INFORMATION SHARING AND ANALYSIS ORGANIZATION (ISAO)

STANDARDS ORGANIZATION

PUBLIC MEETING

ISAO
Standards Organization

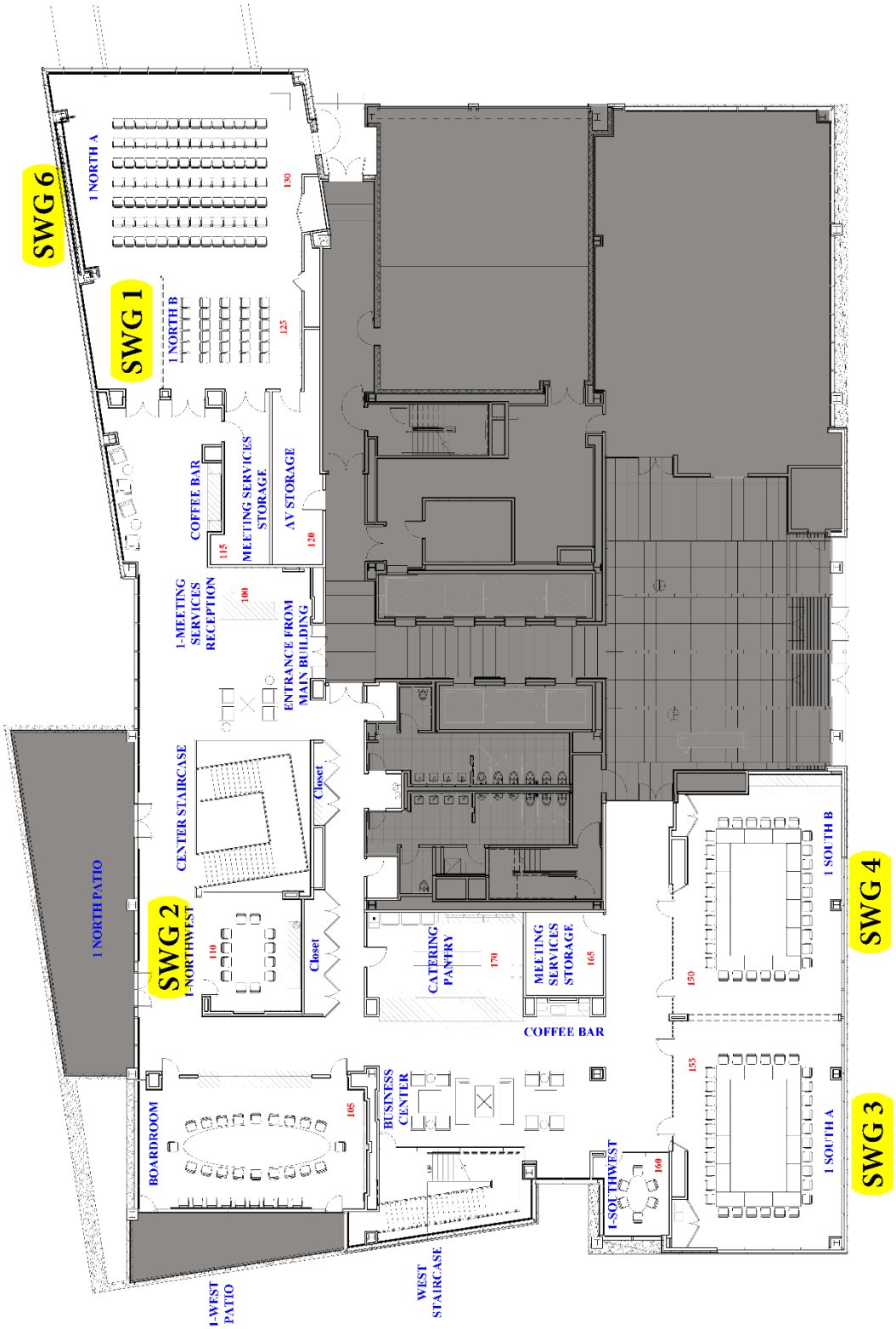
AUGUST 31 – SEPTEMBER 1, 2016

LMI HEADQUARTERS

7940 JONES BRANCH DRIVE, TYSONS VA 22102

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

LMI Conference Center



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 and guidelines 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 facilitate improved coordination across all sectors to respond to cyber threats.

