seeing with information sharing perhaps through some liability protections would certainly also enable us to reach that secure and resilient state for supply chain.

Mission is Possible

JASON:

That's very informative, especially around some of the ways of how to increase that information sharing aspects. I'm also curious of your impressions and thoughts on where the government and industry could do a better job around the topic of information sharing? Matt, I'd like to start from an IC perspective and then transition back over to Lisa again. Because I know there are multiple different information sharing councils and organizations and industry groups. I would appreciate your perspectives on how both government and industry could do a better job there?

MATT:

In my experience, the biggest problem with information from the government side to private industry is that both are very large. Because of that, there are many different outreach venues. And because there were many different outreach venues, you don't know all the data.

If FBI's working on its outreach, but DHS and one of the IC agencies and DOD is doing its outreach. It's gone out in so many avenues. That's one of the difficulties. Another difficulty is getting information out from a threat perspective when you're not sure if you're tipping your hand to the adversaries, so it's trying to figure out that balance to make sure that you have enough information, so that when you put it out you're actually value added and you're not just making the case worse. I wish there were a mechanism to aggregate all of the outreach efforts and information sharing with the private industry, because there's a ton being shared or communicated, but you never know what pocket within the private sector dealing with a what pocket in federal government. That's one of the bigger challenges as I see it. I don't know, I don't know how to fix that.

We've got this way with terrorism information. I think we're getting this way with counterintelligence security information, which was share, share, share, share, share, share, share, which is great. We share a lot, but we share so much that it's not getting where it needs to go.

JASON:

Thank you Matt. Lisa, your perspective on information sharing and how both the government and industry could do better?

LISA:

This is definitely another complex problem. One of the successes I think that we have within CISA I want to highlight is the establishment of the Information and Communications Technology Supply Chain Risk Management Task Force in partnership with industry and federal agencies, it's chaired by CISA, but it has representatives from the information technology and the communication sectors. In some ways, it starts to embody some of the partnerships I think that we have to have in place in order to really collaborate.

CISA is somewhat uniquely positioned because of the critical infrastructure partnership advisory council authorities that it has with regards to being able to seek consensus advice from the private sector.

The challenge that I see, and it's one that comes up, you know, even in the federal enterprise, and it touches on what Matt was talking about is the sharing, handling and protecting of information. We have genuine tensions in the federal government on what we want to share, with whom, when, under what circumstances. We are actually in the process under the Federal Acquisition Security Council of thinking through engaging with private industry, to be able to

identify what are those information sharing triggers that would promote the sharing of relevant risk information. What that supply chain risk information would be.

I think generally the federal government wants to provide relevant supply chain risk information that will inform the private sector. I think the private sector wants to provide that to the federal government, but there are some things we need to work through, including, and the private sector has raised this through the ICT SCRM Task Force, the need for some sort of safe harbor legislation or liability protection, so that they can more openly share within the federal enterprise.

CISA has some authorities in this area to protect information, but it's sort of confined within the department. So we need to find ways in which we can address this, I think through legislation some of the information sharing challenges that we're seeing. And then on the federal side, it's a natural tension and we will work through it because we all want the same end, which is the secure and resilient supply chain for the American people.

JASON:

Thank you, Lisa and Matt, for those answers and insight. The next items and areas that I want to start to go into, are the increasing types of threats that we're seeing within attacks on supply chain and how that impacts the SCRM environment and really preparing for the next generation of supply chain risk and how to protect the supply chain.

Disruptions are continuing to grow, not just in number, but the complexity and severity of impacts. Lisa I'd like for you to address what you see as some of those most significant types of supply chain threats that we're seeing and then turning it over to Matt from the IC perspective.

LISA:

Over the past several years we've seen that supply chain risk management is no longer a distinct discipline, that's removed from broader cyber and physical risk management conversation. It's now integrated at almost every single level.

The ongoing supply chain compromise that was first discovered through Solar Winds only really reinforced this point. We continue to see vulnerabilities in supply chains either developed intentionally or for malicious intent or unintentionally through poor security practices. Those are areas that especially the poor security practices are things that we can certainly address and we should be focusing on. But these types of vulnerabilities, this increased attack surface, if you will. It only enables data and intellectual property theft, loss of confidence and integrity of the system, and exploitations of systems and networks.

