2018NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

Bios for Speakers, Authors, Program Committee Members, Organizers, and Student Awardees

*In alphabetical order by surname*

**Maggie Ahern** is a Junior at Lehigh University studying Computer Science and Engineering. Maggie is on the executive board of her university's Society of Women Engineers and has hosted STEM workshops and served as a counselor at STEM camps for young girls.

\*

**Grant A. Allard** is pursuing his doctorate in Policy Studies at Clemson University. Allard’s research agenda focuses on how science and technology policy and national politics affect the capacities of universities, governments, and industry to translate scientific research into new technologies such as cyberinfrastructure. Allard’s research is transdisciplinary in scope using theory and research methods from policy studies, political science, economics, information science, and sociology.

Allard is interested in cybersecurity because of its vital role in maintaining the integrity of scientific cyberinfrastructure from both policy and technology transfer perspectives. From a policy perspective, it is important to understand how to integrate cyber security into scientific cyberinfrastructure projects without negatively affecting the scientific research process. Many scientific cyberinfrastructure projects are governmentally funded as extramural research meaning it is important to understand the decisions of governments related to promoting cybersecurity. From a technology transfer perspective, it is important to understand how to promote cybersecurity during the process of transferring scientific cyberinfrastructure from the “safer” environment of the laboratory to the “less safe” commercial or government environment.

\*

**Warren Anderson** has a Ph.D. in theoretical physics from the University of Alberta and is the co-author of "Gravitational Wave Physics and Astronomy." He has been a member of the LIGO Scientific Collaboration for the last 20 years, where he has gradually transitioned from physics research to managing computational infrastructure. He has been the lead of the LIGO Identity and Access Management team since 2008 and a member of the LIGO Scientific Collaboration Security Committee since 2012. He has chaired or been a member of several InCommon committees and is currently a member of the the InCommon Community Architecture Committee for Trust and Identity.

\*

**Kay Avila** (kayavila@illinois.edu) is a senior security engineer at the National Center for Supercomputing Applications (NCSA) at the University of Illinois in Urbana-Champaign, where she works on Trusted CI and the Large Synoptic Survey Telescope (LSST) projects.  Since joining Trusted CI in 2017, she has been involved with several engagements focused on developing and assessing security programs.  Prior to this, she held positions in network security at a Fortune 500 insurance company and in higher education.  Kay studied computer science and biology at the University of Northern Iowa.

\*

**Steve Barnet**

\*

**Tom Barton** is Sr. Consultant for Cyber Security & Data Privacy at the University of Chicago and a consultant to Internet2. Previously he was Senior Director and Chief Information Security Officer at U Chicago, and had earlier assignments as Director of IT Infrastructure and Director of Network Services at the University of Memphis, where he was a member of the mathematics faculty before turning to administration. He's a member of the Advisory Committee for Trusted CI, the NSF Cybersecurity Center of Excellence, Internet2’s Community Architecture Committee for Trust and Identity (CACTI), the TIER Community Investors Council, the REFEDS Steering Committee, chaired the TIER Ad Hoc Advisory committee obsoleted by CACTI, and for many years led the Internet2 Grouper project.

\*

**Dr. Jim Basney** is a senior research scientist in the cybersecurity group at the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign. Jim's area of expertise is identity management for scientific collaborations. He is PI of the CILogon and SciTokens projects and co-PI of the Center for Trustworthy Scientific Cyberinfrastructure and the Software Assurance Marketplace. Jim also contributes to the LIGO, LSST, and XSEDE projects. Jim received his PhD in computer sciences from the University of Wisconsin-Madison.

\*

**Tony Baylis** is the senior management advocate for diversity and inclusion for the Laboratory. Tony is responsible for overseeing the laboratory’s interactions and successful execution in building, partnering and collaborating with governmental, educational, industrial, community interests and other stakeholders. LLNL has had a long history in working with Minority Serving Institutions, specifically relationships with American Indian Institutions, Hispanic Institutions, and Historically Black College and Universities. He represents the Laboratory on the subjects of Diversity and Inclusion, STEM, Outreach Efforts, and Student Programs.

