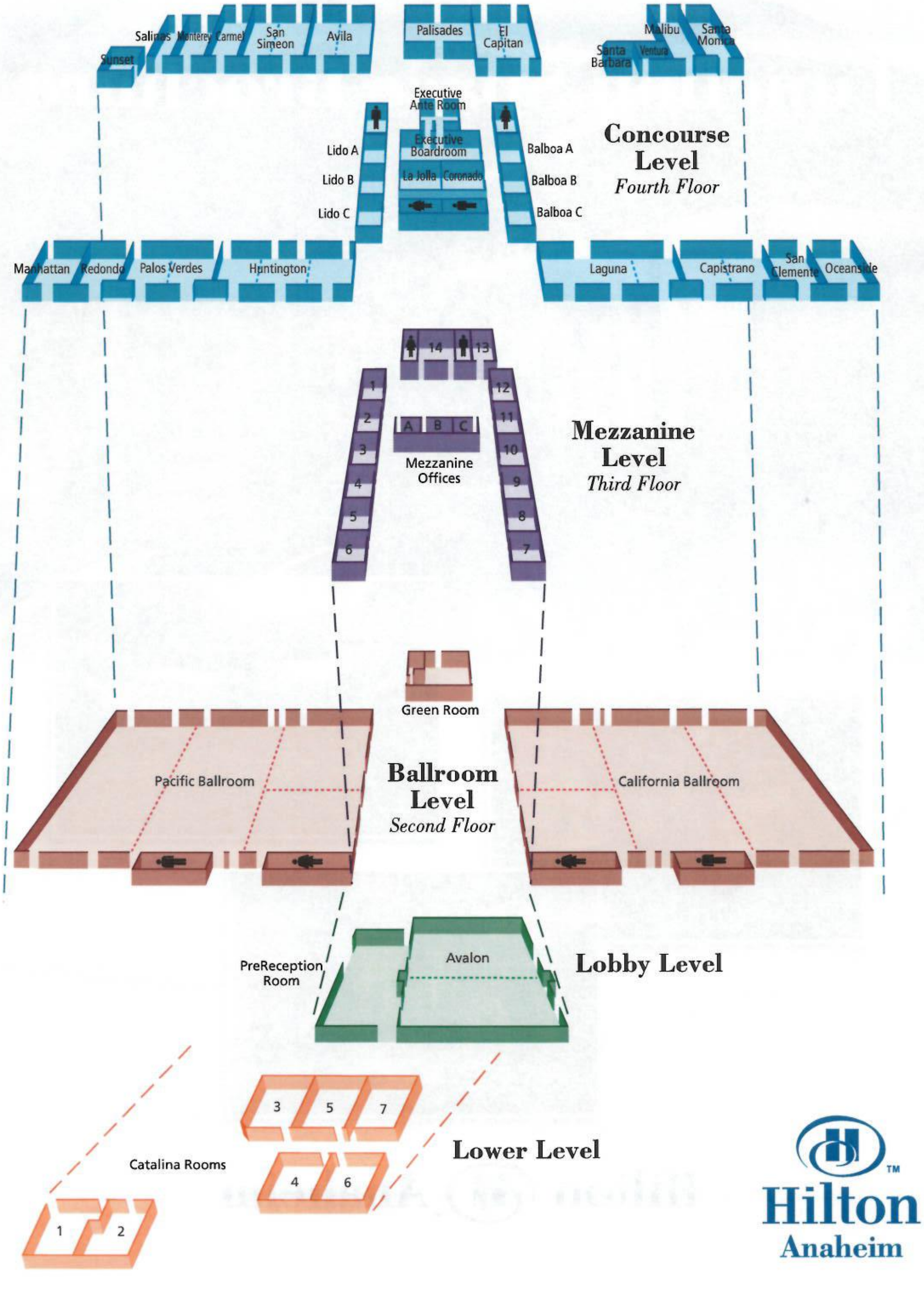
INFORMATION SHARING AND ANALYSIS ORGANIZATION (ISAO) STANDARDS ORGANIZATION PUBLIC MEETING

