JOINT WORKSHOP ON SUPPLY CHAIN SECURITY RISKS AND SOFTWARE SUPPLY CHAIN EXPLOITS

FEDERAL COMMUNICATIONS COMMISSION

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Monday, April 26, 2021

10:00AM **Welcome and Opening Remarks**

Debra Jordan, Deputy Chief, FCC Public Safety and Homeland Security Bureau. Debra Jordan is responsible for matters related to emergency preparedness, disaster response, and national security. Ms. Jordan brings more than 30 years of information technology and communications experience supporting the U.S. Department of Defense (DoD), where she managed a variety of critical information and communications systems.

Jessica Rosenworcel, FCC Acting Chairwoman, believes that the future belongs to the connected. She works to promote greater opportunity, accessibility, and affordability in our communications services in order to ensure that all Americans get a fair shot at 21st century success. She believes strong communications markets can foster economic growth and security, enhance digital age opportunity, and enrich our civic life.

From fighting to protect net neutrality to ensuring access to the internet for students caught in the Homework Gap, Jessica has been a consistent champion for connecting all. She is a leader in spectrum policy, developing new ways to support wireless services from Wi-Fi to video and the internet of things. She also is responsible for developing policies to help expand the reach of broadband to schools, libraries, hospitals, and households across the country.

Named as one of POLITICO's 50 Politicos to Watch and profiled by InStyle Magazine in a series celebrating "women who show up, speak up and get things done," she brings over two decades of communications policy experience and public service to the FCC. Prior to joining the agency, she served as Senior Communications Counsel for the United States Senate Committee on Commerce, Science, and Transportation, under the leadership of Senator John D. Rockefeller IV and Senator Daniel Inouye. Before entering public service, she practiced communications law in Washington, DC.

10:15AM **Keynote Remarks**

Joyce Corell*,* Assistant Director, Supply Chain and Cyber Directorate, National Counterintelligence and Security Center, Office of the Director of National Intelligence. Prior to this posting, she was the Assistant Director for the Strategic Capabilities Directorate in the Office of the National Counterintelligence Executive (ONCIX).

Ms. Corell served at the National Security Agency (NSA) for 23 years. Her last assignment was as the Chief of Technology Policy in the NSA Commercial Solutions Center. Ms. Corell spent a significant portion of her career focused on various aspects of defensive and offensive computer network operations, from capability development to the development of national policy and legislation. Complementing these roles, Ms. Corell also led various activities surrounding partnerships with the private sector ranging from technology transfer, export control licensing, and the development of strategical alliances, both domestic and international. Ms. Corell graduated from William & Mary with a B.A. in Political Science. She received an M.S. in National Security from the National War College.

Brandon Wales, Acting Director, Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Homeland Security. Mr. Wales oversees CISA's efforts to defend civilian networks, manage systemic risk to national critical functions, and work with stakeholders to raise the security baseline of the Nation's cyber and physical infrastructure. Prior to this, he was CISA's first Executive Director, serving as the senior career executive overseeing execution of the Director and Deputy Director's vision for CISA operations and mission support. He was responsible for leading long-term strategy development, managing CISA-wide policy initiatives and ensuring effective operational collaboration across the Agency.

10:45AM **Overview of FCC Supply Chain Efforts**

Justin Faulb, Legal Advisor, Wireline Competition Bureau, FCC, and oversees the FCC supply chain proceeding. He has been at the Commission for four years, and previously served as Acting Special Counsel in the Office of the Chairman of the FCC and as the Designated Federal Officer for the Broadband Deployment Advisory Committee. Prior to the Commission, he was Assistant General Counsel at a large trade association and before that worked as an associate attorney in private practice for six years. He received his law degree from the Catholic University of America–Columbus School of Law with a certificate from the Institute for Communications Law Studies, and his undergraduate degree from Miami University, with honors.

***Remarks* - Nathan Simington,** FCC Commissioner, was nominated by President Donald J. Trump and confirmed by the United States Senate in 2020. Commissioner Simington brings both private and public-sector experience to the Commission. Previously, he served as Senior Advisor at the National Telecommunications and Information Administration. In this role, he worked on many aspects of telecommunications policy, including spectrum allocation and planning, broadband access, and the US Government's role in the Internet. Prior to joining the Commission, he was senior counsel to Brightstar Corp., an international mobile device services company. In this capacity, he led and negotiated telecommunications equipment and services transactions with leading providers in over twenty countries. Prior to joining Brightstar, he worked as an attorney in private practice. Commissioner Simington is a graduate of the University of Michigan Law School. He also holds degrees from the University of Rochester and Lawrence University.