Agenda

Wednesday, August 31st (MEETINGS BY INVITATION)

7:30 a.m. – 5:00 p.m.	**Registration**
8:00 a.m. – 11:00 a.m.	**ISAO SO Leadership Meeting (Boardroom)** • **ISAO SO Staff and SWG Chairs/Vice-Chairs**
11:00 a.m. – 12:00 p.m.	**Leadership Working Lunch (Boardroom)**
12:00 p.m. – 1:00 p.m.	**Leadership Readout to SWG Members (1 North)** • **Rick Lipsey** Deputy Director, ISAO Standards Organization
1:00 p.m. – 5:00 p.m.	**SWG Working Meetings (SWG Members Only)**
	SWG 1: ISAO Creation (1 North B) • **Frank Grimmelmann and Deborah Kobza**
	SWG 2: ISAO Services and Capabilities (1 Northwest) • **Denise Anderson and Fred Hintermister**
	SWG 3: Information Sharing (1 South A) • **Kent Landfield and Michael Darling**
	SWG 4: Privacy and Security (1 South B) • **Rick Howard and David Turetsky**
	SWG 6: Government Relations (1 North A) • **Doug DePeppe**
2:00 p.m. – 4:00 p.m.	**Emerging ISAO Meet Up (By Invitation)** • **Natalie Sjelin** Director of Support, ISAO Standards Organization
4:00 p.m. – 5:00 p.m.	**ISAO 101 (T Northwest – Open to the Public)** • **Rick Lipsey** Deputy Director, ISAO Standards Organization
5:00 p.m. – 7:00 p.m.	**Networking Event (Hilton McLean Tysons Corner)** 7920 Jones Branch Drive

Thursday, September 1st ISAO SO PUBLIC FORUM (1 North)

7:00 a.m. – 5:00 p.m.	**Registration**
7:00 a.m. – 7:45 a.m.	**Continental Breakfast**
7:45 a.m. – 7:50 a.m.	**Administrative Remarks** • **Dr. Heidi Graham** Senior Fellow, LMI
7:50 a.m. – 8:00 a.m.	**Welcome** • **Nelson Ford** President and CEO, LMI
8:00 a.m. – 8:20 a.m.	**Strengthening the Nation's Cybersecurity Posture** • ***Guest Speaker to be Announced***
8:20 a.m. – 9:00 a.m.	**State of the Ecosystem: Where We Are and Where We're Going** • **Dr. Greg White** Executive Director, ISAO Standards Organization
9:00 a.m. – 9:20 a.m.	**Break**
9:20 a.m. – 10:00 a.m.	**State of the Ecosystem: What's Next?** • **Rick Lipsey** Deputy Director, ISAO Standards Organization
10:00 a.m. – 10:40 a.m.	**Supporting New and Emerging ISAOs** • **Natalie Sjelin** Director of Support, ISAO Standards Organization
10:40 a.m. – 11:00 a.m.	**Break**
11:00 a.m. – 12:00 p.m.	**Panel Discussion: ISAO Services and Capabilities** • **Moderator: Brian Engle** Executive Director, Retail Cyber Intelligence Sharing Center • **Denise Anderson** Chair, National Council of ISACs • **Stuart Gerson** Partner and Shareholder, Epstein Becker & Green, P.C. • **Kent Landfield** Director, Standards and Technology Policy at Intel Corporation • **Chip Wickenden** VP of Sector Services, Financial Services ISAC

12:00 p.m. – 1:00 p.m. **Lunch**

1:00 p.m. – 2:00 p.m. **Panel Discussion: Building an ISAO**

- **Moderator: Rick Lipsey**
  Deputy Director, ISAO Standards Organization
- **Doug DePeppe**
  Founder, **eos**edge Legal; Co-Founder, Cyber Resilience Institute
- **Frank Grimmelmann**
  President and CEO, Arizona Cyber Threat Response Alliance
  Norma Krayem
  Co-Chair of Cybersecurity and Privacy, Holland & Knight, LLP
- **Matt Shabat**
  Director of Performance Management, DHS CS&C

2:00 p.m. – 2:10 p.m. **Break**

2:10 p.m. – 3:25 p.m. **Public Discussion on Draft ISAO SO Publications and ISAO Ecosystem Issues**

- **Moderator: Dr. Heidi Graham**
  Senior Fellow, LMI

3:25 p.m. – 3:35 p.m. **Break**

3:35 p.m. – 4:50 p.m. **Public Discussion on Draft ISAO SO Publications and ISAO Ecosystem Issues** (continued)

- **Moderator: Dr. Heidi Graham**
  Senior Fellow, LMI

4:50 p.m. – 5:00 p.m. **Closing Remarks**

- **Rick Lipsey**
  Deputy Director, ISAO Standards Organization

THE HONORABLE NELSON M. FORD

PRESIDENT AND CEO, LMI

WELCOME MESSAGE

Mr. Ford has been chief executive of LMI since January 2009, simultaneously joining the board with his appointment as the company's eleventh president. As chief executive, he is responsible for the general management and strategic direction of LMI. Mr. Ford also serves as board chair of the Center for Strategic and Budgetary Analysis (CSBA) and on the board of the Northern Virginia Technology Council (NVTC).

