Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security	)	
Threats to the Communications Supply	)	WC Docket No. 18-89
Chain Through FCC Programs	)	
	)	

COMMENTS OF RURAL BROADBAND ALLIANCE

David A. LaFuria
Lukas, LaFuria, Gutierrez & Sachs, LLP
8300 Greensboro Drive, Suite 1200
Tysons, VA 22102
(703) 584-8666
dlafuria@fcclaw.com
Attorney for Rural Broadband Alliance

June 1, 2018

TABLE OF CONTENTS

SUMMARY

All network operators in the United States have an obligation to meet security threats by following industry best practices and maintaining appropriate security measures for hardware, software, and other physical assets, including employees and contractors.

The Commission's main proposal is to limit the use of federal universal service support in networks where equipment or services are provided from a suspect source.

These comments have a singular focus: If there is agreement that equipment made by certain Chinese companies presents a national security threat, what constructive steps can the Commission take, either alone or in conjunction with other agencies, to improve our national security?

RBA asked Domain5, a security consulting firm, to provide observations and recommendations for a set of industry best practices that will materially improve national security. These recommendations are discussed below and in the attached white paper.

In sum, there are a number of constructive steps that can be taken to improve our nation's security, much more so than simply barring USF to RBA carriers. RBA urges the Commission to convene industry and inter-agency work groups to develop these best practices.

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security	)	
Threats to the Communications Supply	)	WC Docket No. 18-89
Chain Through FCC Programs	)	
	)	

COMMENTS OF RURAL BROADBAND ALLIANCE

Rural Broadband Alliance ("RBA"), by counsel and pursuant to the Commission's Notice of Proposed Rulemaking ("NPRM") hereby provides comments in the above-captioned proceeding.[1]

I. Introduction.

Members of the RBA coalition are small wireless providers serving rural and remote areas in Alaska, Wyoming, Kansas, Colorado, Nebraska, Oklahoma, South Dakota, Utah, Tennessee, Kentucky, American Samoa.[2] Nearly all are original license holders dating back nearly thirty years, to the days when FCC licenses were awarded by lottery. All have grown their businesses through customer acquisition and retention, obtaining additional spectrum,

[1] Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, *Notice of Proposed Rulemaking*, FCC-18-42A1, WC Docket No. 18-89 (April 18, 2018). *See also*, 83 Fed. Reg. 19196 (May 2, 2018) (designating June 1, 2018 as the deadline for filing comments).

[2] RBA members include Union Wireless, Viaero Wireless, Bristol Bay Cellular, Pine Cellular Phones, Inc., SI Wireless, LLC, United Wireless Communications, and AST Telecom.

issuing debt, and working through various state and regulatory requirements, all while competing in the evolving wireless industry that has now become an oligopoly.

In each rural area served by RBA carriers, the public interest is well served by their presence. Each member represents that its network, its customer service, its pricing, and its overall quality of service is competitive with the "Big 4" carrier networks. RBA carriers attribute a significant portion of their success to the federal Universal Service Fund ("USF"), which provides critical support to build and maintain infrastructure in rural areas that would otherwise not receive services, or service quality, reasonably comparable to that which is available in their respective states' urban areas.[3]

As often acknowledged, the commercial wireless market is a game of scale, requiring constant investment in modernizing networks, network operations, and building alternative revenue streams.[4] In this respect, RBA carriers are in a different place from the Big 4 because they lack the purchasing power for virtually every business input, including but not limited to telecommunications equipment, handsets, towers, special access circuits, software licenses, and many more. Throughout the telecom supply chain, it is a fact of life that small carriers pay more on a per-unit basis for virtually every important thing they purchase. Accordingly, in order to compete, RBA carriers have squeezed every possible cost component and

[3] *See,* 47 U.S.C. § 254(c)(3).

[4] *See* Bahjat el-Darwiche, Pierre Péladeau, Christine Rupp, and Florian Groene, *2017 Telecommunications Trends*, (Price Waterhouse Cooper), at https://www.strategyand.pwc.com/trend/2017-telecommunications-industry-trends.

correspondingly lived with tight EBITDA margins that the nation's largest carriers and their shareholders would never tolerate.[5]

The largest cost component of a telecom network is infrastructure equipment, including the switching core, base stations, and transport equipment. Without the ability to purchase equipment at price points available to the largest carriers, and with thin margins in an increasingly competitive industry, RBA members have stayed in business by lowering costs, including for example, purchasing Chinese-manufactured network infrastructure equipment from competitive providers at price points not offered by other major vendors.

The NPRM seeks comment on issues such as the Commission's authority to act, how broadly the rule should be applied, compliance obligations, and how to enforce any adopted requirements. These comments have a singular focus: If there is agreement that equipment made by certain Chinese companies presents a national security threat, what constructive steps can the Commission take, either alone or in conjunction with other agencies, to improve our national security?

II. RBA Carriers Accept Conclusions Reached by the National Security Community that Protecting Our Nation's Telecommunications Infrastructure is a Critical Priority.

In its NPRM, the Commission properly noted Executive Branch orders, both recent and dating back many years, supporting the policy of the United States:

> to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and

[5] *See, e.g.*, *AT&T, Inc. 2017 Annual Report*, at 23 ("Our Consumer Mobility EBITDA margin was 39.9% in 2017….") found at, https://investors.att.com/~/media/Files/A/ATT-IR/financial-reports/annual-reports/2017/complete-2017-annual-report.pdf; *Verizon Communications Inc. 2017 Annual Report,* at 21 (Wireless Segment EBITDA Margin 44.1%) found at, https://www.verizon.com/about/sites/default/files/2017VerizonAnnualReport.pdf.