11:10AM **Panel 1: ICT-SCRM Initiatives to Promote Supply Chain Integrity of Small- and Medium-sized Businesses**

Bob Kolasky, Moderator
Jon Boyens
Kathryn Condello
Megan Doscher

Rober Mayer
Ola Sage

Bob Kolasky, Assistant Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security. As one of CISA's Assistant Directors, he oversees the Center's efforts to facilitate a strategic, cross-sector risk management approach to cyber and physical threats to critical infrastructure. The Center provides a central venue for government and industry to combine their knowledge and capabilities in a uniquely collaborative and forward-looking environment. Center activities support both operational and strategic unified risk management efforts. As head of the National Risk Management Center, Kolasky has the responsibility to develop integrated analytic capability to analyze risk to critical infrastructure and work across the national community to reduce risk. As part of that, he co-chairs the Information and Communications Technology Supply Chain Risk Management Task Force and leads CISA's efforts to support development of a secure 5G network. He also serves on the Executive Committee for the Election Infrastructure Government Coordinating Council.

Mr. Kolasky's current position is the culmination of years of risk and resilience experience. He most recently served as the Deputy Assistant Secretary and Acting Assistant Secretary for Infrastructure Protection, where he led the coordinated national effort to partner with industry to reduce the risk posed by acts of terrorism and other cyber or physical threats to the nation's critical infrastructure, including election infrastructure.

Jon Boyens, Deputy Chief, Computer Security Division in the Information Technology Laboratory at the National Institute of Standards and Technology (NIST), U.S. Department of Commerce. His responsibilities include Cybersecurity Research and Development at NIST and Cybersecurity Standards and Guidelines for Federal Agency Security Programs. He also leads NIST's Cyber Supply Chain Risk Management (C-SCRM) Program, helps develop and coordinate the Department of Commerce's cybersecurity policy among the Department's bureaus, and represents the Department in the Administration's interagency cybersecurity policy process. Boyens has worked on various White House-led initiatives, including those on trusted identities, botnets, the Cybersecurity Framework and Roadmap, telecommunications supply chain and, more recently, government-wide implementation of the Federal Acquisition Supply Chain Security Act.

Kathryn Condello, Senior Director, National Security / Emergency Preparedness, Disaster Response, Cybersecurity, Critical Infrastructure Protection, and Continuity of Operations. Ms. Condello is an operations-focused leader within Lumen and the Communications Sector, with extensive, executive-level experience in managing and directing broad corporate and industry initiatives in the areas of strategic planning, policy development, government relations, network deployment/operations, and business marketing functions. She currently serves as the Information Sharing Working Group Lead for the ICT-SCRM Task Force. Ms. Condello has

more than 20 years experience in industry level initiatives associated with national security, network reliability, and emergency preparedness programs, planning and policy initiatives.

Megan Doscher, Senior Policy Advisor, National Telecommunications and Information Administration, U.S. Department of Commerce. Ms. Doscher is a Senior Policy Advisor at NTIA and currently leads C-SCRIP, NTIA's Communications Supply Chain Risk Information Partnership for small/midsize and rural communications providers and suppliers. Megan was the lead author for NTIA on the Botnet Report and Road Map mandated by Executive Order 13800. She has spent the last 15 years working on national-level policy issues related to communications and information security. In her prior career, she edited technology and business news for The Wall Street Journal. Megan has a master's degree in criminal justice/security management from George Washington University and a bachelor's degree in journalism from Syracuse University.

Robert Mayer, Senior Vice President, Cybersecurity and Innovation with the USTelecom Association (USTelecom) with responsibility for leading cyber and national security policy and strategic initiatives. He is the current Chairman of the Communications Sector Coordinating Council (CSCC), which represents the broadcast, cable, satellite, wireless and wireline industries in connection with DHS and public-private partnership activities across the U.S. government. Mayer serves as the co-chair of the Department of Homeland Security's ICT Supply Chain Risk Management Task Force, which recently delivered findings and recommendations related to information sharing, threat criteria, qualified bidders and manufacturer lists and proposals to address procurement of counterfeit products. He also serves as co-Chair of the Counsel to Secure the Digital Economy (CSDE), which consists of 13 global ICT infrastructure providers that have produced internationally recognized work on IoT baseline capabilities, an International Anti-Botnet Guide and ICT coordination in the event of a global cyber crisis. Mayer was appointed to the FCC Communications Security Reliability and Interoperability Council (CSRIC V), after having led a 100-person team of cybersecurity professionals that produced a landmark report to adapt the NIST Cybersecurity Framework to the broadcast, cable, satellite, wireless and wireline industries.

