

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

Forum on Cyber Resilience
Member Biographies
as of 2019-04



Fred B. Schneider (NAE), is Samuel B. Eckert Professor of Computer Science at Cornell University. He joined Cornell's faculty in Fall 1978, having completed a Ph.D. at Stony Brook University and a B.S. in engineering at Cornell in 1975. Schneider's research has always concerned various aspects of trustworthy systems—systems that will perform as expected, despite failures and attacks. Most recently, his interests have focused on system security. His work characterizing what policies can be enforced with various classes of defenses is widely cited, and it is seen as advancing the nascent science base for security. He is also engaged in research concerning legal and economic measures for improving system trustworthiness. Schneider was elected a fellow of the American Association for the Advancement of Science (1992), the Association of Computing Machinery (1995), and the Institute of Electrical and Electronics Engineers (2008). He was named Professor-at-Large at the University of Tromsø (Norway) in 1996 and was awarded a Doctor of Science honoris causa by the University of Newcastle-upon-Tyne in 2003 for his work in computer dependability and security. He received the 2012 IEEE Emanuel R. Piore Award for "contributions to trustworthy computing through novel approaches to security, fault-tolerance and formal methods for concurrent and distributed systems". The U.S. National Academy of Engineering elected Schneider to membership in 2011, the Norges Tekniske Vitenskapsakademi (Norwegian Academy of Technological Sciences) named him a foreign member in 2010, and the American Academy of Arts and Sciences elected him in 2017. He is currently a member of the National Academies Naval Studies Board, Computer Science and Telecommunications Board, and is founding chair of the National Academies Forum on Cyber Resilience.



Yair Amir is Professor of Computer Science and the director of the Distributed Systems and Networks (DSN) lab at Johns Hopkins University. From June 2015 to June 2018, he served as the chair of the Department of Computer Science. His goal is to invent resilient, performant and secure distributed systems that make a difference, collecting friends along the way. Dr. Amir is the recipient of the Alumni Association Excellence in Teaching Award for 2014, the highest teaching award in the Whiting School of Engineering, Johns Hopkins University. He was a finalist for the Excellence in Mentoring and Advising award in 2014 and for an Excellence in Teaching award in 2013. Dr. Amir was nominated for the DARPA agency-wide "Performer with Significant Technical Achievement" award in 2004, and was the recipient of the DARPA Dynamic Coalitions program Bytes-for-Buck trophy in 2002. His work received the Best Paper award in the IEEE International Conference on Distributed Computing Systems (ICDCS) in 2017. Dr. Amir served on various technical program committees including co-chair of the IFIP/IEEE Dependable Systems and Networks (DSN) for 2015, and as an associate editor for the IEEE *Transactions on Dependable and Secure Computing* (2010-2013). He is a creator of the Spread toolkit (www.spread.org), the first scalable group communication system with strong semantics. He led Secure Spread, developing the first robust key agreement protocols, as well as the Spines overlay network platform (www.spines.org), the SMesh wireless mesh network (www.smesh.org), the first seamless 802.11 mesh with fast lossless handoff, the Prime Byzantine replication engine, the first to provide performance guarantees while under attack, and the Spire intrusion-tolerant SCADA for the power grid (www.dsn.jhu.edu), the first to protect against both system-level and network-level attacks and compromises. Some of these technologies are deployed in mission critical systems, support data center applications, are included in commercial products, and are used for research and teaching in universities and research labs around the world. Until 2016, Dr. Amir led the development of the LTN

cloud (www.ltnglobal.com). He continues to provide technical leadership at LTN. LTN offers a global transport service for broadcast-quality live TV that is used by major broadcasters including CNN, Fox, Disney, ABC, Bloomberg, CBS, CNBC, ESPN, NBC, PBS, and Turner. Dr. Amir holds B.Sc. (1985) and M.Sc. (1990) from the Technion, Israel Institute of Technology, and a Ph.D. (1995) from the Hebrew University of Jerusalem, Israel.