Tony's career represents 31 years of administrative, project, program, technical, and organizational management. He has worked in a scientific and technical environment for over 23 years and has worked as a consultant in industry as well. Tony has extensive experience networking with a broad range of academic, industry, government and non-profit organizations that has educated him and helped him in his career. He is a DOE Minorities in Energy Champion for the department and also serves on a number of conference program committees and advisory boards that promote STEM and diversity in science and technical careers.

\*

**Richard Biever** is Duke University's chief information security officer and director of identity management. The IT Security Office facilitates IT security initiatives for the university, working closely with our counterparts in the Duke health system, and coordinates campus-wide security efforts through the Security Liaisons Group, which comprises IT security people from departments and schools across Duke. The identity management team manages Duke's electronic identities (also known as NetIDs) as well as the mechanisms used for user authentication and authorization.

Richard joined Duke in February 2011, after previously holding positions with the Georgia Institute of Technology's Office of Information Technology and Hewlett Packard.

Richard is an experienced security professional with SANS GIAC Certified Enterprise Defender (GSED) and Certified Information Systems Security Professional (CISSP) credentials. He holds a bachelor’s degree in political science from the University of Georgia and a master’s degree in international relations from Georgia State University.

\*

**Leslee A. Bohland** serves as the Administrative & Finance Director at Indiana University’s Center for Applied Cybersecurity Research (CACR). She is a graduate of the IU School of Business (B.S. ’93).

Leslee comes to the CACR and CTSC from a background in Management, Finance and Accounting. She has worked with government divisions, as well as in the private sector.

\*

**Diana Borecky** serves as the Events & Communications Manager at Indiana University’s Center for Applied Cybersecurity Research (CACR).  She has worked for IU for 19 years in the IU UITS Finance office, before joining CACR in 2016.

\*

**Michael Corn**

\*

**Robert (Bob) Cowles** is a principal in BrightLite Information Security performing cybersecurity assessments and consulting in research and education about information security. He served as CISO at SLAC National Accelerator Laboratory (1997-¬2012); participated in the development of security policies and procedures for the LHC Computing Grid (2001-¬2008); and was an instructor at the University of Hong Kong in information security (2000¬-2003). A contributor to Indiana University's CACR since 2013, he participated in the XSIM project on identity management and has been working with CTSC since 2015. In 2017, he was honored to be named as a CACR Senior Fellow.

\*

**Sanchari Das** is a PhD Student in the School of Informatics, Computing, and Engineering at Indiana University Bloomington. A security track researcher, her work includes studies in Usable Privacy and Security, User Experience, Social Media Research, and Human-Computer Interaction. Her double Masters degrees were received from Indiana University Bloomington and Jadavpur University, Kolkata, India. She received her Bachelor's in Computer Applications from The Heritage Academy, Kolkata, India and was a Gold-medalist in her batch. She has also interned in prestigious organizations including Infosys Limited and HCL Technologies.

\*

**Erik Deumens** is director for Research Computing in University of Florida Information Technology since 2011. He has a background in computational physics and has architected and written software for simulation of molecular reactions and structure. He is the architect of the super instruction architecture for scaling computational software to ten thousand CPU cores and hundred GPUs. Since 2015 he has been working on designing and implementing cyberinfrastructure for secure and compliant computing to meet FISMA and CUI requirements for research projects.

\*

**Emily Dillon** is currently a technical engineering analyst for the Information Security department at Ascension Technologies. There her focus is on IoT/ medical device security and compliance. Emily is pursuing her Master of Science in Information Assurance and Cybersecurity.

\*

**Rion Dooley** is principal investigator on the Agave Project a Science-as-a-Service API platform allowing researchers worldwide to manage data, run code, collaborate freely, and integrate their science anywhere. His previous projects span areas of identity management, distributed web security, full-stack application development, data management, cloud services, and high performance computing. Rion earned a Ph.D. in computer science from Louisiana State University. Rion actively puts his wife and two daughters at the top of his list of accomplishments. He hopes his work can someday edge out dancing teddy bears and smear-proof lipstick on their lists of favorite inventions.

\*

**Jeannette Dopheide** is senior education outreach and training coordinator at NCSA. Her experience in education and outreach began as a high school teacher before moving onto business systems analysis and applications training for a commercial software company. Jeannette joined Trusted CI and NCSA in 2014 and works primarily on education outreach for projects that impact both Trusted CI and NCSA. Jeannette is a graduate of Illinois State University.