> civil liberties. We can achieve these goals *through a partnership with the owners and operators of critical infrastructure* to improve cybersecurity information sharing and *collaboratively develop and implement risk-based standards*.
>
> The Federal Government *shall work with critical infrastructure owners and operators* and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof.
>
> The Federal Communications Commission, to the extent permitted by law, is to exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies and SSAs as appropriate, on: (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) *working with stakeholders, including industry*, and engaging foreign governments and international organizations *to increase the security and resilience of critical infrastructure within the communications sector* and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends (emphasis added).[6]

None of the RBA carriers dispute conclusions reached by the intelligence community driving the Department of Homeland Security ("DHS") and related agencies to protect the nation from cyber intrusions and threats to our critical telecommunications infrastructure.[7] So,

[6] *See,* Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. *See also,* Executive Order 13800 § 2(b), 82 Fed. Reg. 22391, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017), https://www.whitehouse.gov/presidential-actions/presidential-executiveorder-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[7] *See*, NPRM at paras. 4-6.

at the outset, the RBA companies state unequivocally that they fully accept the need to comply with directives issued by the federal government that further the national interest in securing our telecommunications infrastructure.

In particular, RBA fully supports the excellent work done by the Communications, Security, Reliability and Interoperability Council VI ("CSRIC VI"), and especially Working Group 3 ("WG3"), which is examining network reliability and security risk reduction. In March of this year, WG3 issued a "Report on Best Practices and Recommendations to Mitigate Security Risks to Wireless Protocols," the first of three reports examining security risks to wireless networks, including 5G and IP-based protocols.[8] CSRIC's important work will assist carriers in working together to develop best practices that increase the resilience of our nation's telecom infrastructure. RBA fully expects that by the time CSRIC's work is completed and recommendations implemented, the security of our nation's networks will increase significantly from today's level.

In sum, RBA accepts that all network operators have an obligation to meet security threats by adopting industry best practices and maintaining appropriate security measures for hardware, software, and other physical assets, including employees and contractors. RBA carriers are ready, willing and able to work with the FCC to improve security.

[8] *See,* CSRIC VI Working Group Descriptions, at file:///C:/Users/dlafuria/Downloads/csric6wgdescriptions2-2018.pdf, and CSRIC VI Working Group 3: Network Reliability and Security Risk Reduction, Final Report (March 28, 2018) at https://www.fcc.gov/files/csric6wg3mar18pptx.

III. The Commission's Proposals Are Potentially Extraordinary in Scope.

The Commission seeks comment on its view that, "going forward, no USF support may be used to purchase or obtain any equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain."[9] While the desire to increase national security is entirely appropriate, the proposal's potential scope is extraordinarily broad, including a suggestion that the proposed rule might, "prohibit the use of any USF funds on any project where equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain is being purchased or obtained."[10]

To be clear, disqualifying a carrier from receiving any USF if that carrier uses any equipment or services from Huawei or ZTE would be devastating. It would prevent a carrier from using USF to, for example, (1) build a tower, (2) lease real estate, (3) purchase or lease backhaul links, or (4) purchase non-telecom equipment such as a truck. The practical effect of enforcing such a rule is that RBA carriers would need to tear out roughly $1 billion worth of gear currently used to provide mobile voice and broadband in America's rural areas well before the gear reaches its useful life span and can be depreciated.

Moreover, there are other consequences, both intended and unintended, that deserve to be thought out before any proposal is adopted. In this regard, RBA strongly urges the Commission to, as discussed above, *make this a partnership*, and *work with stakeholders* who

[9] NPRM at para. 13.

[10] NPRM at para. 16.

share the goal of improving our national security. There are ways to materially improve network security and RBA members are prepared to work with the FCC to take whatever steps are needed to do so.

In sum, if the Commission intends to leave most or all RBA members no choice but to tear out entire networks, then the result must be a measurable increase in the security of our nation's telecommunications and Internet infrastructure.

IV. The Current Proposal Will be Ineffective in Increasing Our Nation's Security.

To obtain a more thorough understanding of the threats, and advice on how best to protect US telecom and Internet infrastructure in a world where network equipment made in China makes up such a large proportion of the U.S. market, RBA has asked Domain5, a subsidiary of Federal Data Systems, Inc., to prepare a white paper. RBA asked for a discussion of the Commission's proposal and recommendations for constructive steps that could be taken to increase security in our nation's telecommunications networks.[11] Domain5 makes the following observations about the NPRM:

- The supply chain concerns do not address the fact that much of the network hardware, regardless of where it was finally assembled, may use internal components manufactured or sourced in China.
- Discouraging the use of hardware and software from two Chinese companies will have minimal effect in addressing the security concerns raised by the FBI and Intelligence Community.
- The FCC proposal does not address the integrity of the software used in the equipment or its supply chain. In many cases, there is significant software

[11] *See,* Domain5, *Advancing U.S. Telecommunications Network Security: A Response to FCC Notice of Proposed Rulemaking in the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs* (May 30, 2018) at Exhibit 1. Domain5 is comprised of intelligence experts with deep knowledge of national security issues, including those discussed here.

development conducted in China, as well as complete manufacture of entire assemblies.

- Nation state actors do not need to solely rely on their ability to compromise the equipment used in U.S. telecommunications networks to adversely affect the security of those networks. There already exist significant vulnerabilities which place the security of U.S. communication networks at risk. For example, the inherent vulnerabilities in the Signaling System 7 (SS7) protocol could provide a nation-state actor with the ability to attack U.S. communications networks without having to compromise network hardware.

In order to move forward constructively, it must be established as fact that eliminating all China-sourced equipment currently held by RBA carriers would take only a tiny fraction of such equipment out of the country. A significant portion of telecommunications and Internet equipment currently operating our nation's communications networks was manufactured in Chinese factories, some controlled by Huawei/ZTE, under "white label" agreements with brand name equipment suppliers. RBA-members have a small fraction, surely less than 1% of the nation's telecommunications and Internet infrastructure equipment sourced from China.

Accordingly, before denying federal universal service support to RBA members, the Commission must come to grips with the fact that some substantial portion of all major communications networks has the same issue.[12] Denying federal USF to RBA members while at the same time allowing a substantial percentage of the equipment in use by RBA's competitors to remain does nothing for our nation's security and is unfair to RBA members.

[12] RBA suggests that the Commission send a data request to major equipment sellers here in the U.S., requesting information on what percentage of equipment sales are "white label" or similar arrangements. In order to make a good policy choice, the Commission needs to fully understand who makes what, to know how much equipment from China is being sold into the U.S. market.

