EXHIBIT B

DECLARATION OF DONALD A. PURDY, JR.

I, Donald A. Purdy, Jr., hereby declare, affirm, and state the following:

I. Introduction

1. The facts set forth below are known to me personally, and I have firsthand knowledge of them.

2. I make this declaration in support of comments submitted by Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc. ("Huawei") in response to a Notice of Proposed Rulemaking ("NPRM") promulgated by the Federal Communications Commission ("FCC"), In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, FCC 18-42, on April 18, 2018. The goal of this NPRM is to improve the security of carrier infrastructure by discouraging telecommunications carriers from procuring communications equipment or services from certain providers deemed a national security risk to communications networks or the communications supply chain.

3. In a separate affidavit included in Huawei's filing, John Suffolk, Huawei's Global Cybersecurity and Privacy Officer, makes five points detailing why the stated objective of the FCC in the NPRM cannot be met by singling out a specific country or selected companies, and why it may be counterproductive:

   A. The ICT supply chain is global.

B. Because the ICT supply chain is global, cybersecurity risk arises from the cumulative supply chain, rather than the vendor whose name happens to be on the "box" or who provides the named application.

C. The global supply chain generates thousands of security vulnerabilities from vendors of all countries, including the United States.

D. Governments and companies could do more to protect themselves.

E. Huawei's approach to security by design, development, and deployment improves the security of its products and the supply chain.

4. I agree with the analyses and conclusions laid out in Mr. Suffolk's affidavit. In addition, a realistic analysis of telecom carrier risks associated with vendor selection leads me to conclude that the proposed FCC solution ignores a much broader set of concerns regarding the vulnerable, global telecommunications supply chain; does little to improve the security of targeted infrastructures; and fails even to address fully the primary concern that lead to this proposal, namely, potential Chinese or other nation/state entities leveraging or exploiting telecom vendors and products for malicious purposes. In the end, the exclusion of any individual vendor or set of vendors, based in whole or in part on the location of their headquarters, from participating in carrier-contracted activities would have a negligible positive effect on telecom infrastructure security.

5. In this affidavit, I will discuss how Huawei US's[1] approach to cybersecurity, privacy assurance, and governance supports Huawei's global approach and facilitates the FCC's

[1] "Huawei US" refers only to Huawei Technologies USA, Inc. and Huawei Device USA, Inc., two entities that sell network products and terminal products in the US), and United States. It does not include Futurewei Technologies, Inc., which is also a subsidiary of Huawei Technologies Co., Ltd. in the United States, but is focused on research and development rather than product sales.

goal of improving the security and resilience of U.S. telecom infrastructure. Specifically, I will discuss:

A. Huawei's dedicated and thorough approach to cybersecurity and policy, which permeates every aspect of the company;

B. Huawei US's internal policies and processes, which provide enhanced and transparent protection of customer data and networks and facilitate assurance and transparency; and

C. Huawei US's experience with third-party testing of our hardware and software.

II. Background and Qualifications

6. I am over the age of eighteen and I am a citizen of the United States.

7. I have been employed by Huawei since July 2012 as Chief Security Officer for Huawei US. My current title is Chief Security Officer, Huawei US.

8. My curriculum vitae, including my qualifications, is attached to this declaration as Exhibit 1.

9. The following is a summary of my background.

A. I am Chief Security Officer for Huawei US; in this capacity I oversee Huawei US's cybersecurity assurance program, and support Huawei's global assurance program. I have security (CISSP) and privacy certifications (CIPP/US) and a legal background, although I do not function as an attorney at Huawei.

B. I also serve as the Huawei global lead for the East-West Institute Global Cooperation in Cyberspace Initiative and serve on the Steering Committee of The Open Group Trusted Technology Forum, which developed the Open Trusted

Technology Provider Standard (O-TTPS), recognized as ISO/IEC 20243. I also serve as Huawei's alternate representative to The Open Group Board of Directors.