Bob Blakley is Global Director of Information Security Innovation at Citigroup. He recently served as Plenary chair of the NSTIC Identity Ecosystem Steering Group and as Research and Development Co-Chair of FSSCC – the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. He is currently a member of the Forum on Cyber Resilience – a National Academies Roundtable. Prior to joining Citigroup, Bob was Distinguished Analyst and Agenda Manager for Identity and Privacy at Gartner and Burton group. Before that, he was Chief Scientist for Security and Privacy at IBM. He is past general chair of the IEEE Security and Privacy Symposium and the ACSA New Security Paradigms workshop. He was awarded ACSA's Distinguished Security Practitioner award in 2002, and is a frequent speaker at information security and computer industry events. Bob was general editor of the OMG CORBASecurity specification and the OASIS SAML specification, and is the author of "CORBASecurity: An Introduction to Safe Computing with Objects", published by Addison-Wesley. He was the first chair of the OATH Joint Coordinating Committee. He also participated in the National Academy of Science's panels "Authentication Technologies and Their Privacy Implications" and "Whither Biometrics". Bob holds twenty patents in cryptography and information security, and he publishes regularly in the academic literature on information security and privacy. Bob received the A.B. in Classics from Princeton University, and the MS and PhD in Computer and Communications Science from the University of Michigan.



Fred H. Cate is vice president for research at Indiana University. He is the distinguished professor and the C. Ben Dutton Professor of Law at the Indiana University Maurer School of Law. He also serves as the managing director of the Center for Law, Ethics, and Applied Research in Health Information and a senior fellow and former founding director of the Center for Applied Cybersecurity Research. Professor Cate specializes in information privacy and security law issues. He has testified before numerous congressional committees and speaks frequently before professional, industry, and government groups. He is a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams, LLP, and is a member of Intel's Privacy and Security External Advisory Board, the Department of Homeland Security's Data Privacy and Integrity Committee Cybersecurity Subcommittee, and the National Security Agency's Privacy and Civil Liberties Panel. He serves on the board of directors of The Privacy Projects, the International Foundation for Online Responsibility, and the Kinsey Institute for Research in Sex, Gender and Reproduction. Previously, Professor Cate served as a member of the Academies' Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention, as counsel to the Department of Defense Technology and Privacy Advisory Committee, as a reporter for the third report of the Markle Task Force on National Security in the Information Age, as a member of the Federal Trade Commission's (FTC's) Advisory Committee on Online Access and Security, and on Microsoft's Trustworthy Computing Academic Advisory Board. He chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities. He served as the privacy editor for IEEE's *Security & Privacy* and is one of the founding editors of the Oxford University Press journal *International Data Privacy Law*. He is the author of more than 150 books and articles, and he appears frequently in the popular press. Professor Cate attended Oxford University and received his J.D. and his A.B. with honors and distinction from Stanford University. He is a senator and fellow (and immediate past president) of the Phi Beta Kappa Society, an elected member of the American Law Institute, and a fellow of the American Bar Foundation.



Katherine Charlet is the inaugural director of Carnegie's Technology and International Affairs Program. She works primarily on the security and international implications of evolving technologies, with a focus on cybersecurity and cyber conflict, biotechnology, and artificial intelligence. Charlet most recently served as the acting deputy assistant secretary of defense for cyber policy, where she managed the development of the U.S. Department of Defense's cyber policy and strategy, the development of cyber capabilities, and the expansion of international cyber relationships. Charlet is the recipient of the Secretary of Defense Meritorious Civilian Service Award and has served in senior advisory roles on the Defense Science Board Task Forces on Cyber Deterrence, on Cyber as a Strategic Capability, and on the Presidential Commission on Enhancing National

Cybersecurity. Prior to working on cyberspace issues, Charlet served as the director for strategic planning at the National Security Council, led teams at the U.S. Department of Defense working on Afghanistan strategy and policy, and conducted research on issues at the nexus of science & security at the Center for Strategic and International Studies.



David D. Clark (NAE) is a Senior Research Scientist at the MIT Computer Science and Artificial Intelligence Laboratory. Since the mid 1970s, Dr. Clark has been leading the development of the Internet; from 1981-1989 he acted as Chief Protocol Architect in this development, and chaired the Internet Activities Board. His current research looks at re-definition of the architectural underpinnings of the Internet, and the relation of technology and architecture to economic, societal and policy considerations. He is helping the U.S. National Science foundation organize their Future Internet Design program. Dr. Clark is a member of the National Academy of

Engineering, and is past chairman of the Computer Science and Telecommunications Board of the National Academies. He has contributed to a number of studies on the societal and policy impact of computer communications. He is co-director of the MIT Communications Futures Program, a project for industry collaboration and coordination along the communications value chain. He is Chair of the Open Internet Advisory Committee at the FCC and is a member of the FCC's Technological Advisory Council. Dr. Clark received his Ph.D. in Computer Science from MIT in 1973.