ISAO
Standards Organization

MAY 18 - 19, 2016
HILTON ANAHEIM
777 W. CONVENTION WAY, ANAHEIM, CA 92802

A more secure and resilient Nation that is connected, informed and empowered



Hilton™
Anaheim

Executive Order 13691 – February 13, 2015

Promoting Private Sector Cybersecurity Information Sharing

Encourage the development of information sharing organizations*: This Executive Order encourages the development of Information Sharing and Analysis Organizations (ISAOs) to serve as focal points for cybersecurity information sharing and collaboration within the private sector and between the private sector and government. In encouraging the creation of ISAOs, the Executive Order expands information sharing by encouraging the formation of communities that share information across a sector, region, or any other affinity, or in response to a specific emerging cyber threat. An ISAO could be a not-for-profit community, a membership organization, or a single company facilitating sharing among its customers or partners.*

Develop a common set of voluntary standards for information sharing organizations*: The Executive Order also directs the Department of Homeland Security to enter into an agreement with a non-governmental organization which will develop a common set of voluntary standards and guidelines for ISAOs. Baseline capabilities will enable ISAOs to quickly communicate shared policies and security protocols with potential partners. This will make collaboration safer, faster, and easier, and ensure greater coordination within the private sector to respond to cyber threats.*

Agenda

Wednesday, May 18th (MEETINGS BY INVITATION ONLY)

8:00 a.m. – 12:00 p.m. **ISAO SO Leadership Meeting (Avalon Room)**

- **Dr. Greg White – Welcome**
- **David Weinstein – NJ-CCIC**
- **Dr. Greg White – ISAO SO Vision**
- **Dr. Heidi Graham – Workgroup Collaboration**
- **Rick Lipsey – Comment Adjudication Process**
- **Larry Sjelin – Initial Products Discussion**
- **Larry Sjelin – ISAO SO Strategic Time Line**

12:00 p.m. – 1:00 p.m. **Leadership Working Lunch (Avalon Room)**

1:00 p.m. – 3:00 p.m. **SWG Working Meetings (SWG Members Only)**

SWG 1: ISAO Creation

- **Frank Grimmelmann and Deborah Kobza**
- **Catalina Room 7**

SWG 2: ISAO Capabilities

- **Denise Anderson and Fred Hintermister**
- **Catalina Room 2**

SWG 3: Information Sharing

- **Kent Landfield and Michael Darling**
- **Catalina Room 3**

SWG 4: Privacy and Security

- **Rick Howard and David Turetsky**
- **Catalina Room 4**

SWG 5: ISAO Support

- **Carlos Kizzee and Dr. Alex Crowther**
- **Catalina Room 5**

SWG 6: Government Relations

- **Mike Echols and David Weinstein**
- **Catalina Room 6**

3:00 p.m. – 3:30 p.m. **Break (Refreshments Provided)**

3:30 p.m. – 5:00 p.m. **SWG Working Meetings (Continued)**

5:30 p.m. – 7:00 p.m. **Networking Event @ the Hilton Anaheim**

- **Pool Bar & Grill**

Thursday, May 19th ISAO SO PUBLIC FORUM (Avalon Ballroom)