Ola Sage, Founder and Chief Executive Officer - CyberRx Ms. Sage has spent more than 20 years improving the cybersecurity readiness of small- and medium-sized businesses through engagement with CEOs, business groups, and Congress. As CEO of CyberRx, she leads the development of software platforms and solutions that businesses can use to track, measure, and improve their cybersecurity health and preparedness. Prior to this position, Ms. Sage was President and CEO of a government focused information technology professional services company for 18 years. Ms. Sage serves on the President's National Infrastructure Advisory Council, which includes executive leaders from private industry and government who advise the White House on ways to reduce physical and cyber risks and improve the security and resilience of the nation's critical infrastructure sectors. From 2016 to 2018, Ms. Sage served as the Chair of the Information Technology Sector Coordinating Council (IT SCC) and currently serves on its executive committee. Ms. Sage also serves on the executive committee of the Information and

Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force and is a co-Chair of the ICT SCRM Small and Medium-Sized Businesses Working Group.

***Remarks* - Geoffrey Starks,** FCC Commissioner, is a leader on national security policy, working to eliminate untrustworthy equipment from America's communications networks. s believes that communications technology has the potential to be one of the most powerful forces on Earth for promoting equality and opportunity. His *Find It, Fix It, Fund It* initiative brought national attention to the urgent need to support small and rural companies as they work to make their networks more secure.

At the Department of Justice, he served as a senior advisor to the Deputy Attorney General on a variety of domestic and international law enforcement matters and received the Attorney General's Award for Exceptional Service—the highest honor award a DOJ employee can receive. Before he was appointed Commissioner, Starks helped lead the FCC's Enforcement Bureau, handling a wide variety of complex investigations. Commissioner Starks graduated from Harvard College with high honors and Yale Law School. Before he entered federal public service, Commissioner Starks practiced law at Williams & Connolly, clerked on the U.S. Court of Appeals for the 8th Circuit, served as a legislative staffer in the Illinois State Senate, and worked as a financial analyst.

12:30 PM **<u>Keynote Remarks</u>**

Evelyn Remaley, Acting Assistant Secretary/Administrator, National Telecommunications and Information Administration, U.S. Department of Commerce. Ms. Remaley leads a team of experts providing senior policy support to the Secretary of Commerce and the White House on issues impacting the Internet and digital economy. In addition, Ms. Remaley leads the Department's Cybersecurity Policy efforts. Ms. Remaley has focused NTIA's policy team to position it to meet the demands of the dynamic Internet and cyber policy landscape. Her portfolio includes work on the full scope of today's critical digital policy issues including cybersecurity, supply chain risk management, privacy, the free flow of information, encryption, and the Internet of things. Her team focuses on pursuing policies that bolster the digital economy, while protecting citizens, and works to expand the policy conversation beyond Washington, DC to reach a full spectrum of Internet ecosystem players.

Darrin Jones (by video), Executive Assistant Director for Science & Technology of the FBI's Science and Technology Branch, most recently served as the assistant director of the Information Technology Infrastructure Division. Mr. Jones joined the FBI in 1997 as a special agent in the Salt Lake City Field Office, where he investigated international drug trafficking and cybercrime and helped lead the counterterrorism planning for the 2002 Olympics. In 2003, he was promoted to supervisor and served as a congressional liaison in the Office of Congressional Affairs at FBI Headquarters in Washington, D.C. In 2005, Mr. Jones became a supervisor in the Operational Technology Division at Quantico, Virginia. He created the FBI's Technical Liaison Office, which cultivated close working relationships between the FBI and technology companies. In

2007, Mr. Jones moved to the Albuquerque Field Office as the cyber program supervisor, managing criminal cyber cases and national security intrusion investigations. In 2009, he coordinated the construction of the New Mexico Regional Computer Forensic Laboratory, the FBI's 16th such facility. He also served as director of the lab, which provides digital forensics services to the law enforcement and national security communities. In 2011, Mr. Jones was appointed assistant special agent in charge of the Anchorage Field Office. He returned to FBI Headquarters in 2013 as a section chief in the Operational Technology Division, overseeing technical and policy matters associated with electronic communication interception. He was named special agent in charge of the Kansas City Field Office in March 2017. Prior to working for the FBI, Mr. Jones worked for subsidiaries of ConAgra and Novartis corporations. He earned a bachelor's degree from the University of Nebraska and completed Carnegie Mellon University's Cyber Information Security Officer—Executive Education and Certificate Program in February 2019.

***Remarks* - Brendan Carr**, FCC Commissioner, has been described by Axios as "the FCC's 5G crusader." He has led the FCC's work to modernize its infrastructure rules and accelerate the buildout of high-speed networks. His reforms cut billions of dollars in red tape, enabled the private sector to construct high-speed networks in communities across the country, and extended America's global leadership in 5G. Commissioner Carr is also focused on expanding America's skilled workforce—the tower climbers and construction crews needed to build next-gen networks. His jobs initiative promotes community colleges and apprenticeships as a pipeline for good-paying 5G jobs. And he is recognizing America's talented and hardworking tower crews through a series of "5G Ready" Hard Hat presentations.