Richard J. Danzig is Vice Chair of the Board of Trustees of The RAND Corporation, a member of the Defense Policy Board and The President's Intelligence Advisory Board, a Trustee of Reed College, a Director of the Center for a New American Security and a Director of Saffron Hill Ventures (a European investment firm). Recently he has been a director of National Semiconductor Corporation (NY Stock Exchange) and Human Genome Sciences Corporation (NASDAQ). He has also served as The Chairman of the Board of The Center for a New American Security and Chairman of the Board of the Center for Strategic and Budgetary Assessments. From the spring of 2007 through the Presidential election of 2008, Dr. Danzig was a senior advisor to Senator Obama on national security issues. Dr. Danzig served as the 71st Secretary of the Navy from November 1998 to January 2001. He was the Under Secretary of the Navy between 1993 and 1997. Dr. Danzig is a member

of the Aspen Strategy Group and a senior advisor at the Center for New American Security, the Center for Naval Analyses, and the Center for Strategic and International Studies in Washington DC. His primary activity is as a consultant to the Departments of Defense and Homeland Security on terrorism.



Eric Grosse builds open systems and advises companies on security. He retired from Google as Vice President, Security and Privacy Engineering where his team achieved improved and wider use of SSL, stronger consumer authentication technology, detection and blocking of espionage, transparency on legal requests for data, sophisticated malware analysis, and build tools and frameworks for safer web applications. Before Google, Dr. Grosse was a research director and fellow at Lucent Bell Labs where he worked on security, networking, algorithms for approximation and visualization, software distribution, and scientific computing. He has a Ph.D. in computer science from Stanford University. More at n2vi.com.



Paul Kocher (NAE) is an independent researcher and entrepreneur. Most recently he was President and Chief Scientist of Cryptography Research, a Division of Rambus. Mr. Kocher has gained an international reputation for his research and innovative designs in cryptography. An active contributor to major conferences and leading security initiatives, Mr. Kocher has designed numerous cryptographic applications and protocols which are successfully deployed in real world systems. His accomplishments include discovering timing attacks and Differential Power Analysis (including techniques for preventing against these vulnerabilities), helping author the widely used SSL 3.0 standard, and leading the design of the record breaking DES Key Search machine. He has recently focused on developing anti-piracy technologies for securing digital content. Mr. Kocher was elected to the National Academy of Engineering in 2009. Paul founded Cryptography Research

and leads the company as its President & Chief Scientist. He previously held positions at RSA Security and was a founding member of Valicert, Inc. (now Tumbleweed). He holds a B.S. degree from Stanford University.



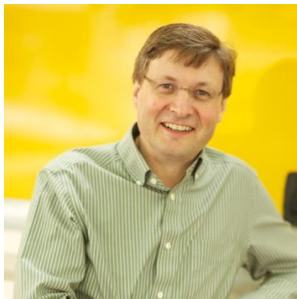
Butler W. Lampson (NAS, NAE) is a Technical Fellow at Microsoft Corporation and an Adjunct Professor at MIT. He has worked on computer architecture, local area networks, raster printers, page description languages, operating systems, remote procedure call, programming languages and their semantics, programming in the large, fault-tolerant computing, transaction processing, computer security, WYSIWYG editors, and tablet computers. He was one of the designers of the SDS 940 time-sharing system, the Alto personal distributed computing system, the Xerox 9700 laser printer, two-phase commit protocols, the Autonet LAN, the SPKI system for network security, the Microsoft Tablet PC software, the Microsoft Palladium high-assurance stack, and several programming languages. He received the ACM Software Systems Award in 1984 for his work on the Alto, the IEEE Computer

Pioneer award in 1996 and von Neumann Medal in 2001, the Turing Award in 1992, and the NAE's Draper Prize in 2004. He is a member of the National Academy of Sciences and the National Academy of Engineering and a Fellow of the Association for Computing Machinery and the American Academy of Arts and Sciences.