Domain5 also notes that a determined state attacker does not need to have telecommunications or Internet equipment located inside the US, or even a person physically present in the US. Again, having equipment manufactured solely in the US (if that were possible) does not eliminate the vast majority of attack vectors.

With respect to the supply chain, a hostile actor's access to any point in the worldwide equipment supply chain presents far greater risks to our security than the small fraction of equipment currently in use in RBA networks. Telecom gear made by all companies is comprised of component parts manufactured around the world and oftentimes assembled in China. Every single part in every single facility, and every shipping facility along the way, is subject to being altered by every person with access to that part. The supply chain issue is enormous, and it exists irrespective of whether RBA members stop using their current equipment.

Domain5 states that recommendations made through the CSRIC process discussed above must be implemented, in large measure to prevent the exploitation of SS7 network infrastructure. Domain 5 strongly supports the FCC's recent request for comment on SS7 security best practices to ensure that the potential vulnerabilities and their consequences are addressed.[13] In addition, Domain5 recommends adoption of the following Security-by-Design best practices that came out of CSRIC Working Group 6:[14]

- CSRIC recommends that security by design/supply chain risk management programs may be appropriately considered and addressed, among other topics, at annual in-person meetings that were contemplated as part of CSRIC IV, Working Group 4's

[13] See, *Public Safety and Homeland Security Bureau Requests Comment on Implementation of Signaling System 7 Security Test Best Practices*, DA 18-333 (released April 3, 2018).

[14] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6 -Final Report: Best Practices Recommendations for hardware and Software Critical to the Security of the Core Communications Network, March 2016, Section 4.1*.

recommendations issued in March 2015. CSRIC recommends against implementing any new or additional regulations to address conformity to a particular supply chain risk assessment mechanism, or any type of written attestation to the same. In-person meetings will continue to foster the public-private sector collaboration encouraged in past CSRIC reports.[15]

- Communications sector members should use the best practices detailed in the [state which report[s]] report as a reference for working with vendors and suppliers to reduce the cybersecurity risk within the core network. Communications sector stakeholders which provide hardware and software products and services for the core network should reference the best practices to help ensure security-by-design principles are collaboratively addressed.[16]

- To enable network stakeholders to keep pace with the dynamic nature of threats to the core network, the voluntary approach embodied by the NIST Cybersecurity Framework (CSF) and available technical approaches to securing the core network should be leveraged to drive future development of security-by-design standards and best practices.[17]

- Public-private coordination and collaboration in advancing security-by-design should be encouraged and enabled in order to avoid inconsistencies in approaches to security-by-design. This also ensures increased intelligence sharing. Information sharing about supplier risk between government and industry is recommended as well.[18]

[15] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6-Final Report: Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Network, September 2016, Section 4.2.*

[16] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6 -Final Report: Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network, March 2016, Section 4.2.*

[17] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6 -Final Report: Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network, March 2016, Section 4.2.*

[18] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6 -Final Report: Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network, March 2016, Section 4.2.*

V. Developing Constructive Policies That Make Our Nation Safer.

In addition to adopting CSRIC recommendations, Domain5 provides a number of constructive recommendations, which can be adopted in part or in whole, to improve our security. Domain5 urges the Commission to embrace an approach to security that focuses on the interconnected nature of *people, processes, and technology*. The objective is to create an environment which obviates the need for carriers to "trust" vendors, but rather to more fully trust the technology solutions delivered for deployment into production networks. The four components of this recommendation, outlined below, are Independent Evaluation, Trusted Delivery, Vendor Personnel Security, and Additional Supporting Processes.

INDEPENDENT EVALUATION:

- Conduct deep independent analysis of all software and firmware (including source code) of all network gear that will be used by wireless carriers, utilizing trusted third-parties located in the U.S.
- Evaluate software development processes, build environments, compilation, and fielding
- Perform continuous testing for every new software release or patch, throughout the complete life-cycle deployment
- Conduct an independent evaluation of hardware designs and implementations.
- Ensure system level testing of all operational environments at every level through production deployment.
- Establish processes for Public Key certificates used for digitally signing the software.

TRUSTED DELIVERY:

- Implementation of a "Trusted Delivery" process that provides a wireless carrier a reasonable guarantee that software and hardware delivered by the vendor of the network gear exactly matches that which was evaluated by the independent evaluator.

- Preclude network gear vendors from delivering software directly to wireless carriers.

- Deliver lab and production software binaries to a U.S. independent evaluator where they are validated against binaries independently compiled by the evaluation team, and then forwarded to the wireless carrier via a secure means. A similar, but less intensive validation will be applied to hardware. This particular process greatly enhances supply chain security. Knowing in advance exactly what is supposed to be delivered and exactly what is deployed into the network, clearly protects against any sort of supply chain interdiction or the introduction of malicious functionality.

VENDOR PERSONNEL SECURITY:

- Take necessary actions to fully secure vendor Technical Assistance Center (TAC) transactions. This will include direct carrier management of network access events, monitoring of transactions, including complete packet capture of these transactions, and timely analysis of each transaction to verify that only authorized activities occurred.

- Limit the abilities of unvetted foreign nationals working within U.S. wireless carrier facilities to perform functions that could possibly compromise the security and integrity of network gear.

- Restrict foreign national access to non-fully evaluated software delivered by the trusted U.S. third-party.

- Prevent network gear vendors from bringing their own laptops onto the wireless carrier physical sites. Only laptops owned by, and in complete control of the wireless carriers will be permitted onsite. Where appropriate, carrier-provided laptops will be equipped with appropriate surveillance software to all comprehensive monitoring of vendor actions.

- Prohibit unevaluated hardware vendor software utilities onsite.

- Perform daily security reviews of wireless carrier laptops for unauthorized changes.

- Request FBI conduct records checks, if not a limited background investigation, of all foreign nationals that will be responsible for selecting, ordering, fielding, operating, maintaining or disposition of network gear.

- Transfer all functions performed by foreign personnel to U.S. citizens as soon as reasonably possible.

- Escort all foreign nationals and visitors to wireless carrier's physical sites in accordance with an established physical security plan.

