Randy Bishop, Guardtime

Randy Bishop has over 30 years of experience in cybersecurity, counterintelligence and program security for the federal government, US military, the intelligence community and industry. Randy is the General Manager for Critical Infrastructure at Guardtime, a cybersecurity software firm specializing in data and systems integrity. As such he leads the integration of keyless signature infrastructure and industrial scale blockchain, the first and only platform for ensuring the integrity of systems, networks and data at industrial scale security across the critical enterprise and key integrators.

As former Chief Marketing Officer and EVP for Strategy, Randy directed Kingfisher Systems business development and strategic mission support to national security efforts supporting law enforcement, intelligence and counterintelligence activities. When he was Director of Transformation and Experimentation, Directorate for Strategy and Transformation for the Department of Defense Counterintelligence Field Activity (CIFA), he led the transformation of the Department's counterintelligence community to serve the needs of DoD through research, development, testing and evaluation, exercises, lessons learned, experimentation and studies. Prior to joining the DoD Counterintelligence Field Activity, Mr. Bishop spent nearly twenty years with the Air Force Office of Special Investigations, leading myriad technical and cyber support operations. Mr. Bishop also served as Special Agent in Charge of Technology Crimes for the Department of Energy (DOE) Inspector General, where he established their first-ever DOE computer crime program. Mr. Bishop spent nearly a decade at the Pacific Northwest National Laboratory as a senior security advisor in the area of nuclear weapons security and advanced technology program protection, including threats to cybersecurity.

Mr. Bishop earned a Bachelor of Arts in Criminal Justice from Columbia College in 1988, and completed the Joint Military Intelligence College Postgraduate Intelligence Program in 1996. Mr. Bishop is also a Senior Fellow, having graduated from the Excellence in Government fellows program in 2006.

J. Peter Brady, Dartmouth College

J. Peter Brady is a second-year PhD student of Computer Science at Dartmouth College, working with Dr. Sean Smith and Dr. Sergey Bratus. His research interests include new ways to secure and maintain the systems and kernel level of Linux-based devices. He received his BSEE from Clarkson University in 1978 and his MSEE from Worcester Polytechnic Institute in 2014. With over 35 years of industry development and consulting experience, he previously was a Senior Principal Software Engineer for BAE Systems in New Hampshire.

Martin Burns, US National Institute of Standards and Technology

Martin Burns is Associate Director for Testbed Science, US National Institute of Standards and Technology, Engineering Laboratory, Smart Grid and Cyber-Physical Systems Program Office with over 35 years of experience in the design, implementation, and standardization of smart

energy systems. His interests at NIST extend from Smart Grid to Cyber-Physical Systems, federated testbed design and experimentation, and simulation of complex systems. Marty has a BS ChE '73 Cornell University, MS&PhD ChE '77 University of Pennsylvania.

Dennis Gammel, Schweitzer Engineering Laboratory
Dennis Gammel is a graduate of the University of Idaho with a B.S. in Applied Mathematics and has been actively working in the computing and communications industries since 1996. His career experience includes network security, network architecture, database application development, ASIC simulation, and design software, as well as RTOS application development. Dennis is presently the R&D Director over Communication Systems at Schweitzer Engineering Laboratories, Inc. (SEL), responsible for the quality, development, and marketing of the SEL Communication Systems product lines. He has been with SEL since March 2005 and has 20 years of secure software engineering experience. Dennis served an External Advisory Board (EAB) member for the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center and currently serves as an Industrial Advisory Board (IAB) member for the Cyber Resilient Energy Delivery Consortium (CREDC).

Deniz Gurkan, University of Houston
Deniz Gurkan has been with the University of Houston Computer Engineering Technology faculty since 2004, after receiving her PhD in Electrical Engineering from the University of Southern California. She has been interested in repeatable and applied research of computer networking. She has extensive experience in building network infrastructures for various testbed, instruction, domain science support along with security considerations of networking protocols.

Adam Hahn, Washington State University
Adam Hahn is currently an Assistant Professor in the Department of Electrical Engineering and Computer Science at Washington State University. His research interests include cybersecurity of the smart grid and cyber-physical systems (CPS), including intrusion detection, risk modeling, vulnerability assessment, and secure system architectures. He received M.S. and Ph.D. degrees from the Department of Electrical and Computer Engineering at Iowa State University in 2006 and 2013. Previously, he worked as a Senior Information Security Engineer at the MITRE Corporation, supporting numerous cybersecurity assessments within the federal government and leading research projects in CPS security.

Carol Hawk, U.S. Department of Energy
Carol Hawk, Ph.D. is Manager of the Cybersecurity for Energy Delivery Systems (CEDS) R&D Program for the office of Electricity Delivery and Energy Reliability in the Department of

Energy (DOE). Dr. Hawk conducted her Ph.D. research in High-Energy Physics at Rutgers University as a member of the Collider Detector at Fermi National Accelerator Laboratory Collaboration. The CEDS R&D program is working to advance the energy sector's Roadmap vision of resilient energy delivery systems designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functions. In addition, she brings a variety of work experiences to DOE including telecommunications (at Bell Communications Research) as well as fuel cell electrochemistry (at United Technologies Research Center and later at the University of Connecticut). Prior to joining the DOE, Dr. Hawk performed operations research with the Center for Naval Analyses.