I would defer to Matt more on the threat side. That is the Intelligence Community's wheelhouse.

MATT:

Happy to talk about it. One of the things that I like to do when I talk about this, Jason, is first as Lisa said, supply chain security, supply chain risk management is a growing discipline. Two, three years ago, this was a niche organization, but it is no longer a niche, it has grown. One, because the federal government has been pushing and pulling on this issue on supply chain security. And in my opinion, it's one of the areas where the federal government actually leads private industry. Normally it's the other way around. The federal government saw it as an issue early on.

Mission is Possible

I want to add that, because there may be people listening that are new to this as it grows in their organization. So what do we mean by a supply chain attack or what do we mean by a supply chain threat?

And what we in the IC, particularly in my entity at, NCSC, we are focusing on generally the foreign intelligence entities and not on the criminal entities. So, while criminals do use supply chain attacks, we at NCSC don't generally focus on those.

When you look at supply criminal supply chains you can think of; cargo theft, some sort of fraud. You could think of a supply chain attack that deals in ransomware. Those are criminal attacks, and not necessarily the type that we are focused on at NCSC. We are focused on the foreign intelligence entities, and when I say foreign intelligence entities, we specifically are country agnostic. It doesn't matter what country because the threat vectors are the same and the methodologies are going to be the same.

What we are looking at is an untoward amount of foreign ownership control or influence. That's what we are looking at from a supply chain perspective. We don't say, “China bad, Russia bad,” we don't list countries and just say, they're bad. We look for where is that untoward amount of foreign ownership controller interest? That's what we're looking at. More generally, I like to break down supply chain attacks into two generalized types of attacks. I think that's important for private industry to look at these this way, because it helps when you talk to the federal government. The first one would be sabotage, and that is what it says it is, the straight up cease in functionality, turning something off, whether it's the ability to shut down a radar system or shut down a camera system that's providing security somewhere, or turn off the electricity on the Eastern seaboard. Those are sabotage attacks. It is conceivable that a foreign intelligence entity would want to conduct a sabotage attack against a private company in the United States, and they would cause economic pain to the United States.

The next type of generalized attack that we look at is information theft. And we specifically use information as the term, we keep that broad because information falls into various types of buckets, depending on what the information is. It could be classified information, straight up U.S. Government classified information that has plans, intents, methods and sources, things of that nature. It could be intellectual property by the true legal definition of intellectual property. It could be proprietary data. It could be plans of a company, new product designs. Or it could be PII, personally identifiable information, that is in the unclassified space. So we purposely keep that term as broad, saying information theft as opposed theft of classified plans.

The other reason we want to stress that private industry information is of value to a foreign intelligence entity, even if it is not classified data. Unclassified data is of great value to a foreign intelligence entity. Because in a lot of the foreign or adversarial countries that we deal with, their private industry is supported by government activities. So in the United States, the NSA does not spy on foreign companies to give U.S. companies economic advantage. That happens in foreign countries, where the economic support by those intelligence entities is real. They will steal U.S. information, give it to a private company in their country to increase the economic advantage in their industry.

While they are different, the mitigation strategies for the foreign intelligence entities, also provide mitigation to the criminal attacks. The strategies for protecting your supply chain don't vary much at all, whether it's a foreign intelligence entity or a criminal entity.

Mission is Possible

JASON:

Thank you, Matt. Supply chain attacks happen against both government as well as industry, and in some sectors you may say that it's even more increasing in the commercial world, in terms of importance and impact. What are some increasing tangible steps that industry can take to protect their supply chain as it's moving from, what used to be a niche capability and specialty, into a more wide ranging requirement for all of these groups to have, and how do you balance that requirement of a more robust program with the knowledge and discovery of both known threats, unknown threats, and how can companies help the government better anticipate some of the risks that they might be facing to help protect the supply chain?