ADDITIONAL SUPPORTING PROCESSES:

- Require digital signing of software.

- Validate digital signatures appended to the software and firmware used in network equipment.

- Perform certificate revocation.

- Distribute new software updates and patches into network gear securely.

- Integrate validated cyber threat analysis into routine and regular security processes.

The four part framework set forth above would create a telecommunications security environment that provides a supportable basis for carriers to trust the hardware and software presented for deployment in their networks and ultimately would materially improve our nation's security. RBA recognizes that there will be questions concerning the Commission's authority to impose some of the requirements above. However, if the Commission is serious about security, RBA urges the Commission to convene an interagency group of experts to examine these problems, determine what best practices should be implemented, under what authority, and how best to do so.

In sum, banning USF from being used in any network that has equipment from Huawei/ZTE will not increase our national security. If progress is to be made, we need a better way.

VI. Proposed Alternatives if the FCC Adopts its Proposal.

Should the Commission choose to adopt its proposal, RBA offers the following alternatives that could reduce the extraordinary burden placed on small carriers using Huawei/ZTE equipment.

First, a long runway. For any carrier, tearing out 4G LTE network is an enormous physical and economic challenge. For small carriers, such an action has heretofore been unthinkable, as replacing a network before its useful lifespan is exhausted and it is fully depreciated is an existential threat to the entire business. Accordingly, RBA asks the Commission for a consultative process to develop a rational runway, to allow existing equipment to be rolled off in an orderly fashion. Key to this is avoiding the possibility that entire networks will be torn out prematurely, a potentially catastrophic result.

Second, the Commission should conduct an intra-governmental search for funding to reimburse small carriers for the cost of replacing network equipment.

Third, the Commission should limit the order's scope by allowing carriers to purchase non-China equipment and services with USF. Some carriers can purchase towers and other network components not made by banned companies, while not tearing out entire networks. In other cases, where it is impossible to invest around the ban, the Commission should engage in a consultative process with the affected carrier and find ways to liberally grant waivers to avoid catastrophic results.

CONCLUSION

RBA fully supports efforts to improve national security, however the Commission's proposal to limit the use of USF in rural America is simply not a reasonable means to accomplish that critical goal. Included with these comments is a framework for improving security, set forth by experts in the field. RBA requests the Commission to not adopt its proposal to bar USF from any network where equipment or services provided by a suspect Chinese company are present, but rather to seek alternatives that produce substantial improvements in our nation's security.

Respectfully submitted,

RURAL BROADBAND ALLIANCE

By:_____
David A. LaFuria
Its Attorney

June 1, 2018

EXHIBIT 1

DOMAIN 5

Advancing U.S. Telecommunications Network Security: A Response to FCC *Notice of Proposed Rulemaking in the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, FCC 18-42

EXECUTIVE SUMMARY: The Federal Communications Commission (FCC) recently released a Notice of Proposed Rulemaking (NPRM), *in the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, FCC 18-42,* aimed at prohibiting wireless carriers from using support from the Universal Services Fund (USF) to purchase communications equipment or services from certain providers deemed a national security risk to communications networks or the communications supply chain.[1] This white paper is a response to the FCC's request for comments on the impact to small and rural wireless Tier III carriers that would result from the adoption of this NPRM.[2]

Prohibiting carriers from using USF support for communications equipment and services from specific vendors will not *alone* improve the security of U.S. critical communication networks. Rather, the restriction will disproportionately and negatively impact the daily operations of the U.S. critical communication networks, negatively affect consumers, municipal governments, and educational organizations across rural America. Not only will the cost to provide and maintain service for providers and consumers increase, the reliability of voice and text communications for rural Americans could also be put at risk. Further, the exclusion of any single vendor or set of vendors from participating in U.S. carrier network contracts does little to address the actual risks that form the basis of the FCC's primary threat concerns.

Currently, there is no disputing the validity of the FCC's concerns regarding the possibility that the Chinese Government might directly leverage the participation of Chinese telecom vendors in U.S. telecom infrastructure contracts for malicious purpose. That said, the premise of the NPRM does not address the supply chain issue. Specifically, the FCC ignores the very well documented fact that ALL major telecom vendors employ equipment and devices having significant development and manufacturing operations located in China, which could similarly be exploited by the Chinese Government.[3]

To assume that the threat is limited to Chinese vendors creates a framework wherein all other vendors are to some extent more trusted, leaving unabated a wide array of potential dangerous risks. A more effective approach would be to create a telecommunications security framework that precludes the need for telecom carriers to trust any vendor's technology solution. The outcome of such an approach would be a framework that provides a supportable basis for carriers to have significant trust in the hardware and software presented for deployment in their networks. Proposing a comprehensive solution and program of prioritized security implementation for U.S.

---

[1] Commission FCC 18-42, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, April 18, 2018.

[2] The views expressed in this white paper are those of the authors and do not necessarily represent a specific industry or vendor point of view.

[3] "China's penetration of U.S. supply chain runs deep, says report," Derek B. Johnson, *The Business of Federal Technology*, April 23, 2018; *State Department Telecommunications: Information on Vendors and Cyber Threat Nations*, U.S. Government Accountability Office, July 27, 2017.

communications networks that more completely mitigates threats and manages risk would better serve to carry out the FCC's stated goals.

SECURITY CHALLENGES FOR WIRELESS CARRIERS

The security threats posed by adversarial nation states are real and significant. There are potentially countless ways state-backed attackers could undermine the security of the U.S. telecommunication networks. In its NPRM, the Commission properly recognizes that a foreign government could have undue influence over the manufacturing of network products that will be used within U.S. communications networks and that this could adversely affect both network security and content traversing the networks.

As noted above, the U.S. Government is concerned about the use of products manufactured by two specific Chinese companies as well as the integrity of the supply chain for such products. However, the potential for Chinese influence goes well beyond the named companies. A February 14, 2018 CNN article quotes FBI Director Chris Wray's statements made before the Senate Intelligence Committee: "there is a risk of letting any company beholden to foreign governments inside the country's telecommunications infrastructure. It provides the capacity to maliciously modify or steal information," and "it provides the capacity to conduct undetected espionage."[4]

The NPRM does not address the verifiable issues associated with the supply chain vulnerabilities as well as other security issues. In particular:

- The supply chain concerns do not address the fact that much of the network hardware, regardless of where it was finally assembled, may use internal components manufactured or sourced in China.

