NCCoE Virtual Workshop on Telehealth Smart Home Integration
(May 25, 2022 / 1:00-4:00 PM)
Speaker Biographies

Welcome and Opening Remarks

Kevin Stine
National Institute of Standards and Technology (NIST)
Kevin Stine is the Chief of the Applied Cybersecurity Division in the National Institute of Standards and Technology's Information Technology Laboratory (ITL). He is also NIST's Chief Cybersecurity Advisor and Associate Director for Cybersecurity in NIST's ITL.

Workshop Host

Ronald Pulivarti
Healthcare Program Manager
NIST/NCCoE
Ronald Pulivarti is a senior cybersecurity engineer who leads the Healthcare team at the National Cybersecurity Center of Excellence (NCCoE), which is part of the National Institute of Standards and Technology (NIST). He and his team promote the acceleration of businesses' adoption of standards-based, advanced cybersecurity technologies for the healthcare sector. Mr. Pulivarti has a strong technical background and cybersecurity experience in multiple high-value asset applications. Prior to NIST, he worked within the Department of Health and Human Services and has served in many IT leadership roles for over 20 years.

Moderator for Panel 1

Sue Wang
MITRE/NCCoE
Sue Wang is a principal cybersecurity engineer at the MITRE Corporation and currently serves as the healthcare sector technical lead at the National Cybersecurity Center of Excellence. Ms. Wang has coauthored multiple cybersecurity guidance documents for the healthcare sector.

Previously, Ms. Wang supported Department of Homeland Security, Intelligence Advanced Research Projects Activity, and MITRE research projects in software assurance, secure programming, static analysis, and software weaknesses. Prior to joining MITRE in 2011, Ms. Wang had nearly 20 years of experience in system development life cycle and project management.

Ms. Wang received a bachelor's degree in computer science and a master's degree in software engineering from the University of Maryland.

Moderator for Panel 2

Jeff Marron
NIST

Jeff Marron is an IT Specialist at NIST. He supports several NIST efforts, such as outreach to small- and medium-sized businesses (SMBs) regarding cybersecurity, cybersecurity for the Internet of Things (IoT), and smart grid cybersecurity. He previously supported the NIST Cybersecurity Framework project. Prior to joining NIST, Jeff spent over 10 years working in IT Security within the Department of Health and Human Services (HHS). Among other things, his work included conducting security engineering and integration work at the Food and Drug Administration (FDA). In the more distant past, Jeff was an elementary school teacher of English as a Second Language in Maryland schools.

Moderator for Panel 3

Julie Haney
NIST

Julie Haney is a computer scientist and lead for the Usable Cybersecurity program at the U.S. National Institute of Standards and Technology (NIST). She conducts research about the human element of cybersecurity, including the usability and adoption of security solutions, work practices of security professionals, and people’s perceptions of privacy and security. Previously, Julie spent over 20 years working in the U.S. Department of Defense as a security professional and technical director. She has a PhD and M.S. in Human-Centered Computing from University of Maryland, Baltimore County, an M.S. in Computer Science from University of Maryland, and a B.S. in Computer Science from Loyola University Maryland.

Closing Remarks and Next Steps

Nakia Grayson
NIST/NCCoE

Nakia Grayson is an IT Security Specialist who leads Supply Chain Assurance & Autonomous Vehicle project efforts at the National Cybersecurity Center of Excellence (NCCoE), which is part of the National Institute of Standards and Technology (NIST). She is also a part of the Privacy Engineering Program at NIST, where she supports the development of privacy risk management best practices, guidance, and communications efforts. Grayson serves as the Contracting Officer Representative for NIST cybersecurity contracts. She holds a bachelor’s in criminal justice from University of Maryland-Eastern Shore and a master’s in information technology, information assurance and business administration from the University of Maryland University College.

Workshop Panelists

Andrew G Coyne, CISSP
Mayo Clinic
Andrew has led Mayo Clinic's Office of Information Security since 2016, building the information security capabilities needed to meet Mayo Clinic's primary value: "the needs of the patient come first".

Previously served as a leader in PwC's healthcare cybersecurity practice, developing information security programs for Fortune 500 clients.