7:00 a.m. – 7:30 a.m.	Breakfast and Registration
7:30 a.m. – 7:35 a.m.	Administrative Remarks ➢ Dr. Heidi Graham
7:35 a.m. – 7:50 a.m.	Opening Remarks ➢ Dr. Greg White
7:50 a.m. – 8:20 a.m.	CISA Update ➢ Matthew Shabat
8:20 a.m. – 8:50 a.m.	Regulator Forum Perspectives ➢ Jeffrey Goldthorp
8:50 a.m. – 9:20 a.m.	Interoperability, Automation and Sharing at Net Speed ➢ Dr. Peter Fonash
9:20 a.m. – 9:40 a.m.	Break
9:40 a.m. – 10:20 a.m.	Public Comment and Debate on ISAO Creation ➢ Frank Grimmelmann and Deborah Kobza
10:20 a.m. – 11:00 a.m.	Public Comment and Debate on ISAO Capabilities ➢ Denise Anderson and Fred Hintermister
11:00 a.m. – 11:40 a.m.	Public Comment and Debate on Information Sharing ➢ Kent Landfield and Michael Darling
11:40 a.m. – 1:00 p.m.	Lunch (Numerous restaurants located in the Hilton and nearby)
1:00 p.m. – 1:40 p.m.	Public Comment and Debate on Privacy and Security ➢ Rick Howard and David Turetsky
1:40 p.m. – 2:20 p.m.	Public Comment and Debate on ISAO Support ➢ Carlos Kizzee and Dr. Alex Crowther
2:20 p.m. – 3:00 p.m.	Public Comment and Debate on Government Relations ➢ Mike Echols and David Weinstein
3:00 p.m. – 3:30 p.m.	Public Comment Session – Q & A ➢ Dr. Heidi Graham
3:30 p.m. – 3:40 p.m.	Closing Remarks ➢ Rick Lipsey
3:40 p.m. – 4:00 p.m.	Break

4:00 p.m. – 5:00 p.m. **SWG Working Meetings (SWG Members Only)**

SWG 1: ISAO Creation

- **Frank Grimmelmann and Deborah Kobza**
- **Catalina Room 7**

SWG 2: ISAO Capabilities

- **Denise Anderson and Fred Hintermister**
- **Catalina Room 2**

SWG 3: Information Sharing

- **Kent Landfield and Michael Darling**
- **Catalina Room 3**

SWG 4: Privacy and Security

- **Rick Howard and David Turetsky**
- **Catalina Room 4**

SWG 5: ISAO Support

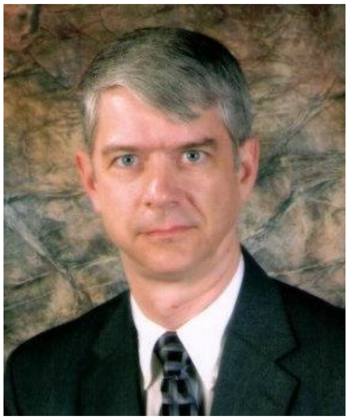
- **Carlos Kizzee and Dr. Alex Crowther**
- **Catalina Room 5**

SWG 6: Government Relations

- **Mike Echols and David Weinstein**
- **Catalina Room 6**

DR. GREG WHITE

Executive Director, ISAO Standards Organization



Dr. Gregory White has been involved in computer and network security since 1986. He spent 30 years with the Air Force and Air Force Reserves. He obtained his Ph.D. in Computer Science from Texas AandM University in 1995 conducting research in the area of Computer Network Intrusion Detection and he continues to conduct research in this area today. He currently serves as the Director of the Center for Infrastructure Assurance and Security (CIAS) and is a Professor of Computer Science at The University of Texas at San Antonio (UTSA).

Dr. White helped build the nation’s first undergraduate information warfare laboratory at the U.S. Air Force Academy. At UTSA, he continues to develop and teach courses on computer and network security. He has also been very active in the development and presentation of cyber security exercises for states and communities around the nation and with the development of training designed to help states and communities develop viable and sustainable cyber security programs. In addition, he is also very active in development of cyber security competitions and was instrumental in the development of the National Collegiate Cyber Defense Competition and the CyberPatriot National High School Cyber Defense Competition.

Dr. White received the 2011 Educator Leadership award for Exceptional Leadership in Information Assurance Education at the Colloquium for Information Systems Security Education (CISSE). In 2012, he was awarded the Air Force Association Distinguished Sustained Aerospace Education Award for his efforts in cyber security education. In 2014, he was made a Distinguished Fellow of the Information Systems Security Association. In addition to being the director of the CIAS at UTSA, Dr. White also serves as the Executive Director of the Information Sharing and Analysis Organizations (ISAO) Standards Organization (SO) and is the Director of the National Cybersecurity Preparedness Consortium (NCPC).

RICK LIPSEY

Deputy Director, ISAO Standards Organization

Richard A. Lipsey serves as Deputy Director of the ISAO Standards Organization and is also the senior strategic cyber lead for LMI. In this capacity he coordinates a multi-disciplinary portfolio of cyber-related management and analytical services across all LMI business units and regions.