\*

**Leah Dorman** is a student at the University of Maine-Augusta studying Business Management, with a concentration in Computer Information Systems. Many of her research and presentations have rooted from her work and interest in Cybersecurity. Along with being a student, she also works on the Information Systems Security team at Eastern Maine Healthcare Systems, where her role has involved implementing an Identity & Access Management provisioning system, leading the user provisioning of several clinical, financial, and technical systems, as well as reviewing, testing, and implementing security plans and providing technical support, system documentation, and training materials to end users. Her career in Cybersecurity has led to the opportunity to present an Identity & Access Management Solution to other potential IAM customers as well as presenting at the Maine Science Festival, to make kids in the community both aware of the threats, but also to spark interest in possible future careers in the field. Identity & Access Management is so crucial to Cybersecurity now and due to her experience with it, it has become a passion of hers to help her company develop it further and use the automation functionality to its full advantage in order to cut down on internal risks.

\*

**Amy Friedlander** was named Deputy Office Director in the Office of Advanced Cyberinfrastructure, Directorate for Computer and Information Science and Engineering (CISE/OAC) in January, 2016 where she had served as Acting Deputy Division Director since November, 2014. Since joining NSF in 2010, she has led several strategic activities, including SBE 2020, resulted in the widely-distributed report *Rebuilding the Mosaic (2011)*, and coordination of NSF-wide activities for the Public Access Initiative.

Prior to her NSF appointment, Dr. Friedlander held positions in the non-profit and private sectors, which included establishing the Washington, DC cultural resource management office for an international consulting firm with a substantial nation-wide program in environmental management and compliance; leading the firm’s first international preservation planning project; and serving as senior program manager for the DHS-funded DNSSEC deployment project. She participated in the Blue Ribbon Task Force on Sustainable Digital Preservation and Access, funded largely by NSF; led the initial strategic planning for the Library of Congress’ National Digital Information Infrastructure and Preservation Program; and served as editor-in-chief of the ACM *Journal on Computing and Cultural Heritage*. At the Corporation for National Research Initiatives, she was the founding editor of D-Lib Magazine ([www.dlib.org](http://www.dlib.org)) and the author of a series of studies of the historical development large-scale technology infrastructures in the U.S.

Dr. Friedlander graduated from Vassar College, where she was elected to Phi Beta Kappa, and holds the M.A. and Ph.D. in History from Emory University and the M.S.L.I.S. from The Catholic University of America.  She pursued postdoctoral work on quantitative methods and computer-assisted social science research at the Newberry Library in Chicago, IL.

\*

**Dr. David Halstead**

\*

**Grayson Harbour** is a member of the Class of 2019 at the Indiana University Maurer School of Law in Bloomington. He is also pursuing his masters degree in cybersecurity risk management. His current work encompasses analyzing cybersecurity regulation and developing policy to ensure a secure, economic, and valuable IT environment for the scientific community at large. He is a graduate of the School of Journalism (B.A.J. 2015, Indiana University Bloomington) and a former Press Freedom Fellow at the International Press Institute in Vienna, Austria. Before law school Grayson was a writer and assistant to multiple documentary production companies in Los Angeles.

\*

**Elisa Heymann** is a Senior Scientist at the Computer Sciences Department of the University of Wisconsin­Madison, and an Associate Professor in the Computer Architecture and Operating Systems Department at the Autonomous University of Barcelona (UAB). She co­directs the MIST software vulnerability assessment project in collaboration with her colleagues at the University of Wisconsin. Heymann is part of Trusted CI, the NFS cyber security center for excellence, where she works on Software Assurance training and engagements.

Heymann carries out training in universities, companies, and conferences around the world. Heymann's research interests include security and resource management for Grid and Cloud environments, and cyber­security in transportation. Her research is supported by NSF, the Spanish government, the European Commission, and NATO.  Heymann received her M.S. and Ph.D. degrees in Computer Science from the Autonomous  University  of Barcelona (Spain) in 1995 and 2001 respectively.