C. I was the U.S. senior cybersecurity official at the Department of Homeland Security (DHS) from 2004-2006. Prior to joining the DHS, I was a member of the White House staff where I helped to draft the U.S. *National Strategy to Secure Cyberspace* (2003). At DHS, I helped to form and then led the National Cybersecurity Division (NCSD) and the U.S. Computer Emergency Readiness Team (US-CERT) (as Acting Director). At DHS, I also served as Co-chair of the National Cyber Response Coordination Group (NCRCG), then the principal US interagency group to prepare for and respond to cyber incidents of national significance, and was the DHS representative to the Committee on National Security System (CNSS) that sets policy for the nation's classified IT networks.

D. Immediately before joining Huawei, I was the Chief Cybersecurity Strategist for Computer Sciences Corporation (CSC). In this role, I provided strategic input to the development and implementation of a coordinated, company-wide initiative to address the cybersecurity needs of CSC's global client base, and worked in national and international venues to influence cybersecurity public policy and awareness.

E. Before joining the White House staff, I served as Acting General Counsel and Chief Deputy General Counsel at the U.S. Sentencing Commission, where I gained substantial experience with organizational compliance.

F. Earlier in my career I served as a federal prosecutor in Philadelphia, Pennsylvania; Senior Staff Counsel of the House Select Committee on

Assassinations (President John Kennedy); Special Counsel to the U.S. House Ethics Committee; and Counsel to the U.S. Senate Impeachment Trial Committee (Judge Walter Nixon). I also served for five years in network television news as an Associate Producer for NBC News magazines, and Producer for the CBS News broadcast NIGHTWATCH with Charlie Rose in Washington, D.C.

G. I am a graduate of the College of William and Mary and the University of Virginia Law School. I am a member of the Bar (inactive status) in the District of Columbia, Maryland, Pennsylvania, and Missouri.

III. Huawei Global Assurance Program for Cybersecurity and Privacy

10. Since 2011, Huawei has established, implemented, and improved a transparent global assurance program (the Program) for cybersecurity and privacy.

11. The Program reflects a strong cybersecurity and privacy commitment by Huawei's top corporate leadership, and leadership of the various business groups and units, to protect customer data and access to customer networks; to ensure that Huawei and its employees comply with government mandates, customer requirements, and Huawei policy and practices; and to fulfill Huawei's commitment through a program of end-to-end assurance and internal compliance.

12. Under the Program, Huawei's Global Cybersecurity and Privacy Protection Committee (GSPC) conducts enterprise-wide governance of cybersecurity and privacy policies and procedures, which are implemented by the Global Cybersecurity and Privacy Protection Office (GSPO). Huawei also ensures regional and national oversight by cybersecurity and privacy committees and security personnel.

13. All relevant internal business groups and functions are subject to detailed cybersecurity requirements based on legal and regulatory requirements, customer requirements, and Huawei internal policies and processes (global, regional, and national).

14. Huawei also utilizes a robust supply chain assurance process of vetting and monitoring suppliers to ensure that suppliers are compliant with Huawei cybersecurity and privacy requirements for suppliers, including requirements that they assess and address the risk related to their products and services; and annual performance requirements for business units that include cybersecurity and privacy protection criteria.

15. All Huawei employees are required to conform to cybersecurity and privacy policies. Nonconformance directly affects merit pay, annual increases, retention, and promotions, and individuals are incentivized to fully correct problems that are identified. Employees receive cybersecurity and privacy training and are tested on cybersecurity and privacy policies.

16. Huawei implements a separation-of-duties principle to ensure that those who must meet requirements are different than the employees who monitor conformance to those requirements.

17. Huawei has a strong internal compliance program—globally, regionally, and nationally—that has strengthened the clarity and completeness of compliance requirements related to cybersecurity and privacy, and has implemented a process of self-checks relative to cybersecurity and privacy requirements that assesses the status of compliance semi-annually between audits. The program includes periodic, unannounced audits of regional and national cybersecurity and privacy protection programs conducted by a dedicated team.

18. The Program ensures that Huawei's cybersecurity and privacy protection efforts remain transparent, effective, and innovative, and are subject to ongoing improvement. The Program includes periodic research and publication of global cybersecurity, privacy and other white papers; briefings of customers and stakeholders; and participation in public events concerning these issues.

