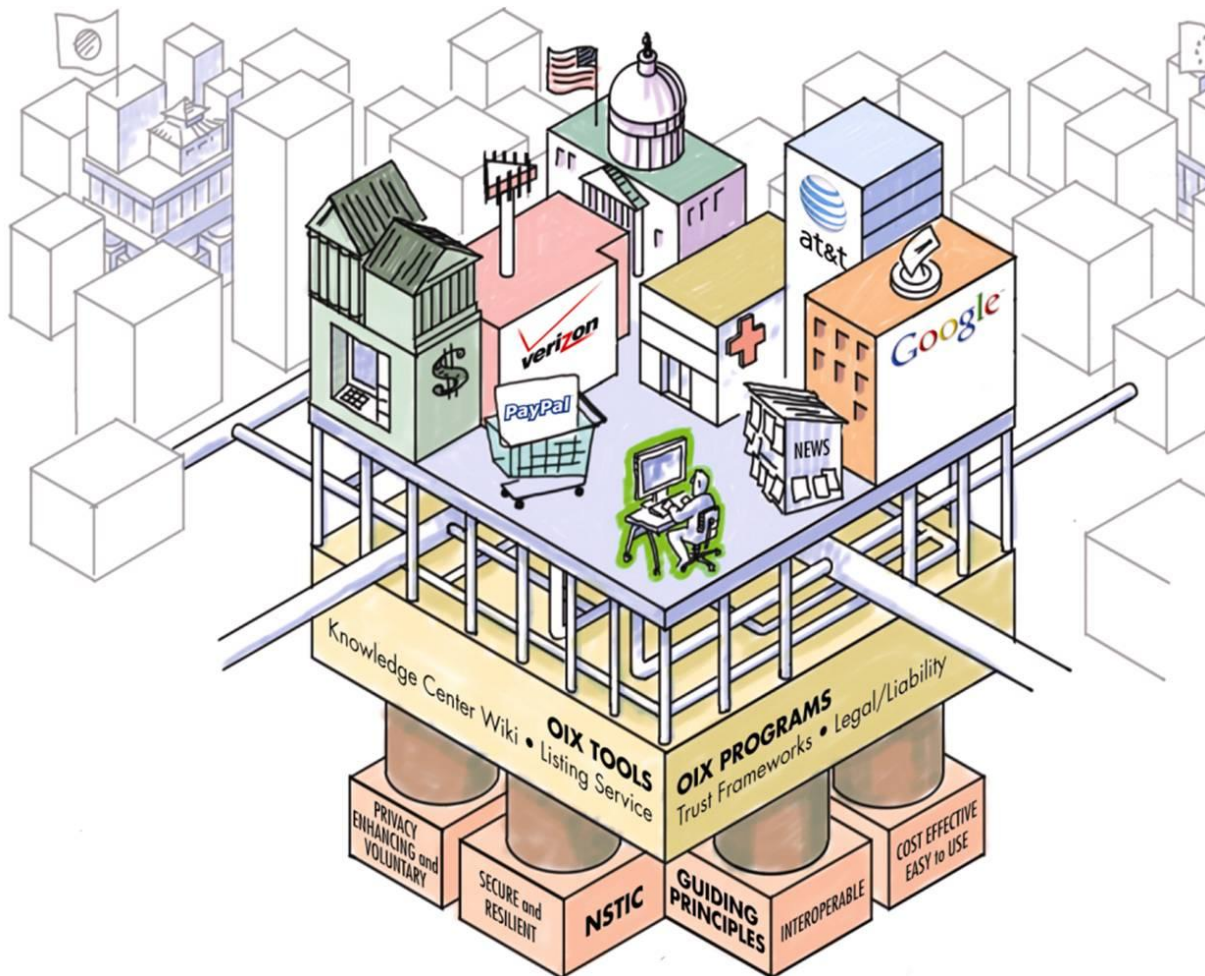


OPEN IDENTITY EXCHANGE ADVISORY BOARD

REPORT 2012-1



Comments on U.S. NSTIC Steering Group Draft Charter and Related Governance Issues

May 1, 2012

INTRODUCTION

The National Institute of Standards (NIST) is currently in the process of selecting a Secretariat as a first step in setting up a Steering Group that will seek to advance the execution of the White House's National Strategy for Trusted Identities in Cyberspace (NSTIC). To guide this initiation of NSTIC governance, NIST has published a draft "Charter" document that suggests certain organizational and operational elements for the Steering Group.