\*

**Florence Hudson** is on the Program Committee for the 2018 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure. She is Special Advisor for Next Generation Internet at the Northeast Big Data Innovation Hub at Columbia University, on the Editorial Board for the journal Blockchain in Healthcare Today, Co-Founder of the IEEE-ISTO Blockchain in Healthcare Global, and Founder & CEO of Florence D. Hudson International, LLC, consulting on advanced technology and diversity & inclusion.  Hudson was PI for the NSF SaTC EAGER: Cybersecurity Transition to Practice (TTP) Acceleration (NSF award 1650445). Through this EAGER, Florence worked with a team to bring together cybersecurity researches with CI and cybersecurity practitioners including CIOs, CISOs, industry, regional networks and start-ups to enable collaboration and matchmaking between cybersecurity researchers and practitioners, creating opportunities to accelerate cybersecurity research transition to practice. Formerly an IBM Vice President and Chief Technology Officer, and Internet2 Senior Vice President and Chief Innovation Officer, she earned a BSE in Mechanical and Aerospace Engineering at Princeton University, and attended executive education at Harvard Business School and Columbia University.

\*

**Craig Jackson** (scjackso@iu.edu) is Chief Policy Analyst at the Indiana University Center for Applied Cybersecurity Research (CACR), where his research interests include information security program development and governance, cybersecurity assessments, legal and regulatory regimes' impact on information security and cyber resilience, evidence-based security, and innovative defenses. He is a Co-PI of the NSF Cybersecurity Center of Excellence, and leads CACR’s collaborative efforts with Naval Surface Warfare Center Crane, where he is presently employed as temporary faculty. He is a co-author of *Security from First Principles: A Practical Guide to the Information Security Practice Principles*. Craig is a graduate of the IU Maurer School of Law, IU School of Education, and Washington University in St. Louis. In addition to his litigation experience, Craig’s research, design, project management, and psychology background includes work at the IU Center for Research on Learning and Technology and the Washington University in St. Louis School of Medicine.

\*

**Ryan Kiser** is a System Analyst at the Indiana University Center for Applied Cybersecurity (CACR) and Trusted CI. Ryan comes to CACR and Trusted CI from a system administration and small business consulting background. In addition to his role with Trusted CI, his current responsibilities include performing security assessments for public and private sector IT systems as well as risk assessment and regulated data efforts for Indiana University's central IT systems.

\*

**Charley Kneifel**, PhD, is Senior Technical Director at OIT. He joined Duke University in 2012. Dr. Kneifel manages Duke’s central technology infrastructure and Software Defined Networking Project. He has coordinated several technology grants at Duke including the National Science Foundation’s Data Infrastructure Building Blocks (DIBBS) grant to build campus cyberinfrastructures.

Prior to working at Duke, Dr. Kneifel was chief information officer at the American Kennel Club for nine years. He has also held multiple technical positions at NC State University. Dr. Kneifel holds a B.S. in Chemistry from Carnegie Mellon University and a Ph.D. in Chemistry from the State University of New York at Stony Brook.

\*

**Richard Knepper** is Deputy Director of the Cornell University Center for Advanced Computing, which provides the Red Cloud private cloud service for Cornell, and is the leading institution of the Aristotle Federated Cloud program, one of the NSF's Data-Intensive Building Blocks Programs.  In his role at the CAC, Dr. Knepper works to help Cornell researchers meet their computational needs and is manager of the NSF XSEDE project's Cyberinfrastructure Resource Integration team.  In his research, Dr. Knepper examines the virtual organizations supporting large-scale cyberinfrastructure, their evolution and support of science disciplines over time.

\*

**Mark Krenz** is the Lead Security Analyst at Indiana University's Center for Applied Cybersecurity Research with over two decades of experience in information security and system administration spread across multiple sectors. His interests at CACR include policy development, operational security development, security auditing and security education. He studied Computer Science and Mathematics at Indiana University.

\*

**John Michael Lowe** is the senior engineer for the National Science Foundation’s Jetstream project.  He has been working in HPC, virtualization, and cloud computing at Indiana University for the past 12 years.

\*

**James A. Marsteller**, Jr. is the Pittsburgh Supercomputer Center Chief Information Security Officer. He has extensive security leadership experience with the TeraGrid and XSEDE security operations team and is a Co-PI for the Center For Trustworthy Scientific Cyberinfrastructure, the NSF Cybersecurity Center of Excellence. James also has served as the program chair for annual NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure since 2007. He has also served on the board of directors for the Pittsburgh chapter of the FBI Infragard program for many years. He holds a Master of Information Technology Management from Carnegie Mellon University and is a Certified Information Systems Security Professional.

