ACCESS DENIED: KEEPING ADVERSARIES AWAY FROM THE HOMELAND SECURITY SUPPLY CHAIN

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

AND THE

SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JULY 12, 2018

Serial No. 115–71

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

34–348 PDF WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
CLAY HIGGINS, Louisiana
THOMAS A. GARRETT, JR., Virginia
BRIAN K. FITZPATRICK, Pennsylvania
RON ESTES, Kansas
DON BACON, Nebraska
DEBBIE LESKO, Arizona

BENNIE G. THOMPSON, Mississippi
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California

BRENDAN P. SHIELDS, *Staff Director*
STEVEN S. GIAIER, *Chief Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
HOPE GOINS, *Minority Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PETER T. KING, New York, *Chairman*

LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
WILL HURD, Texas
MIKE GALLAGHER, Wisconsin
MICHAEL T. MCCAUL, Texas *(ex officio)*

KATHLEEN M. RICE, New York
SHEILA JACKSON LEE, Texas
WILLIAM R. KEATING, Massachusetts
BENNIE G. THOMPSON, Mississippi *(ex officio)*

MANDY BOWERS, *Subcommittee Staff Director*
NICOLE TISDALE, *Minority Staff Director/Counsel*

SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

SCOTT PERRY, Pennsylvania, *Chairman*

JOHN RATCLIFFE, Texas
CLAY HIGGINS, Louisiana
THOMAS A. GARRETT, JR., Virginia
RON ESTES, Kansas
MICHAEL T. MCCAUL, Texas *(ex officio)*

J. LUIS CORREA, California
KATHLEEN M. RICE, New York
NANETTE DIAZ BARRAGÁN, California
BENNIE G. THOMPSON, Mississippi *(ex officio)*

DIANA BERGWIN, *Subcommittee Staff Director*
ERICA D. WOODS, *Interim Subcommittee Minority Staff Director*

CONTENTS

Page

APPENDIX

ACCESS DENIED: KEEPING ADVERSARIES AWAY FROM THE HOMELAND SECURITY SUPPLY CHAIN

Thursday, July 12, 2018

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE, AND
SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY,
Washington, DC.

The subcommittees met, pursuant to notice, at 10:05 a.m., in room HVC–210, Capitol Visitor Center, Hon. Peter King [Chairman of the Subcommittee on Counterterrorism and Intelligence] presiding.

Present: Representatives King, Perry, Hurd, Donovan, Rice, Correa, Barragán, and Keating.

Mr. KING. Good morning. The Committee on Homeland Security Subcommittees on Counterterrorism and Intelligence and Oversight and Management Efficiency will come to order.

The subcommittees are meeting today in a joint hearing to examine threats in the Department of Homeland Security's supply chain and assess tools and authorities for DHS to mitigate those threats. I now recognize myself for an opening statement.

There is no question that nation-states and criminal actors are constantly trying to exploit U.S. Government and private-sector systems to steal information or insert potentially harmful hardware or software. The recent cases involving Kaspersky, ZTE, and Huawei underscore the threats posed to the Federal supply chain and the urgency in developing stronger mechanisms to secure it.

In March 2017, the Office of the Director of National Intelligence, ODNI, released a background paper on the supply chain risk management, stating: "Even as the U.S. Government and private sector have implemented programs to mitigate and counter supply chain threats, the evolution of directed, sophisticated, and multifaceted threats threatens to outpace our countermeasures. Traditional remedies such as trade agreements, economic sanctions, and legal actions are reactionary in nature and cannot keep pace with the evolution of threats."

The Federal Government is behind the curve in establishing robust supply chain security measures. It is clear that additional tools, policies, resources, and legal authorities are urgently needed to address this challenge. I am pleased that the White House re-

leased a legislative proposal on Tuesday developed through the interagency process that was initiated in April.

The proposal seeks to strengthen SCRM's efforts across the Government, enhance information sharing, and harden the Federal procurement process to identify and mitigate threats. Additionally, I want to highlight that DHS is making great strides to implement SCRM measures throughout the Department.

Last year, DHS issued policy directives for high-value assets requiring that all DHS components develop and implement SCRM strategies for sensitive payments, educate and train staff and contractors about supply chain risks, and enforce good supply chain hygiene by establishing contractual requirements and audit mechanisms for suppliers.

The purpose of today's hearing is to review current capabilities and authorities and assess whether additional authorities are needed to better protect the Department of Homeland Security's supply chain.

The Department of Defense and the intelligence community have existing authorities to block certain procurement efforts if security risks are identified. Even now, more is being done to protect our sensitive supply chain. The recently-passed National Defense Authorization Act enhances DOD's authorities, and the Intelligence Authorization Act which is on the floor today further strengthens the intelligence community's SCRM toolkit.

As a National security agency, it is vital that DHS also have robust supply chain risk management practices and tools to identify, mitigate, and remove potential threats to our systems and contracts. In addition to reviewing the OMB proposal, both subcommittees are working on specific legislation to provide DHS with similar SCRM authorities to DOD.

At the end of the day, the ability of any agency to address supply chain risk survives on a robust intelligence framework. The foundation of any SCRM program is the ability to proactively identify entities seeking to exploit the DHS acquisition process, become trusted vendors, and then steal from or otherwise harm the Homeland Security enterprise.

In order to fully understand DHS intelligence SCRM capabilities and specific threats to the supply chain, I expect that after an initial round of questions in the open session, we move to a closed session to better discuss those issues.

I again want to thank the witnesses for being here and express appreciation for Chairman Perry and Ranking Member Correa for working with us on this joint hearing.

[The statement of Chairman King follows:]

STATEMENT OF CHAIRMAN PETER T. KING

JULY 12, 2018

There is no question that nation-states and criminal actors are constantly trying to exploit U.S. Government and private-sector systems to steal information or insert potentially harmful hardware or software. The recent cases involving Kaspersky, ZTE, and Huawei underscore the threats posed to the Federal supply chain and the urgency in developing stronger mechanisms to secure it.

In March 2017, the Office of the Director of National Intelligence (ODNI) released a background paper on the supply chain risk management stating: "Even as the U.S. Government and private sector have implemented programs to mitigate and

counter supply chain threats, the evolution of directed, sophisticated, and multi-faceted threats threatens to outpace our countermeasures. Traditional remedies such as trade agreements, economic sanctions, and legal actions are reactionary in nature and cannot keep pace with the evolution of threats."

The Federal Government is behind the curve in establishing robust supply chain security measures. It is clear that additional tools, policies, resources, and legal authorities are urgently needed to address this challenge.

I am pleased that the White House released a legislative proposal on Tuesday developed through the interagency process initiated in April. The proposal seeks to strengthen SCRM efforts across the Government, enhance information sharing, and harden the Federal procurement process to identify and mitigate threats.

Additionally, I want to highlight that DHS is making great strides to implement SCRM measures throughout the Department. Last year, DHS issued policy directives for high-value assets requiring that all DHS components develop and implement SCRM strategies for sensitive systems, educate and train staff and contractors about supply chain risks, and enforce good supply chain hygiene by establishing contractual requirements and audit mechanisms for suppliers.

The purpose of today's hearing is to review current capabilities and authorities and assess whether additional authorities are needed to better protect the Department of Homeland Security's supply chain.

The Department of Defense and the intelligence community have existing authorities to block certain procurement efforts if security risks are identified. Even now, more is being done to protect their sensitive supply chain. The recently-passed National Defense Authorization Act enhances DOD's authorities and the Intelligence Authorization Act, on the Floor today, further strengthens the intelligence communities SCRM toolkit. As a National security agency, it is vital that DHS also have robust supply chain risk management practices and tools to identify, mitigate, and remove potential threats to its systems and contracts.

In addition to reviewing the OMB proposal, both subcommittees are working on specific legislation to provide DHS with similar SCRM authorities to DOD. At the end of the day, the ability of any agency to address supply chain risk survives on a robust intelligence framework.

The foundation of any SCRM program is the ability to proactively identify entities seeking to exploit the DHS acquisition process, become trusted vendors, and then steal from or otherwise harm the homeland security enterprise.

In order to fully understand current DHS intelligence SCRM capabilities and specific threats to the supply chain, I expect that after an initial round of questions in the open session we will move into a closed session to better discuss those issues.

I again want to thank the witnesses for being here and express appreciation for Chairman Perry and Ranking Member Correa for working with us on this joint hearing.

Mr. KING. I am pleased to recognize the Ranking Member of the Subcommittee on Counterterrorism and Intelligence, the gentlelady from New York, Miss Rice, for her opening statement.

Miss RICE. Thank you, Chairman King and Chairman Perry, for holding this important hearing, and thank you to the witnesses for coming to testify today.

The Department of Homeland Security has the enormous responsibility of securing the Federal Government's vast supply chain, particularly information technology, from a wide variety of foreign threats. Today the most pressing threats come from Chinese and Russian IT companies that until recently were used widely throughout the United States and by several Federal agencies. For example, last year we learned that the Russian cybersecurity company Kaspersky Lab was operating compromised antivirus software on U.S. Government computers. Despite being a long-time Government vendor, the FBI had reason to believe the Kaspersky programs contained back doors that could be accessed by Russian intelligence. Thankfully, DHS acted to wipe the software from all Government systems.

Additionally, Members of Congress have long been warned that the Chinese telecommunications companies Huawei and ZTE also

pose risks to our National security. ZTE and Huawei are two of the world's largest telecommunication companies and were used widely in the United States. However, the companies have close ties to the Chinese Government and were believed to be possible vehicles for cyber threat and espionage.

In 2016, we imposed stiff penalties on ZTE for violating U.S. sanctions by making hundreds of shipments of telecommunications equipment made with U.S. parts to Iran, Sudan, North Korea, Syria, and Cuba. After yet another breach in April, ZTE faced additional U.S. penalties, including a ban on U.S. suppliers selling equipment to ZTE. The following month, both ZTE and Huawei were also banned from being sold on U.S. military bases.

These bans were not only warranted but, in my opinion, long overdue. These companies and their government clearly pose a threat to our National security and we had a responsibility to act, which makes the actions of President Trump all the more surprising. It appears President Trump has placed his own business interests above our National security. Not long after a soon-to-be Trump-branded resort in Indonesia received loans from the Chinese Government, the President tweeted a promise to save ZTE from the punishing penalties. Just yesterday, the Trump administration and the Chinese Government signed an agreement to end the ban on U.S. exports to ZTE.

The President's lack of candor and leadership on this issue, coupled with the urgent threats facing our supply chains, calls for the Federal Government to develop a comprehensive strategy to protect our supply chains from foreign threats. During this hearing, I hope to learn more about what the Department of Homeland Security is doing to advance their counterintelligence programs, specifically with the proposed use of section 806 authority.

I think it is also important that we know whether the White House is playing an active role in coordinating supply chain security across the Federal Government. But most importantly, this committee needs to know what additional resources and support are needed by supply chain risk management programs to carry out its mission effectively. As I understand, there are only two employees dedicated to the SCRM program, which seems completely inadequate, given the task ahead.

It is time that we finally listen to the intelligence community and create a comprehensive strategy to counter the mounting threats facing our supply chains. I look forward to hearing from our witnesses today and I do hope this will be a constructive conversation. Thank you, Mr. Chairman.

[The statement of Ranking Member Rice follows:]

STATEMENT OF RANKING MEMBER KATHLEEN RICE

JULY 12, 2018

The Department of Homeland Security has the enormous responsibility of securing the Federal Government's vast supply chain—particularly information technology—from a wide variety of foreign threats. Today, the most pressing threats come from Chinese and Russian IT companies, that until recently were used widely throughout the United States and by several Federal agencies.

For example, last year we learned that the Russian cybersecurity company Kaspersky Lab was operating compromised anti-virus software in U.S. Government computers. Despite being a long-time Government vendor, the FBI had reason to be-

lieve the Kasperksy programs contained back doors that could be accessed by Russian intelligence. Thankfully, DHS acted to wipe the software from all Government systems. Additionally, Members of Congress have long been warned that the Chinese telecommunications companies Huawei and ZTE also posed risks to our National security.

ZTE and Huawei are two of the world's largest telecommunications companies and were used widely in the United States. However, the companies have close ties to the Chinese government and were believed to be possible vehicles for cyber theft and espionage.

In 2016, we imposed stiff penalties on ZTE for violating U.S. sanctions by making hundreds of shipments of telecommunications equipment made with U.S. parts to Iran, Sudan, North Korea, Syria, and Cuba. After yet another breach in April, ZTE faced additional U.S. penalties, including a ban on U.S. suppliers selling equipment to ZTE. The following month both ZTE and Huawei were also banned from being sold on U.S. military bases. These bans were not only warranted but, in my opinion, long overdue. These companies and their Government clearly pose a threat to our National security and we had a responsibility to act.