Prior to joining LMI, he established Lipsey Cyber Consulting, where he advised clients from small businesses to Fortune 500 companies on cyber risk management strategies, cyber weapons systems development, and cyber service portfolios tailored to meet mission requirements.

Mr. Lipsey served 28 years in the United States Air Force where he distinguished himself in providing strategic leadership in the application of communications, computer, networking, and cybersecurity capabilities to meet operational mission requirements. In addition to assignments with six operational communications units, he served as the Director for C4 Systems for Air Force Central Command, where he was responsible for all deployed Air Force cyberspace capabilities in the CENTCOM area of responsibility. He also served on the staff of U.S. European Command, where he led the establishment of DoD's first combatant command Network Warfare Center. In his final assignment, he served as Vice Commander of 24th Air Force, the Air Force component of U.S. Cyber Command, which is responsible to extend, operate, and defend the Air Force portion of the DoD global network, as well as to plan and conduct full-spectrum cyberspace operations.

Mr. Lipsey holds a BS in computer systems analysis from Miami University and an MA in management and procurement from Webster University. He also earned a Master of Strategic Studies degree from the Air War College, where he graduated with academic distinction. In addition, he holds a CISSP certification and is an active life member of the Armed Forces Communications-Electronics Association.

BRIAN ENGLE

Executive Director, Retail Cyber Intelligence Sharing Center

Brian Engle serves as the Executive Director of the Retail Cyber Intelligence Sharing Center (R-CISC), the resource supporting the retail and commercial services industries for sharing cybersecurity information and intelligence. The R-CISC, and its operation of the Retail and Commercial Services Information Sharing and Analysis Center (RCS-ISAC), create a trusted environment for robust collaboration for its members and partners. As Executive Director, Brian provides the leadership and oversight of all aspects of the R-CISC's mission, goals and operations for the delivery of effective and high quality services to the R-CISC membership.

Brian's previous information security roles include CISO and Cybersecurity Coordinator for the State of Texas, CISO for Texas Health and Human Services Commission, CISO for Temple-Inland, Manager of Information Security Assurance for Guaranty Bank, and Senior Information Security Analyst for Silicon Laboratories. Brian has been a professional within Information Security and Information Technology for over 25 years.

Brian is a past president and Lifetime Board of Directors member of the ISSA Capitol of Texas Chapter, is a member of ISACA and InfraGard, and holds CISSP and CISA certifications.

MATTHEW SHABAT

Director of Performance Management, DHS Office of Cybersecurity and Communications

Since starting at the Department of Homeland Security in 2008, Matt has served as a policy analyst and then the Deputy Chief of Staff for the National Cyber Security Division. Subsequently, he became the Director of Performance Management within the DHS Office of Cybersecurity and Communications. In that role, he contributes to strategic planning, oversees associated program performance and provides business process analysis support across the organization. Active projects include analyzing the costs of a cyber incident and leadership of the Department's involvement in an ongoing cyber insurance and risk management data repository dialogue. Earlier this year, he led DHS's development of guidance and procedures required by Title I of the Cybersecurity Act of 2015. In 2013, he co-led the joint interagency-private sector working group that developed performance goals for the National Institute of Standards and Technology Cybersecurity Framework and contributed perspectives during the Framework's evolution.

Matt graduated from The George Washington University's Elliott School of International Affairs with a M.A. in Security Policy Studies. While pursuing his Masters, Matt was a Research Fellow with the Project on National Security Reform where he served as the Deputy to the project's Structure Working Group Leader and a member of the Core Study Team. His research included the study of interagency problems relating to lines of authority and the division of labor at and across the national, regional, country team, state and local and multilateral levels of national security engagement. Prior to returning to graduate school, Matt practiced corporate, mergers and acquisitions, and securities law with Mayer Brown LLP in Chicago. His representations included clients in the financial, energy, food product, insurance and heavy industry sectors. Matt earned his J.D. from the University of Pennsylvania Law School and he received his B.A. from Stanford University.