\*

**Dr. Daniel Massey**

\*

**Dr. Ashwin J. Mathew** is a visiting scholar and lecturer at the UC Berkeley School of Information, a fellow at the Slow Science Institute, and a researcher at Packet Clearing House. He studies trust and

coordination problems in the operation of Internet infrastructure, focusing on the relationships, practices, and institutions of the Internet's technical personnel. He holds Ph.D. and Masters degrees from the UC Berkeley School of Information. Prior to his doctoral work, Dr. Mathew spent a decade working as a software engineer and technical architect in companies such as Adobe Systems and Sun Microsystems.

\*

**Kim Milford** began serving as Executive Director of REN-ISAC in April 2014. She works with members, partners, sponsors, and advisory committees to direct strategic objectives in support of members, providing services and information that allow higher educational institutions to better defend local technical environments and is responsible for overseeing administration and operations.

Since joining Indiana University in June 2007, Ms. Milford has served in several roles leading strategic IT initiatives. As Chief Privacy Officer, she coordinated privacy-related efforts while serving on IU's Assurance Council, chairing the Committee of Data Stewards, and directing the work of the University Information Policy Office including IU's IT incident response team. From 2005 – 2007, Ms. Milford worked as Information Security Officer at the University of Rochester leading an information security program that included disaster recovery planning, identity management, incident response, and user awareness. In her position as Information Security Manager at University of Wisconsin-Madison from 1998 - 2005, she assisted in establishing the university's information security department and co-led in the development of an annual security conference.

Ms. Milford provides cybersecurity, information policy, and privacy expertise and presentations at national and regional conferences, seminars and consortia. Ms. Milford has a B.S. in Accounting from Saint Louis University in St. Louis, Missouri and a J.D. from John Marshall Law School in Chicago, Illinois.

\*

**Barton Miller** the Vilas Distinguished Achievement Professor and the Amar and Belinder Sohi Professor in Computer Sciences at the University of Wisconsin-Madison. He is Chief Scientist for the DHS Software Assurance Marketplace research facility. He co­directs the MIST software vulnerability assessment project in collaboration with his colleagues at the Autonomous University of Barcelona. He also leads Paradyn Parallel Performance Tool project, which is investigating performance and instrumentation technologies for parallel and distributed applications and systems. His research interests include systems security, binary and malicious code analysis and instrumentation extreme scale systems, and parallel and distributed program measurement and debugging.

Miller's research is supported by the U.S. Department of Homeland Security, U.S. Department of Energy, National Science Foundation, NATO, and various corporations. In 1988, Miller founded the field of Fuzz random software testing, which is the foundation of many security and software engineering disciplines. In 1992, Miller (working with his then­student, Prof. Jeffrey Hollingsworth) founded the field of dynamic binary code instrumentation and coined the term “dynamic instrumentation”. Dynamic instrumentation forms the basis for his current efforts in malware analysis and instrumentation.

Miller was the chair of the IDA Center for Computing Sciences Program Review Committee, a member of the Los Alamos National Laboratory Computing, Communications and Networking Division Review Committee, and has been on the U.S. Secret Service Electronic Crimes Task Force (Chicago Area), the Advisory Committee for Tuskegee University's High Performance Computing Program, and the Advisory Board for the International Summer Institute on Parallel Computer Architectures, Languages, and

Algorithms in Prague. Miller received his Ph.D. degree in Computer Science from the University of California, Berkeley in 1984. He is a Fellow of the ACM.

\*

**Austin Mitts** is the Information Technology Support Specialist for Indiana University's Center for Applied Cybersecurity Research (CACR). He has been with CACR and Trusted CI since March 2018. Austin has a Bachelor’s Degree in Informatics from Indiana University’s School of Informatics and Computing.