Mr. Ford has extensive experience leading organizations and developing enduring, practical solutions to some of the most complex problems in the public sector, with particular emphasis on national security, financial management, healthcare, and resource management.

Under his leadership, LMI has expanded its regional presence and broadened its capabilities into emerging federal and international markets, receiving multiple "small business partner" and "best place to work" awards along the way.

Before leaving government to lead LMI, Mr. Ford served as the Under Secretary of the Army from 2007 to 2009. Prior to that, he served as Assistant Secretary of the Army for Financial Management and Comptroller from 2006 to 2007 and Principal Deputy Assistant Secretary of the Army for Financial Management and Comptroller from 2005 to 2006. From 2002 through 2004, he was Deputy Assistant Secretary for Health Budgets & Financial Policy in the Department of Defense.

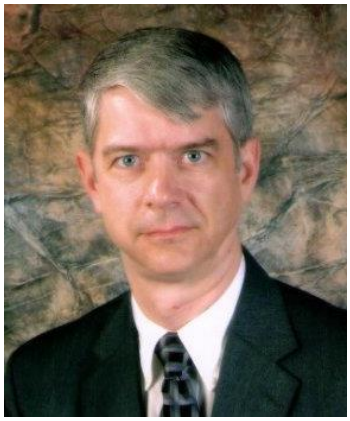
He was President and CEO of a medical manufacturing company from 1997 to 2000 and was the Chief Operating Officer and Chief Financial Officer at Georgetown University Medical Center from 1991 to 1997. During the 1980's, he managed the health care consulting practice for Coopers & Lybrand and has extensive experience in the governance of health care organizations.

Mr. Ford holds a BA in history from Duke University and an MA in education from the University of Delaware and has completed additional professional training at the University of Pennsylvania. His wife is a retired government attorney and their three children all currently serve in the active duty military.

DR. GREG WHITE

EXECUTIVE DIRECTOR, ISAO STANDARDS ORGANIZATION

STATE OF THE ECOSYSTEM: WHERE WE ARE AND WHERE WE'RE GOING



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 A&M 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

STATE OF THE ECOSYSTEM: WHAT'S NEXT?

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.

NATALIE SJELIN

DIRECTOR OF SUPPORT, ISAO STANDARDS ORGANIZATION

SUPPORTING NEW AND EMERGING ISAOS

Natalie Sjelin is the Associate Director of Training for the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas San Antonio. She began with the CIAS in 2002 and brings over 14 years of cybersecurity experience to the CIAS training staff.

Ms. Sjelin also serves as the Director of Support for the ISAO Standards Organization. In this role she is leading the development of the ISAO SO's Support Group to assist ISAOs in their overall development and to help them hone their capabilities and services. In addition, Ms. Sjelin plays a significant role in the National Cyber Preparedness Consortium (NCPC) initiatives to design and deliver cyber security training for the nation.

The majority of Ms. Sjelin's experience has been in designing, facilitating and executing cyber security exercises and developing and delivering cyber security training at various levels. Her focus has been working with communities to build viable and sustainable cyber security programs.

She received her degree in Computer Information Systems and has earned the CompTIA Security + Certification, as well as a Certified Training Professional certification from Texas A&M University.

She speaks regularly for professional groups, meetings, panels and conferences across the country, and has appeared at the prestigious RSA conference. Ms. Sjelin has co-authored several white papers on community cyber security topics and most recently co-authored a chapter for a new book on cyber-physical security that will be published soon.

PANEL DISCUSSION: ISAO SERVICES AND CAPABILITIES

MODERATOR: BRIAN ENGLE

EXECUTIVE DIRECTOR, RETAIL CYBER INTELLIGENCE SHARING CENTER

Brian Engle helps lead and advise the ISAO Standards Organization and also serves as the Executive Director of the Retail Cyber Intelligence Sharing Center (R-CISC), the organization 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.

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.

DENISE ANDERSON

CHAIR, NATIONAL COUNCIL OF ISACS

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 Critical Infrastructure/Key Resources (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.

THE HONORABLE STUART M. GERSON

PARTNER AND SHAREHOLDER, EPSTEIN BECKER & GREEN, P.C.