JEFF GOLDTHORP

Associate Chief, Cybersecurity and Communications Reliability, FCC

Jeff Goldthorp is the Associate Bureau Chief for Cybersecurity and Communications Reliability and also serves as the Acting Chief of the Bureau's Cybersecurity and Communications Reliability Division. He has a leadership role in the Commission's effort to engage communications providers in the development of a market-driven cybersecurity risk management approach, which relies on voluntary measures and assurances from communications providers as a substitute for traditional regulation. He serves as the Designated Federal Officer of the Communications Security, Reliability, and Interoperability Council advisory committee and served in the same role for its predecessor, the Network Reliability and Interoperability Council.

As Acting Division Chief, Mr. Goldthorp leads a technical and legal staff that addresses cybersecurity and network and 911 reliability, including administration of the Commission's communications disruptions reporting rules, the Network Outage Reporting System, Disaster Information Reporting System, and 911 Reliability Certification database. Before joining PSHSB, Mr. Goldthorp was Chief of the Network Technology Division in the FCC's Office of Engineering and Technology.

Before joining the FCC in November of 2001, Mr. Goldthorp was the General Manager of the Network Access Engineering Services practice at Telcordia Technologies. Mr. Goldthorp holds a patent for a DSP-based, near-end crosstalk simulator that is in use today in Telcordia's laboratories. He earned a BSEE from Lehigh University and a MSEE from Princeton University. He is a member of Phi Beta Kappa as well as honor societies Tau Beta Pi, and Eta Kappa Nu.

DR. PETER M. FONASH

Chief Technology Officer, Office of Cybersecurity and Communications, DHS

Peter M. Fonash is the Chief Technology Officer for the Office of Cybersecurity and Communications in the Department of Homeland Security. He has previously held positions as Director of the National Communications System; Special Assistant to the Staff Director, Federal Reserve Board; and Director of Technology, Chief of the Advanced Technology Office, and Chief of the Joint Combat Support Applications Division at the Defense Information Systems Agency.

Dr. Fonash received a Bachelor of Science Electrical Engineering and a Master of Science in Engineering from the University of Pennsylvania; a Master of Business Administration from the University of Pennsylvania Wharton School; and a Ph.D. in Information Technology and Engineering from George Mason University. He is Adjunct Faculty at the University of Tulsa, an Advisory Board Member at George Mason University School of Engineering, and a Member of the Institute of Electrical and Electronics Engineers, IEEE.

STANDARDS WORKING GROUP ONE: ISAO CREATION

FRANK GRIMMELMANN

CO-CHAIR FOR STANDARDS WORKING GROUP 1

Frank J. Grimmelmann is president and CEO/Intelligence Liaison Officer for the non-profit Arizona Cyber Threat Response Alliance (ACTRA), closely affiliated with the FBI's AZ Infragard Program. In this capacity, Mr. Grimmelmann represents the private sector in the Arizona Counterterrorism Information Center (ACTIC), and is the first private sector representative on its executive board.

He also serves as the ACTIC's private sector liaison to the FBI Cyber Squad, the ACTIC, and the FBI's Arizona Infragard Program. ACTRA's focus is to enable the private sector to respond to the escalating national cyber threat, and to leverage Infragard's vast private sector volunteer membership as a force multiplier in protecting our nation's critical infrastructure and national security.

DEBORAH KOBZA

CO-CHAIR FOR STANDARDS WORKING GROUP 1

Deborah Kobza, as President/CEO of the Global Institute for Cybersecurity + Research, leads a public/private critical infrastructure partnership to advance critical infrastructure resilience. In partnership with NASA/Kennedy Space Center and in collaboration with the U.S. Department of Homeland Security, NIST, government agencies, academia and private industry, GICSR serves as the trusted international collaborative facilitating open dialogue, critical insight and thought exchange linking critical infrastructure stakeholders to define and deliver scalable, flexible and adaptable cybersecurity resilience solutions.