IV. Huawei US Cybersecurity and Privacy Policies and Governance

19. Huawei's corporate structure includes governance that occurs at a national and regional level, in order to ensure that the entirety of the company conforms with legal, regulatory, customer, and Huawei requirements.

20. Cybersecurity and privacy are key components of the overall compliance requirements of Huawei US, derived from Huawei's global policy and process, United States statutes and regulations, customer requirements, and Huawei US policy and procedure.

21. Huawei US has a Cybersecurity and Privacy Committee modeled after the GSPC, which conducts nationwide governance of cybersecurity and privacy policies and procedures.

    A. Huawei US's Cybersecurity and Privacy Committee is chaired by me in my capacity as Chief Security Officer.

    B. Members of the Committee are appointees designated by the CEO of the Huawei Technologies USA Inc. (comprised of the Carrier and Enterprise Business Groups) and Huawei Device USA, and include representatives of the Business Groups and Departments (e.g., BG rep, services delivery, procurement, supply chain management, legal, HR, sales, and security).

22. Like its global counterparts, Huawei US is subject to unannounced, periodic cybersecurity and privacy audits by an independent internal team, with the report and

action requirements provided to the US CEO and cybersecurity and privacy officials. Audit results impact organizational and individual performance assessment that impacts retention, bonuses, compensation, and opportunities for promotion.

23. Huawei US conducts internal, semi-annual self-checks of adherence to cybersecurity and privacy policy and procedure.

24. Huawei US products and software are designed and tested to meet strict security protocols. In addition, as discussed further in Section VI, below, Huawei US products and software have been subject to third-party testing. This has included software such as updates and patches, which have been externally validated before deployment. Huawei has various internal and external processes that can detect and protect against possible malicious acts by third parties or insiders; for example, the plant of a backdoor or other hidden functionality not covered in the product manual, or vulnerability, or allowing significant, known vulnerabilities to remain unpatched.

25. Huawei US also ensures the integrity and security of any customer data and access to customer networks, in policy and in practice. For example, Huawei US mandates use of the Secure Network Access Solution (SNAS),[2] as depicted in Figure 1, below. SNAS allows secure data access between customer network and the Huawei TAC terminals. SNAS only allows access to customer networks by approved U.S.-based Huawei personnel using secure configured laptops, and then only via a secured configured server, and uses a recorded logging system that facilitates customer monitoring and auditing of

[2] The SNAS utilizes was developed for Huawei US by a U.S. owned and operated virtualized solutions company.

all access and transactions. The Huawei Intranet (internal corporate network) and the SNAS are isolated from one another.