MATT:

I was speaking to the executive director for the Healthcare Coordinating Council, and he used the analogy, which has been around for many years. People are conducting ransomware attacks against the healthcare industry and against hospitals, the same reason that Willie Sutton robbed banks. Because that's where the money is. That's why private entities in the United States are being targeted for supply chain attacks. Because that's where the intellectual property is, that's where the money is. It's a target rich environment.

So what can private industry do? What steps can they do to address it? The first thing which is happening more and more, which we're glad to see, is the understanding that they are a target. Realizing that an organization does have to worry about their supply chain security is the first step. You got to admit you have a problem, before you can address it.

With that comes the executive level commitment. We are seeing that more and more as we do our outreach to executives, without that executive level of commitment, you're not going to get the resources and buy-in within the organizations to address it.

The second thing, is understanding that you cannot treat everything at the same level in your supply chain. Not everything is critical to your organization's operations or mission statement. You need to do a criticality assessment in your organization and determine where are we going to put limited resources to protect what's most important to us? You've got to have a criticality assessment, so then you can determine what's critical to your organization, at what level, so that you can devote those appropriate resources to it.

LISA:

I was actually going to point to three tangible products that were developed in partnership with industry that really start to help both the private sector and the public sector with understanding where to start when you're thinking about supply chain risk management.

One of the products is a Threat Scenarios Report that was released under CISA's ICT Supply Chain Risk Management Task Force. It's a practical example-based guide on supplier SCRM threat analysis and evaluation that can be applied to the acquisition and procurement environments and personnel.

Another product that CISA put out was a Supply Chain Risk Management Essentials Guide, for leaders to be able to take actionable steps to help with establishing a supply chain risk management program to be thinking about supply chain risks. And that was developed based off of work that NIST had done, best practices, standards, things like that. And again, engaging with private industry to make sure that what we were putting out made sense for the private sector.

Mission is Possible

And the third element is, Department of Commerce/NIST, both as a member of the federal acquisition security council, but also in their own right, has been focusing on supply chain risk management for several years and they've put out some really good practical examples of things to do, and be able to provide around foundational practices, enterprise wide practices in terms of effective enterprise wide activity. And just sort of building off established risk management processes.

Those three elements are just example products of tangible things that the private sector or the public sector could pick up and start to look at to start building out what they need to do within their own agencies or organizations.

JASON:

There's another aspect to supply chain issues that I think is important to, to address in terms of the threats, at the same point that we're seeing greater calls for protecting the supply chain and consolidating trustworthy and trusted vendors and suppliers or products.

There's also a call for diversifying the supply chain and finding alternate suppliers and sources of parts components and sub components. Could you both talk about what that means in a practical sense?

MATT:

A good question that we get a lot is diversification, and does that answer the mail on the question of resiliency and does it add to security risk? The answer to all of it is yes. It can add to resiliency, but it can also add to the risk. If you're conducting appropriate due diligence on your purchases or contracts that the service contracts that you're entering into, you're giving yourself additional work if you broaden that list too much. And you are increasing the threat areas that an actor could use to enter into your supply chain, But at the same token, if you have a sole supplier and that sole supplier is critical to your security operation, do you have an unrealized risk? It's a difficult question to answer. I think the best that I've been able to think about is diversify enough that you have some resiliency, but not enough that it adds to your risk outside of your risk appetite.

LISA:

What we're going to see is that there is going to be an even stronger need for the Federal Acquisition Security Council.

Because federal departments and agencies are going to be asking regularly, is this something I should acquire? Is it not something I should acquire? What are the risks? What are the implications if I would purchase some covered article from a particular source?

That is what the FASC was intended to be able to provide to departments and agencies, a thorough risk analysis and risk based assessment on covered articles that the federal government might think might pose to the enterprise, and be able to do a very in-depth thorough analysis, to be able to make a decision on whether or not to purchase a particular software service, hardware; or remove it from the federal enterprise.

As corporations and organizations look at diversifying their supply chains in order to build that resiliency, from the federal side, we have to be thinking about what does that mean in terms of what we are acquiring and how do we still start to know and understand what's within that supply chain based off of the sort of more distributed nature of what's being acquired

downstream or upstream, or how we want to talk about it. It's going to be interesting the next couple of years.