Deborah founded the National Health Information Sharing and Analysis Center (NH-ISAC), serving as Executive Director from 2010 to 2015. In collaboration with the FDA (NH-ISAC/FDA MOU) and the medical device community, Mrs. Kobza led NH-ISAC in supporting development of a Medical Device Cybersecurity Framework and to address reporting and remediation of medical device vulnerabilities.

Prior, Mrs. Kobza served as CEO of the IT Center of Excellence, and provided consulting services to the U.S. Department of Homeland Security, state governments and private industry.

Deborah serves on various cybersecurity working groups with the U.S. Department of Homeland Security, Department of Defense, and private industry, including serving as Chair of the Global Forum to Advance Cyber Resilience.

Standards Working Group Two: ISAO Capabilities

Denise Anderson

Chair for Standards Working Group 2

Denise Anderson has over 25 years of management level experience in the private sector and is Executive Director of the National Health Information Sharing and Analysis Center (NH-ISAC), a non-profit organization that is dedicated to protecting the health sector from physical and cyber attacks and incidents through dissemination of trusted and timely information.

Denise currently serves as Chair of the National Council of ISACs and participates in a number of industry groups such the Cross-Sector Cyber Security Working Group (CSCSWG). She was instrumental in implementing a CI/KR industry initiative to establish a private sector liaison seat at the National Infrastructure Coordinating Center (NICC). She is a health sector representative to the National Cybersecurity and communications Integration Center (NCCIC) and sits on the Cyber Unified Coordination Group, (UCG).

Denise holds a BA in English, magna cum laude, from Loyola Marymount University and an MBA in International Business from American University. She is a graduate of the Executive Leaders Program at the Naval Postgraduate School Center for Homeland Defense and Security.

Fred Hintermister

Vice-Chair for Standards Working Group 2

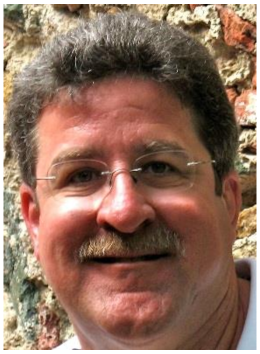
Fred Hintermister is a manager and key member of the Energy Subsector, Information Sharing and Analysis Center (ES-ISAC) for the North American Reliability Corporation (NERC). He plays a vital role in the providing true security for the bulk power system on both the physical side and the cyber front. Mr. Hintermister works closely with both government and industry to mitigate threats and vulnerabilities they face and to deliver greater reliability to the grid. His previous roles have embraced innovation, business development, public-private partnerships, security, and the development of insurance.

Mr. Hintermister has an MBA and a bachelor's degree from Cornell University and an MS in Technology Commercialization from the University of Texas at Austin.

STANDARDS WORKING GROUP THREE: INFORMATION SHARING

KENT LANDFIELD

CHAIR FOR STANDARDS WORKING GROUP 3



Kent Landfield has spent 30+ years in software development, global network operations and network security arenas. Kent is currently Director of Standards and Technology Policy at Intel. He has been extremely active in the NIST Cybersecurity Framework development, actively participating and presenting in workshops and supplying comments. He is a co-author of ‘The Cybersecurity Framework in Action: An Intel Use Case’. Kent has been a participating member of multiple subcommittees of the President’s National Security Telecommunications Advisory Committee (NSTAC) efforts. Kent has lead and a worked on multiple cyber threat information sharing research, standards and development efforts. He is co-author on RFC 7203, *An Incident Object Description Exchange Format (IODEF) Extension for Structured Cybersecurity Information.* Previously Kent was Director of Content Strategy, Architecture and Standards for McAfee Labs and was the chief McAfee Labs Vulnerability Group Architect as well as one of McAfee’s Principal Architects. As Director of Security Research, Kent managed the global Risk and Compliance Security Research teams. He has been actively involved in global security automation development efforts for many years. Kent was one of the founding members of the CVE Editorial Board. He is an OVAL Board member and is active in SCAP related development projects, both from a content and product perspective. Kent holds patents in DNS, Email and software patch distribution technologies.