Andrew has an MBA from the University of Chicago Booth School of Business, and an Undergrad in Computer Science with Information Engineering, from the University of Hull, UK.

Joseph Davis
Microsoft
Joseph Davis is Microsoft's Chief Security Advisor focused on the Healthcare and Life Sciences in the US where he supports Microsoft customers on industry-related cybersecurity and compliance matters. He acts as an extension of Microsoft's customers' security teams by routinely providing them with security advice, guidance, and recommendations for their digital transformation initiatives and helping them safely move data-sensitive workloads to the Cloud.
Prior to Microsoft, he most recently led Accenture/Avanade Security Advisory in North America. Joseph drove organizational transformation by assessing and reducing risk to Accenture's and Avanade's clients and their customers.

From 2002 to 2016, Joseph Led the Information Security, Compliance, and Data Privacy programs at two large multinational medical device, supplies, and pharmaceuticals development and manufacturing companies.

Joseph has over 26 years' experience in all areas of Information Security, Risk, Compliance & Data Privacy.

As an expert in the medical device safety arena, Joseph participated in drafting FDA Guidance on connected medical device safety and was an active member of Medical Device Innovation, Safety and Security Consortium (MDISS).

Joseph's career highlights include leading two large publicly traded multinational companies as a CISO responsible for building security & data privacy programs for large enterprises, speaking engagements, co-authoring FDA guidance on connected medical device safety & security testing, educating the next generation of Information Security professionals as an adjunct professor, and community involvement through The Open Group, ISSA, InfraGard, ISC2, CIS, IANS and SANS.

Michelle Holko
Google
Michelle Holko, PhD, PMP, is a strategic innovator working at the intersection of biology, technology, and security. She is currently a Principal Architect and Scientist at Google working as the technical lead with the Google Cloud healthcare and life sciences team. She also holds a PI appointment at the International Computer Science Institute (ICSI) at Berkeley, leading a research area at the intersection of biotech and cybersecurity. Prior to joining Google, she served in government as a Presidential Innovation Fellow (PIF), during which time she worked with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the Department of Defense (DoD) Chemical and Biological Defense Program (CBDP), the NIH's All of Us Research Program, HHS BARDA, OSTP and NSC. Prior to joining the PIF program, she worked with DARPA and HHS BARDA, and was a fellow in the 2018 cohort of Johns Hopkins University's Center for Health Security's Emerging Leaders in Biosecurity Initiative. She has also served as a Staff Scientist at NIH's NCBI, working with the primary data archives to promote re-use and re-analysis of biomedical research data. Dr. Holko's technical expertise is in genomics and bioinformatics, and she has experience working on pandemic prevention and preparedness, infectious diseases, cancer, biosurveillance, biosecurity, data science, emerging technologies, health technologies, precision medicine, cybersecurity, and machine learning/artificial intelligence. Dr. Holko is an inclusive, empathetic leader, interested in building security into biotechnology and health innovations to promote innovations in biomedical research. She has spent her career leveraging technology to foster scientific discovery.

Mark Paul Jarrett
Northwell Health
Mark P. Jarrett MD, MBA, MS, HCISSP currently serves as Senior Health Advisor for Northwell Health and a Professor of Medicine at the Donald and Barbara Zucker School of Medicine at Hofstra/Northwell. He currently serves as the Vice Chair of the Healthcare and Public Health Sector Coordinating Council and the National Healthcare Sector Chief for National InfraGard as well as the Sector Chief for NY Metro InfraGard. He is on the HPH Cyber Working Group Executive Council. His previous position for ten years was as Chief Quality Officer for Northwell Health where he was responsible for system-wide initiatives in quality and safety, and also served as Northwell's Deputy Chief Medical Officer.

He previously served as Chief Medical Officer and DIO at Staten Island University Hospital (SIUH). Prior to that appointment, Dr. Jarrett was Director of Rheumatology at SIUH from 1982-1999. Dr. Jarrett has extensive research experience and has been published on the subjects of immune response in systemic lupus erythematosus, quality, and cybersecurity in health care.