JASON:

No discussion of supply chain and supply chain risk is complete without addressing cybersecurity of the supply chain. Cybersecurity is increasingly a more critical and broad aspect of supply chain security. Solar Winds is really just the most current and tangible example of those types of cyber threats.

Lisa, DHS CISA is uniquely positioned at the cross-government perspective to identify, share information, discuss cybersecurity, for the supply chain.

LISA:

At CISA, we understand there's a lot of risk out there and to effectively manage these risks we have to prioritize our approach. We don't have a never-ending stream of resources. But nowhere, I think is a risk more apparent than when we start thinking about managing supply chain risks. Almost every aspect of the government and industry is becoming increasingly digitalized and dependent on data for efficient, effective, operations. It starts with our national security, but it stands true for a full range of the national critical functions that the U.S. relies upon.

We've touched on already the vulnerabilities and the attacks surface, but vulnerabilities can be exploited through a variety of means; from deliberate mislabeling and counterfeits, unauthorized production, tempering theft and reinsertion of malicious software code. We're seeing all those things play out in the current environment.

All of these risks impact supply chain and could be a fundamental degradation of our ability to understand the confidentiality, integrity, and availability of what we're acquiring and what's within our supply chains.

Certainly the recent compromises and other security events have revealed just how new and inherent vulnerabilities and supply chains have cascading impacts that are affecting all users of technology and services within and across federal government and certainly within and across the United States from within our companies and organizations.

I think that CISA is in a unique role, both from the cybersecurity standpoint, and in the engagement with the private sector we've been building for the past 10 years these public-private partnerships, maybe longer. We've been focusing on partnering, and building trust, and building relationships so that we can collectively come together to address what we're seeing play out now on the cybersecurity side of supply chain risks.

JASON:

I do have one final question for you both. Is there a message that you would like to send to both government agencies as well as commercial industry and the public at large on behalf of your agencies, about the topic of supply chain, supply chain risk, and where we're going for the future?

MATT:

Mission is Possible

One of the things I like to stress to private industry and government, is this notion that supply chain security decisions can only be made with the addition, or can only be made well, with the addition or inclusion of classified reporting or classified information from U.S. Government holdings.

There is a great misperception I've heard from many within the private sector that they desire this access to classified information because they can't make good supply chain security decisions without it. And I will say from the Intelligence Community perspective, from what we see and from our engagement on these issues, that is false. The vast majority of supply chain security decisions, to include decisions made in the federal government, are made with unclassified, publicly available data. Due diligence research, that is done prior to an acquisition or a contract. That's one of the things I really want to stress and really want to get out to people, is engaging with that publicly available data to do your supply chain security assessments.

Now you may need to work with a private contracting company to do that. Some of the services like Guidehouse offers, or some of the other companies that offer those services, if you don't have the expertise or the data aggregation capabilities in your organization. It's publicly available data. You don't need TS reporting to know I should be cautious adding Huawei to my system. That's publicly available data to make those decisions.

LISA:

Partnerships and risk analysis. I've touched on it quite a bit, federal partnerships, public-private partnerships, and certainly doing our due diligence, the risk analysis and the assessment that is leveraging publicly available data and information business intelligence, due diligence, all of that collectively starts to come together so that we can make better informed decisions on what we're acquiring and what needs to be removed from our network systems and services.

JASON:

Thank you, both. This has been a fascinating discussion, it's obvious that you both are very passionate about the topics of supply chain security and appreciate your participation, sharing your insights and knowledge and looking forward to next conversations that we can have.

MATT:

Jason, on behalf of my leadership with acting director Mike Olando, and assistant director Joyce Corell at NCSC, thank you very much for having me on this.

LISA:

Thank you, Jason. Thanks Matt for being a good supply chain colleague.

SASHA:

On behalf of Guidehouse and American University, I'd like to thank all of our speakers for joining us today. To learn more, or to listen to other episodes of Guidehouse and American University Mission is Possible series, please visit us at guidehouse.com