This report has been prepared by the Open Identity Exchange (OIX) Advisory Board in response to a request from OIX Chair Don Thibeau for an initial review of the proposed NSTIC Steering Group from a "governance" perspective, to identify possible issues, challenges, structures, and solutions along the path forward as it is currently contemplated. Please see OIX WG Report 2012-1 background documents for further context.

The OIX Advisory Board has examined the proposal regarding the Steering Group, and has identified for further discussion, the following three categories of issues regarding enhanced organization of the Steering Group:

1. Principles and goals of the Steering Group to be addressed in its "Charter"
2. Functions and operations of the Steering Group to be addressed in its "Bylaws"
3. Form and structure of the Steering Group as a legal entity to be address in its organizational "Articles"

In addressing these fundamental aspects of governance, the OIX Advisory Board does not seek to answer all of the questions surrounding the end game of the NSTIC—the Steering Group will need to decide many of those answers itself. The OIX Advisory Board seeks merely to answer the NIST National Program Office (NPO)'s call for private sector leadership by suggesting some key discussion points on governance in hopes of advancing a structural foundation for NSTIC Steering Group success.

1. PRINCIPLES AND GOALS OF THE STEERING GROUP – THE "CHARTER"

The NSTIC provides that the Steering Group has two general responsibilities.¹ The Steering Group will:

1. Administer the process for policy and standards development for the Identity Ecosystem Framework in accordance with the Guiding Principles in this strategy; and
2. Ensure that accreditation authorities validate participant's adherence to the requirements of the Identity Ecosystem Framework.

The Identity Ecosystem Framework that the Steering Group is tasked to develop is defined as "the overarching set of interoperability standards, risk

Principles and Goals—the Charter

The **Charter** is a brief, principles-level document that describes the purpose of the organization and sets forth its mission and goals.

OIX OPEN IDENTITY EXCHANGE
advisory board

¹ [National Strategy for Trusted Identities in Cyberspace](#), April 2011, page 25.

models, privacy and liability policies, requirements, and accountability mechanisms that structure the Identity Ecosystem.”² The Steering Group is responsible for administration of the process for policy and standards development for this document, but it must do so, “in accordance with the guiding principles.”

The Charter for the Steering Group should directly address these responsibilities in a brief, principles-level document that describes the purpose of the organization and sets forth its mission and goals. The draft Steering Group Charter proposed by NIST, however, presents a mix of principles and operational details. Operational elements in the draft Charter should be moved to the Bylaws.

Those sections of the draft Charter that address the foregoing responsibilities – i.e., draft Charter Sections 1.1 (Mission), 1.2 (Scope of Activities), and 1.3 (Adherence to the NSTIC Guiding Principles) – raise a number of questions regarding the scope and authority of the Steering Group, as well as the nature of the document (the Identity Ecosystem Framework) that it will be developing. For example:

- Approach to Standards. What exactly will the Steering Group be doing with respect to “policy and standards development for the Identity Ecosystem Framework?” What should it do? Will the Steering Group be developing new technology and/or legal standards? Will it be selecting from existing standards to designate the preferred (or mandatory) approach to be used in the Ecosystem Framework? Will it merely be identifying standards that are “acceptable” without selecting any preferred approach? Will it be incorporating such standards in the Identity Ecosystem Framework it is developing?
- Relationship with Standards Development Organizations (SDOs). The scope of Steering Group activity should be further detailed in the context of the broader ecosystem. How will the Steering Group interact with existing standards development organizations? Will it be competing with such SDOs? Will it directly participate in their standards development processes or otherwise provide input to those processes? Will the Steering Group be developing technical standards to fill gaps among existing and future standards? Will the Steering Group be developing legal/policy standards? Will the Steering Group run a certification program and corresponding Trustmark program against those standards? What will the Steering Group’s goals be? Will the SDO’s be given a seat on the Steering Group to express their viewpoint (and lobby for their standards)? Will the Steering Group try to influence the development by SDOs of new standards or the modification of existing standards to conform to its guiding principles? How will relevant international standards factor in?
- Technology Neutrality. Will the Steering Group be selecting (or certifying) one or more specific technologies as meeting its Guiding Principles, and will normative cross-references by the Identity Ecosystem to other specifications have that “selective” effect? Or will it seek to adopt a position of technology neutrality and develop the Identity Ecosystem Framework in a manner that allows for the use of any technology?
- Approach to Innovation. Will the Identity Ecosystem Framework lock-in the trust frameworks it governs to a particular approach to identity systems, or will it be more of an enabling document that is designed to accommodate and/or facilitate the use of any approach and technology regarding identity?
- Nature of the Identity Ecosystem Framework Document. What exactly is the nature of the Identity Ecosystem Framework document the Steering Group will develop? Is the Ecosystem Framework designed to remove barriers? Is it a regulatory document? Is it designed to promote the

² Id., 24.

development of identity systems? Is it designed to ensure that identity systems meet certain requirements (defined by the Steering Group) regarding interoperability, ease of use and privacy? Is it all of these? What else should it cover? Does it become a meta-system (aka “stakeholder community”) governance document?

- Trustmark. What will be required of trust framework developers in order to obtain the NSTIC trustmark?
- Role of the Identity Ecosystem Framework. What is the intended role of the Identity Ecosystem Framework to be developed by the Steering Group?
- Priorities. What are the Steering Group priorities? How will conflicts of priorities be resolved?
- Role of Guiding Principles. NSTIC requires the Steering Group to administer the process for policy and standards development for the Identity Ecosystem Framework in accordance with the Strategy's Guiding Principles. What limitations does that impose on the work and mission of the Steering Group?
- Driving Adoption. How can the Steering Group attract stakeholder participation? What is the value to stakeholders? How will that affect organization and operation of the Steering Group?
- Privacy by Design. NSTIC raises various privacy concerns without providing guidance on how to achieve sustainable, scalable, easy to use solutions. The Charter should not create requirements that cannot be practical or adoptable.
- Relationship of the Secretariat to the Steering Group. It appears that the Secretariat will play much more than a mere administrative role, particularly during the early stages of the Steering Group. This role, and that of the Ombudsman, requires clarification.

Since “form follows function,” the answers to these and similar questions will be critical to the further development of the Steering Group Bylaws, Articles and other organizational and operational documents.

2. FUNCTIONS AND OPERATIONS OF THE STEERING GROUP – THE “BYLAWS”

The Bylaws of any organization are the internal governance “how to” manual. They typically provide details of officer and director powers and responsibilities. Thus, the respective roles and powers of the Plenary and the Management Committee should be detailed in the Bylaws. Likewise, novel issues raised by the inclusion of a Secretariat and the Ombudsman and the participation of the NIST National Program Office would be appropriately detailed in the Bylaws.

Questions that should be considered in developing the Bylaws for the Steering Group should include the following:

- Qualifications for Offices. Bylaws can provide prerequisites where desired for certain officers.

Functions and Operations—the Bylaws

The **Bylaws** of any organization are the internal governance “how to” manual, typically providing details of officer and director powers and responsibilities.