Stuart Gerson is a member of the firm of Epstein Becker & Green, P.C., in its Washington, D.C. and New York offices. Mr. Gerson was acting Attorney General of the United States during the early Clinton Administration, after having served as President G.H.W. Bush's appointee as Assistant Attorney General for the Civil Division of the Department of Justice. He also has been an advisor to both Presidents Bush. A former federal prosecutor, he originally joined Epstein Becker as a partner in 1980.

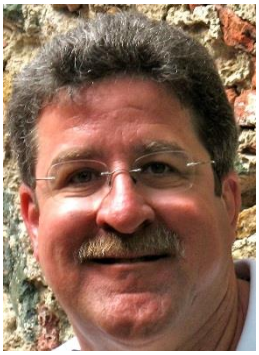
Stuart Gerson's connection with cybersecurity dates back to his time as an Air Force counterintelligence officer in Korea following the 1968 capture of the intelligence ship USS Pueblo. In the early 1990's at the Department of Justice, then Assistant Attorney General Gerson was involved in developing policies and procedures directed at protecting government and commercial data and detecting and prosecuting data thieves.

In private practice, Gerson has been active in digital data security, compliance and breach enforcement and litigation defense. Gerson advises providers, investors, business associates and others concerning HIPAA compliance and also larger cybersecurity issues including the establishment of best practices as described in the President's Executive Order and the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.

Among his successes in litigating cyber issues, Gerson recently won an emblematic case on behalf of two health plans, achieving the unusual result of getting a court to deny class certification in a mass-breach case. He also has represented various entities in responding to federal and state enforcement challenges presented by data breaches.

KENT LANDFIELD

DIRECTOR, STANDARDS AND TECHNOLOGY POLICY AT INTEL CORPORATION



Kent Landfield has spent 30+ years in software development, global network operations and network security arenas. Kent is currently the Director of Standards and Technology Policy at Intel. He has been extremely active in development of the NIST Cybersecurity Framework, 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. Kent has led and 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 also 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.

CHIP WICKENDEN

VICE PRESIDENT OF SECTOR SERVICES, FINANCIAL SERVICES ISAC

As vice president of Sector Services for the Financial Services Information Sharing and Analysis Center (FS-ISAC), Chip Wickenden is responsible for outreach to other cyber intelligence communities and sectors. In this role he is working with other ISACs, ISAOs, and sharing communities to develop community defenses and enhance cross-community dialogue and sharing.

FS-ISAC is one of the oldest and largest information sharing communities globally with more than 7,000 members representing over 70 countries. FS-ISAC also provides community sharing services to four other ISACs and ISAOs today: the Real Estate ISAC, the Retail Cyber Information Sharing Center, The Legal Services ISAO and the Oil and Natural Gas ISAC.

Chip has many years of experience building cross-sector communities, working extensively with the National Automated Clearing House Association (NACHA) to develop the electronic bill presentment and payment industry through his leadership of the Electronic Bill Presentment and Payment Council. He is deepening his knowledge in the intelligence trade, with 5 years focusing on Anti-Money Laundering (AML), fraud and CTI, and he has more than 25 years of experience in banking and financial services, with posts at IBM, FIS, and Bank of America. Chip holds a Master of Business Administration degree and an undergraduate degree in Architecture and Urban Planning from Miami University in Ohio.

PANEL DISCUSSION: BUILDING AN ISAO

MODERATOR: RICK LIPSEY

DEPUTY DIRECTOR, ISAO STANDARDS ORGANIZATION

Richard A. Lipsey serves as Deputy Director of the ISAO Standards Organization and is 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.

Mr. Lipsey served 28 years in the United States Air Force where he distinguished himself in providing strategic leadership in the application of cyber-related capabilities to meet operational mission requirements. He served as the Director for C4 Systems for Air Force Central Command, and 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 United States Cyber Command.

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.

DOUG DEPEPPE

FOUNDER, **EOS**EDGE LEGAL; AND CO-FOUNDER, CYBER RESILIENCE INSTITUTE

Doug DePeppe practices cyberlaw with **eos**edge Legal, a cyberlaw pure-play firm he founded, as well as leads several information sharing ventures and programs stemming from his national programs work while with DHS and the military. In 2009, he served on the White House 60 - day Cyberspace Policy Review, as part of the Lawyers Working Group.

He presently sits as Chair, RC3 Cyber Working Group, Co-Founder of the Cyber Resilience Institute (CRI). Recently, CRI's Sports – ISAO project functioned as a public-private community cyber testbed with the Colorado National Guard and other partners supporting American athletes competing in Rio for the Olympic Games. Doug also serves as leader of a subgroup of the ISAO Standards Organization; and he is a cybersecurity master degree professor at UMUC. Doug retired from the US Army JAG Corps, and has the following academic credentials: two LLM, one JD, and one BA degree.