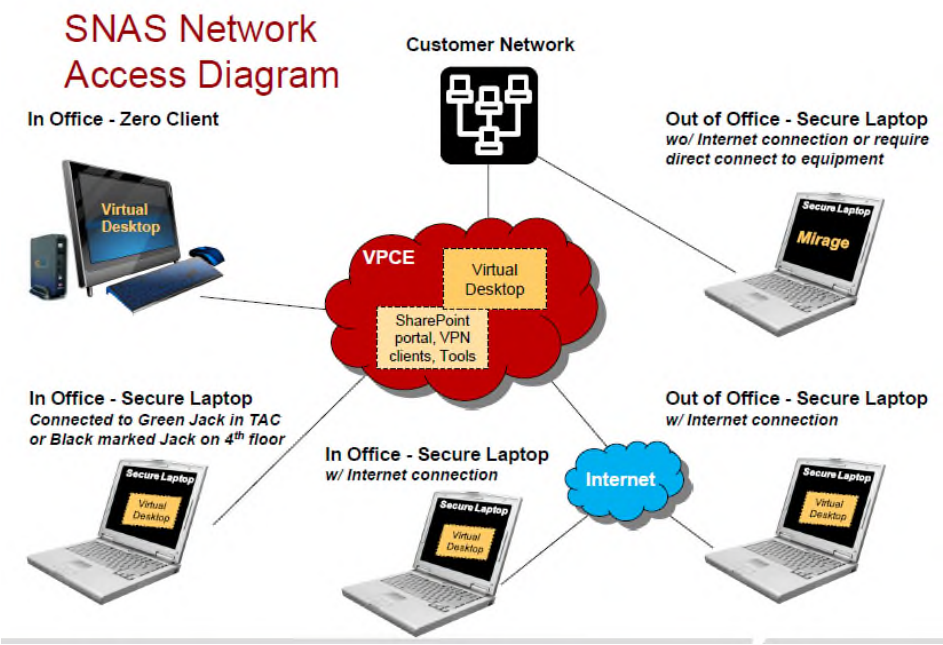


Fig. 1. SNAS Network Access Diagram

26. Huawei maintains a U.S.-based Technical Assistance Center (US TAC) for remote support of customer's networks. Customers may perform an audit of the US TAC. Huawei has developed a culture to follow U.S. cybersecurity policy and process regarding all U.S. access to customer data and networks. If and when customers decide to conduct an audit, US TAC is available to provide them with logs and access approvals as needed. This demonstrates Huawei's commitment to cybersecurity and transparency.

27. Huawei US performs quarterly checks of customer support for adherence to cybersecurity policy and process for engineers (examples: deleting passwords; following three levels of approval for data transfer and two levels of approval for access). Huawei US's security assurance rules and customer service practices are discussed in greater detail in Section V, below.

V. Huawei US Services Cybersecurity Policy (SCSP) for US Customers

28. Huawei US implements a "Services Cybersecurity Policy" (SCSP), centered on auditable, enhanced protection of customer data and networks.

29. The abstract of the SCSP is as follows: As part of Huawei US efforts to enhance Cybersecurity for each customer, raise awareness of issues and make certain that everyone follows the appropriate steps to ensure the security of customer's information. The USA Delivery & Service Security Team has released the "Services Cybersecurity Policy".

30. The SCSP provides a formal set of rules by which those people who are given access by Huawei to "Huawei US" customer network(s) must abide.

    A. It is mandatory for all personnel working with/on any Huawei USA customer network(s) to know and abide by the SCSP.

    B. All personnel working with/on any Huawei USA customer network(s) have an annual requirement to obtain an internal Cybersecurity Certificate with mandatory training and exams.

    C. All personnel working with/on any Huawei US customer network(s) must sign the Cybersecurity Commitment letter pledging to follow Huawei US policy and procedure.

31. The SCSP serves several purposes. The main purpose is to inform company users—employees, contractors, and other authorized representatives—of their obligatory requirements for protecting the technology and information assets of the company and those of customers. The cybersecurity policy describes the technology and information

assets that Huawei must protect and identifies many of the potential threats to those assets.

32. The SCSP imposes specific requirements that must be strictly followed. For example:

A. Under no circumstances is access to the Huawei US Secure Network Access Solution or any customer network allowed from outside of North America.

B. SNAS "User" accounts are to be used only for services-related activities and/or technical support to the Customer via the Virtual Private Cloud Environment ("VPCE"). The servers providing the VPCE for Huawei US are physically located in the U.S., isolated from Huawei's intranet, and managed by US citizens. All computing and data activity is contained within SNAS where the Zero Clients and Secure Laptops are only a virtualization of the data (viewable pixels and physical key presses). On Secure Laptops and Zero Clients, access can only be made with authorized accounts and devices are locked from external devices (e.g., USB). Account authorization and issuance of Secure Laptop requires several levels of management authorization, training, and certification prior to access being granted to a user. Passwords have minimum complexity and expiration requirements. Further, within the system, segregation of authority is maintained to minimize horizontal access such that authorization by the authorized customer interface for each engineer is needed for each customer's data or network access.

C. Users are responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore, they are prohibited from making unauthorized copies of such

confidential information and/or distributing it to unauthorized persons outside of the company.

D. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to company systems for which they do not have authorization.

E. All data collected for analysis is only maintained within the Secure Network Access Solution. Transfer of data/information outside of the environment requires specific written authorization from customers.

F. When inside the US TAC secure area, each engineer should use only Zero Client to access Customer network and perform any operations. Huawei-corporate laptops/desktops cannot access the SNAS virtual desktop environment.