Susan Landau is Bridge Professor of Cyber Security and Policy in the Fletcher School of Law and Diplomacy and the School of Engineering, Department of Computer Science, Tufts University. Landau works at the intersection of cybersecurity, national security, law, and policy. Her new book, *Listening In: Cybersecurity in an Insecure Age*, was published by Yale University Press in 2017; Landau is also the author of *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, (MIT Press, 2011) and *Privacy on the Line: the Politics of Wiretapping and Encryption*, co-authored with Whitfield Diffie (MIT Press, 1998). Landau's early work was on fast algorithms for algebraic problems; for the past twenty years

she has focused on issues in cybersecurity, national security, and privacy, with particular emphasis on cryptography policy, surveillance, and communications metadata. She has testified before Congress and frequently briefed US and European policymakers on encryption, surveillance, and cybersecurity issues. Landau has been a Senior Staff Privacy Analyst at Google, a Distinguished Engineer at Sun Microsystems, and a faculty member at Worcester Polytechnic Institute, the University of Massachusetts Amherst, and Wesleyan University. She has served on the National Academies Computer Science and Telecommunications Board (2010-2016), and the National Science Foundation Computer and Information Advisory Board (2010-2013). A 2015 inductee in the Cybersecurity Hall of Fame and a 2012 Guggenheim fellow, Landau was a 2010-2011 fellow at the Radcliffe Institute for Advanced Study and the recipient of the 2008 Women of Vision Social Impact Award. She is also a fellow of the American Association for the Advancement of Science and of the Association for Computing Machinery.



John Launchbury is the Chief Scientist at Galois, collaborating with government and industry leaders to fundamentally improve the security of software and cyber-physical systems through applied formal mathematical techniques. Prior to rejoining Galois in 2017, John was the Director of the Information Innovation Office (I2O) at DARPA, where he led nation-scale investments in cybersecurity and artificial intelligence. Before founding Galois in 1999, Dr. Launchbury was a full professor in Computer Science, and he is internationally recognized for his work on the analysis and semantics of functional programming languages. John received First Class Honors in Mathematics from Oxford University in 1985. He holds a Ph.D. in Computing

Science from University of Glasgow and won the British Computer Society's distinguished dissertation prize. In 2010, John was inducted as a fellow of the Association for Computing Machinery (ACM).



Steven B. Lipner (NAE) is executive director of SAFECode, a non-profit organization dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. He retired in 2015 as partner director of software security in Trustworthy Computing at Microsoft Corporation. His expertise is in software security, software vulnerabilities, Internet security, and organization change for security. He is the founder and long-time leader of the Security Development Lifecycle (SDL) team that has delivered processes, tools and associated guidance and oversight that have significantly improved the security of Microsoft's software. Mr. Lipner has over 40 years of experience as a researcher, development manager, and general manager in IT security. He served as executive vice president and

general manager for Network Security Products at Trusted Information Systems and has been responsible for the development of mathematical models of security and of a number of secure operating systems. Mr. Lipner was one of the initial 12 members of the U.S. Computer Systems Security and Privacy Advisory Board (now the Information Security and Privacy Advisory Board) and served two terms and a total of ten years on the board. He is the author of numerous professional papers and has spoken on security topics at many professional conferences. He is named as inventor on 12 U.S. patents in the fields of computer and network security and has served on numerous scientific boards and advisory committees, including as a current member of the NRC Committee on Future Research Goals and Directions for Foundational Science in Cybersecurity and the NRC Committee on Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption: Options and Tradeoffs. Mr. Lipner was elected in 2015 to the National Cybersecurity Hall of Fame and in 2017 to the National Academy of Engineering.



John Manfredelli is Professor of the Practice and executive director of the Cybersecurity and Privacy Institute at Northeastern University. Immediately prior, Manfredelli was Engineering Director for Production Security Development at Google. Prior to Google, he was a senior principal engineer at Intel Corporation and co-PI (with David Wagner) for the Intel Science and Technology Center for Secure Computing at the University of California at Berkeley. He was also a member of the Information Science and Technology advisory group at DARPA and is a member of the Defense Science Board. Prior to Intel, J Manfredelli was a distinguished engineer at Microsoft and was an affiliate faculty member in computer science at the University of Washington. He was responsible for computer security, cryptography, and systems research, as well as research in quantum computing. At