- Discouraging the use of hardware and software from two Chinese companies will have minimal effect in addressing the security concerns raised by the FBI and Intelligence Community.

- The FCC proposal does not address the integrity of the software used in the equipment or its supply chain. In many cases, there is significant software development conducted in China, as well as complete manufacture of entire assemblies.

- Nation-state actors do not need to solely rely on their ability to compromise the equipment used in U.S. telecommunications networks to adversely affect the security of those networks. There already exist significant vulnerabilities which place the security of U.S. communication networks at risk. For example, the inherent vulnerabilities in the Signaling System 7 (SS7) protocol could provide a nation-state actor with the ability to attack U.S. communications networks without having to compromise network hardware.

In sum, a more comprehensive approach is needed that considers people, processes and technology.

[4] http://money.cnn.com/2018/02/14/technology/huawei-intelligence-chiefs/index.htm, accessed May 20, 2018; U.S. Senate Select Committee on Intelligence Hearing, Tuesday, February 14, 2018, 9:30am, https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-hearing-1

CSRIC as a Logical Starting Point to Improve Security

The foundational network architecture of our nation's telecommunications networks is extremely vulnerable due to its design, as well as implementation of the SS7 protocol. The pedigree of hardware and software does not mask the fact the architecture itself is vulnerable from any determined U.S. adversary. The FCC's Communications, Security, Reliability and Interoperability Council (CSRIC) Working Groups have identified numerous inherent vulnerabilities and deficiencies in the architecture of U.S. critical communications networks which could potentially make it vulnerable to nation-state attacks regardless of where the network hardware or software was manufactured.

In March 2017, CSRIC recommended that communications service providers implement certain security measures to help prevent exploitation of carrier SS7 network infrastructure. These recommendations were intended to increase awareness of SS7 signaling vulnerabilities and included risk mitigation strategies for the continued use of SS7. The recommendations also list measures, such as filtering and authentication of traffic between service provider networks, designed to promote the security of SS7 communications network traffic.

CSRIC examined security practices and made recommendations related to next generation protocols that will interact with SS7 and Session Initiation Protocol (SIP) infrastructures, such as Diameter, which is the protocol that supports the accounting and authorization responsibilities of SS7 in the all-IP network and most 3G and beyond wireless networks.[5] [6] We strongly support the FCC request for comment in Public Notice, DA 18-333, released on April 3, 2018, titled *Public Safety and Homeland Security Bureau Requests Comment on Implementation of Signaling System 7 Security Test Best Practices* (reply by June 4, 2018) to ensure that the potential vulnerabilities and their consequences are addressed.

The FCCs proposal to restrict USF support to communications providers using equipment and services from specific companies because of the potential security risks identified by the FBI and Intelligence Community does nothing to address the inherent vulnerabilities of U.S. communications networks already identified by the FCC, through CSRIC.

Operational Implications

The operational impacts resulting from the NPRM would also be significant. Tier III wireless providers serving rural and remote areas in Alaska, Wyoming, Kansas, Colorado, Nebraska, Oklahoma, South Dakota, Utah, Tennessee, Kentucky, and American Samoa will be particularly negatively affected if the USF is withdrawn. It will take small, remote and rural wireless providers at least five years to replace the hardware and software, to obtain professional support services, and retrain the technical staff needed to operate and maintain the new equipment. The logistics to replace the equipment before its projected End-of-Life is complicated by the fact that much of the equipment is located in remote and rural areas which are not physically accessible throughout the year due to weather and environmental concerns. The loss of USF would have serious negative implications for a small carrier's ability to provide reliable and high-quality services to their customers, which include municipal governments and schools. It would also require those providers to increase the price of their services. This will

[5] FCC Public Notice DA 18-333, *Public Safety and Homeland Security Bureau Requests Comment on Implementation of Signaling System 7 Security Best Practices,* April 3, 2018.
[6] FCC Public Notice DA 18-333, *Public Safety and Homeland Security Bureau Requests Comment on Implementation of Signaling System 7 Security Best Practices,* April 3, 2018.

seriously affect their competitive position in the marketplace. For some, it may not be economically viable to continue providing services to some of their customers without subsidy.

MAJOR TELECOMMUNICATIONS SECURITY INITIATIVES PROMOTED BY THE U.S. GOVERNMENT

The FCC has been working diligently for many years to address security issues with U.S. core and Radio Access Network (RAN) communications networks, in part through CSRIC. The CSRIC is composed of Subject Matter Experts (SMEs) from U.S. commercial industry and the federal government. One of CSRIC's responsibilities is to provide recommendations to the FCC on how to improve the reliability and security of the nation's telecommunications systems. The CSRIC established numerous working groups to address a wide range of topics of importance to the FCC.

For example, CSRIC V's Working Group 6 was tasked with providing recommendations to help ensure the security of the supply chain for critical communications infrastructure and to promote the use of security-by-design practices within the core public communications networks. The supply chain consists of several distinct segments—design and development, distribution, and maintenance—each of which has its own inherent risks and vulnerabilities.

Working Group 6 determined the most efficient way to address these concerns is in the form of voluntary recommendations and best practices designed to enhance the security of hardware and software in the core public communications network. In addition, Working Group 6 has been tasked with developing a means to assure the FCC and the public that the identified recommended security capabilities are being implemented by network equipment vendors. To provide this assurance, in a future report, this Working Group will identify voluntary mechanisms by which providers can demonstrate the success of these recommendations and best practices.[7]

CSIRC V's Working Group 6 defined the best practices for telecommunication service providers to manage their cybersecurity risks implementing hardware, software and technical services obtained from vendors, suppliers and system integrators for use within their respective infrastructures. Working Group 6 used input from the National Institutes of Standards and Technology (NIST) and the Department of Homeland Security (DHS) to assist in their analysis and developing recommendations.