Unsurprisingly however, President Trump appears to have placed his own business interests above our National security. Not long after a soon-to-be Trump-branded resort in Indonesia received loans from the Chinese government, the President Tweeted a promise to save ZTE from the punishing penalties. Just yesterday, the Trump administration and the Chinese government signed an agreement to end the ban on U.S. exports to ZTE.

The President's lack of candor and leadership on this issue, coupled with the urgent threats facing our supply chains, calls for the Federal Government to develop a comprehensive strategy to protect our supply chains from foreign threats.

During this hearing, I hope to learn more about what the Department of Homeland Security is doing to advance their counterintelligence programs specifically with the proposed use of Section 806 authority. I also want to know whether the White House is playing an active role in coordinating supply chain security across the Federal Government.

But most importantly, this committee needs to know what additional resources and supports are needed by the Supply Chain Risk Management program to carry out its mission effectively. As I understand, there are only two employees dedicated to the SCRM Program. That seems completely inadequate given the task ahead. It is time that we finally listen to the intelligence community and create a comprehensive strategy to counter the mounting threats facing our supply chains.

Mr. KING. Thank you, Miss Rice.

I now recognize the Chairman of the Subcommittee on Oversight and Management Efficiency, Mr. Perry, for an opening statement.

Mr. PERRY. Thank you, Mr. Chairman.

Good morning. I thank you, Chairman King, for holding this hearing today and including the Oversight and Management Efficiency Subcommittee in this very important timely discussion on the Department of Homeland Security's efforts to secure its supply chain.

In today's interconnected world, the Federal Government is increasingly reliant on the procurement of products and services with supply chains that originate from outside our borders. DHS is no exception. Global supply chains are integral to the Department's ability to carry out the mission of securing the homeland. However, recent incidents involving Government contractors and foreign-based suppliers, like Kaspersky Lab, ZTE, and Huawei, have shed light on the security risks associated with the global nature of supply chains. Potential threats to international supply chains, ranging from interference by foreign adversaries to poor product manufacturing practices, present a unique and complex challenge for both DHS and National security.

To assess and counter supply chain threats, organizations employ supply chain risk management strategies which leverage risk assessments to neutralize threats associated with the global and dis-

tributed nature of modern supply chains. Risk assessments are made by utilizing open- and closed-source research, to allow organizations to better understand their supply chain and identify the threats specific to it. To assist the Federal Government in this effort, the National Institute for Standards and Technology has released Government-wide best practices for agencies to use as a model for their own supply chain risk management strategies.

Agencies like DHS rely on contracts for products and services to carry out their daily operations. As such, in the case of the Department, ensuring supply chain security is intrinsic to the mission of ensuring National security. Unfortunately, given the threat environment, I too am concerned that the Department does not currently possess the sufficient tools to effectively carry out supply chain risk management.

Under the regulations governing Federal procurements, DHS maintains limited authority to terminate procurement contracts for unforeseen circumstances and to bar irresponsible entities from doing future business with the Federal Government for up to 3 years.

Additionally, the Federal Information Security Modernization Act of 2014 granted the Department the authority to issue binding operational directives, which are compulsory orders for Federal agencies to take action to safeguard information in IT systems when a security vulnerability has been identified. Unfortunately, these authorities are generally viewed as reactive measures that open the Department up to costly liability and litigation and are not agile enough to address today's supply chain threats.

DHS needs the proper authorities to be able to decisively act when a threat to its supply chain has been identified. That is why in the near term, I will be joining with my colleague Chairman King in introducing legislation to provide DHS with the tools to effectively carry out supply chain risk management in order to secure its supply chain. Modelled after statutory authority given to the Department of Defense in 2011, this legislation will empower the Secretary of DHS to block entities who pose a security risk from being a DHS vendor. This legislation will also encourage information sharing across the Department when a supply chain risk has been identified.

Again, I thank our distinguished panel for testifying this morning and I look forward to learning more about supply chain risk management at the Department. It is my intention to use today's discussion to help further shape a legislative solution for securing DHS's supply chain.

Thank you, Mr. Chairman. I yield the balance.

[The statement of Chairman Perry follows:]

STATEMENT OF CHAIRMAN SCOTT PERRY

JULY 12, 2018

Good morning. I would like to thank Chairman King for holding this hearing today and including the Oversight and Management Efficiency Subcommittee in this very important and timely discussion on the Department of Homeland Security's efforts to secure its supply chain.

In today's interconnected world, the Federal Government is increasingly reliant on the procurement of products and services with supply chains that originate from

outside our borders. DHS is no exception. Global supply chains are integral to the Department's ability to carry out the mission of securing the homeland.

However, recent incidents involving Government contractors and foreign-based suppliers like Kaspersky Lab, ZTE, and Huawei have shed light on the security risks associated with the global nature of supply chains. Potential threats to international supply chains ranging from interference by foreign adversaries to poor product manufacturing practices present a unique and complex challenge for both DHS and National security.

To assess and counter supply chain threats, organizations employ supply chain risk management strategies, which leverage risk assessments to neutralize threats associated with the global and distributed nature of modern supply chains. Risk assessments are made by utilizing open- and closed-source research to allow organizations to better understand their supply chain and identify the threats specific to it. To assist the Federal Government in this effort, the National Institute for Standards and Technology has released Government-wide best practices for agencies to use as a model for their own supply chain risk management strategies.

Agencies like DHS rely on contracts for products and services to carry out their daily operations. As such, in the case of the Department, ensuring supply chain security is intrinsic to the mission of ensuring National security.

Unfortunately, given the threat environment, I am concerned that the Department does not currently possess the sufficient tools to effectively carry out supply chain risk management. Under the regulations governing Federal procurements, DHS maintains limited authorities to terminate procurement contracts for unforeseen circumstances and to bar irresponsible entities from doing future business with the Federal Government for up to 3 years. Additionally, the Federal Information Security Modernization Act of 2014 granted the Department the authority to issue binding operational directives, which are compulsory orders for Federal agencies to take action to safeguard information and IT systems when a security vulnerability has been identified. Unfortunately, these authorities are generally viewed as reactive measures that open the Department up to costly liability and litigation and are not agile enough to address today's supply chain threats.

DHS needs the proper authorities to be able to decisively act when a threat to its supply chain has been identified. That is why, in the near term, I will be joining with my colleague Chairman King in introducing legislation to provide DHS with the tools to effectively carry out supply chain risk management in order to secure its supply chain.

Modeled after statutory authority given to the Department of Defense in 2011, this legislation will empower the Secretary of DHS to block entities who pose a security risk from being a DHS vendor. The legislation will also encourage information sharing across the Department when a supply chain risk has been identified.

I want to thank our distinguished panel for testifying this morning and I look forward to learning more about supply chain risk management at the Department. It is my intention to use today's discussion to help further shape a legislative solution for securing DHS's supply chain. Thank you and I yield back the balance of my time.

Mr. KING. Thank you, Mr. Perry. I am pleased that our two subcommittees are working together to address this vital issue.

I now recognize the Ranking Member of the subcommittee, Mr. Correa, for an opening statement.

Mr. CORREA of California. Thank you, Chairman Perry, Chairman King, and Vice Chairperson Rice, for today's hearing. This morning the two subcommittees will hear from witnesses on DHS's current authority on mitigating threats to our supply chain. We urgently need a National strategy for supply chain risk management.

Foreign nation-states like Russia and China view information and communication technology as a strategic sector in which they have invested significant capital and exercise tremendous influence. IT products and services through the global supply chain are threats that continue to evolve every day. Bad actors continue to target U.S. Government contractors and other private-sector entities that do business with the Government and try to gain advantage and undermine our security.

Over the past year, DHS has mitigated the risks and secured the Government supply chain. DHS launched a new supply chain risk management, or SCRM, program. While the goals of the program are commendable, its mission far exceeds its resources. As of this May, there are only two employees dedicated to the program. I hope to work with the Department and my colleagues across the aisle to provide this office with the proper resources and manpower it deserves.

Last, I look forward to hearing from today's witnesses on how the DHS SCRM program fits into the Federal Government's overarching approach to supply chain security. Without a cybersecurity coordinator within the administration, I am also concerned about consolidation efforts underway within multiple Federal agencies to address the National security implications of supply chain vulnerability.

The Federal Government supply chain is a target for our adversaries and we need to ensure that commercial off-the-shelf goods and services are not the subject of manipulation. It is imperative that we streamline these efforts to better protect against supply chain threats, and I hope to work with the administration to that end.

With that, I yield.

[The statement of Ranking Member Correa follows:]

STATEMENT OF RANKING MEMBER J. LUIS CORREA

JULY 12, 2018

This morning the two subcommittees will hear from several distinguished witnesses on DHS's current authority related to mitigating threats to its supply chain. As previously mentioned by my colleagues in their opening statements, the United States needs a National strategy for supply chain risk management—and it needs it now.

Foreign nation-states like Russia and China rely on information and communication technology as a "strategic sector," in which the two countries' governments have invested significant capital and exercise substantial influence.

In 2012, the House Permanent Select Committee on Intelligence found that the risks posed by China's largest telecommunications manufacturers, ZTE and Huawei, "could undermine core U.S. National security interests." In 2017, after "concern[s] about the ties between certain Kaspersky officials and Russian intelligence," DHS directed all Federal agencies to remove the Russian-based firm's products from their networks.

The exploitation of IT products and services through the global supply chain is a threat that continues to evolve each day. Bad actors continue to target U.S. Government contractors and other private-sector entities that do business with the Government to try to gain advantage and pursue other state goals.

Over the past year, DHS has taken several steps to mitigate the risk and secure the Federal Government's supply chain. Just recently, DHS launched a new Supply Chain Risk Management (SCRM), or "SKRIM" Program, within its National Programs and Protection Directorate. This new office was established to examine security concerns arising from the use of certain vendors and subcontractors.

However, while the goals of the program are laudable, its mission far exceeds its resources. As of May, there were only 2 employees dedicated to the program.

Considering that the risk is great, I hope to work with the Department and my colleagues across the aisle on providing this office with the proper resources and manpower that it deserves. Especially when we are considering expanding DHS's authority related to denying procurements based on National security concerns.

Last, I look forward to hearing from today's witnesses on how the DHS SCRM Program fits into the Federal Government's overarching approach to supply chain security.

Without a Cybersecurity Coordinator within the Trump administration, I am concerned about the White House's ability to consolidate the numerous efforts under-

way within multiple Federal agencies to address the National security implications of supply chain vulnerabilities.

The Federal Government's supply chain is a target for our adversaries, and we need to ensure that commercial off-the-shelf goods and services are not subject to manipulation. Hence why it is imperative that we streamline these efforts to better protect against supply chain threats, and I hope to see the administration work towards this.

Mr. KING. I thank the gentleman. I thank Mr. Correa.

Other Members of the subcommittee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JULY 12, 2018

The threats to the United States from China and Russia are not new. For years, it has been reported that Chinese companies like ZTE and Huawei could be used to carry out cyber theft, spying, and espionage.

Last year, Kaspersky Labs demonstrated the Russian government's capability to use anti-virus products to compromise Federal information and information systems, directly affecting U.S. National security.

In a letter to Mississippi's Secretary of State in September, I spoke of "an unacceptable amount of risk" to our National security posed by these products, not only to the supply chain but also to the security of our elections.

I am reiterating that concern today, especially since the threat from Russia and China to the United States has become more complicated and troubling in the wake of on-going actions by President Trump.

After the blatant violation of U.S. sanctions in 2016 by ZTE and its subsequent breach this year, the Department of Defense initiated a ban on the sale of ZTE and Huawei products on military bases due to security concerns.

Despite these concerns, in May, the President took to Twitter to commit to saving ZTE and Chinese jobs days after a Trump-branded resort received a substantial loan from the Chinese government to build property in Indonesia.

This sent a clear message: the U.S. President will do business with you if you do business with him.

These policies continue to erode U.S. institutions and interests abroad, downplaying the seriousness of U.S. sanctions and National security to the global community.

The Federal Government supply chain is a target for our adversaries.

And while the threats from our adversaries are great, so is the opportunity to identify vulnerabilities and mitigate the risks.

Today, we are considering expanding DHS's authority to address supply chain risk by excluding contractors based on National security concerns.

Such authority would provide DHS with additional opportunities to mitigate supply chain risk during the acquisition phase.

The Defense Department currently has authority, known as Section 806 authority, to exclude contractors from information technology procurements if evidence of National security risk is identified and mitigation measures are not available. It has only been used this authority once.

Although the legislation is a good first step, we should consider whether refinements are necessary based on DOD's lessons learned.

Providing the authority won't address the fact that the Trump administration lacks a coherent, Government-wide strategy to adequately address the challenges we continue to face from Russia and China.