Microsoft, John also worked as a senior researcher, software architect, product unit manager, general manager at Microsoft and was responsible the development of the next-generation secure computing base technologies and the rights management capabilities currently integrated into Windows, for which he was the original architect. He joined Microsoft in February 1995 when it acquired his company, Natural Language Inc., based in Berkeley, California. At Natural Language, Manfredelli was the founder and, at various times, vice president of research and development and CEO. Other positions he has held include staff engineer at TRW Inc., computer scientist and mathematician at Lawrence Livermore National Laboratory, and principal investigator at Bell Labs. He was also an adjunct associate professor at Stevens Institute of Technology. Manfredelli's professional interests include cryptography and cryptographic mathematics, combinatorial mathematics, operating systems, and computer security. He is also a licensed Radio Amateur (AI6IT). Manfredelli has a bachelor's degree in physics from Cooper Union for the Advancement of Science and Art and a PhD in mathematics from the University of California, Berkeley.



Deirdre K. Mulligan is an Associate Professor in the School of Information at UC Berkeley, a faculty Director of the Berkeley Center for Law & Technology, and a PI on the new Hewlett funded Berkeley Center for Long-Term Cybersecurity. Mulligan's research explores legal and technical means of protecting values such as privacy, freedom of expression, and fairness in emerging technical systems. Her book, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*, a study of privacy practices in large corporations in five countries, conducted with UC Berkeley Law Prof. Kenneth Bamberger was recently published by MIT Press. Mulligan and Bamberger received the 2016 International Association of Privacy

Professionals Leadership Award for their research contributions to the field of privacy protection. She is a member of the National Academy of Science Forum on Cyber Resilience. She is Chair of the Board of Directors of the Center for Democracy and Technology, a leading advocacy organization protecting global online civil liberties and human rights; a trustee of the recently announced Partnership for AI, and a founding member of the standing committee for the AI 100 project, both focused on understanding and guiding developments in artificial intelligence to benefit society; and a founding member of the Global Network Initiative, a multi-stakeholder initiative to protect and advance freedom of expression and privacy in the ICT sector, and in particular to resist government efforts to use the ICT sector to engage in censorship and surveillance in violation of international human rights standards. She is a Commissioner on the Oakland Privacy Advisory Commission. Prior to joining the School of Information, she was a Clinical Professor of Law, founding Director of the Samuelson Law, Technology & Public Policy Clinic, and Director of Clinical Programs at the UC Berkeley School of Law.



Audrey L. Plonk is the director of government in public policy at Intel. She is a seasoned public policy professional with 13 years of experience working at the intersection of high technology, public policy and business strategy. As a Senior Director of Public Policy at Intel Corporation, Audrey leads a global team of policy experts focused on connectivity, data, artificial intelligence and autonomous driving policy issues. She also specialized in China cyber policy and advises Intel business and product teams on China strategy. Prior to joining Intel in 2008, Audrey worked for the Organisation for Economic Co-operation and Development (OECD) based in Paris, France. Audrey led the OECD's security policy work on critical information infrastructure protection and malware. In that role, she also served as

liaison to the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group, the International Telecommunication Union and the Internet Governance Forum. From 2003 to 2006, Audrey worked as a consultant for the U.S. Department of Homeland Security's National Cyber Security Division, primarily focusing on international cybersecurity policy issues in their International Affairs Division. Audrey attended The George Washington University in Washington, D.C. and received her B.A. in international affairs with a focus on the European Union and received a double minor in French and dance.



Tony Sager is a Senior VP and Chief Evangelist for the Center for Internet Security. He leads the development of the *CIS Critical Security Controls*, a worldwide consensus project to find and support technical best practices in cybersecurity. Tony also serves as the Director of the SANS Innovation Center, a subsidiary of The SANS Institute. Tony retired from the National Security Agency (NSA) after 34 years as an Information Assurance professional. He started his career in the Communications Security (COMSEC) Intern Program, and worked as a mathematical cryptographer and a software vulnerability analyst. In 2001, Tony led the release of NSA security guidance to the public. He also expanded NSA's role in the development of open standards for security. Mr. Sager holds a B.A. in Mathematics from Western Maryland College and an M.S. in Computer Science from The Johns Hopkins University.