G. All necessary software tools used for interacting with a customer network are already preloaded in the VPCE. Any tools identified to be missing shall be requested through the D&S Security Team – Department Owner, who is responsible to assess and approve introduction of tools.

VI. Huawei US Experience with Third-Party Testing of Huawei Hardware and Software

33. Several years ago, acting on similar concerns as those articulated by the FCC, a Tier 1 U.S. telecom carrier put in place a policy framework designed to eliminate the need to fully trust any vendor, accepting the reality that there existed very little basis for such trust. The ultimate goal was to implement a security methodology that would allow the carrier to collect sufficient evidence in order to facilitate greater trust of the technology and systems being delivered for deployment into the production network. In simple terms, vendors competing for carrier contracts were required to submit their technology

solutions to an approved independent evaluator and agree to a comprehensive trusted delivery process that eliminated significant supply chain risk concern. These requirements were applied to all vendors of the Tier 1 carrier, and included most of the major global telecom vendors, including Huawei.

34. Over the past five years, EWA North America (EWA NA) has performed and continues to perform as an independent evaluation laboratory contracted to conduct high assurance security evaluations and Trusted Delivery verifications in support of multiple carrier network development and modernization efforts. During its involvement in the program, Huawei was among several vendors subjected to identical security scrutiny. Technologies addressed by EWA NA during this period included 3G CDMA and 4G LTE-TDD/FDD.

35. The evaluation activities conducted by EWA NA are executed in multiple secure laboratory facilities. EWA NA personnel involved in these activities are highly vetted and all possess high-level Government security clearances. These laboratories contain exact replicas of vendor corporate software build/compile environments, as well as elements of operational environments necessary to facilitate system testing.

36. EWA NA evaluation efforts include in-depth analysis of source code and resulting binaries, including design and actual available functionality; firmware; and an array of system-level testing processes executed in both EWA NA and carrier laboratory environments. The extensive evaluation methods employed by EWA NA have been mapped to current threats and risks that are of concern to both carriers and an array of Government stakeholders. This methodology was designed to create a verifiable, fully auditable set of processes that permit end users and carriers to fully trust the technologies

and systems deployed in their networks, and eliminate the critical need for determining whether or not a specific vendor should simply be trusted to deliver secure solutions.

37. Early concerns that certain vendors, if they were collaborating with nation/state actors, might deliberately attempt to circumvent test and evaluation protocols, were addressed from the onset of the effort. Vendors under evaluation are not provided any insights into test protocols, evaluation tool selection, or specific security assurance standards being applied. Test protocols and custom-developed evaluation tools are rotated and continuously evolved to prevent any realistic possibility of any entity "engineering around the test protocols".

38. To further these efforts, Huawei employed a "Trust" solution to ensure that test subject evaluations would go directly from the third-party tester to the customer, rather than to Huawei. The Trust solution was extended across the full lifecycle of the technology deployment through implementation of an ongoing, highly rigorous, Trusted Delivery process.

39. In this program, for Trusted Delivery, all software was required to be delivered to supported carriers by EWA NA, after verification of binaries provided by vendors. EWA NA conducts in-depth testing of a statistically significant sample of assemblies that are chosen at random by the Carrier organization. All software releases, patches and hardware upgrades throughout the lifecycle of the deployment, were fully evaluated by EWA NA prior to deployment.

40. While the discussion above is a somewhat simplified description of the methodology that has been continuously improved over the years, it has long been validated by both carrier and key government experts as a valid solution to a wide array of threat/risk concerns.

This solution very seriously mitigates concerns over malicious changes in systems or software. It certainly creates a situation where a customer can maintain full surveillance of all aspects of the systems and software designated for deployment, and it provides high-fidelity protection against the malicious introduction of unevaluated technology.

41. There have been few issues across vendors in complying with the above requirements. In the case of Huawei, mitigation efforts to correct any identified defects or vulnerabilities have always been aggressive, demonstrating Huawei's full commitment to delivering security transparency. In many cases, Huawei out-performed other vendors in delivering mandated mitigations.