National Security experts, business associations and Members of this committee have communicated their concerns to the administration, about the need to secure Federal supply chains.

Mr. KING. I now would like to ask unanimous consent that the Chairman of the Emergency Preparedness Subcommittee, Mr. Donovan, be able to sit on the dais and participate in today's hearing. Without objection, so ordered.

We are grateful to have a very distinguished panel here today to testify before us. And let me remind the witnesses that their entire written statements will appear in the record.

Our first witness, Ms. Soraya Correa—did I get that right?

OK good. Serves as the chief procurement officer for the Department of Homeland Security. Ms. Correa provides leadership, policy, oversight, support, and professional work force development for the DHS contracting work force of approximately 1,500 individuals. As the senior procurement executive, she also oversees a centralized certification and training program for the DHS acquisition work force and also assists the chief acquisition officer in managing major acquisition programs.

Prior to being appointed to this position in January 2015, Ms. Correa served as the associate director of the U.S. Citizenship and Immigration Service Enterprise Services Directorate.

The Chair now recognizes Ms. Correa for her opening statement. Thank you.

STATEMENT OF SORAYA CORREA, CHIEF PROCUREMENT OFFICER, OFFICE OF THE CHIEF PROCUREMENT OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. CORREA. Thank you.

Chairman King, Chairman Perry, Ranking Member Correa, and Ranking Member Rice and Members of the subcommittees, thank you for this opportunity to discuss ways the Department of Homeland Security can enhance its ability to effectively manage supply chain risk in the procurement process.

As the chief procurement officer and senior procurement executive for the Department, I am responsible for the DHS procurement line of business. My DHS colleagues will speak to supply chain risk and the Department's response to this risk. I am here to discuss the additional authority needed to ensure the procurement process can effectively and efficiently address identified threats and vulnerabilities in the supply chain while protecting intelligence information.

The DHS National security and cybersecurity mission warrants additional authority in order to protect its systems and networks. From a procurement perspective, it is essential that we promote business processes and use authorities that enable us to be more consistent in our training, implementation, and management of those authorities across the Government.

If we do, we can improve understanding and ease implementation for industry, especially for new companies and small businesses. Today, Federal agencies are finding increasing similarities in the products and services that we acquire, in the ways we work with the various industries, and in National security considerations that impact our mission. Therefore, providing certain authorities for use across the Federal Government to ensure a fair and effective process for addressing supply chain risks throughout the acquisition life cycle is essential.

I would like to briefly describe how the rules governing the procurement process impact DHS when the Department needs to take action on intelligence information. Currently, DHS contracting officers, or COs, regardless of their security clearance level, are unable

to receive specific intelligence information. Instead, COs are advised broadly that there is a risk and provided the potential mitigation strategies to offset that risk, or they are advised if there is a risk that cannot be mitigated. When a risk cannot be mitigated, there are sufficient authorities in a Classified procurement to take immediate action. However, in an unclassified procurement, where the vast majority of DHS procurements are actually conducted and administered, the CO's actions are restricted, because the process is designed to balance the equities of the contracting parties, ensuring due process for contractors and full disclosure of the Government's reasons for pursuing contractual remedies in the event of a performance or integrity failure.

The Federal acquisition regulation and underpinning statutes were designed around the procurement of commodities and services that were neither anticipated to be vulnerable to nor the target of the sophisticated foreign intelligence activities witnessed in recent years, especially those associated with the globalized information and communications technology supply chain.

In fact, during the preaward process or during the preaward phase of the competitive procurement process, which includes the evaluation of proposals submitted by competing vendors, a CO cannot take action on intelligence information if it would preclude the further participation of an interested vendor. The competitive process is designed to ensure fair and equitable treatment of participating vendors, thereby requiring sufficient transparency in the Government's decision to exclude a vendor.

Ideally, we need to anticipate risks in our planning phase and find mitigation strategies before we begin the procurement process. Unfortunately, sometimes risks are not identified until a particular vendor or their proposed solution is evaluated. While we will always turn to our DHS colleagues to mitigate such risks, additional authority is needed for those instances when the risk cannot be mitigated and the vendor or particular product or service must be excluded.

There are existing authorities to manage risk on awarded contracts. These include temporary stop work orders, termination of contracts, and suspension and debarment actions, as appropriate. However, these remedies were not designed to address a security threat based on intelligence information.

I would like to make an important point before I close. As the Department's chief procurement officer and senior procurement executive, I take my obligations to maintain the integrity of the procurement process seriously. This is why I support strong safeguards against the abuse of any authorities granted to enhance our ability to protect the supply chain and protect intelligence information used in the procurement process. Therefore, I support ensuring accountability at a high level within the Department for use of such authority as well as appropriate fact-finding, resulting in well-documented determinations.

Thank you again for your interest in this very important matter and I look forward to any questions that you may have.

[The joint prepared statement of Ms. Correa, Mr. Zangardi, and Ms. Manfra follow:]

JOINT PREPARED STATEMENT OF SORAYA CORREA, JOHN ZANGARDI, AND JEANETTE MANFRA

JULY 12, 2018

INTRODUCTION

Chairman King, Chairman Perry, Ranking Member Correa, Ranking Member Rice, and Members of the subcommittees, thank you for this opportunity to discuss with you ways to improve the Department of Homeland Security's (DHS) ability to effectively manage supply chain risk. The Secretary of DHS has two primary sets of supply chain risk management responsibilities related to information and communications technology (ICT). In one set, the Secretary is responsible for procurement and supply chain risk management within DHS's ICT environment. These responsibilities are carried out by the DHS chief procurement officer (CPO) and DHS chief information officer (CIO). In carrying out the other set of responsibilities, the Secretary of DHS, in consultation with the Office of Management and Budget (OMB), administers the implementation of Government-wide information security policies and practices. These responsibilities are carried out by the National Protection and Programs Directorate (NPPD).

ICT is critical to an agency's ability to carry out its mission efficiently and effectively. Supply chain risks could contribute to the loss of confidentiality, integrity, or availability of information or information systems and result in adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Cyber Supply Chain Risk Management (C–SCRM) is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains. C–SCRM spans the entire life cycle of ICT, including design, development, acquisition, distribution, deployment, maintenance, and product retirement.

CURRENT SUPPLY CHAIN RISKS

The ICT supply chain is widely viewed as a source of significant risk to ICT products, systems, and services. Vulnerabilities in ICT can be exploited intentionally or unintentionally through a variety of means, including deliberate mislabeling and counterfeits, unauthorized production, tampering, theft, and insertion of malicious software or hardware. If these risks are not detected and mitigated, the impact to the ICT could be a fundamental degradation of its confidentiality, integrity, or availability and potentially adverse impacts to essential Government or critical infrastructure systems.

Increasingly sophisticated adversaries seek to steal, compromise, alter, or destroy sensitive information on systems and networks, and risks associated with ICT may be used to facilitate these activities. The Office of the Director of National Intelligence (ODNI) acknowledges, "The U.S. is under systemic assault by foreign intelligence entities who target the equipment, systems, and information used every day by government, business, and individual citizens."[1] The globalization of our supply chain can result in component parts, services, and manufacturing from sources distributed around the world. ODNI further states, "Our most capable adversaries can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversion. Our adversaries are also able to use this complexity to obfuscate their efforts to penetrate sensitive research and development programs, steal intellectual property and personally identifiable information, insert malware into critical components, and mask foreign ownership, control, and/or influence (FOCI) of key providers of components and services."

MANAGING INFORMATION AS A STRATEGIC RESOURCE

Current law governing information security of Federal information resources requires agencies to implement an agency-wide information security program that ensures that information security is addressed throughout the life cycle of each agency information system (44 U.S.C. 3554(b)). On July 27, 2016, OMB released an update to Circular A–130, *Managing Information as a Strategic Resource,* the Federal Government's governing document for management of Federal information resources. Among other things, the revisions require agencies to establish a comprehensive approach to improve the acquisition and management of their information resources.

[1] *https://www.dni.gov/files/NCSC/documents/products/20170317-NCSC_SCRM-Background.pdf.*

This includes requirements for agencies to implement and oversee the implementation of supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, and insertion of malicious software throughout the system development life cycle. Moreover, appropriate supply chain risk management plans to ensure the integrity, security, resilience, and quality of information systems are described in the National Institute of Standards and Technology (NIST) Special Publication 800–161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.*

THE CURRENT RULES FOR UNCLASSIFIED PROCUREMENTS

C–SCRM is no longer an emerging threat, it is pervasive. However, the rules under which procurements are conducted have not kept pace with the evolution of this threat. The Federal Acquisition Regulation is designed to balance the equities of the contracting parties, ensuring due process for contractors and full disclosure of the Government's reasons for pursuing contractual remedies in the event of performance or integrity failure. These rules, however, were designed around the procurement of commodities and services that were not anticipated to be vulnerable to, nor the target of, the sophisticated foreign intelligence activities witnessed in recent years, especially those associated with a globalized ICT supply chain. For instance, the current procurement rules and their underpinning statutes did not imagine the need to use and protect intelligence information in unclassified procurements. While there are tools available to pursue correction of contractor performance issues or address integrity failures, they do not provide the flexibility to react swiftly to or protect intelligence information when exclusion of a source is the only way to mitigate supply chain risk. In fact, some currently available procurement tools that address performance issues, such as Government-wide exclusion from doing business with any agency for a period of time, are too harsh, unless an agency investigation deems the contractor to be at fault for the performance issue. New rules are needed to combat the threat to our Nation's Federal information technology networks when intelligence information identifies risks that cannot be mitigated.

USING AND PROTECTING INTELLIGENCE INFORMATION

Gaps exist in the DHS's authority to use intelligence information to support its procurement decisions when a significant supply chain risk cannot be mitigated. Mitigation, which is an action initiated by the Government to preclude a supply chain risk from causing a security concern, is the preferred and least disruptive method of addressing supply chain risk. However, in those exceptional cases where mitigation is not possible, DHS does not have the capability to react swiftly while appropriately restricting disclosure of intelligence and other National security sensitive information.

DHS CYBER SUPPLY CHAIN RISK MANAGEMENT (C–SCRM)

In order to appropriately manage supply chain risks, stakeholders need increased visibility into, and understanding of, how the products and services they buy are developed, integrated, and deployed, as well as the processes, procedures, and practices used by ICT manufacturers and purveyors to assure the integrity, security, resilience, and quality of those products and services. The DHS Office of the Chief Information Officer (OCIO) has initiated work focused on establishing a C–SCRM effort executed Department-wide.

The effort will include a governance structure that will update existing policy and procedures for C–SCRM. Documentation will be developed that will align with current policies while providing programmatic subject-matter expertise to DHS stakeholders and risk owners. Integral to the success of these efforts will be the functions and capabilities to conduct vulnerability and threat identification and analysis. To accomplish this, a process will be established to produce timely supply chain risk assessments of companies, products, and services based on an analysis of publicly and commercially available information about the company and product, or service being purchased and information shared through liaisons with the U.S. intelligence community (IC) threat assessment centers and DHS Office of Intelligence and Analysis (I&A), as appropriate.

Working closely with NPPD and the DHS CPO, the initiative will develop education and training to ensure the effective use of the new authority. Guidance will also be provided to assist buyers in determining criticality, priority, and risk tolerance for the product or service to be purchased as well as assisting buyers and sellers with determining mitigation actions where supply chain risks have been identified.

The DHS CIO knows first-hand that all tiers of the supply chain are targeted by increasingly sophisticated and well-funded adversaries seeking to steal, compromise, alter, or destroy information and is committed to establishing a robust enterprise approach to better managing the risk and vulnerabilities associated with ICT components. Although DHS is investing in C–SCRM with the goal to broaden and further strengthen our approach, additional authority is needed to ensure that risk is assessed and mitigated in a timely manner, and that disclosure of intelligence sources and other information is restricted.

GOVERNMENT-WIDE CYBER SUPPLY CHAIN RISK MANAGEMENT (C–SCRM)

The administration has been working to establish a strategic statutory framework to protect our Federal supply chain by conducting supply chain risk assessments, creating mechanisms for sharing supply chain information, and establishing exclusion authorities—both within agencies and in a centralized manner—to be utilized when justified. Earlier this week, the administration shared its proposed legislation with Congress, the "Federal Information Technology Supply Chain Risk Management Improvement Act of 2018." We look forward to supporting the administration's work with Congress on the bill and strengthening our ability to help agencies execute Departmental missions in an environment of changing vulnerabilities and threats.