Additionally, NIST has developed and published a *Cybersecurity Framework* in collaboration with SMEs throughout the U.S. Government and commercial industry. All U.S. federal agencies and departments are required to comply with the *NIST Cybersecurity Framework* and it is an excellent resource to help entities analyze their architectures from a cybersecurity viewpoint, establish a risk profile, and prioritize their mitigation efforts based on the severity of their findings.

CSIRC V's Working Group 6 used several documents from the NIST to assist them. These documents included, but were not limited to, the following:[8]

- *NIST Cybersecurity Framework*
- *NIST SP 800-53, Security and Privacy Controls for Federal Information systems and Organizations*

[7] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6 -Final Report: Best Practices Recommendations for hardware and Software Critical to the Security of the Core Communications Network,* March 2016, Section 3.1.
[8] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6 -Final Report: Best Practices Recommendations for hardware and Software Critical to the Security of the Core Communications Network*, March 2016, Appendix 1.

- *NIST SP 800-160, DRAFT System Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*
- *NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- *DHS "Build Security In" – Improve Security and software Assurance Tackle the CWE Top 25 Most Dangerous Software Errors*
- *Financial Services Information Sharing and Analysis Center (FSISAC). Appropriate Software Security Control Types for Third Party Service and Product Providers (version 2.1.3)*
- *ISO/IEC 20243:2015, Information Technology – Open Trusted Technology Provider TM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*
- *ISO/IEC 27002, Information Technology – Security Techniques – Code of practice for information Systems controls*
- *ISO/IEC/IEEE 15288.2015, Systems and software Engineering – Systems Lifecycle processes*
- *NDIA Engineering for System Assurance (version 1)*
- *Version 1.1, Open Group Trusted Technology Provider Standard (O-TTPS) Accreditation Program, Version 1.1*
- *Software Integrity Controls, An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain*
- *The Software Supply Chain Integrity Framework, Defining Risks and Responsibilities for Securing Software in the Global Supply Chain*

CSRIC Working Group 6 also identified the following security-by-design best practices:[9]

- **Governance, Risk Assessment and Risk Management.** Ensure that suppliers have an organizational security policy that governs design, development, and production of the products and services; nine specific best practices listed.

- **Access Controls.** Ensure that suppliers limit access to: 1) assets and associated facilities used to design, develop, and produce applicable solutions, and; 2) the products and services, to authorized users, processes and devices and limit access to only authorized activities and transactions' seven specific best practices listed.

- **Data Security.** Ensure that information and records (data) relevant to products and services residing on applicable solutions are managed to protect and ensure the confidentiality, integrity and availability of information; six specific best practices listed.

- **Maintenance.** Ensure that suppliers have in place mechanisms to ensure that: 1) performing maintenance and repair of relevant products and services in a timely manner, and; 2) approving, logging and performing remote maintenance of products and services in a manner that prevents unauthorized access.

- **Protective Technology.** Ensure that supplier's information resources that may impact applicable products and services are sufficiently hardened which may involve disabling unused networking or other computing

[9] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6 -Final Report: Best Practices Recommendations for hardware and Software Critical to the Security of the Core Communications Network, March 2016, Section 4.1.*

functionality. Supplier may also ensure that technical security solutions are managed to ensure the security and resilience of supplier's information resources relevant to products and services; four specific best practices listed.

- **Anomalies and Event Detection.** Ensure that: 1) Supplier has tools in place to detect anomalies and events relevant to products and services, and; 2) such events are analyzed to understand attack targets and methods.

- **Security Continuous Monitoring.** Ensure that supplier information system and assets relevant to products and services are monitored to identify cybersecurity events and verify the effectiveness of cybersecurity measures; six specific best practices listed.

- **Detection Processes.** Ensure that suppliers have in place detection processes and procedures for identifying security events that may impact products and services, e.g., intrusion detection or intrusion detection and prevention systems, that monitor traffic interacting with a sector member's information resources, are maintained to ensure timely awareness of anomalous events. This may include event detection and supplier should ensure they have a documented procedure to be followed in the event of an actual or suspected attack and promptly notify sector member whenever there is a successful attack upon, intrusion upon, unauthorized access to, loss to or other breach of sector member's information resources.

- **Response Planning and Communications.** Ensure that supplier has a documented process in place to remediate security vulnerabilities relevant to products and services to detected cybersecurity events and that response activities are coordinated with customers and external stakeholders (as appropriate), which may include support from law enforcement or other agencies.

- **Analysis and Mitigation.** Ensure that supplier is conducting analysis to ensure adequate response and support recovery activities relevant to products and services including determining the impact of the incident, forensics, and notifications as appropriate and that activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident or contain its impact.

- **Recovery Planning.** Ensure that suppliers have in place recovery processes and procedures covering the products and services that can be executed and maintained to ensure the timely restoration of relevant systems and assets affected by cybersecurity events.

The significant and comprehensive work of CSRIC and NIST to identify and address specific and substantive security concerns is the foundation for a whole-of-government and industry response to implement recommended best practices.

RECOMMENDATIONS TO ENHANCE THE SECURITY OF THE NATION'S TELECOMMUNICATIONS NETWORKS

Adopt the FCC CSRIC Working Group 6 Proposed Recommendations:

- "CSRIC recommends that security-by-design/supply chain risk management programs may be appropriately considered and addressed, among other topics, at annual in-person meetings that were

contemplated as part of CSRIC IV, Working Group 4's recommendations issued in March 2015. CSRIC recommends against implementing any new or additional regulations to address conformity to a particular supply chain risk assessment mechanism, or any type of written attestation to the same. In-person meetings will continue to foster the public-private sector collaboration encouraged in past CSRIC reports."[10]

- "Communications sector members should use the best practices detailed in the report as a reference for working with vendors and suppliers to reduce the cybersecurity risk within the core network. Communications sector stakeholders which provide hardware and software products and services for the core network should reference the best practices to help ensure security-by-design principles are collaboratively addressed."[11]

- "To enable network stakeholders to keep pace with the dynamic nature of threats to the core network, the voluntary approach embodied by the *NIST Cybersecurity Framework* (CSF) and available technical approaches to securing the core network should be leveraged to drive future development of security-by-design standards and best practices."[12]