VII. Attestation

42. As the Chief Security Officer for Huawei US, I report directly to John Suffolk, Huawei's Global Cybersecurity and Privacy Officer, and the Head of the Public Affairs and Communications Department at Huawei Technologies USA, Inc., Regent Zhang. I am accountable—along with the CEOs of Huawei Technologies USA, Inc. and Huawei Device USA, Inc.—for security and privacy across the Huawei US business groups and departments. In my nearly six years at Huawei I can confirm that I have never been unduly influenced by any person within Huawei, or outside of Huawei, to take any action that I felt was inappropriate in the assessment or management of cybersecurity or privacy risk, or that was contrary to the need to assure compliance with law and regulation, customer requirements, and Huawei global and Huawei US policy and procedure. Nor have I become aware of such inappropriate action by another person.

43. I confirm that during my time at Huawei, I have never been unduly influenced to refrain from any action I believed was necessary or appropriate to the assessment or

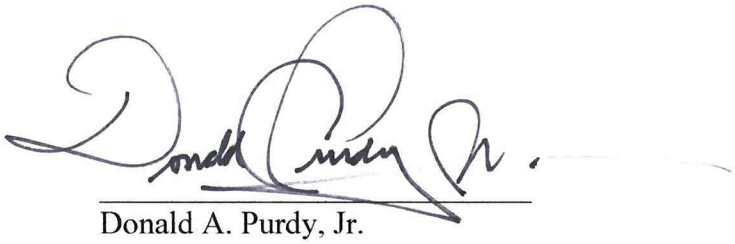
management of cybersecurity or privacy risk, or that was contrary to the need to assure compliance with law and regulation, customer requirements, and Huawei global and Huawei US policy and procedure. Nor have I become aware of such inappropriate conduct by another person.

44. I confirm that during my time at Huawei, I have never learned any facts, nor have I received, or learned of, any allegations or been informed of allegations or even suspicions, that any employee, contractor, supplier, or partner of Huawei cooperated inappropriately with any government or any other organization or individual, to allow Huawei products (or third-party components) to be used for the unauthorized insertion of code (including for improper purposes, such as malicious code, programmable software, or code with an exploitable vulnerability) or, for malicious purpose, to intentionally allow a known, exploitable vulnerability to remain in code after discovery.

45. I also confirm that I do not know of any improper relationship between anyone associated with Huawei and anyone associated with the government of any country, including China; nor do I know of any influence, much less undue influence, by anyone associated with the government of any country, including China.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on May 31, 2018.



Donald A. Purdy, Jr.

DECLARATION OF DONALD A. PURDY, JR. EXHIBIT 1

DONALD A. (ANDY) PURDY, JR., J.D., CISSP, CIPP/US

8201 Kenfield Court *Andy.Purdy@comcast.net* *• 202/289-4019 - o*
Bethesda, MD 20817 *• 202/486-0720 - c*

OBJECTIVE: **IDENTIFY BOARD AND ADVISORY BOARD OPPORTUNTIES TO STRENGTHEN CYBER SECURITY AND PRIVACY RISK MANAGEMENT, INTERNAL GOVERNANCE, AND COMPLIANCE. POTENTIAL CYBERSECURITY AND PRIVACY ASSET FOR A CORPORATE RISK COMMITTEE.**

TO LEVERAGE A UNIQUE COMBINATION OF LEGAL AND CSO EXPERIENCE, AS A FEDERAL PROSECUTOR AND CONGRESSIONAL COUNSEL, AND AS ACTING GENERAL COUNSEL WITH THE U.S. SENTENCING COMMISSION, WORKING WITH THE U.S. ORGANIZATIONAL SENTENCING GUIDELINES AND CORPORATE COMPLIANCE PROGRAM REQUIREMENTS, AND AS A CORPORATE CSO EXPERIENCED WITH CYBERSECURITY AND PRIVACY RISK MANAGEMENT AND INTERNAL GOVERNANCE.

HIGHLIGHTS

- First CSO for Huawei Technologies USA; cybersecurity and privacy certifications.
- Advisor to emerging technology companies, including two that were acquired (BigFix by IBM and Lancope by Cisco).
- Chief Cybersecurity Strategist for CSC.
- Lead cybersecurity official for the U.S. government at DHS;
- White House role in helping to draft the *National Strategy to Secure Cyberspace*;
- Helped to formulate the Federal Sentencing Guidelines for organizations and individuals;
- Rich, diverse experience as a member of the national media and staffer on Capitol Hill; and
- Persuaded an initially incredulous congressional committee that the inescapable validity of the "single-bullet theory" proved that a single gunman killed President John F. Kennedy.