NPPD carries out the DHS Secretary's responsibilities to administer the implementation of Government-wide information security policies and practices (44 U.S.C 3553(b)). These statutory responsibilities include monitoring agency implementation; convening senior agency officials; coordinating Government-wide efforts; providing operational and technical assistance; providing, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies; and developing and overseeing implementation of binding operational directives, among other actions. DHS leverages the full range of authorities to address supply chain risks across the Federal Government.

DHS is working with the Department of Defense (DOD), the intelligence community, and other agencies to address key supply chain risks. In January 2018, NPPD established a C–SCRM initiative to centralize DHS's efforts to address risks to the ICT supply chains of Federal agencies, critical infrastructure owners and operators, and State, local, Tribal, and territorial governments. The mission of the C–SCRM initiative is to identify, assess, prevent, and mitigate risks associated with ICT product and service supply chains throughout the life cycle. Initially this initiative will focus on identifying and addressing supply chain risks related to the Federal Government's high-value assets (HVAs), or those assets, Federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to U.S. National security interests, foreign relations, the economy, or to the public confidence, civil liberties, or public health and safety of the American people. Additionally, DHS, in partnership with the General Services Administration, is working to bridge the gap between the procurement and ICT professional by providing acquisition professionals with awareness, training, and educational content to be available through the Federal Acquisition Institute.

Since 2017, NPPD now requires Continuous Diagnostics and Mitigation (CDM) vendors to complete a SCRM questionnaire as part of their application to place a product on the CDM-approved products list. The questionnaire provides information to agencies about how the vendor identifies, assesses, and mitigates supply chain risks in order to facilitate better-informed decision making. The information is intended to provide visibility into, and improve the buyer's understanding of, how the products are developed, integrated, and deployed; as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of those products.

INTELLIGENCE SUPPORT AND COUNTERING ILLICIT ACTIVITY

Despite the gaps in DHS's ability to use intelligence information to support its procurement actions, DHS has a variety of efforts currently underway within our existing authorities to help address these risks. One such effort is the strengthening of our counterintelligence capabilities. These capabilities include resources within DHS I&A as well as strengthening partnerships across other key components of the U.S. IC. Additionally, DHS components, including the U.S. Secret Service, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement, play a critical role in identifying and disrupting illicit activity impacting supply chain risk. In collaboration with the Federal Bureau of Investigation, and the Departments of State, Treasury, Commerce, and Defense, we are actively leveraging our

individual and collective authorities to counter malicious actors and mitigate supply chain risks.

CONCLUSION

As DHS looks at the current threat landscape and the risk posed by increasingly sophisticated adversaries, we appreciate the committee's interest in supply chain risk management and look forward to working with the Members and your staff on these issues. Thank you for the opportunity to testify before the subcommittees. We are happy to answer any questions you may have.

Mr. KING. Thank you very much, Ms. Correa. I appreciate that.

Our second witness, Dr. John Zangardi, is the chief information officer for DHS. Previously, Dr. Zangardi served as the DOD principal deputy chief information officer and later the acting chief information officer. Dr. Zangardi's background includes acquisition, policy, legislative affairs, resourcing, and operations. He is a retired Naval flight officer and served in a variety of command and staff assignments.

The Chair now recognizes Dr. Zangardi. Thank you for being here today.

STATEMENT OF JOHN ZANGARDI, CHIEF INFORMATION OFFICER, OFFICE OF THE CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. ZANGARDI. Chairman King, Chairman Perry, Ranking Member Correa, Ranking Member Rice, and Members of the subcommittees, thank you for this opportunity to discuss ways to improve the Department of Homeland Security's ability to effectively manage supply chain risk.

The Department's Secretary has two primary sets of supply chain risk management responsibilities related to information and communications technology. In one set, the Secretary is responsible for procurement and supply chain risk management within DHS's information and communications environment. These responsibilities are carried out by DHS's chief procurement officer and the chief information officer.

In carrying out the other set of responsibilities, the Secretary of DHS, in consultation with the Office of Management and Budget, administers the implementation of Government-wide information security policies and practices. These responsibilities are carried out by the National Protection and Programs Directorate, or NPPD. My focus today will be on the supply chain risk management activities within DHS's information and communications technology environment.

Gaps exist in the Department's authority to use intelligence to support its procurement decisions when a significant supply chain risk cannot be mitigated. Mitigation is the preferred and least disruptive method of addressing supply chain risk. However, in those exceptional cases where mitigation is not possible, the Department needs the capability to react swiftly while appropriately restricting a disclosure of other National security-sensitive information.

The administration has been working to establish a strategic statutory framework to protect our Federal supply chain by conducting supply chain risk assessments, creating mechanisms for sharing supply chain information, and establishing exclusion authorities, both within agencies and in a centralized manner, to be

utilized when justified. We look forward to supporting the administration's work with Congress on the bill and strengthening our ability to execute mission in an environment of changing vulnerabilities and threats.

DHS needs flexibility while protecting the integrity of the procurement process. DHS will ensure important safeguards, such as requiring factual findings, written determinations, and concurrences by specified senior DHS officials are in place when the authority as proposed by the administration is used. We do not see using this authority to drive sole-source procurements. Competition, particularly in the IT space, is critical to ensure that DHS gets the best solution at the right cost.

DHS procedures will facilitate the timely assessment and mitigation of risk and preclude compromising DHS systems. It is key to ensure we have a strong process surrounding supply chain risk management. A strong supply chain risk management process needs to ensure that vendors are queried on supply chain risk process, there is awareness of the systems on the network and a rapid response to intelligence tippers, and there is a close working relationship with the component CIOs and CISOs, the chief procurement officer, the acquisition community, intelligence, and NPPD.

As the IT technical authority for DHS, my chief information security officer, or CISO, has initiated work to directly support and execute technical assessments, providing subject-matter expertise, and be the integration point for all enterprise supply chain management efforts.

In addition, this team will develop program documentation that will align with current policies and procedures while providing programmatic subject-matter expertise to DHS stakeholders and risk owners.

With the support of the DHS components and offices, my team will continue to focus on governance by enhancing policy, procedures, and compliance monitoring capability of SCRM activities, services, by providing supply chain risk management services such as informations and communications technology assessments and intelligence analysis reporting and operations, which includes the execution and implementation of supply chain risk management recommendations and selected IT acquisitions.

DHS recognizes the importance of establishing an enterprise approach to managing supply chain risk associated with information and communications technology. The supply chain for information and communications technology is complex. We have our work cut out for us. Working closely with our partners, we will find the best and most realistic approach for strengthening our supply chain.

The Department appreciates the support of this committee on these important matters. We will continue to work with Congress to address existing gaps in authority where resources are required to effectively manage supply chain risk within DHS.

Thank you for the opportunity to testify today, and I look forward to your questions.

Mr. KING. Thank you very much, Dr. Zangardi.

Our third witness, Ms. Jeanette Manfra, serves as the assistant secretary of the Office of Cybersecurity and Communications at the National Protection and Programs Directorate within DHS. Ms.

Manfra leads the Department's mission of strengthening the security and resilience of the Nation's critical infrastructure. Prior to this position, she served as the acting deputy under secretary for cybersecurity and the director for strategy, policy, and plans for the NPPD. Ms. Manfra served in the U.S. Army as a communications specialist and a military intelligence officer. I now recognize Ms. Manfra for an opening statement. Thank you.

STATEMENT OF JEANETTE MANFRA, ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. MANFRA. Chairman King, Chairman Perry, Ranking Member Correa, Ranking Member Rice, Members of the subcommittees, thank you for today's opportunity to discuss the Department's ongoing efforts to assess and mitigate supply chain risk.

The information and communications technology supply chain is a source of significant risk. The globalization of our supply chain results in component parts, services, and manufacturing from sources distributed around the world. Vulnerabilities in technology can be created intentionally or unintentionally through a variety of means, including deliberate mislabeling and counterfeits, unauthorized production, tampering, theft and insertion of malicious software or hardware. If these risks are not detected and mitigated, the result is adverse impacts to essential Government or critical infrastructure systems.

The Office of the Director of National Intelligence acknowledges that the United States is under systemic assault by foreign intelligence entities, who target the equipment, systems, and information used every day by Government, business, and individual citizens. Our adversaries are able to use the supply chain's complexity to obfuscate their efforts to penetrate sensitive research and development programs, steal intellectual property and personally identifiable information, insert malware into critical components and mask foreign ownership, control, and/or influence of key providers of components and services.

Cyber supply chain risk management requires addressing product security throughout its life cycle, including design, development, acquisition, distribution, deployment, maintenance, and product retirement. Current law governing information security for Federal information resources requires agencies to implement an agency-wide information security program that ensures that information security, including supply chain security, is addressed throughout the life cycle of each agency information system.

At the National Protection and Programs Directorate, or NPPD, we carry out the Secretary's responsibilities to administer the implementation of Government-wide information security policies and practices and to coordinate the overall Federal effort to enhance the security and resilience of our Nation's critical infrastructure. These statutory responsibilities for Federal agencies include monitoring implementation, convening senior officials, coordinating Government-wide efforts, providing operational and technical assistance, providing, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents, and developing

and overseeing implementation of binding operational directives, among other actions. We leverage the full range of these authorities to address supply chain risks across the Federal Government.

In January 2018, we at NPPD established a cyber supply chain risk management program to facilitate National efforts to address risks to the information and communications technology supply chains of Federal agencies, critical infrastructure owners and operators, and State, local, Tribal, and territorial governments. We are working with DOD, the intelligence community, and other agencies in these efforts.

Initially, this program is focusing on identifying and addressing supply chain risks related to the Federal Government's high-value assets. Additionally, in partnership with the General Services Administration, we are working to bridge the gap between procurement and information technology professionals by providing awareness, training, and educational content through the Federal Acquisition Institute. Through the continuous diagnostics and mitigation program, NPPD procures cybersecurity tools to deploy inside Federal agency networks.

Since 2017, NPPD has required CDM vendors to complete a supply chain risk management questionnaire as part of the product approval process. The questionnaire provides information to agencies about how the vendor identifies, assesses, and mitigates supply chain risks in order to facilitate better-informed decision making. The information is intended to improve the buyer's understanding of how the products are developed, integrated, and deployed as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of those products.

Before closing, I would note that this administration is working to establish a strategic framework to protect our Federal supply chain by conducting supply chain risk assessments, creating mechanisms for sharing supply chain risk and mitigation information, and establishing exclusion authorities, both within agencies and in a centralized manner, to be utilized when justified.

As the Department works to address the risk posed by increasingly sophisticated adversaries, we appreciate the committee's interest in this topic and the work that you have done and look forward to working with Members and your staff on these issues.

Thank you for the opportunity to testify, and I look forward to your questions.

Mr. KING. Thank you, Ms. Manfra, I appreciate that.

Our fourth witness is Mr. Gregory Wilshusen, the director of information security issues at the U.S. Government Accountability Office.

Mr. Wilshusen leads information security-related studies and audits of the Federal Government. He has over 30 years of auditing, financial management, and information system experience.

The Chair now recognizes Mr. Wilshusen for his opening statement. Thank you.

STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR OF INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Thank you. Chairman King, Chairman Perry, Ranking Members Rice and Correa, and Members of the subcommittee, thank you for the opportunity to testify at today's hearing on the Homeland Security supply chain.

Information technology systems are essential to the operations of the Federal Government. These systems are created and delivered through a complex global supply chain that involves a multitude of organizations, individuals, activities, and resources.

My testimony today provides an overview of the information security risks associated with the supply chains used by Federal agencies to procure IT systems. As requested, I will also discuss our 2012 assessment of the extent to which 4 National security-related agencies, the Departments of Defense, Justice, Energy, and Homeland Security, had addressed these risks. Before I do, if I may, I would like to recognize two members of my team, Jeff Knott and Rosanna Guerrero, for their efforts in developing my statement. Thank you.

In several reports issued since 2012, we have pointed out that the reliance on complex global IT supply chains introduces multiple risks to Federal information and communication systems. This includes the risk that these systems are being manipulated or damaged by leading foreign cyber threat nations, such as Russia, China, Iran, and North Korea. Threats and vulnerabilities created by these cyber threat nations, vendors, or suppliers closely linked to cyber threat nations and other malicious actors can be sophisticated and difficult to detect and, thus, pose a significant risk to organizations and Federal agencies.

As we reported in March 2012, supply chain threats are present at various phases throughout a system's development life cycle. These threats include insertion of harmful or malicious software and hardware, installation of counterfeit items, disruption in the production or distribution of essential products and services, reliance on unqualified or malicious service providers, and installation of software and hardware containing unintentional vulnerabilities.

These threats can be exercised by exploiting vulnerabilities that can exist at multiple points in the supply chain. Examples of these vulnerabilities include weaknesses in agency acquisition practices, such as acquiring products or parts from sources other than the original manufacturer or authorized reseller, incomplete information on IT suppliers, and installing hardware and software without sufficiently inspecting or testing them.