Peter Swire is the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business. He has appointments by courtesy with the College of Computing and School of Public Policy. In 2015, the International Association of Privacy Professionals, among its over 20,000 members, awarded him its Privacy Leadership Award. In 2013, he served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. In 2012-13, he was global co-chair of the Do Not Track standard of the World Wide Web Consortium. In 2009-10, he was Special Assistant to the President for Economic Policy, in the National Economic Council. He is Senior Fellow with the Future of Privacy Forum, and Senior Counsel with Alston & Bird, LLP. Under President Clinton, Swire was Chief Counselor for Privacy in the Clinton Administration, the first person to have U.S. government-wide responsibility for privacy policy. His activities in that role included being White House coordinator for the HIPAA Privacy Rule, chairing a White House Working Group on encryption, and helping negotiate the Safe Harbor agreement with the E.U. Swire is author of six books and numerous scholarly papers. He has testified often before the Congress, and been quoted regularly in the press. Swire graduated from Princeton University, summa cum laude, and the Yale Law School, where he served as an editor of the Yale Law Journal.



Parisa Tabriz is the Director of Engineering at Google, Inc. She manages Google's information security engineering team at Google, which is responsible for improving Google's product security. This team of "hired hackers" conducts security design and code reviews, builds and enhances Google technology to make secure development possible and easy, conducts security engineering training, and does vulnerability response. Parisa received her B.S. and M.S. from the University of Illinois, Urbana-Champaign and was

advised by Nikita Borisov.



Mary Ellen Zurko is a staff member at MIT Lincoln Laboratory and was recently a member of the Office of the CTO, Security Business Group, at Cisco Systems, and a Principal Engineer on the Next Generation Firewall team there. Mez has worked extensively in security; in product development, early product prototyping, and in research, and has over 20 patents. She was security architect of one of IBM's earliest clouds; SaaS for business collaboration. She defined the field of User-Centered Security in 1996. As a senior research fellow at the Open Group Research Institute, she led several innovative security initiatives in authorization policies, languages, and mechanisms that incorporate user-centered design elements. She started her security career at DEC working on an A1 VMM, on which she recently coauthored a retrospective with a fellow member of the Forum on Cyber Resilience. She has written on active content security, public key infrastructures, distributed authorization, user-centered security, and security and

the web. She is a contributor to the O'Reilly book "Security and Usability: Designing Secure Systems that People Can Use." She is on the steering committees of New Security Paradigms Workshop and Symposium on Usable Privacy and Security. Mez received S.B and S.M. degrees in computer science from MIT.

Staff



Lynette I. Millett is the Director of the Forum on Cyber Resilience and Associate Director of the Computer Science and Telecommunications Board, National Research Council of the National Academies. Ms. Millett has extensive experience as program manager, team leader, analyst, researcher, and writer with specific expertise in information technology policy. She is skilled in working with diverse and expert work groups and since 2000 has been developing, directing, and overseeing National Research Council studies and teams of national experts examining public policy issues related broadly to information technology, computing, software, and communications. Her

portfolio at the National Research Council includes a suite of studies on computing research, several examinations of government IT and infrastructure needs, and in-depth explorations of privacy, identity and cybersecurity. She has a proven track record of leading and working with diverse ad hoc teams to produce actionable, authoritative, and independent advice in fast-moving policy and technical environments. She has an M.Sc. in computer science from Cornell University, where her work was supported by graduate fellowships from the National Science Foundation and the Intel Corporation; and a B.A. with honors in mathematics and computer science from Colby College, where she was elected to Phi Beta Kappa.



Emily Grumbling is a Program Officer at the Computer Science and Telecommunications Board of the National Academies. She previously served as an AAAS Science and Technology Policy Fellow in the Directorate for Computer and Information Science and Engineering at the National Science Foundation (2012-2014), and an ACS Congressional Fellow in the U.S. House of Representatives (2011-2012). Emily received her Ph.D. in Physical Chemistry from the University of Arizona in 2010, and her B.A. with a double-major in Chemistry and Film/Electronic Media Arts from Bard College in 2004.



Katiria Ortiz is an Associate Program Officer at the Computer Science and Telecommunications Board of the National Academies. She previously served as a Research Associate for CSTB. Before joining the Academies, she served as an intern for the FBI and as an Undergraduate Research Assistant at the Cybersecurity Quantification Laboratory at the University of Maryland. She received her M.A. in International Science and Technology Policy from the George Washington University in 2016 and a dual-degree from the University of Maryland in Cell Biology and Molecular Genetics and Criminology and Criminal Justice in 2014.