EXPERIENCE

Chief Security Officer (July 2012 to Present)
Huawei Technologies USA

Oversees Huawei USA's cyber security assurance and privacy strategy and program, and supports Huawei's global security assurance program. Chairs the Huawei USA Cyber Security and Privacy Committee.

Also the Huawei global lead for the East-West Institute Global Cooperation in Cyberspace Initiative and serves as the Vice Chair of the Open Group Trusted Technology Forum, which developed the Open Group Trusted Technology Provider Standard (O-TTPS), recognized by ISO as ISO/IEC 20243.

Chief Cybersecurity Strategist (February 2010 to June 2012)
CSC (Computer Sciences Corporation)

Provided strategic input to the development and implementation of a coordinated, company-wide initiative to address the cybersecurity needs of CSC's global client base, and worked in national and international venues to influence cyber security public policy and awareness.

Advisor to Emerging Companies (November 2006 to January 2010)
BigFix, Lancope, 3VR, HB Gary, Trust Defender

Acting Director and Privacy Officer (April 2003 to October 2006)[a]
National Cyber Security Division (NCSD)/
U.S. Computer Emergency Readiness Team (US-CERT)
Department of Homeland Security

- Recruited from the White House staff to be a member of the senior leadership team that built and launched the NCSD)/US-CERT.
- Named by Secretary Tom Ridge to be Acting Director of NCSD/US-CERT to lead the effort by the Department of Homeland Security to work collaboratively with government and private sector stakeholders to reduce risk in cyberspace and protect America's cyber assets (October 2004);
- Drafted a strategic plan to implement the cyber security mission pursuant to the authorities of the Homeland Security Act and Strategy, the National Cyber Strategy, and Homeland Security Presidential Directive-7.
- Managed the efforts of 30 government employees and over 125 contractors to address the overarching priorities of the strategic plan – to build a National Cyber Security Response System and a national cyber risk management program. Manage a FY 06 budget of over $100 million that grew from $79 million in FY05.
- Built a robust cyber security response system that entailed collaboration with the private sector and key government entities at the Federal, state, and local levels – and internationally – to build cyber situational awareness, attack attribution capabilities, coordinated response and mitigation capabilities, and the ability to reconstitute and recover after successful cyber attacks or the cyber consequences of cyber or physical attacks or natural disasters.
- Under the National Infrastructure Protection Plan, cyber risk management involved partnership with key government and private sector entities in the IT sector – and through lead agencies for other sectors – to identify assets and interdependencies, assess vulnerabilities and the consequences of their exploitation, and to assess cyber risk and the priority measures necessary to reduce that risk.
- Priority risk mitigation efforts included: Internet Disruption Working Group, Control Systems Security Program, and Software Assurance Security Program (including close partnership with the Office of Information Assurance of the U.S. Department of Defense).
- Co-Chair of the Committee on National Security Systems Working Group on Globalization of IT. Mission to address the security challenges to national security systems and critical infrastructure owners and operators posed by the increasing globalization of information technology.

[a] Deputy Director through September 2004.

Deputy to the Vice Chair (April 2002 to April 2003)
Senior Advisor for IT Security and Privacy[b]
Deputy to the Vice Chair
The President's Critical Infrastructure Protection Board (PCIPB)
The White House

- Advisor on privacy and cybercrime-related issues in formulation of the *National Strategy to Secure Cyberspace*.
- Leadership role in the following strategic and implementation issues:
  - enhancing the cybersecurity of the financial services sector;
  - government procurement of secure IT;
  - creation of a government cyber incident sharing and analysis consortium;
  - Education committee's priorities involving creation of a national cybersecurity academy and the initiative to facilitate the formation of a private, independent body for the certification of IT professionals; and
  - development and improvement of cybersecurity awareness and education efforts.