These threats and vulnerabilities can potentially lead to a range of harmful effects, including allowing adversaries to take control of systems, extract or manipulate data, or decrease the availability of resources needed to develop or operate systems.

In March 2012, we reported that the Departments of Defense, Justice, Energy, and Homeland Security varied in the extent to which they had addressed IT supply chain risks. Of the 4 agencies, Defense had made the most progress and had implemented several risk management efforts. Conversely, the other 3 agencies had

made limited progress addressing supply chain risk for their information systems.

We made 8 recommendations to Justice, Energy, and DHS to develop and document policies, procedures, and monitoring capabilities that address IT supply chain risk. The agencies subsequently implemented 7 recommendations and partially implemented the eighth. These actions better positioned the agencies to monitor and mitigate their supply chain risks.

In summary, the global IT supply chain introduces a myriad of security risks to Federal information systems that, if realized, could jeopardize the confidentiality, integrity, and availability of the systems and the information they contain. Thus, the potential exists for serious adverse impacts on an agency's operations, assets, and employees. These factors highlight the importance of Federal agencies appropriately assessing, managing, and monitoring IT supply chain risk as part of their agency-wide information security programs.

Chairman King, Chairman Perry, Ranking Members Rice and Correa, and other Members of the subcommittees, this concludes my oral statement. I will be happy to answer your questions.

[The prepared statement of Mr. Wilshusen follows:]

STATEMENT OF GREGORY C. WILSHUSEN

JULY 12, 2018

Chairmen King and Perry, Ranking Members Rice and Correa, and Members of the subcommittees: Thank you for the opportunity to testify at today's hearing on keeping adversaries away from the homeland security supply chain. As you know, Federal agencies and the owners and operators of our Nation's critical infrastructure rely extensively on information technology (IT) and IT services to carry out their operations. Securing this technology, its supply chain, and the information it contains is essential to protecting National and economic security.

Since 1997, we have identified Federal information security as a Government-wide high-risk area. In 2003, we expanded this high-risk area to include protecting systems supporting our Nation's critical infrastructure.[1]

My statement provides an overview of the information security risks associated with the supply chains used by Federal agencies to procure IT equipment, software, or services.[2] The statement also discusses our 2012 assessment of the extent to which 4 National security-related agencies—the Departments of Defense, Justice, Energy, and Homeland Security (DHS)—had addressed these risks.[3]

In developing this testimony, we relied on our previous reports,[4] as well as information provided by the National security-related agencies on their actions in response to our previous recommendations. We also considered information contained in special publications issued by the National Institute of Standards and Technology (NIST) and a directive issued by DHS. A more detailed discussion of the objectives, scope, and methodology for this work is included in each of the reports that are cited throughout this statement.

---

[1] See, most recently, GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO–17–317 (Washington, DC: Feb. 15, 2017).

[2] The National Institute of Standards and Technology (NIST) has defined the term "supply chain" as a set of organizations, people, activities, information, and resources that create and move a product or service from suppliers to an organization's customers. NIST defines "information technology" as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes, among other things, computers, software, firmware, and services (including support services).

[3] GAO, *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks,* GAO–12–361 (Washington, DC: Mar. 23, 2012).

[4] See GAO–12–361; *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations,* GAO–17–688R (Washington, DC: July 27, 2017); and *Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment,* GAO–13–625T (Washington, DC: May 21, 2013).

The work on which this statement is based was conducted in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

The design and development of information systems can be complex undertakings, consisting of a multitude of pieces of equipment and software products, and service providers. Each of the components of an information system may rely on one or more supply chains—that is, the set of organizations, people, activities, information, and resources that create and move a product or service from suppliers to an organization's customers.

Obtaining a full understanding of the sources of a given information system can also be extremely complex. According to the Software Engineering Institute, the identity of each product or service provider may not be visible to others in the supply chain. Typically, an acquirer, such as a Federal agency, may only know about the participants to which it is directly connected in the supply chain. Further, the complexity of corporate structures, in which a parent company (or its subsidiaries) may own or control companies that conduct business under different names in multiple countries, presents additional challenges to fully understanding the sources of an information system. As a result, the acquirer may have little visibility into the supply chains of its suppliers.

Federal procurement law and policies promote the acquisition of commercial products when they meet the Government's needs. Commercial providers of IT use a global supply chain to design, develop, manufacture, and distribute hardware and software products throughout the world. Consequently, the Federal Government relies heavily on IT equipment manufactured in foreign nations.

Federal information and communications systems can include a multitude of IT equipment, products, and services, each of which may rely on one or more supply chains. These supply chains can be long, complex, and globally distributed and can consist of multiple tiers of outsourcing. As a result, agencies may have little visibility into, understanding of, or control over how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to ensure the integrity, security, resilience, and quality of the products and services. Table 1 highlights possible manufacturing locations of typical components of a computer or information systems network.

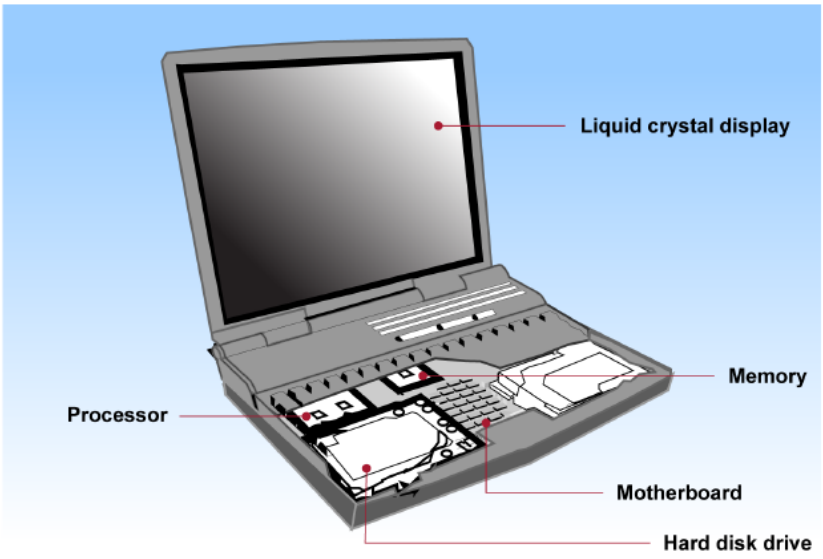
TABLE 1.—POSSIBLE MANUFACTURING LOCATIONS OF TYPICAL NETWORK COMPONENTS

Component	Possible Manufacturing Locations
Workstations	United States, Israel, Spain, China, Malaysia, Singapore, United Kingdom.
Notebook computers	United States, Israel, Spain, China, Malaysia, Singapore, United Kingdom.
Routing and switching	United States, India, Belgium, Canada, China, Germany, Israel, Japan, Netherlands, Poland, United Kingdom.
Fiber optic cabling	China, Malaysia, Vietnam, Japan, Thailand, Indonesia.
Servers	Brazil, Canada, United States, India, Japan, France, Germany, United Kingdom, Israel, Singapore.
Printers	Japan, United States, Germany, France, Netherlands, Taiwan, China, Malaysia, Thailand, Vietnam, Philippines.

Source: GAO analysis of public information/GAO–18–667T.

Moreover, many of the manufacturing inputs required for these components—whether physical materials or knowledge—are acquired from various sources around the globe. Figure 1 depicts the potential countries of origin of common suppliers of various components in a commercially available laptop computer.

Figure 1: Potential Origins of Common Suppliers of Laptop Components



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Source: GAO analysis of public information. | GAO-18-667T

Federal Laws and Guidelines Require the Establishment of Information Security Programs and Provide for Managing Supply Chain Risk

The Federal Information Security Modernization Act (FISMA) of 2014 requires Federal agencies to develop, document, and implement an agency-wide information security program to provide information security for the information systems and information that support the operations and assets of the agency.[5] The act also requires that agencies ensure that information security is addressed throughout the life cycle of each agency information system. FISMA assigns NIST the responsibility for providing standards and guidelines on information security to agencies. In addition, the act authorizes DHS to develop and issue binding operational directives to

[5] FISMA 2014 (Pub. L. No. 113–283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as *Title III, E-Government Act of 2002,* Pub. L. No. 107–347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this statement, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

agencies, including directives that specify requirements for the mitigation of exigent risks to information systems.

NIST has issued several special publications (SP) that provide guidelines to Federal agencies on controls and activities relevant to managing supply chain risk. For example,

- NIST SP 800–39 provides an approach to organization-wide management of information security risk, which states that organizations should monitor risk on an on-going basis as part of a comprehensive risk management program.[6]
- NIST SP 800–53 (Revision 4) provides a catalogue of controls from which agencies are to select controls for their information systems. It also specifies several control activities that organizations could use to provide additional supply chain protections, such as conducting due diligence reviews of suppliers and developing acquisition policy, and implementing procedures that help protect against supply chain threats throughout the system development life cycle.[7]
- NIST SP 800–161 provides guidance to Federal agencies on identifying, assessing, selecting, and implementing risk management processes and mitigating controls throughout their organizations to help manage information and communications technology supply chain risks.[8]

In addition, as of June 2018, DHS has issued one binding operational directive related to an IT supply chain-related threat. Specifically, in September 2017, DHS issued a directive to all Federal Executive branch departments and agencies to remove and discontinue present and future use of Kaspersky-branded products on all Federal information systems.[9] In consultation with interagency partners, DHS determined that the risks presented by these products justified their removal.

Beyond these guidelines and requirements, the *Ike Skelton National Defense Authorization Act for Fiscal Year 2011* also included provisions related to supply chain security. Specifically, Section 806 authorizes the Secretaries of Defense, the Army, the Navy, and the Air Force to exclude a contractor from specific types of procurements on the basis of a determination of significant supply chain risk to a covered system.[10] Section 806 also establishes requirements for limiting disclosure of the basis of such procurement action.

IT SUPPLY CHAINS INTRODUCE NUMEROUS INFORMATION SECURITY RISKS TO FEDERAL AGENCIES

In several reports issued since 2012,[11] we have pointed out that the reliance on complex, global IT supply chains introduces multiple risks to Federal information and telecommunications systems. This includes the risk of these systems being manipulated or damaged by leading foreign cyber-threat nations such as Russia, China, Iran, and North Korea.[12] Threats and vulnerabilities created by these cyber-threat nations, vendors, or suppliers closely linked to cyber-threat nations,[13] and other ma-

---

[6] NIST, *Managing Information Security Risk: Organization, Mission, and Information System View,* SP 800–39 (Gaithersburg, MD: March 2011).

[7] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations,* SP 800–53, Revision 4 (Gaithersburg, MD: April 2013).

[8] NIST, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,* SP–800–161 (Gaithersburg, MD: April 2015).

[9] DHS, *Removal of Kaspersky-Branded Products,* BOD–17–01 (Washington, DC: Sept. 13, 2017).

[10] The act defines "supply chain risk" as "risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."

[11] GAO–12–361, GAO–13–652T, and GAO–17–688R.

[12] The Office of the Director of National Intelligence has identified Russia, China, Iran, and North Korea as leading cyber-threat nations in its *Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Feb. 9, 2016 and Feb. 13, 2018).

[13] The Department of State Authorities Act, Fiscal Year 2017, defines "closely linked" as, with respect to a foreign supplier, contactor, or subcontractor and a cyber threat nation: (1) Incorporated or headquartered in the territory; (2) having ties to the military forces; (3) having ties to the intelligence services; or (4) the beneficiary of significant low-interest or no-interest loans, loan forgiveness, or other support of a leading cyber threat nation. The Act also included a provision for GAO to review the Department of State's (State) critical telecommunications equipment or services obtained from manufacturers or suppliers that are closely linked to the leading cyber threat nations. Based on GAO's open source review of generalizable samples of 52 telecommunications device manufacturers and software developers supporting the State's critical telecommunications capabilities and 100 of State's telecommunications contractors, GAO identified 16 companies—12 equipment manufacturers and software developers and 4 telecommunications contractors—with suppliers reported to be headquartered in cyber threat nations. All of

Continued

licious actors can be sophisticated and difficult to detect and, thus, pose a significant risk to organizations and Federal agencies.

As we reported in March 2012,[14] supply chain threats are present at various phases of a system's development life cycle. Key threats that could create an unacceptable risk to Federal agencies include the following.