- "Public-private coordination and collaboration in advancing security-by-design should be encouraged and enabled in order to avoid inconsistencies in approaches to security-by-design. This also ensures increased intelligence sharing. Information sharing about supplier risk between government and industry is recommended as well."[13]

The FCC directed CSRIC VI's Working Group 3 to recommend mechanisms to reduce the risks to network reliability and security, including: 1) best practices to mitigate the network reliability and security risks associated with the Diameter protocol, an industry standard for connecting and authenticating subscribers to mobile networks; 2) mechanisms to best design and deploy 5G networks to mitigate risks to network reliability and security posed by the proliferation of Internet of Things (IoT) devices, vulnerable supply chains, and open-source software platforms used in 5G networks and; 3) best practices and tools to improve reliability and reduce security risks in IP-based networks and protocols.[14]

ADDITIONAL RECOMMENDATIONS FOR CONSIDERATION

Although we fully support the recommendations proposed by the FCC CSIRC Working Groups 6 and 3, we believe there are several additional safeguards that more directly address the FCC's national security concerns and would have a positive impact on improving the security of U.S. communication networks, regardless of where the network hardware was manufactured, where the software was written or how professional services are provided. Network software and firmware are critical to the operation and security of wireless network equipment. There

[10] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6-Final Report: Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Network, September 2016, Section 4.2.*
[11] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6 -Final Report: Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network, March 2016, Section 4.2.*
[12] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6 -Final Report: Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network, March 2016, Section 4.2.*
[13] *CSRIC Secure Hardware and Software: Security-by-Design Working Group 6 -Final Report: Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network, March 2016, Section 4.2.*
[14] *CSRIC Working Group 3: Network Reliability and security Risk Reduction Final Report, March 28, 2018.*

is no such thing as zero risk or vulnerability when it comes to hardware and software security. Therefore, the best approach to risk management is an application of a comprehensive framework.

Over the past five years, many U.S. carriers have adopted a cybersecurity approach which focuses on the interconnected nature of **people, processes, and technology**. Most major international telecom vendors (including Huawei USA) have participated in the initiation of this methodology and in the network development. Allowed to mature, this security methodology has the potential to dramatically improve the security of national telecom infrastructure. Among the goals of this approach, is to create an environment which obviates the need for carriers to "trust" vendors, because there is no reasonable basis to do so. The desired outcome is an evidence-based solution that allows a carrier to more fully trust the technology solutions delivered for deployment into production networks. This proven methodology, integrated into a security program that also incorporates the CSIRC recommendations discussed above, would more likely support achievement of the desired FCC outcomes. The specific elements of this methodology that are relevant to achieving the stated FCC goals include the following:

Independent Evaluation:

- Conduct deep independent analysis of all software and firmware (including source code) of all network gear that will be used by wireless carriers, utilizing trusted third-parties located in the U.S.

- Evaluate software development processes, build environments, compilation, and fielding.

- Perform continuous testing for every new software release or patch, throughout the complete life-cycle deployment.

- Conduct an independent evaluation of hardware designs and implementations.

- Ensure system level testing of all operational environments at every level through production deployment.

- Establish processes for Public Key certificates used for digitally signing the software.

Trusted Delivery:

- Implementation of a "Trusted Delivery" process that provides a wireless carrier a reasonable guarantee that software and hardware delivered by the vendor of the network gear exactly matches that which was evaluated by the independent evaluator.

- Preclude network gear vendors from delivering software directly to wireless carriers.

- Deliver lab and production software binaries to a U.S. independent evaluator where they are validated against binaries independently compiled by the evaluation team, and then forwarded to the wireless carrier via a secure means. A similar, but less intensive validation will be applied to hardware. This particular process greatly enhances supply chain security. Knowing in advance exactly what is supposed to be delivered and exactly what is deployed into the network, clearly protects against any sort of supply chain interdiction or the introduction of malicious functionality.

Vendor Personnel Security:

- Take necessary actions to fully secure vendor Technical Assistance Center (TAC) transactions. This will include direct carrier management of network access events, monitoring of transactions, including complete packet capture of these transactions, and timely analysis of each transaction to verify that only authorized activities occurred.

- Limit the abilities of unvetted foreign nationals working within U.S. wireless carrier facilities to perform functions that could possibly compromise the security and integrity of network gear.

- Restrict foreign national access to non-fully evaluated software delivered by the trusted U.S. third-party.

- Prevent network gear vendors from bringing their own laptops onto the wireless carrier physical sites. Only laptops owned by, and in complete control of, the wireless carriers will be permitted onsite. Where appropriate, carrier-provided laptops will be equipped with appropriate surveillance software to all comprehensive monitoring of vendor actions.

- Prohibit unevaluated hardware vendor software utilities onsite.

- Perform daily security reviews of wireless carrier laptops for unauthorized changes.

- Request FBI conduct records checks, if not a limited background investigation, of all foreign nationals that will be responsible for selecting, ordering, fielding, operating, maintaining or disposition of network gear.

- Transfer all functions performed by foreign personnel to U.S. citizens as soon as reasonably possible.

- Escort all foreign nationals and visitors to wireless carrier's physical sites in accordance with an established Physical Security Plan.

ADDITIONAL SUPPORTING PROCESSES:

- Require digital signing of software.

- Validate digital signatures appended to the software and firmware used in network equipment.

- Perform certificate revocation.

- Distribute new software updates and patches into network gear securely.

- Integrate validated cyber threat analysis into routine and regular security processes.

CONCLUSION

The security of U.S. telecommunications networks is not entirely reliant of the pedigree of hardware and software. Security is best achieved through a balanced combination of managed secure technology, people, and processes; all three components are necessary to enhance security. We fully support the FCC's goal of advancing and improving the security of U.S. communications networks. In addition, we strongly advocate carrier implementation recommendations adopted by CSRIC Working Groups 6 and 3 to improve the security of their telecommunications infrastructures. However, the FCC's proposal to eliminate specific vendors by denying carriers access to USF as a means to improve the security of U.S. communications networks is a risk avoidance strategy that ultimately will not produce the desired outcome. Rather, a risk-management-based approach based on the above recommendations would have a more significant impact on improving the security of critical U.S. telecommunications networks.