Frequent speaker on behalf of the White House to further stakeholder engagement in the development of the Strategy and to raise cybersecurity awareness.

Chief Deputy General Counsel (1987 to April 2002)[c]
(Acting General Counsel, Nov. 1999 to Jan. 2001)
United States Sentencing Commission

- As a member of the senior management team, provided legal, strategic, administrative, and ethical advice to chair and commissioners, staff director and unit chiefs.
- As Acting General Counsel led the Commission through the historic 2000 and 2001 amendment cycles highlighted by promulgation of the economic crime amendments that dramatically restructured penalties for economic and new technology offenses across the nation.
- Developed expertise on the compliance plans incentivized by the Corporate Guidelines.
- As chief counsel for new technology issues, organized the National Symposium on Sentencing Policy for Economic Crimes and New Technology Offenses (10-01)
- Vice Chair/contract manger for the acclaimed 1995 national conference "Corporate Crime in America: Strengthening the 'Good Citizen' Corporation."
- Frequent speaker and trainer for federal judges, attorneys, and probation office.

---

[b] On detail from the Sentencing Commission.
[c] On detail to the White House.

Counsel (July 1989 to October 1989)[d]
U. S. Senate Impeachment Trial Committee
(Articles Against Judge Walter Nixon)

- Developed committee strategy and procedure.
- Explored the factual and legal issues raised by pre-trial motions and hearings.
- Briefed the full committee in closed meetings and by written memoranda.
- Advised committee members and staff during the trial, and during the Senate Executive Session.
- Co-drafted the committee's report to the full Senate.

Producer for News and Politics (1984-1987)
CBS News nightly broadcast NIGHTWATCH

- Covered national news stories for the Washington Bureau of CBS News (August 1986 on).
- As Producer for News and Politics for the CBS News broadcast NIGHTWATCH, with Charlie Rose,
  - managed news and political coverage and supervised fifteen professional staff members;
  - produced three two-hour specials on law-related issues: police corruption in Philadelphia, organized crime (hosted by Fred Graham), and the Chicago police.

Investigative Producer (1982-1984)
NBC News Magazines

- Managed breaking news coverage and produced news stories for the NBC News Washington Bureau (April to October, 1984).
- Covered national news events, conducted interviews, and produced and packaged news stories for NIGHTLY NEWS, THE TODAY SHOW, NBC NEWS AT SUNRISE, MONITOR and FIRST CAMERA (Consultant/Associate Producer to news magazines from November ‘82 to April 84).

Special Counsel (July 1982 to November 1982)
Committee on Standards of Official Conduct
U.S. House of Representatives

- Led congressional investigation of then-Rep. Fred Richmond (D-NY) into allegations of securities, tax, and other violations.
- Led investigative stage of allegations of drug and sexual abuse of Capitol Hill Pages.

[d] On detail from the Sentencing Commission.

Assistant United States Attorney (April 1979 to June 1982)
Eastern District of Pennsylvania (Philadelphia)
U.S. Department of Justice

- Prosecuted complex white collar crime cases, including: RICO, tax evasion and fraud, embezzlement, narcotics, complex financial fraud, and police corruption.
- Served as Special Assistant U.S. Attorney in Miami (1980) and Atlanta (1981).
- Instructor at the Attorney General's Trial Advocacy Institute.
- Received Outstanding Achievement Award from the U.S. Department of Justice for successful nine-week trial in Atlanta of a $20 million RICO fraud case.

Senior Staff Counsel (December 1976 through December 1978)
Select Committee on Assassinations
U.S. House of Representatives

- Led the investigation into the possibility that Jack Ruby conspired with Lee Harvey Oswald, or others, to kill President John F. Kennedy.
- Led inquiry into the medical/autopsy evidence to determine if there was only one gunman.

EDUCATION

University of Virginia School of Law
Juris Doctor

College of William and Mary
B.A. High Honors (Govt.-Economics)

BAR MEMBERSHIP (INACTIVE)
Washington, D.C., Maryland, Missouri, Pennsylvania

HOBBIES: GOLF, SURFING, AND WORKING OUT.

PUBLICATIONS AND REFERENCES AVAILABLE UPON REQUEST