Dr. Jarrett is board certified in internal medicine and rheumatology. He is a Fellow of the American College of Physicians and the American College of Rheumatology, and past president of the Richmond County Medical Society.

Dr. Jarrett earned his medical degree from New York University School of Medicine. He completed his residency in internal medicine at Montefiore Medical Center, and a fellowship at Montefiore Medical Center and Albert Einstein College of Medicine.

Dr. Jarrett also holds an MBA from Wagner College and an MS in Medical Informatics from Northwestern University. He is also a certified Healthcare Information Security and Privacy Practitioner (HCISPP).

Nate Lesser
Children's National Hospital
Nate has spent the last 20+ years driving innovation at the nexus of technology and security. He has held technical and executive positions in government, non-profits, and the private sector. As the Children's National Hospital (CNH) VP & Chief Information Security Officer (CISO), Nate is responsible for leading the cybersecurity function and protecting CNH patients, families, and staff.

Prior to joining Children's National, Nate served as the Managing Director of Cypient, where he advised clients on enterprise cybersecurity capabilities, conducted standards-based assessments, and designed solutions to reduce clients' cyber risk. Before Cypient, Nate served as the Deputy Director of the National Cybersecurity Center of Excellence (NCCoE), at the National Institute of Standards and Technology (NIST).

Earlier in his career, Nate spent several years in Booz Allen Hamilton's cybersecurity practice, leading a team of cybersecurity engineers supporting several federal agencies. He also worked at the Office of Management and Budget (OMB) as a policy analyst and Presidential Management Fellow. Nate holds bachelor's and master's degrees in electrical engineering from Columbia University. He is a frequent public speaker with over 30 publications and presentations on various topics in cybersecurity.

Matt McMahon
Philips
Matt is currently the Sr Product Manager of Cybersecurity for Diagnostic Imaging at Philips, a Graduate Adjunct Professor of Healthcare and Cybersecurity with Salve Regina University as well as a Cybersecurity Subject Matter Expert with MIT (Horizon.) Matt's past experience in the field includes integrating voice recognition software with MEDITECH, working with the Point of Care division of Siemens Healthineers as a Product Security Expert and the Acting Product Security Officer of EMEA as well as the Sr Manager of Cybersecurity and the "Internet of Medical Things," (IoMT) with Booz Allen Hamilton.

Christopher M. Plummer
Dartmouth-Hitchcock Health
Christopher Plummer is the Senior Cybersecurity Architect for Dartmouth-Hitchcock Health, New Hampshire's only academic health system, serving a population of 1.9 million patients across northern New England.

His 25-year career spans a broad spectrum of challenging, high impact work for dotcoms, large multinationals including IBM and VF, eleven years of civilian contractor support to the US Navy, and the past five years as a senior cybersecurity strategist for New Hampshire hospitals.

Chris was a speaker at Infosecurity North America 2018 in New York City, was selected in 2021 to the prestigious MDIC/FDA/MITRE medical device threat modeling bootcamp and was selected to the federal Health Sector Coordinating Council Cybersecurity Working Group, where his areas of focus are healthcare supply chain and legacy medical devices. He holds a B.S. from the University of New Hampshire and is a 2009 (ISC)2 CISSP.

Anahi Santiago
ChristianaCare

Anahi Santiago is the Chief Information Security Officer at ChristianaCare, the largest healthcare provider in the state of Delaware. Prior CCHS, she spent over 10 years as the Information Security and Privacy Officer at Einstein Healthcare Network. In her role as CISO she has overall responsibility for the organization's cybersecurity and assurance program. Santiago leads a team of information security professionals in supporting CCHS's strategic initiatives by collaborating with clinical and business leaders, managing cybersecurity risks, implementing policies and controls, generating overall awareness and fostering a culture of security and safety.

Anahi Santiago holds a B.S. in electrical and computer engineering as well as an executive MBA from Drexel University. She also holds a Certified Information Security Manager (CISM) certification. She is an active contributor and member of several local, state and federal cybersecurity organizations including H-ISAC Board of Directors, Healthcare Sector Coordinating Council's Cybersecurity Working Group, Delaware Healthcare Cybersecurity Alliance and WiCyS.