Kyle Hussey, Grant County PUD
Kyle Hussey served eight years in the military, followed by 20 years in technology. 16 years being in the Electric Utility industry with the last 10 years heavily involved in the NERC CIP standards. For a short period of time, he was also a CIP Compliance Enforcement specialist with SERC. Functional areas have been in programming, operations, network architecture, operational technology, NERC CIP compliance enforcement, and cyber security. Focus has always been on resiliency, business continuity, and risk mitigation. A member of many Electric industry groups including, but not limited to, LPPC, NWPPA, WICF, EnergySec, WECC user group, ISSA, NIST forums, and FERC DAMS security sector.

Benjamin Justus, Siemens Corporate Technology
Dr. Benjamin Justus is a Security Expert at Siemens Corporate Technology, USA. He has over 10 years of industry experience delivering cyber security expertise and supporting the development of security services and enhancing product security features. He consulted for the telecommunication and defense industry in the past, and held senior positions in EU and USA. He was project leader among many key R&D projects in the security domain, and has successfully led the development of several key technologies in the area of network function & virtualization & software defined network.

Bheshaj Krishnappa, ReliabilityFirst
Bheshaj Krishnappa, joined ReliabilityFirst in 2012, and currently works as a Principal in the Risk Analysis and Mitigation department. Mr. Krishnappa had led multiple risk analysis engagements and mitigation activities that enhance the security, reliability and resilience of Bulk Power System. Prior to his current role, Mr. Krishnappa was a Critical Infrastructure Protection (CIP) Auditor for 2 years. During a career spanning over 22 years, Mr. Krishnappa has worked in various sectors including energy, software services, manufacturing, aerospace, mortgage, and finance companies in consulting and senior management roles. During this time he was instrumental in leading several small to large scale IT and security projects that have enabled

businesses to transform and be resilient in delivering their organization's mission. Mr. Krishnappa is an Electrical Engineer from Bangalore University, India, and obtained his MBA in Renewable Energy from Marylhurst University, USA. Mr. Krishnappa currently holds CISSP, CISM and Carnegie Mellon University's Executive CISO certifications.

Annabelle Lee, Nevermore Security
Annabelle's experience comprises 40 years of technical experience in IT system design and implementation and over 25 years of cyber security design, specification development, and testing. Over her career she has authored or co-authored many documents on cyber security, cryptography, and testing. She began her career in private industry concentrating on IT systems specifications, software testing, and quality assurance. Annabelle has been a guest speaker at many conferences, has written many articles published in journals, and has been interviewed extensively.

Currently, Annabelle is an independent consultant focusing on cyber security for the energy sector. Her company is Nevermore Security. Her areas of expertise include cyber security:
- Strategy and risk management
- Design and architecture
- Specification, guidance, and requirements development
- Assessments against standards
- Training
- Applied cryptography

Annabelle participates in various federal and international cyber security and standards working groups for the electric sector and serves as a technical advisor for several research projects. She is on cyber security technical advisory committees for the North American Electric Standards Board (NAESB) and several DOE laboratory projects.

Annabelle was a Principal Technical Executive in Power Delivery and Utilization at EPRI. She was the lead for coordination and strategic planning across the EPRI sectors of Generation, Nuclear, and Power Delivery and Utilization. Annabelle was the program manager for the DOE funded project on a Secure Policy Based Configuration Framework (PBCONF). The objective is to assist utilities in applying a common security policy across all the various devices and vendors. Annabelle was the Program Manager for the National Electric Sector Cybersecurity Organization Resource (NESCOR), a DOE funded public-private partnership. Annabelle led a team that developed cyber security failure scenarios for the electric sector. Utilities, vendors, and researchers are using these worldwide as they address potential cyber security events.

Tianyuan Liu, University of Illinois at Urbana-Champaign
Tianyuan Liu is a Ph.D. student from University of Illinois at Urbana-Champaign advised by Professor Klara Nahrstedt. He received his Bachelor's degree in Computer Science from Shanghai Jiao Tong University in 2015. His research interests are applied cryptography and secure protocol design for cyber-physical systems, with an emphasis on authentication of distributed applications.

Scott Neumann, Open Access Technology International, Inc.
Scott Neumann is currently the Principal System Architect at OATI. Scott has over 35 years of experience in the industry with a focus on system architecture, applications and integration for operations systems used to manage the electricity grid. Prior to OATI, Scott worked for Control Data (now Siemens), Configured Energy Systems (CES, now Oracle), Utility Integration Solutions (UISOL), Alstom and GE. Scott has a degree in Electrical Engineering from the University of Minnesota, is an IEEE Senior Member and since 2001 has been the US Technical Advisor to IEC TC57.