\*

**Laura Paglione** is an entrepreneurial, technically versatile, resourceful leader who thrives at the intersection of creative, technical and business environments. She currently serves as the Director of Strategic Initiatives, and was formerly the Technical Director of ORCID, where she directed the technical efforts in ORCID’s mission to address name ambiguity for researchers, and serve as a gateway to connect their research activities from disparate sources. Previously as Director, Advancing Innovation at the Kauffman Foundation, Laura directed the efforts of the iBridge Network, an innovation catalyst for university collaboration and technology commercialization. In prior positions at Ford Motor Company and Avid Technology, as well as several start-up/gazelle companies, Laura has turned around, launched and led 4 other high-profile initiatives, the most visible of which was for Ford Motor Company’s Board of Directors.

\*

**Susan Ramsey** is a Risk Assessor and Security Engineer at the National Center for Atmospheric Research. She has over twenty years of experience building enterprise infrastructure and cloud computing. She joined NCAR in 2014 and promptly launched multiple initiatives to tackle compliance and identity management. Her latest projects include building a FISMA moderate segment and an organization wide Continuous Monitoring Plan. She has an MS in Computer Information Technology from Regis University, (thesis on Vulnerability Assessment). She is currently working towards a second Master of Science degree, in Information Security Engineering, from SANS Technical Institute.

\*

**Preston Ruff** is a senior undergraduate student who studies computer science at New Mexico Tech. He has been seen researching orthopedic instrument patents and acting as a consultant to evaluate the usability of a concept mapping application. Also, he previously managed the New Mexico Tech Inventors and Entrepreneurs conference website for a time. Preston enjoys riding his bike and writing elaborate plans for DIY microcontroller systems such as thermostats or garden watering systems that he never seems to have enough time to implement. Recently he has been conducting research for TrustedCI with the goal of creating a due care cybersecurity reference for software developers to better mitigate software weaknesses during the development phase.

\*

**Scott Russell** (scolruss@indiana.edu) is a Senior Policy Analyst with the Indiana University Center for Applied Cybersecurity Research (CACR), where his work focuses on the improvement of federal privacy and cybersecurity policy. A lawyer and researcher, Scott specializes in privacy, cybersecurity, and international law, and his past research has included principled cybersecurity, cybersecurity assessments, cybersecurity due diligence, cybersecurity self-governance, international data jurisdiction, and constitutional issues on digital surveillance. He is a co-author of Security from First Principles: A Practical Guide to the Information Security Practice Principles, and a key contributor to CACR’s collaborative efforts with Naval Surface Warfare Center Crane. He received his B.A. in Computer Science and History from the University of Virginia, received his J.D. from Indiana University, interned at MITRE, and served as a postdoctoral fellow at CACR.

\*

**Phil Salkie** is a computer scientist who has been working as an industrial controls and automation engineer since 1984. His software and hardware designs serve sectors as diverse as food packaging, broadcast television, emergency power generation, water purification, sewage processing, medical device manufacturing, and UV photochemistry. He is managing partner of Jeneriah Industrial Automation, designing, supporting, and securing PLC, HMI, and SCADA systems, as well as embedded controllers using Linux and RTOS. He was honored to present the lunch Keynote address at the 2017 CACR CyberSecurity Summit - "Automation: Ready or not, here it comes."

\*

**Anurag Shankar** is a senior security analyst at Indiana University’s Center for Applied Cybersecurity Research (CACR). His expertise includes regulatory compliance (HIPAA, FISMA, CUI) and cybersecurity risk management. He has helped numerous institutions tackle HIPAA compliance and is responsible for developing a NIST based risk management framework and using it to align IU's central research and enterprise cyberinfrastructures with HIPAA. His prior engagements include nearly twenty years with IU’s central IT organization developing, delivering, and managing Unix support, massive data storage, the national Teragrid project, and supporting the research mission of the IU School of Medicine. He played a key role in building IU's research data storage environments, for supporting IU's Indiana Genomics Initiative and other life sciences efforts, and for creating information infrastructures and technology solutions for the Indiana Clinical and Translational Sciences Institute (CTSI). He is a computational astrophysicist by training (Ph.D. University of Illinois, '90).

\*

**Adam Slagell** received an M.S. in computer science from the University of Illinois at Urbana-Champaign in 2003, a masters degree in mathematics from Northern Illinois University (NIU) in 2000, and a B.S. in mathematics from NIU in 1999. He currently serves as the director of the Cybersecurity and Networking Division and Chief Information Security Officer at the National Center for Supercomputing Applications (NCSA) where he co-leads the security office for the NSF-funded XSEDE project, serves on the University of Illinois IT Leadership Team Security Working Group, and is a co-PI for the NSF Bro Center of Excellence, which brings its network security monitoring expertise and support to NSF-funded cyber-infrastructure and Higher Ed.