OIX OPEN IDENTITY EXCHANGE
advisory board

- Member/Shareholder Issues. Will the Steering Group have members? If so, will they vote? What will they vote on? What economic interests, if any, should Stakeholders have in the Steering Group? If there are no members, will the Plenary Stakeholder Groups be “self-perpetuating?” Will any voting be “weighted” based on plenary group size, etc.? How will notices and meetings be structured to maximize transparency and access by stakeholders?
- Election of Management Committee Members. What are the Provisions for election, removal, resignation, disqualification, vacancies, etc. that will be needed to assure balance and fair representation?
- Management Committee Processes. What are the Details of voting, meetings, notice, compensation and other Management Committee processes to provide assurance that the Steering Group is being managed consistent with NSTIC goals?
- Committee Provisions: The Steering Group Plenary is anticipated to have some standing committees and will likely require additional committees all of which would be covered in Bylaws. What are the provisions for creation, delegated authority, limitations, requirements and membership of committees?
- Officers: What are the provisions relating to officers, such as the Chair of the Plenary and the Chair of the Management Committee, as well as the Ombudsman who will help to define these roles?
- Indemnification: Will the Bylaws provide for indemnification of officers and directors against certain lawsuits relating to their work for the organization? This is often helpful to induce participation.
- Amendments to Bylaws: What are the provisions and processes for amendment of the Bylaws, particularly in the early days of operation? The process should be fluid, and designed to not stall normal operations of the Steering Group.


3. FORM AND STRUCTURE OF THE STEERING GROUP – THE “ARTICLES”

As noted above, the resolution of Charter issues will inform choice of legal entity, so any discussion of that choice is preliminary and is directed at identifying possible available forms that could help to resolve some current governance challenges. Ultimately the Steering Group functionality will be housed in one or more entities.

The choice of entity is not a neutral one; a poor choice will hobble Steering Group function, while a well thought-out choice, and careful attention to the required “customization” through the Articles, Bylaws and Charter, will enhance the Steering Group. It is useful to consider “choice of entity” issues early, recognizing that the ultimate selection of the entity will take place only after the anticipated functions (such as those contemplated in the Charter document) have been mapped out.

Form and Structure—the Articles

The **Articles** of any organization are the rough equivalent to the “operating system” of the legal programming of an entity. The choice of system affects later design and deployment decisions, as does the choice of entity.

 **OPEN IDENTITY EXCHANGE**
advisory board

States authorize a variety of different forms of legal entities, each offering their own advantages and downsides. The OIX Advisory Board has engaged in preliminary examination of several available options in the U.S., including corporations (not-for-profit, for-profit “benefit” corporations, regular “for profit”), partnerships (general and limited), trusts, co-operatives, limited liability companies (LLCs), low-profit limited liability companies (L3Cs), agency arrangements, associations, quasi-governmental entities, public/private partnerships, contractual arrangements of various sorts, self regulatory organization structures, and various unincorporated organizations.

The Advisory Board has also initiated the review of other entity qualifications under federal law such as qualification of a state not-for-profit corporation under Internal Revenue Code 501(c)(3), 501(c)(6) and other sections of IRC 501, IRC “S” Corp. status, IRC section 115 exemption strategies, the National Cooperative Research and Production Act of 1993, and others. Examples of potential options identified to date (and potential challenges to applicability) include:

- State Non-profit Corporation. May have state law limitations inconsistent with NSTIC. Note possible use of state not-for-profit that doesn’t seek IRC exemption under IRC 501.
- 501(c)(3). Scope of available purposes may be too narrow, i.e., “educational,” “lessening the burdens of government.
- 501(c)(6). Limitations on funding by “dues” and performance of member services may be too narrow for NSTIC sustainable entity.
- State For-Profit “Benefit” Corporation. New form of corporation in about six states. Like a regular corporation, except can name group to benefit through conformity to a third party standard. The Steering Group Plenary’s stakeholders might be appropriate “benefitted parties,” and NSTIC an appropriate “third party standard” under those laws.

Many or most of the “needs” identified and initially defined by NSTIC are associated with relatively recent phenomena arising as a result of increasingly broader dependence on a highly networked information system environment, which present many new and unique challenges. Consequently, the NSTIC “needs” do not fit easily into many of the more traditional forms of organization.