Commissioner Carr leads the groundbreaking FCC telehealth initiative at the FCC, the Connected Care Pilot Program, which supports the delivery of high-quality care to low-income Americans and veterans over their smartphones, tablets, or other connected devices. He spends time outside Washington to help inform his approach to the job and regularly hits the road to hear directly from the community members, local leaders, and small business owners that are impacted by the FCC's policies at town halls and other events across the country.

Commissioner Carr brings over a dozen years of private and public sector experience in communications and tech policy to his position. Before joining the agency as a staffer back in 2012, he worked as an attorney at Wiley Rein LLP in the firm's appellate, litigation, and telecom practices, where he litigated cases involving the First Amendment and the Communications Act. He clerked on the U.S. Court of Appeals for the Fourth Circuit for Judge Dennis Shedd. He attended Georgetown University for undergrad and earned his J.D., *magna cum laude,* from the Catholic University of America's Columbus School of Law where he served as an editor of the Catholic University Law Review.

1:05 PM **<u>Panel 2: Protecting the Software Supply Chain in the Communications Sector</u>**

Joyce Correll, Moderator

Allan Friedman
Trey Herr
Michael Iwanoff
Keith Nakasone

Allan Friedman, Director of Cybersecurity Initiatives at the National Telecommunications and Information Administration (NTIA) in the U.S. Department of Commerce, coordinates NTIA's multistakeholder processes on cybersecurity, focusing on addressing vulnerabilities in IoT and across the software world. Prior to joining the Federal Government, Friedman spent over 15 years as a noted cybersecurity and technology policy researcher at Harvard's Computer Science Department, the Brookings Institution and George Washington University's Engineering School. He is the Co-Author of the popular text "Cybersecurity and Cyberwar: What Everyone Needs to Know" and has a degree in computer science from Swarthmore College and a Ph.D. in public policy from Harvard University.

Trey Herr, Director, Cyber Statecraft Initiative, Scowcroft Center for Strategy and Security, Atlantic Council, and co-author of Broken Trust. His team works on cybersecurity and geopolitics including cloud computing, the security of the internet, supply chain policy, cyber effects on the battlefield, and growing a more capable cybersecurity policy workforce. Previously, he was a senior security strategist with Microsoft handling cloud computing and supply chain security policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.

Keith Nakasone, Deputy Assistant Commissioner, IT Acquisition, Office of Information Technology Category (ITC), Federal Acquisition Service (FAS), U.S. General Services Administration. The Federal Acquisition Service provides buying platforms and acquisition services to Federal, State, and Local governments for a broad range of items from office supplies to motor vehicles to information technology and telecommunications products and services. As an organization within FAS, ITC provides access to a wide range of commercial and custom IT products, services and solutions.

Michael Iwanoff, Senior Vice President and Chief Information Security Officer at iconectiv, leads the Global Information Security organization and is responsible for building and implementing enhanced security policies, standards, and technology controls and establishing security strategy and direction for the company. With more than 19 years of experience in IT Risk and Security, Iwanoff has successfully built and implemented comprehensive IT Security, Risk and Compliance programs for global organizations. His professional experience spans telecom and financial services at leading organizations including AIG, Barclays, Comcast, and AT&T. Prior to his current position, he served as the Vice President -- Chief Security Officer for the Property Casualty division of AIG, a global financial business. Iwanoff is a member of the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force.

2:20 PM **Concluding Remarks and Adjournment**

Lisa Fowlkes, Chief, FCC Public Safety and Homeland Security Bureau. Under her leadership, the Bureau develops and implements policies, consistent with the FCC's statutory authority, to ensure that first responders and the American public have access to effective, reliable, and secure communications, and collaborates with Federal government partners responsible for protecting the nation's communications infrastructure.

For over a decade, Chief Fowlkes has led initiatives to ensure that people who dial 911 can reach emergency assistance and that first responders can locate those who need help. She has also led efforts to ensure that consumers have access to accurate and timely emergency alerts, including the introduction of Wireless Emergency Alerts and its ongoing enhancements. She has promoted resilient and secure communications systems through public-private collaboration as well as investigations into significant 911 and other communications network outages.

Chief Fowlkes previously served as a Deputy Chief of the Public Safety and Homeland Security Bureau, where she was responsible for the FCC's policies on cybersecurity, communications reliability, and emergency alerting. During her more than 26-year career at the FCC, Chief Fowlkes also served as Deputy Chief of the former Public Safety and Private Wireless Division; Acting Deputy Chief, Assistant Chief, and Senior Legal Advisor in the Enforcement Bureau; Acting Director of the Office of Communications Business Opportunities; Supervisory Attorney in the former Cable Services Bureau; and Attorney-Advisor in the Office of General Counsel and former Mass Media Bureau. She also spent two years in private practice at a Washington, D.C. law firm where she represented public safety agencies on regulatory matters. Chief Fowlkes earned a Juris Doctor from the University of Pittsburgh School of Law.