- Installation of hardware or software containing malicious logic, which is hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. Malicious logic can cause significant damage by allowing attackers to take control of entire systems and, thereby, read, modify, or delete sensitive information; disrupt operations; launch attacks against other organizations' systems; or destroy systems.
- Installation of counterfeit hardware or software, which is hardware or software containing non-genuine component parts or code. According to the Defense Department's Information Assurance Technology Analysis Center, counterfeit IT threatens the integrity, trustworthiness, and reliability of information systems for several reasons, including the facts that: (1) Counterfeits are usually less reliable and, therefore, may fail more often and more quickly than genuine parts; and (2) counterfeiting presents an opportunity for the counterfeiter to insert malicious logic or back doors[15] into replicas or copies that would be far more difficult in more secure manufacturing facilities.[16]
- Failure or disruption in the production or distribution of critical products. Both man-made (e.g., disruptions caused by labor, trade, or political disputes) and natural (e.g., earthquakes, fires, floods, or hurricanes) causes could decrease the availability of material needed to develop systems or disrupt the supply of IT products critical to the operations of Federal agencies.
- Reliance on a malicious or unqualified service provider for the performance of technical services. By virtue of their position, contractors and other service providers may have access to Federal data and systems. Service providers could attempt to use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.
- Installation of hardware or software that contains unintentional vulnerabilities, such as defects in code that can be exploited. Cyber attackers may focus their efforts on, among other things, finding and exploiting existing defects in software code. Such defects are usually the result of unintentional coding errors or misconfigurations, and can facilitate attempts by attackers to gain unauthorized access to an agency's information systems and data, or disrupt service.

We noted in the March 2012 report that threat actors[17] can introduce these threats into Federal information systems by exploiting vulnerabilities that could exist at multiple points in the global supply chain. In addition, supply chain vulnerabilities can include weaknesses in agency acquisition or security procedures, controls, or implementation related to an information system. Examples of the types of vulnerabilities that could be exploited include:

- acquisitions of IT products or parts from sources other than the original manufacturer or authorized reseller, such as independent distributors, brokers, or on the gray market;
- lack of adequate testing for software updates and patches; and
- incomplete information on IT suppliers.

If a threat actor exploits an existing vulnerability, it could lead to the loss of the confidentiality, integrity, or availability of the system and associated information. This, in turn, can adversely affect an agency's ability to carry out its mission.

---

these suppliers were reported to be headquartered in China or, in one case, Russia. The data did not establish whether State's telecommunications capabilities were supported by equipment or software originating from suppliers linked to companies in GAO's samples. GAO did not identify any reported military ties, intelligence ties, or low-interest loans involving cyber threat nations among any of the suppliers. See GAO–17–688R.

[14] GAO–12–361.

[15] A "back door" is a general term for a malicious program that can potentially give an intruder remote access to an infected computer.

[16] Information Assurance Technology Analysis Center, *Security Risk Management for the Off-the-Shelf (OTS) Information and Communications Technology (ICT) Supply Chain, An Information Assurance Technology Analysis Center State of the Art Report,* DO 380 (Herndon, VA: August 2010).

[17] Supply chain-related threat actors include foreign intelligence services and militaries, corporate spies, corrupt government officials, cyber vandals, disgruntled employees, radical activists, purveyors of counterfeit goods, or criminals.

FOUR NATIONAL SECURITY-RELATED AGENCIES HAVE ACTED TO BETTER ADDRESS IT SUPPLY CHAIN RISKS FOR THEIR INFORMATION SYSTEMS

In March 2012, we reported that the four National security-related agencies (i.e., Defense, Justice, Energy, and DHS) had acknowledged the risks presented by supply chain vulnerabilities.[18] However, the agencies varied in the extent to which they had addressed these risks by: (1) Defining supply chain protection measures for Department information systems, (2) developing implementing procedures for these measures, and (3) establishing capabilities for monitoring compliance with, and the effectiveness of, such measures.

Of the four agencies, the Department of Defense had made the most progress addressing the risks. Specifically, the Department's supply chain risk management efforts began in 2003 and included:

- a policy requiring supply chain risk to be addressed early and across a system's entire life cycle and calling for an incremental implementation of supply chain risk management through a series of pilot projects;
- a requirement that every acquisition program submit and update a "program protection plan" that was to, among other things, help manage risks from supply chain exploits or design vulnerabilities;
- procedures for implementing supply chain protection measures, such as an implementation guide describing 32 specific measures for enhancing supply chain protection and procedures for program protection plans identifying ways in which programs should manage supply chain risk; and
- a monitoring mechanism to determine the status and effectiveness of supply chain protection pilot projects, as well as monitoring compliance with and effectiveness of program protection policies and procedures for several acquisition programs.

Conversely, our report noted that the other three agencies had made limited progress in addressing supply chain risks for their information systems. For example:

- The Department of Justice had defined specific security measures for protecting against supply chain threats through the use of provisions in vendor contracts and agreements. Officials identified: (1) A citizenship and residency requirement and (2) a National security risk questionnaire as two provisions that addressed supply chain risk. However, Justice had not developed procedures for ensuring the effective implementation of these protection measures or a mechanism for verifying compliance with, and the effectiveness of these measures. We stressed that, without such procedures, Justice would have limited assurance that its Departmental information systems were being adequately protected against supply chain threats.
- In May 2011, the Department of Energy revised its information security program, which required Energy components to implement provisions based on NIST and Committee on National Security Systems guidance. However, the Department was unable to provide details on implementation progress, milestones for completion, or how supply chain protection measures would be defined. Because it had not defined these measures or associated implementing procedures, we reported that the Department was not in a position to monitor compliance or effectiveness.
- Although its information security guidance mentioned the NIST control related to supply chain protection, DHS had not defined the supply chain protection control activities that system owners should employ. The Department's information security policy manager stated that DHS was in the process of developing policy that would address supply chain protection, but did not provide details on when it would be completed. In the absence of such a policy, DHS was not in a position to develop implementation procedures or to monitor compliance or effectiveness.

To assist Justice, Energy, and DHS in better addressing IT supply chain-related security risks for their Departmental information systems, we made 8 recommendations to these 3 agencies in our 2012 report. Specifically, we recommended that Energy and DHS:

- develop and document Departmental policy that defines which security measures should be employed to protect against supply chain threats.

We also recommended that Justice, Energy, and DHS:

- develop, document, and disseminate procedures to implement the supply chain protection security measures defined in Departmental policy, and

[18] GAO–12–361.

- develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

The 3 agencies generally agreed with our recommendations and, subsequently, implemented 7 of the 8 recommendations. Specifically, we verified that Justice and Energy had implemented each of the recommendations we made to them by 2016. We also confirmed that DHS had implemented 2 of the 3 recommendations we made to that agency by 2015.

However, as of fiscal year 2016,[19] DHS had not fully implemented our recommendation to develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protections. Although the Department had developed a policy and approach for monitoring supply chain risk management activities, it could not provide evidence that its components had actually implemented the policy. Thus, we were not able to close the recommendation as implemented. Nevertheless, the implementation of the 7 recommendations and partial implementation of the eighth recommendation better positioned the 3 agencies to monitor and mitigate their IT supply chain risks.

In addition, we reported in March 2012 that the 4 National security-related agencies had participated in interagency efforts to address supply chain security, including participation in the Comprehensive National Cybersecurity Initiative,[20] development of technical and policy tools, and collaboration with the intelligence community. In support of the cybersecurity initiative, Defense and DHS jointly led an interagency initiative on supply chain risk management to address issues of globalization affecting the Federal Government's IT. Also, DHS had developed a comprehensive portfolio of technical and policy-based product offerings for Federal civilian departments and agencies, including technical assessment capabilities, acquisition support, and incident response capabilities. The efforts of the 4 agencies could benefit all Federal agencies in addressing their IT supply chain risks.

In summary, the global IT supply chain introduces a myriad of security risks to Federal information systems that, if realized, could jeopardize the confidentiality, integrity, and availability of Federal information systems. Thus, the potential exists for serious adverse impact on an agency's operations, assets, and employees. These factors highlight the importance and urgency of Federal agencies appropriately assessing, managing, and monitoring IT supply chain risk as part of their agency-wide information security programs.

Chairmen King and Perry, Ranking Members Rice and Correa, and Members of the subcommittees, this completes my prepared statement. I would be pleased to answer your questions.

Mr. KING. You still had 17 seconds to go. Good job. Thank you very much, Mr. Wilshusen.

I appreciate all of you being here today. I now recognize myself for 5 minutes. A number of us on the panel believe that DHS should have powers similar to DOD, similar to section 806.

Now, I guess I would ask the three representatives from DHS how that would strengthen you if similar legislation was adopted for DHS? But also, looking back on it, it appears that DOD was given this authority in 2011, did not issue regulations until 2015, and I don't even know if they have begun to implement them yet. So if this authority is given to you, how quickly would you be able to implement it and how would it improve your capabilities? Ms. Correa.

Ms. CORREA. So, sir, I have looked at the authority, and I have also looked at the proposal that has been put before—the latest legislative proposal. We would act very quickly and swiftly to implement.

---

[19] GAO reviews agency actions to implement its recommendations and may decide to close a recommendation as not implemented if an agency has not implemented the recommendation within 4 fiscal years of GAO making the recommendation. Fiscal year 2016 was the fourth fiscal year after GAO made the recommendations to DHS in its March 2012 report.

[20] Begun by the Bush administration in 2008, the Comprehensive National Cybersecurity Initiative is a series of initiatives aimed at improving cybersecurity within the Federal Government. This initiative, which is composed of 12 projects with the objective of safeguarding Federal Executive branch information systems, includes a project focused on addressing global supply chain risk management.

We would look at our business process to see how we can immediately train our staff and ensure that they have a full understanding of what this authority grants us to do, and we would issue immediate guidelines and instructions, including to our employees but also to share with industry, on how we would use that authority. But the very specifics, the time line, I would have to go back and look at how quickly we could actually implement.

Mr. ZANGARDI. Sir, thank you. I concur with Soraya. The need for this type of capability or authority is important from a CIO's perspective. My responsibility that I have to take under consideration and work very hard every day is the security of the DHS network, just not for the headquarters but for the components.

Having the ability to react swiftly to make the right decisions with removal of network systems or IT systems that are threatening is very important for us in carrying out our mission. We will work very closely with the intelligence community and NPPD on tippers, so we know what is going on. My team will do the technical assessment and talk very closely with the chief procurement officer, to make sure the lines of communication and what we are doing is very clear and understandable.

Mr. KING. Ms. Manfra.

Ms. MANFRA. The only thing I would add is to just note that the administration proposal would be for this authority to be granted Government-wide. So in addition to DHS having this ability, we want all of the Executive branch to be able to have this authority and this capability.

Mr. KING. This is I guess the open question to you. Do you have sufficient personnel on board now to carry out your mission?

Ms. CORREA. I am sorry. The question was? I want to make sure I understood the question.

Mr. KING. Do you have sufficient personnel on board now to carry out this mission?

Ms. CORREA. To carry out this mission? From a procurement perspective, the answer is yes, because we would be relying on our contracting officers, our policy and legislative team, who actually implement any accompanying guidelines. We put out guides. We do this on a very regular basis. So the answer is yes, we have the staff that can do this right now.

Mr. KING. Doctor.

Mr. ZANGARDI. Sir, from a CIO perspective and with regards to my mission for protecting the DHS network, I feel that I have sufficient folks on board in my shop. I also feel that the communication between the technical folks and my CISO shop and the component chief information security officers and CIOs is more than adequate to carry this out.

Mr. KING. Ms. Manfra.

Ms. MANFRA. Our role would be different in that we wouldn't necessarily be in charge of implementing this authority for the Department. We are looking across the Federal Government and building an initiative to ensure that supply chain risk assessments are being done, that we are following up and potentially providing continuous monitoring.

We have just started building that program, as noted. We currently do only have 2 people solely identified for that, but we are

building that program and were recently appropriated some additional program dollars. So that program will be built over the next 2 years to get to full capacity.

Mr. KING. I am down to 40 seconds. Mr. Wilshusen, based on your studies of the departments, including DHS, over the years, if we did give 806 authority to DHS, how long do you think it would take them to implement it?

Mr. WILSHUSEN. That I wouldn't know exactly, but I would say that one of the key things with the 806 authority given to DHS is making sure that this committee and GAO and/or the inspectors general have an opportunity to review the process and the procedures that the Department implements in order to effect that particular capability and authority that it has. It is just making sure that one is able to review what DHS does in implementing it and making sure it is done in accordance with the law.

Mr. KING. Thank you. Miss Rice.

Miss RICE. Thank you, Mr. Chairman.

Ms. Correa, I would like to start with you. This hearing is about some of the threats we face from adversarial foreign governments. I think in order to counter these threats, we must first fully acknowledge them and their intentions. So, with that in mind, do you agree with the intelligence community's January 2017 assessment and the Senate Intelligence Committee's findings that Russia interfered in the 2016 election to benefit the Trump campaign?