We recommend the FCC consider a more comprehensive approach to address security concerns of U.S. telecommunications networks that includes, but is not limited to the following:

- Adopt CSRIC *Secure Hardware and Software: Security-by-Design Working Group 6 – Final Report: Best Practices Recommendations for Hardware and software Critical to the Security of the Core Communications Network*, March 2016.

- Adopt CSRIC *Secure Hardware and Software: Security-by-Design Working Group 6 – Final Report: Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Network*, September 2016.

- Adopt CSRIC *Working Group 3: Network Reliability and Security Risk Reduction – Final Report*, March 28, 2018.

- Correct the inherent vulnerabilities of SS7.

- Incentivize carriers to implement the additional recommendations for consideration identified in this white paper (p.8).

- Address the security risks associated with the entire supply chain of the most critical hardware, software and services that are used in the U.S. critical communications networks rather than focus narrowly on a small segment of the supply chain.

Finally, we advocate for an FCC-directed whole-of-government approach to devise and encourage a proportional cost-sharing approach among the wireless communications industry to achieve and maintain acceptable levels of risk and security for all wireless carriers. Ensuring that the implementation of security measures is achievable by all wireless carriers, regardless of tier status, benefits the resiliency and viability of the entire U.S. telecommunications infrastructure.

Domain5 Matrixed Team

Charles Bradley, *Technical Cybersecurity Advisor*. Charlie has over 35 years of experience as a senior intelligence officer in Information Assurance and IT with the NSA. He served in multiple technical and operational leadership positions, most notably as the Technical Director of the Technology Directorate, responsible for NSA's global operational network. He has deep experience and expertise in the development and use of a broad range of SIGINT collection and exploitation. He is an accomplished senior technology leader and engineer with decades of creative and widely recognized achievements in addressing unforeseen challenges and mission success. Charlie works with clients to develop custom-fit cybersecurity solutions.

Steven Clemmons, *Telecom Cyber Security Consultant*. Steve is the President of Information and Infrastructure Technologies, Inc. (IIT). He established the IIT Telecom Sector cybersecurity practice more than a decade ago, and has supported a number of U.S. Telecom carriers and their vendors in developing cybersecurity solutions to address advance persistent threats, including those presented by nation/state entities. These efforts have included acting as an independent security evaluator and the creation of comprehensive security testing protocols and techniques to improve supply chain security. Steve directly manages IIT's cybersecurity, Intelligence Community and technology-focused business practice areas. Prior to joining IIT, Steve served for over 27 years as an Army Intelligence officer, with numerous assignments at NSA, CIA and combatant commands. Mr. Clemmons led complex engineering R&D efforts, from conceptualization through operational deployment throughout the Intelligence Community, delivering state-of-art capabilities to address National-Level requirements He also served in an array of assignments commanding operational intelligence units, including service during Operation JUST CAUSE in Panama, DESERT STORM in Iraq, ELUSIVE HUNTER in Bosnia, and several foreign countries supporting both U.S. Counterterrorism and Counternarcotics operations.

Joseph Mettle, *Information Assurance Advisor.* Joe has over 40 years of experience in Information Assurance and cybersecurity with the NSA and commercial industry. He retired from the US Government as a Defense Intelligence Senior Leader and received numerous Department of Defense (DoD) and Intelligence Community (IC) awards for his work in cybersecurity, including the Meritorious Defense Intelligence Senior Level Presidential Rank Award. Joe has extensive experience in technical counterintelligence, Public Key Cryptography (PKI), securing information technology networks, continuous monitoring, insider threat, risk assessments, and white-hat hacking. His extensive experience and insight into the "adversarial playbook" provides invaluable guidance to protect clients from technical, physical, and personnel Advanced Persistent Threats. Joe helps clients design, architect, and assess cybersecurity solutions.

Karen Hopkinson, *Supply Chain Risk Advisor*. Karen has over 30 years of experience in offensive and defensive NSA organizations, serving in both technical and leadership roles. She has an extensive

background in national technology policy, including export controls, technology transfer, and the Committee on Foreign Investment in the United States (CFIUS), particularly in encryption. These efforts entailed broad collaboration across the Executive and Legislative branches of government. She served in the UK as the Senior US Liaison Officer for cryptanalysis and cryptomathematics research. Most recently, she has focused on Supply Chain Risk Management, with a concentration on the intersection of US and foreign commercial IT/telecommunications technologies, in partnership with other members of the DoD and Law Enforcement communities. Karen works with clients to help them secure their supply chains.

Viktoria Herson, PhD, *Research and Risk Intelligence Analyst, Slavic Language Specialist*. Vikki brings 30 years of experience in academic, industry, and IC research and analysis. She is a former CIA Intelligence Officer with extensive experience working on and managing collection and analytic teams. During her service at CIA, Vikki facilitated technical and analytical strategic partnership projects across the IC, served three Joint Duty Assignment tours at the Office of Naval Intelligence, the National Reconnaissance Office, and spent two years as an integree at the NSA. She also has private sector experience in business intelligence and as a Public Information Office for the Minneapolis Police Department. Vikki's scholarly work focused on South Slavic and Balkan sociolinguistics. She holds an MA in Russian language and a PhD in Slavic linguistics. Vikki supports clients with counterintelligence and risk intelligence research and analysis.

George Mallory, *Research and Risk Intelligence Analyst, Asian Language Specialist.* George is a leader in all-source intelligence specializing in Asian language research. George is a retired NSA and Navy Senior Intelligence Analyst with over 50 years of experience as an intelligence analyst. George has worked as a Chinese and Korean Language Analyst with current Korean language training and certification, and as Intelligence Analyst/Reporter with target expertise in Asia and the Middle East. His analytic experience has focused on Asia, intelligence, counterintelligence, counter-narcotics, and global networks, most recently focused on technical counterintelligence. George holds advanced degrees and certificates in Asian studies, Information Systems and Human Resource Management and Development. George works with clients to support counterintelligence and risk intelligence research and analysis requirements.