FRANK GRIMMELMANN

PRESIDENT AND CEO, ARIZONA CYBER THREAT RESPONSE ALLIANCE

Frank J. Grimmelmann is president and CEO (as well as Intelligence Liaison Officer) for the non-profit Arizona Cyber Threat Response Alliance (ACTRA), closely affiliated with the FBI's Arizona 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.

NORMA KRAYEM

SENIOR POLICY ADVISOR & CO-CHAIR OF CYBERSECURITY AND PRIVACY, HOLLAND & KNIGHT

Norma Krayem serves as Senior Policy Advisor and Co-Chair of the Cybersecurity and Privacy Team at Holland & Knight. Ms. Krayem has held executive-level positions in the U.S. Departments of State, Commerce, and Transportation, as well as a consultant at the Federal Emergency Management Agency. She has more than 20 years of experience in the national and international arena, having served both in government and the private sector. She works with public sector and Fortune 500 clients to develop strategies designed to build and maintain a competitive edge. She specializes in the impacts of cyber and privacy issues in critical sectors, including banking and financial services, insurance, energy, communications, health, transportation and many others.

Using her diverse experience, she helps clients navigate complex national and international issues, utilizing creative, leading-edge and practical approaches to solve problems. Key to this is the ability to help clients understand current and evolving policy and regulatory regimes that go hand-in-hand with new dynamic technology solutions, including FinTech, multifactor authentication, Smart Grid, intelligent vehicles (Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I)), Health Information Technology and much more. Inherent to this is an understanding on the need to manage the new world of "Big Data" and the "Internet of Things," and helping clients focus the need for both "privacy by design" as well as "security by design".

She works closely with key decision makers in Congress, White House, DHS, Treasury, DOC, DOT, DOE, DOD, HHS as well as the FCC, SEC, NRC, FERC and many more.

MATT 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. His active projects include analyzing the costs of a cyber incidents 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.

STANDARDS WORKING GROUP ONE: ISAO CREATION

FRANK GRIMMELMANN

CO-CHAIR FOR STANDARDS WORKING GROUP 1

Frank J. Grimmelmann is president and CEO (as well as Intelligence Liaison Officer) for the non-profit Arizona Cyber Threat Response Alliance (ACTRA), closely affiliated with the FBI's Arizona 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 organization 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

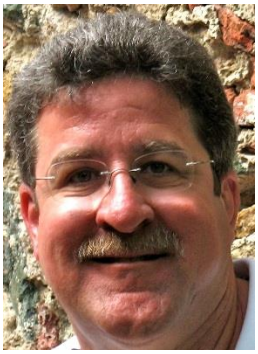
Fred Hintermister is a manager and key member of the Energy Subsector, Information Sharing and Analysis Center (ES-ISAC) for the North American Reliability Corporation (NERC). He plays a vital role providing true security for the bulk power system on both the physical side and the cyber front. Mr. Hintermister 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 the Director of Standards and Technology Policy at Intel. He has been extremely active in development of the NIST Cybersecurity Framework, 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. Kent has led and 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 also 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

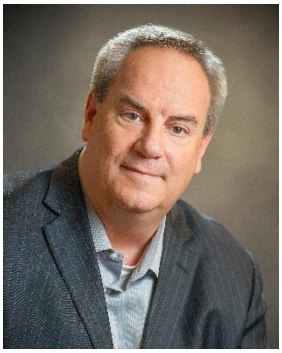
Michael Darling is currently a Director within the Cybersecurity and Privacy practice of PwC focused on information sharing. Prior to joining PwC he was the Director of the Enterprise Performance Management Office at the Department of Homeland Security's Office of Cybersecurity and Communications responsible 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 SIX: GOVERNMENT RELATIONS

DOUG DEPEPPE

ACTING CHAIR FOR STANDARDS WORKING GROUP 6

Doug DePeppe practices cyberlaw with **eos**edge Legal, a cyberlaw pure-play firm he founded, as well as leads several information sharing ventures and programs stemming from his national programs work while with DHS and the military. In 2009, he served on the White House 60-day Cyberspace Policy Review, as part of the Lawyers Working Group.

He presently sits as Chair, RC3 Cyber Working Group, Co-Founder of the Cyber Resilience Institute (CRI). Recently, CRI's Sports – ISAO project functioned as a Public-Private community cyber testbed with the Colorado National Guard and other partners supporting American athletes competing in Rio for the Olympic Games. Doug also serves as leader of a subgroup of the ISAO Standards Organization; and he is a cybersecurity master degree professor at UMUC. Doug retired from the US Army JAG Corps, and has the following academic credentials: two LLM, one JD, one BA degree.

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.