Ms. CORREA. So, ma'am, I am not intimately familiar with that information. What I can tell you is that I agree that we have to have the authorities in place——

Miss RICE. OK, I have to stop you there.

Ms. CORREA. OK.

Miss RICE. In your position, you are saying you can't answer this question?

Ms. CORREA. Not directly, no, ma'am.

Miss RICE. How about indirectly?

Ms. CORREA. That is what I was trying to do. That I believe we have to have the mechanisms in place to address these vulnerabilities and ensure that the threat assessments, the risks, the vulnerabilities are properly addressed through the procurement process.

Miss RICE. You are the chief procurement officer for the Department of Homeland Security, and you do not have an opinion about whether the Senate Intelligence Committee's findings and the entire intelligence community's findings that Russia interfered with the 2016 election to support President Trump, you have no opinion about that?

Ms. CORREA. Ma'am, unfortunately, no, not with respect to this.

Miss RICE. That is frightening, frightening to me.

How about you, Doctor?

Mr. ZANGARDI. Yes, ma'am. Thank you for the opportunity to respond.

Miss RICE. Yes or no, do you agree with the findings?

Mr. ZANGARDI. Ma'am, I am here to testify on this authority.

Miss RICE. No, you are here to answer questions. You are talking about actions that all of you are taking on behalf of the Department of Homeland Security regarding interference, whether it is

procurement process or whatever it is. If we can't get people here, all four of you, to acknowledge that there was interference in the 2016 election, none of you should be in the positions that you are in to protect us in 2018 or 2020.

So yes or no, do you have an opinion about whether Russia interfered in the 2016 election, yes or no?

Mr. ZANGARDI. Ma'am, my responsibility is to protect the DHS network——

Miss RICE. Your responsibility is to answer the question. Yes or no? Say no.

Mr. ZANGARDI. Ma'am, I do not have an opinion.

Miss RICE. You have no opinion. Again, frightening.

OK, let's move on to Ms. Manfra. Yes or no, do you agree with the opinion of the entire intelligence——

Ms. MANFRA. I agree with the intelligence community assessment, ma'am, and I have said so publicly previously.

Miss RICE. Thank you.

Mr. WILSHUSEN. I would also have to agree with the Intelligence Committee, but, again, I haven't examined it.

Miss RICE. I appreciate your willingness to answer a question that everyone on the panel should be able to answer.

Despite warnings from the Federal Communications Commission, the Department of Commerce, the Department of Defense, and other intelligence agencies, President Trump publicly expressed support for the Chinese telecommunications company ZTE.

Ms. Correa, I will start with you. Have you discussed your concerns with the Chinese telecommunications companies with President Trump?

Ms. CORREA. No, ma'am, I have not had any discussions with the President.

Miss RICE. Have you discussed it with the Secretary of the Department of Homeland Security?

Ms. CORREA. No, ma'am. No, I have not.

Miss RICE. You are the chief procurement, head of procurement?

Ms. CORREA. That is correct.

Miss RICE. Again, a frightening, frightening answer. Do you think you should speak to her about that?

Ms. CORREA. Ma'am, I work in conjunction with my colleagues and look at what the risks are——

Miss RICE. OK. So again, you are not going to answer the question.

Doctor, how about you, have you had any discussions about——

Mr. ZANGARDI. No.

Miss RICE. Do you have any concerns about the President's approach to ZTE, whatever his motivations are? We don't even have to go into them. Do you, in your position, have concerns about the President's stated position about ZTE, yes or no?

Mr. ZANGARDI. Ma'am, I have made sure that the network has no ZTE equipment on it.

Miss RICE. OK. So I am going to answer for you. That would be yes, you do have concerns?

Mr. ZANGARDI. Ma'am, my responsibility is for the network for DHS. I have ensured that the appropriate steps have been taken to preclude the use of equipment——

Miss RICE. So is there a reason why you can't say, answer a question in a way that might come across as being critical of the President? Is there a reason? Because I have never heard an inability from Ms. Correa and you to answer a simple yes-or-no question. So I am just wondering why you can't or won't.

Mr. ZANGARDI. Ma'am, my position is to work and ensure that the network is safe every day, and that is what I do.

Miss RICE. OK. What is frightening to me is that people like you are in the positions that you are in, who will not make statements of fact that everyone in the intel community has made.

Mr. Chairman, I thank you for your indulgence. I want to thank at least the 2 of you for being willing to answer what I think is a pretty simple question.

Thank you, Mr. Chairman.

Mr. KING. Thank you, Miss Rice.

Without getting into a debate—we can have it—first of all, it was not only composed of the intelligence community. It was the FBI and the CIA and DNI agreed in part. The other 14 did not take a position. There are legitimate questions about the extent of the involvement. I have no doubt there was meddling. We can debate it in another forum.

But having been through 65, 70 witnesses on the Intelligence Committee on this, it is not as clear as you may think as far as who they were favoring. There is no doubt there was meddling. But, again, it was only Brennan and Comey who agreed in full with that recommendation.

Mr. Perry.

Mr. PERRY. Thanks, Mr. Chairman.

I thank the witnesses for their testimony in answering some questions for us here. We are trying to get to the process, I think, and understand the process that you all go through and then find out how we, from a legislative and policy standpoint, can support your efforts. I think all of us, regardless of our political affiliation, don't want us to be on defense, don't want us to be reactive, want us to be proactive. I think that is what we are trying to get to. So I am trying to understand, and so my questions will be in that vein.

I am wondering what the DHS does to recognize and address that might already exist from products that are currently implemented or being used by the Department. How does that process work? Is there a continual reevaluation? I am thinking in the context of, you know, I have got two of these things and I have got a couple iPads and then desktop computers. I don't know what the schedule is, but on a pretty regular basis, you know, you have got to put in your code and update the software and all that stuff.

I will be honest with you, I have no idea what is happening in there. Something's happening, right? But I am hoping that you folks do and deal with that, and I am trying to understand how that works. If any one of you can answer that question, you know.

Mr. ZANGARDI. So, sir, you know, the current IT environment, as mentioned by another witness, is global. It is complicated. It is characterized by mergers and acquisitions in an ever-changing territory. So we have to work very hard to deal with that. So intelligence tippers is really a key way in which we start the process.

But more importantly, backing up within the whole acquisition process, we have to be involved at the very beginning as the program is being looked at to determine what systems, hardware components, software are going in there. Then we have developed a set of questions that have to be answered by every program.

We have also in our 4300A handbook developed a requirement for the components and the programs to develop policies related to supply chain management. So we have put those in place. My chief technical officer also vets all software against the State Department Committee on Foreign Investment in the United States. So these are embedded in the process as we are going toward to build something out.

So when we are notified about a risk, we look at it very closely from a technical point of view and determine if it is something that we should mitigate or remove. Removal takes time. It isn't an overnight process. So mitigation might involve something simple, like setting configurations or settings on a firewall.

My ESOC, or my Enterprise Security Operation Center, monitors this on a daily basis, looking for proxy signals. They monitor it daily and they will tip off if they find anything. We also do scans of our network and review the logs to ensure that nothing is, you know, askew. We work very closely with the CISOs and the component CIOs to ensure that the communication and standards are set.

I think part of your question deals with making sure that patches and other things are done to make sure the network is modern and upgraded to the current standards.

I view cyber hygiene as part and parcel of what I do. What I mean by cyber hygiene is ensuring that we are moving to modern operating systems, that our patching is done up to date and as soon as possible, and we are doing things like two-factor authentication and PKI.

Mr. PERRY. A lot of this is pretty technical for all of us, and we just—I hate to say it, but we are counting on you folks to have the technical expertise that is necessary.

Just out of curiosity, is DHS using software products with Russian-based security codes, such as Kaspersky, NGINX, Nordic ANT, Oxygen. I know I see a U.S. Secret Service request for DHS, 20 licenses from Oxygen, which is a Russian-based company. I am wondering, as a matter of protocol, does DHS look into—I imagine but I just want to be sure—relationships with the Russian government and—well, I will just leave it at that. If you can answer those questions.

Mr. ZANGARDI. So, sir, we do, and we take that into account as part of our technical assessment.

Mr. PERRY. Wait. You use those?

Mr. ZANGARDI. No, sir. You asked if I take that into account.

Mr. PERRY. OK. Yes, I just want to be clear. Right.

Mr. ZANGARDI. Yes, sir. So we take it into account. To make sure that it is part of our technical assessment, we consider the leadership of companies, where the company is based, those sort of qualitative factors, if you will.

Mr. PERRY. Do you know if you use any of the companies that I listed?

Mr. ZANGARDI. So, sir, I would have to take some of that as a QFR. For companies like Huawei——

Mr. PERRY. If you could, please, I would like to——

Mr. ZANGARDI. We do not have any Huawei or ZTE.

Mr. PERRY. I am happy to know that. Let me ask you this: Do you have a—does DHS have a requirement for the companies that you procure from that determines what security standard they have? Somebody is writing the code. Somebody is building the piece of equipment.

Does DHS have a requirement? Is there a minimum standard, a minimum security standard, background checks, et cetera, for the vendors or the producers? Is that something that is a part of what you do, Ms. Correa?

Ms. CORREA. Yes. Yes, sir. We actually vet the vendors, and we do have security standards that are specified in the actual solicitation as well as we include cyber hygiene clauses that are in the contracts and solicitations, as determined by the program offices and the CIO for inclusion that identify the different documentation and the standards that they have to meet, the training that they have to take, and the documents that they have to submit for us to validate that they are meeting the security standards.

Mr. PERRY. So one final question, with the Chair's indulgence. I wonder why it took so long to identify Kaspersky as a risk. It seemed to me—look, I come from Pennsylvania State government. We used Kaspersky throughout the State government as our security vendor, and through the complaints we kept using it until finally the Federal Government said, hey, there is a problem here. What took so long?

Ms. MANFRA. I can take that one, sir. I can't comment in detail about maybe why it took so long. I can tell you for when I was in my position, we looked in—and working with our intelligence analysis, looked into all the available information, both Classified and unclassified. It just came to a point that this was not a risk that we were willing to accept on our networks, and that is when we began the process of identifying tools available to remove them from our networks, and that led to the binding operational directive.

Mr. PERRY. So from a layman's standpoint, and I will close with this, it seems to me that people like me would think as soon as you see anything questionable, as soon as you see anything questionable from a country like Russia, China, Iran, or whatever that we are buying things like this from, that is a problem and we should terminate it. But I will close with that.

Thank you, Mr. Chair, and I yield.

Mr. KING. I would just join the gentleman in saying I know for a number of years we were hearing about Kaspersky, and I could never understand why we retained them, but in any event.

Mr. Correa, you are recognized.

Mr. CORREA of California. Thank you very much. I only have 5 minutes here, so let me try to be succinct and I would appreciate succinctness of your answers to my questions.

But, you know, recently the administration seems to have changed its position on Huawei and ZTE. Does that change your perspective, your view on the security threat that these products

pose on the supply chain? Meaning are we OK to buy them now? Are you going to buy them, or does this not change your perspective on the threat of ZTE and Huawei to our National security?

Ms. MANFRA. Sir, I am not exactly sure what you mean by changing positions. If you are referring to the Commerce act on ZTE——

Mr. CORREA of California. Yes.

Ms. MANFRA. So that is specific to ZTE, not Huawei. I would say, similar to what we discussed with Kaspersky, what we are looking at is less about the company and more about the laws that that company is compelled to follow. Both Chinese and Russian laws compel access that we are concerned about. So what we are doing is a risk assessment on companies that are subject to those laws and looking at the tools that we have available to us to address that risk.

Mr. CORREA of California. So when you say we are looking at the risk assessment, what would change of that risk assessment? It is my understanding that certain countries, Russia and China being two, are generally their style of economy, so to speak. Those companies are essentially controlled or are accountable to their central government. So that model of operating would never change, at least not in the short term.

So, I am trying to figure out, is I guess our classification of ZTE would change, what would change in your assessment of that company in how we would do business with them in the United States?

Ms. MANFRA. I want to separate the Commerce action on ZTE, which was a specific action for something that they violated, from our work in assessing risk. We can walk through some more details in the closed session. But just at a high level, we are looking at risk both now and in the future.

Mr. CORREA of California. Let me pull back, given we will go through that in closed session. But a bigger general question is, mitigation versus removal. Chain of command. You all operate under a chain of command, I presume. There are certain issues you need to bring forth to the committee, individuals that can respond to give you authority and so on and so forth, respond to your concerns.

Do you have the ability to jump above the chain of command should you feel that your issues are not being addressed to bring your concerns forth?

Ms. MANFRA. I haven't experienced that. I have the full support of the Secretary.

Mr. CORREA of California. The same question to all of you, yes/no also?