David M. Nicol, University of Illinois at Urbana-Champaign
David M. Nicol is the Franklin W. Woeltge Professor of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign, Director of the Information Trust Institute, and Principal Investigator of both CREDC and the DHS-funded Critical Infrastructure Resilience Institute. Previously, he held faculty positions at the College of William and Mary and at Dartmouth College. His research interests include high-performance computing, simulation modeling and analysis, and security. He was elected Fellow of the ACM for his contributions in those areas. He is co-author of the widely used textbook Discrete-Event Systems Simulation and was the inaugural awardee of the ACM Special Interest Group on Simulation's Distinguished Contributions Award, for his contributions in research, teaching, and service in the field of simulation.

Muslum Ozgur Ozmen, Oregon State University
Muslum Ozgur Ozmen received his bachelor's degree in electrical and electronics engineering from the Bilkent University, Turkey. He is currently pursuing a PhD degree in Computer Science with the School of Electrical Engineering and Computer Science, Oregon State University. His research interests include light-weight cryptography for IoT systems (drones and medical devices), wireless sensor network security, privacy enhancing technologies (dynamic symmetric and public key based searchable encryption) and post-quantum cryptography.

Bryan Owen, OSIsoft LLC

Bryan Owen is the principal cyber security manager for OSIsoft LLC, makers of the PI System for real time monitoring. Bryan leads OSIsoft's global security initiatives such as SDL, incident response task force, and cyber security advisory board. Industry activities include AFPM cyber security subcommittee, DHS joint working group ICSJWG, and ISA99 voting member. Bryan is a professional engineer with an industrial automation background and decades of OT experience.

Al J. Rivero, ANG Consulting, LLC

As President of ANG Consulting, responsible for working and engaging with clients who desire developing strategic technology plans and growths strategies. Our clients engage us to assist in the development of long-term (3 to 5 year) strategic technology plans to ensure reliable and secure migration of technologies. We also work with development companies to ensure alignment with industry expectations for platform use.

Have more than thirty years of energy industry experience having held various positions ranging from staff engineer, project manager, operations management, technology management to managing Chevron's regulatory strategy group focusing on developing CVX-wide strategy for addressing energy-related regulatory issues and assisting key stakeholders with assuring compliance with regulatory requirements. Have extensive IT/OT integration project experience SAP, JDE OneWorld, as well as several Honeywell and Foxboro DCS system installations at chemical plants and refineries. Have run large capital projects, ranging from centralized control room installations, and major plant debottlenecks to green field construction projects of new facilities.

Bachelors of Science degree in Electrical Engineering from Cal State Fullerton and a Bachelor of Science degree in Computational Mathematics from University of California Irvine. Have either authored or co-authored a variety of papers on critical infrastructure protection for API, AGA, and DOE and have worked with DOE and DHS on critical infrastructure protection planning.

Lori Ross O'Neil, Pacific Northwest National Laboratory

Lori Ross O'Neil is a lead researcher and project manager at the Pacific Northwest National Laboratory (PNNL) in Richland, Washington. Her work focuses on cybersecurity of a variety of critical infrastructure sectors, including the energy and nuclear sectors, in support of DOE, NNSA, DHS, IAEA, NRC, NERC, UNICRI, and private industry. She has managed or contributed technically on numerous control systems security and blended cyber-physical security research projects, including an IEEE article on GPS spoofing, development of Cybersecurity Procurement Language for Energy Delivery Systems, as well as standing up one of the first multi-lab deceptive networks for DOE. Lori has also led the development of a Secure Power Systems Professional certification that was the foundation for the SANS GICSP (Global

Industrial Cyber Security Professional). Her degree is in Computer Science, and she holds CISSP and PMP certifications.

Sachin Shetty, Old Dominion University
Sachin Shetty is an Associate Professor at the Virginia Modeling, Analysis and Simulation Center at Old Dominion University. Sachin Shetty received his PhD in Modeling and Simulation from the Old Dominion University in 2007. He also holds a dual appointment as an Engineer at the Naval Surface Warfare Center, Crane. His research interests lie at the intersection of computer networking, network security and machine learning. His laboratory has received over $10 million in funding to conduct cloud, mobile and critical infrastructure security research. He has published over 125 research articles in journals and conference proceedings and two books. He is recipient of DHS Scientific Leadership Award and has been inducted in Tennessee State University's million dollar club.

Tim Yardley, University of Illinois at Urbana-Champaign
Tim Yardley is the Associate Director of Technology and a Senior Researcher at the Information Trust Institute at the University of Illinois at Urbana-Champaign. His primary duties focus on defining the vision and direction for applied research through emerging technology as well as conducting research to address the core mission of the Institute. His research is focused on trustworthiness and resiliency in critical infrastructure, with particular focus on cyber security in systems like the power grid and telecommunications. Through development of advanced testbed environments, Mr. Yardley helps to apply research to prove out theory and validate those efforts prior to field deployment, speeding the process of technology transition and the realism of fundamental research. His work covers a variety of areas, including control systems, telecommunications systems, critical incident response, and simulations of real-world systems. Other areas of interest include health technology, mobile system security, financial systems, and dynamically tailored environments. Beyond research, he is involved in security assessments, external relations, national working groups, technology development and transfer, and entrepreneurial activities. Through being an active contributor in open-source projects around the world and having come from industry, Mr. Yardley provides a unique perspective with a proven track record of solving difficult problems.