MICHAEL DARLING

VICE-CHAIR FOR STANDARDS WORKING GROUP 3

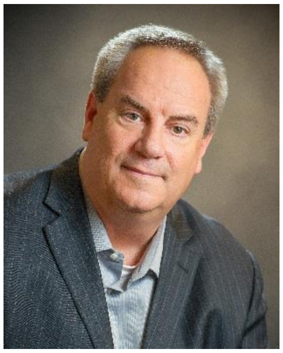
Michael Darling is currently a Director within the Cybersecurity and Privacy practice of PwC focused on information sharing. Prior to joining PwC he was the Director of the Enterprise Performance Management Office at the Department of Homeland Security’s Office of Cybersecurity and Communications responsible for strategy, performance management, international engagement, and legislative policy. He was also a Senior Program Examiner in the Office of Management and Budget within the Executive Office of the President focused on cybersecurity budget and policy issues. Previously, Michael was a senior management and security consultant at Wittenberg Weiner Consulting working on Navy security operations in Europe and the Middle East.

He also served on active duty with the Marine Corps in a variety of leadership assignments in the U.S., Europe, Iraq, and Afghanistan. Michael holds a bachelor’s degree from Wayne State College and a master’s degree from Johns Hopkins University.

Standards Working Group Four: Privacy and Security

Rick Howard

Chair for Standards Working Group 4



Rick Howard is the Chief Security Officer (CSO) for Palo Alto Networks where he oversees the company's internal security program, leads the Palo Alto Networks Threat Intelligence Team (Unit 42), directs the company's efforts on the Cyber Threat Alliance Information Sharing Group, hosts the Cybersecurity Canon Project, and provides thought leadership for the company and the Cybersecurity community at large. His prior jobs include the CISO for TASC, the GM of iDefense, the SOC Director at Counterpane and the Commander of the U.S. Army's Computer Emergency Response Team where he coordinated network defense, network intelligence and network attack operations for the Army's global network.

Rick holds a Master of Computer Science degree from the Naval Postgraduate School and an engineering degree from the US Military Academy. He also taught computer science at the Academy from 1993 to 1999. He has published many academic papers on technology and security and has contributed as an executive editor to two books. The Christian Science Monitor named him a Passcode Influencer in 2015: a pool of 70 experts who are big thinkers on security and privacy.

David Turetsky

Vice-Chair for Standards Working Group 4

With more than 30 years in business, government and the legal industry, David Turetsky is co-leader of Akin Gump's cybersecurity, privacy and data protection practice and focuses his practice on public law and policy matters, with an emphasis on cyber law and policy; privacy; data breach issues; competition law; and telecom, media and technology (TMT). Mr. Turetsky joined Akin Gump Strauss Hauer and Feld LLP after serving as a senior official with the Federal Communications Commission (FCC), where he spent most of his tenure as chief of the FCC's Public Safety and Homeland Security Bureau, leading the agency's efforts to improve the nation's cybersecurity. He served as the FCC's representative in interagency policymaking to implement the president's Executive Order on Improving Critical Infrastructure Cybersecurity and the Presidential Policy Directive on Critical Infrastructure Security and Resilience, and as a member of the Executive Committee created by the president's Executive Order on National Security and Emergency Preparedness Communications.

In addition to attaining his BA from Amherst College and his JD from the University of Chicago Law School, Mr. Turetsky also studied at the London School of Economics and Political Science from 1977 to 1978.

STANDARDS WORKING GROUP FIVE: ISAO SUPPORT

CARLOS KIZZEE

CHAIR FOR STANDARDS WORKING GROUP 5

Carlos Kizzee is the Executive Director of the Defense Security Information Exchange (DSIE). Mr. Kizzee is responsible for overseeing the administrative management and operations of the DSIE, an organization focused on enhancing the cyber security of Defense Industrial Base entities. Mr. Kizzee served as the Center for Internet Security's Vice-President for Multi-Sector Initiatives and was responsible for developing partnerships between the Center and its portfolio of threat intelligence/risk mitigation capabilities and other threat intelligence, analytical, data sharing, risk management, and operational organizations and mechanisms relevant to cyber security and critical infrastructure protection.