Mr. ZANGARDI. Yes, sir, I feel that I have the full support of the Secretary, and if there is an issue I can go up the chain of command. In fact, I have a dual reporting chain to the Secretary and to the under secretary for management.

Mr. CORREA of California. Ms. Correa.

Ms. CORREA. Similar to Dr. Zangardi. We are in the same reporting chain. So I report to the under secretary for management, who reports to the Secretary, and we do have the ability to raise concerns on any procurement-related matters.

Mr. CORREA of California. Would you say that your concerns are responded to affirmatively, meaning they are addressed?

Ms. CORREA. Yes. I can say yes, that my concerns are addressed.

Mr. ZANGARDI. Yes, sir.

Ms. MANFRA. Yes, sir.

Mr. WILSHUSEN. I am with GAO, and I certainly have the—can go up to the Comptroller General if I have a concern about any issue, but I haven't had that yet.

Mr. CORREA of California. I only have less than a minute and I wish I could delve into this a little bit more. But I guess my concern in the back of my head here I am thinking mitigation versus removing. You know what countries pose a threat. You know geopolitically the challenges out there. They are not new. They continue to be what they are.

So, to me, if you have a bad actor that has acted poorly or badly in the past, mitigation versus removing, I am not sure what the difference would be or why we would go back to dealing with certain firms, knowing the threats that they present to our country.

I have only 15 seconds. Let me make a closing statement and then you can answer, which is, you know, a lot of the stuff that has been going on, my thought in the back of my mind, at what point do these intrusions by these foreign governments represent a declaration of war on our country or not? Because a lot of the stuff they are doing is, you know, essentially posing a threat to us either today or in the future.

If you have any comments, Mr. Chair, I am going to stop my comments, but I would like to see if anybody can address my comments.

Mr. ZANGARDI. Sir, I would like to address the mitigation versus removal. So I am going to specifically talk to mitigation. That is preferred. Now, when we say mitigation, we are not talking about continued procurement of the particular hardware or software. What we are talking about is looking at it and going, oh, is the threat major or minor? Are there simple changes that I can make to some protocols or firewall settings that preclude it from doing whatever it was going to do? Then eventually remove it. Remember, everything has to be balanced in a cost-benefit sort-of equation. So if you could preclude it from being a threat with a simple mitigation, that is the preferred course of action.

Mr. KING. The gentleman's time has expired. Anybody else have anything on this? No, OK.

Mr. Donovan.

Mr. DONOVAN. Thank you, Mr. Chairman.

I am a little bit older than Chairman Perry, so I really don't understand this. I am not as old as Chairman King, but I am older than Chairman Perry. I am sure every one of these incredibly intelligent young folks behind you know a whole lot more about this than all of us combined. I was told once that there is more capability in this little machine than we had when we put a man on the moon in 1969. It is just amazing to me.

So, knowing that these items, whether it be a phone, whether it be a 9–1–1 system, the component parts are made elsewhere, sometimes they are even put together elsewhere, do we have in place something that will secure our security before we find a vulner-

ability, or do we wait for something to happen before we realize there is a problem with the 9–1–1 system in New York City or an iPhone that is being used by a Member of Congress?

Mr. ZANGARDI. So, sir, it is impossible to build a perfect defense. So we take prudent precautions to develop a security infrastructure that protects us against known and anticipated threats. We put that in place by looking at intelligence. We put that in place by understanding the technology.

I will take it a step further. Every time we sit down with a company—and we do meet with a lot of companies—we ask them about their supply chain management process, because what you are talking about is it is a global marketplace and for that phone you have there, the parts come from many different countries. So we have to understand how those suppliers of the hardware and software we need are building out their product. So that is an area we focus on.

As I mentioned earlier, we have procedures in our 4300 instruction that the components have to put this in place. We address this during the acquisition process by putting in place questions that the program office has to answer. My chief technical officer and my chief information security officer are very involved in the vetting of hardware and software components that we procure.

Ms. MANFRA. Sir, if I could just add, we model what we do in cybersecurity similar to what is practiced in physical security. So you don't just think about defense on your perimeter. You think about putting a lot of different alerts and warning capability. You think about what happens if an individual gets past one perimeter, how do we deal with them elsewhere? How do we secure very high-valuable assets in a highly secure way, put resources toward that, extra protections around that? That is similar to what happens in cybersecurity; it just becomes very technical.

So there are a lot of different ways that as we learn about what an adversary might be doing that is not necessarily related to patching a specific vulnerability where we can put what we call compensating controls in place.

So if we know that an adversary leverages legitimate credentials, so they steal somebody's password and username, for example, say through spear phishing or something like that—we know that is a very common way—that they will then masquerade as a legitimate user on a network. So what we do is then we design our network so they can't just move laterally across the entire system and have access to everything.

We also put in place identity monitoring as part of the CDM program, so that we can see if there a user behaving in a way that is not usual for that user to behave. That would alert a SOC, for example.

So there are a lot of different practices and technologies that are in place that can monitor for this sort of behavior that we can take action on. But, again, like Dr. Zangardi said, it is not perfect. You can never have that 100 percent security. We just want to have a lot of layers, and we want to raise the cost for the adversary to get to those highest-value targets that we are working to protect.

Mr. DONOVAN. I remember speaking with Jamie Dimon at JPMorgan, saying they are always concerned about the attack that

is already there laying dormant, not the ones that are trying now, and thinking about if when this phone was made if a component part was compromised and it is laying dormant in all of our phones right now and is that able to be detected. But I guess maybe we can talk about that in a closed setting as well.

Let me just ask, the Chairman was asking about 806 authority. Are there any other authorities? I mean, we are lawmakers. We are supposed to listen to you, you are supposed to tell us what you need, and then we are supposed to help you get there.

Are there any other authorities that would help you to secure, whether it be our equipment, our systems, that you would like to see Congress pass?

Ms. MANFRA. Congressman I can start with—no, I do not have a laundry list. Of course, the committee has worked very hard on the authorization for our Cybersecurity and Infrastructure Security Agency, which is a name change for our organization. We are hoping that we can get that passed into law.

We have the administration's legislation proposal, which would have the 806-like authority in addition to codifying sort-of the process by which the Department and other agencies would be able to continuously share this information and act on it. So that full legislative proposal is really what we are looking for.

Ms. CORREA. I would like to add that I am encouraged by that kind of legislation, because what I think is extremely important is that we have consistency across the Government in how we apply our rules and how we are going to look at this process.

I did want to touch on one other thing when Dr. Zangardi was speaking answering your previous question. We also include the assessment of what the technologies are that they are using, what the composition of the products are, and even the backgrounds of the companies as part of the proposal evaluation process. So there is a process there where we do look at companies.

Mr. DONOVAN. Mr. Chairman, my time has expired, so I yield back the time that I don't have anymore.

Mr. KING. Very generous of you.

I recognize the gentleman from Massachusetts, Mr. Keating.

Mr. KEATING. Thank you, Mr. Chairman.

Yesterday, we had a hearing in full Committee on Homeland Security about what the Department is doing to try and help our local and State election apparatus to protect itself from a cyber attack. The attack was obviously the attack that our intelligence community has told us that President Putin, the Russian government, aspired to do and did, indeed, do against our country.

So I am sitting here and I am saying, we are trying to reach out to our local and State election commissioners or secretaries of state, saying, we are here to help you prevent against this attack. We are the Department of Homeland Security and we have grants to do this.

So how could you possibly expect them to take it seriously, Ms. Correa, if the chief procurement officer for the U.S. Department of Homeland Security, and Mr. Zangardi, as the chief information officer, sit here in a public committee the very next day, the very next day, and are saying, well, we can't tell you this happened. How can that be taken seriously? What do you say? Would you have that

same comment to all our election commissioners and secretaries of state and say, you know, we can't tell you that that is happening? We are not going to publicly admit that. Ms. Correa? No, Ms. Correa.

Ms. CORREA. OK. Sir, what I am here to do is try to identify how we can safeguard the procurement process to ensure that there are no bad actors out there and that we address any risks of vulnerability.

Mr. KEATING. You are not prepared to say who did it?

Mr. ZANGARDI. No, sir, I am not.

Mr. KEATING. You know, I sat here through the last Congress with many of my colleagues saying, boy, we can't go get these radical extremists unless we call them by name. But you are not calling them by name, the people that gave a hostile attack on our country's democracy. It is the same thing I heard all through the last Congress.

It is just beyond me how we are being expected to be taken seriously, the Department is expected to be taken seriously when you won't even admit it publicly when we are trying to prevent, less than 4 months away, another attack.

I just have a question on ZTE now. Mr. Zangardi said, well, we are not going to consider any ZTE products or apparatus. But I was listening to Ms. Manfra, who said, well, we really look at the technical side and we evaluate it from that, regardless of what the product would be, to see if it is safe.

Don't you think that it should be automatically excluded from any procurement, not because of the technical ability of the product, but because they twice broke the law on sanctions against our country, again, with hostile countries like Iran, North Korea? Isn't that enough by itself to say, no matter how much it is technically reviewed, how much we feel comfortable with it, can you sit here and say, we are not going to under any circumstances use any ZTE products for Homeland Security procurement? Can you say that, Mr. Zangardi, without qualification?

Mr. ZANGARDI. So my intent is to keep ZTE hardware off our network.

Mr. KEATING. No, not your personal intent, but yes or no, you are not going to do it. You are not going to use their products. They have twice broken the law.

Mr. ZANGARDI. We do not use their product and it is based upon a technical assessment.

Mr. KEATING. Well, obviously, you are not using it now. But now that things have changed, can you say you will exclude it, period, going forward?

Mr. ZANGARDI. So our decisions need to be based on risk and based on a technical——

Mr. KEATING. So it is not based on their actions. OK. I think we need to separate the question.

Quickly, Mr. Wilshusen. The conclusion in your report dealt with the serious adverse impacts in risks here. Can you give us like what you think are among the most serious quickly? This is pretty serious stuff.

Mr. WILSHUSEN. Sure. If an adversary is able to install malicious software or hardware into an information system, they may be able

to extract or change, modify, even delete very sensitive information that may be residing on that system.

That, of course, depends upon the system and what type of information it contains on that system. That could be personally identifiable information, proprietary information, or National security, public health——

Mr. KEATING. National security and public health.

Mr. WILSHUSEN [continuing]. Related information.

Mr. KEATING. Thank you. Thank you. That is something for us all to think very carefully about in relation to my prior questions.

I yield back.

Mr. KING. The gentleman yields back.

Unless there are further questions, that concludes the public portion of the hearing. I ask unanimous consent that the subcommittees now recess for a brief period and reconvene the hearing in a closed session, pursuant to House rule XI(2)(g)(2), and we plan to reconvene in HVC–302 in 10 minutes.

Without objection, the subcommittees will recess.

[Whereupon, at 11:17 a.m., the subcommittees proceeded in closed session and subsequently adjourned at 12:28 p.m.]

APPENDIX

QUESTION FROM CHAIRMAN SCOTT PERRY FOR THE DEPARTMENT OF HOMELAND SECURITY

Question. Is the Department of Homeland Security currently using or in the process of procuring any software products with Russian-based source code (i.e. Kaspersky, NGINX, Nordacind, Oxygen)? If so, which ones and for what purposes?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR THE DEPARTMENT OF HOMELAND SECURITY

Question 1a. On April 24, Assistant Secretary Jeanette Manfra testified before the Senate Homeland Security and Government Affairs Committee that the surge in risk and vulnerability assessments for elections infrastructure created "a significant backlog in other critical infrastructure sectors and Federal agencies" waiting for similar assessments. The President's 2019 budget did not request an increase in resources sufficient to overcome this backlog.

Are more resources necessary to support the increased requests from State and local governments without delaying other assessments?

Answer. Response was not received at the time of publication.

Question 1b. What is the current RVA backlog? What is the prognosis for that backlog over the next calendar year?

Answer. Response was not received at the time of publication.

Question 2a. Based on the RVAs that DHS has carried out for State and local election officials, do most States and localities have the resources required to sufficiently mitigate their cybersecurity vulnerabilities (including equipment, staffing, training, and other components that factor into security)?

Answer. Response was not received at the time of publication.

Question 2b. If not, how big is the shortfall?

Answer. Response was not received at the time of publication.

Question 3. In the guidance NPPD issued to election officials on how to spend security funding, NPPD emphasizes the importance of deploying auditable voting systems.

How important is it that States have auditable paper trails and conduct post-election audits to verify the digital tallies of election results?

Answer. Response was not received at the time of publication.

Question 4. Much of DHS's mission requires close coordination with other agencies, especially with respect to cybersecurity.

How has the Department's ability to synchronize its cyber mission with other agencies been affected by the elimination of the Cybersecurity Coordinator position and the recent high rate of turnover at the National Security Council?

Answer. Response was not received at the time of publication.