\*

**Susan Sons** serves as Chief Security Analyst at Indiana University's Center for Applied Cybersecurity Research, as well as ISO (Information Security Officer) for NSF-funded Open Science Grid and senior personnel on the Software Assurance Marketplace and TrustedCI, the NSF Cybersecurity Center of Excellence.  Susan co-authored the Information Security Practice Principles, a touchstone for teaching security professionals and non-security personnel to deal with cybersecurity on a first-principles basis, along with CACR colleagues Craig Jackson and

Scott Russell.  She is also currently President of the Internet Civil Engineering Institute, a nonprofit dedicated to supporting the development and stewardship of reliable, secure, and open source internet infrastructure software. More on Susan's projects can be found at <https://security.engineering>.

\*

**Victoria Stodden** is an associate professor in the [School of Information Sciences](http://www.lis.illinois.edu/people/faculty/vcs) at the University of Illinois at Urbana-Champaign, with affiliate appointments in the School of Law, the Department of Computer Science, the Department of Statistics, the Coordinated Science Laboratory, and the National Center for Supercomputing Applications. She is also a faculty affiliate of the Center for Informatics Research in Science and Scholarship (CIRSS) in the School of Information Sciences at the University of Illinois.

Victoria completed both her PhD in statistics and her law degree at Stanford University, and graduated magna cum laude from the University of Ottawa.

\*

**Jeremy Straub** is the Associate Director of the NDSU Institute for Cyber Security Education and Research and an Assistant Professor in the Department of Computer Science at the North Dakota State University. He is also an Editor-in-Chief for the Journal of Cybersecurity and Privacy.  Straub holds a Ph.D. in Scientific Computing, an M.S. and an M.B.A. and two B.S degrees. Straub’s research spans the gauntlet between technology development, technology policy and commercialization. It has recently focused on cyber-physical system security, robotic command and control, aerospace command and 3D printing quality assurance.

\*

**Steven Tuecke** is co-founder and director of Globus ([www.globus.org](http://www.globus.org)), with a focus on delivering commercial-quality, cloud-based software application and platform services to global, non-profit research communities, as a sustainable, non-profit business within the University of Chicago (UC). From 2009-2016, Tuecke was also Deputy Director of the Computation Institute at UC. Prior to UC, Steven was co-founder, CEO and CTO of Univa Corporation from 2004-2008, providing open source and proprietary software for the high-performance computing and cloud computing markets.  Before that, he spent 14 years at Argonne National Laboratory as research staff. Tuecke graduated with a B.A in mathematics and computer science from St. Olaf College.

\*

**Romain Wartel** ​has been fighting botnets and bad actors for many years, while protecting the Worldwide LHC Computing Grid. This distributed cyber-infrastructure, supporting CERN’s Large Hadron Collider, spans across hundreds of organizations worldwide. Romain specializes in large-scale security intrusions, affecting multiple organizations and mission critical services. This implies focusing on malware, malicious infrastructures, forensics, threat intelligence, and building international collaborations to prepare for and manage crises. Beside operational security, Romain is involved in identity federation, and he also leads a CERN project focusing on modern hardware adoption, called Techlab.

\*

**Von Welch** is the director of the Indiana University Center for Applied Cybersecurity Research. CACR has a unique focus - improve real world cybersecurity for organizations with missions that challenge for traditional cybersecurity approaches. Examples include research and development, open science, and highly distributed collaborations. CACR project partners and funders include the US Department of Defense, National Science Foundation, Department of Homeland Security, as well as private sector organizations - and Von’s roles span research, development, operations, and leadership.

\*

**Brett Zupan** is a Security Analyst & D.C. Liaison for the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) and a Risk Analyst at Gate 15, with experience in all-hazards analysis, exercise development, and information sharing. He has supported analysis, preparedness, and operations for a number of critical infrastructure communities, including Higher Education, the Water and Wastewater Systems Sector, and the Commercial Facilities Sector, among other projects. Before joining Gate 15 in 2016, he worked at the Georgia State Senate. Brett received his Masters of International Relations from American University.