Mr. Kizzee also served within DHS as the Deputy Director, Stakeholder Engagement and Cyber Infrastructure Resilience Division, and the Program Manager for implementing key operational information sharing and support activities. Mr. Kizzee served as the Director of Strategic Cyber Initiatives for the Critical Infrastructure and Cyber Protection Branch, Counsel for the National Operations Center, Senior Counsel for Infrastructure Protection, and as a Senior Attorney-Advisor for the DHS Office of General Counsel. Mr. Kizzee served as Counsel for the U.S. Air Force Office of Special Investigations. Prior to 2003, he was a Marine Corps attorney and a Federal Special Assistant U.S. Attorney in Arizona and the Southern District of California.

A graduate of the US Naval Academy, Mr. Kizzee has a BS degree in Mathematics, a JD from the Georgetown University Law Center, and a Master of Laws from the Judge Advocate General's School of the Army at the University of Virginia's School of Law.

DR. ALEX CROWTHER

VICE-CHAIR FOR STANDARDS WORKING GROUP 5

Glenn Alexander Crowther is currently the Director of Research and a Cyber Policy Specialist at the Center for Technology and National Security Policy (CTNSP) in the Institute for National Strategic Studies (INSS) at the National Defense University in Washington, DC. He is also an adjunct Senior Political Scientist at the RAND Corporation and an adjunct Research Professor of National Security Studies at the Strategic Studies Institute (the Army's think tank). Alex has experience teaching at the graduate level and routinely instructs on cyber issues. He also has extensive experience as a public speaker and as a conference organizer. Alex has a BA in International Relations from Tufts University, an MS in International Relations from Troy University, and a Ph.D. in International Development from Tulane University.

STANDARDS WORKING GROUP SIX: GOVERNMENT RELATIONS

MICHAEL ECHOLS

CHAIR FOR STANDARDS WORKING GROUP 6

Michael Echols is the Director, Cyber Joint Program Management Office (JPMO) within the Cybersecurity and Communications (CSandC) component at the Department of Homeland Security (DHS). He leads cybersecurity information sharing programs. This includes being the point person for the rollout of Presidential Executive Order 13691 – *Promoting Private Sector Cyber Information Sharing.*

In 2014, Mr. Echols launched a small- and medium-sized business initiative for DHS. Formerly, Mr. Echols was Chief of the Government-Industry Planning and Management Branch, National Communications System (NCS) from 2009 - 2013. He chaired the Communications Sector's Communications Government Coordinating Council (CGCC), and the Network Security Information Exchange (NSIE). Additionally, Mr. Echols managed the stand-up of the Joint Program Office under executive Order 13618, supporting national security and emergency preparedness (NS/EP) communications. Mr. Echols developed and led the public/private effort to create the 2012 National Sector Risk Assessment for Communications. He also managed the President's National Security Telecommunications Advisory Committee (NSTAC), 30 chief executive level NSTAC members representing IT, Defense and Communications companies, for four years.

Mr. Echols engineered networks in the private sector for more than 20 years Mr. Echols is a graduate of the National Preparedness Leadership Initiative – Harvard Kennedy School of Public Health and the Federal Executive Institute. He holds a MBA, a MS in Biotechnology, a Graduate Certificate in Technology Management, and a BS in Criminal Justice; all from the University of Maryland. Mr. Echols also holds a CISSP Certification.

DAVID WEINSTEIN

VICE-CHAIR FOR STANDARDS WORKING GROUP 6

David Weinstein is currently serving as New Jersey's Cybersecurity Advisor. Dave previously served as a senior civilian at the United States Cyber Command in Fort Meade, Maryland, and a cyber risk consultant with Deloitte.

Dave has been recognized by Forbes as a "top 20 cyber policy expert" and his analysis and commentary on the subject has been featured in numerous media and academic publications, including the *Georgetown Journal of International Affairs, Foreign Affairs, Foreign Policy,* CNN.com, and *The Boston Globe*. In addition to his duties in New Jersey, he is also a non-resident fellow with the New America's Cybersecurity Initiative and "Influencer" for the Christian Science Monitor's security and privacy project.