Regardless of the form of entity, the article of organization will need to address a variety of issues. Those include: who will act as the incorporator, the name of entity, the state of organization (the law of which affects its structure), the duration of the entity, purposes and powers of the entity, limitations on its powers, members (e.g., partners, members, shareholders, etc.), directors, limitations on director liability (and/or indemnification of directors), registered agent, and dissolution.

Please see OIX Advisory Board Report 2012-1 background documents for elaboration of these issues.

ABOUT THE OIX ADVISORY BOARD



JOHN BRADLEY is an Identity Management subject matter expert and IT professional with a diverse background. Mr. Bradley has over 15 years experience in the information technology and identity management field. Mr. Bradley advises Government Agencies and commercial organizations on the policy and technical requirements of Identity Management, Federated Identity, PKI and smart card solutions. Mr. Bradley communicates effectively with clients, vendors, staff and standards organizations to brief them on complex state-of-the-art identity management concepts, best practices, and technical requirements. He is also Chair of the Federation Interoperability WG at Kantara. He is treasurer of the openID Foundation, on the advisory board for OIX, and an active contributor to SAML and other OASIS specifications at OASIS. . Mr. Bradley is one of the leaders of OSIS, and the Kantara Interoperability Review Board, forums that vendors use for industry interoperability testing, and thus has an in-depth understanding not only of the factors that contribute to success, but of upcoming trends that affect whether strategic planning will ensure optimal effectiveness for future operability. Recently John has been co-authoring the ICAM protocol profiles at Protiviti Government Services on behalf of GSA, and continues to support the FICAM interoperability Lab. Current projects include co-authoring the next version of the openID specification and related standards.



SALVATORE D'AGOSTINO is the CEO of IDmachines LLC and provides design, integration, strategic and tactical consulting services. IDmachines' practice runs across the identity, credentialing, access, security, machine learning and technology transfer markets and its participants. Prior to IDmachines Sal was the Executive Vice President at CoreStreet, whose software provides identity and credential validation and distributed access control solutions for many governments and global enterprises. Prior to that Sal worked at and was promoted to CEO of Computer Recognition where, among other things, he helped to design and deploy EZPass and other electronic toll collection systems, upgrade the United States Capitol Physical Security System, and responsible for over 100 applications of industrial, transportation and security machine vision systems in supervisory control and data acquisition (SCADA) systems.

Sal is very active in developing industry standards, education and best practices through professional affiliations that besides the OIX Advisory Board include; Secretary of the Smart Card Alliance Identity Council and Secretary of its Access Control council, Vice-Chair of the Security Industry Association PIV Working Group, member of the IT Security Council of the American Society for Industrial Security, Chair of the Kantara Initiative Attribute Management Discussion Group, friend and former member of the Transportation Research Board's Freeway Operation Committee, member of the RTCA Special Committee 224 on Airport Security Access Control Systems and a charter member of the Society of Manufacturing Engineers' Machine Vision Association. Sal is a graduate of Harvard College, and former All-Ivy and All-East wrestler, shares a patent on sentient geosynchronous displays and has worked with Ha-Ha on exhibits at the Hyde Park Art Museum and the Massachusetts Museum of Contemporary Art.



SCOTT L. DAVID is a partner in the K&L Gates LLP law firm. His practice focuses on transaction structuring and providing legal advice associated with emerging technologies including information/data law, compliance with privacy, data security and identity law, electronic commerce, online payment structures, standards setting, tax and intellectual property issues. Current Work Scott provides advice to firm clients on issues of compliance with federal and state privacy and data security laws; structuring of online contracts, terms of use, privacy policies and electronic payment and tax administration systems; networked data risk and liability management; online and telecommunications entity organization and affiliation structuring; technology development and transfer; participation in technical standards setting organizations; international, federal, state and local internet and telecommunications taxation; intellectual property licensing and structuring and non-profit and tax-exempt status and related issues. Scott's publications include chapters relating to telecommunications law and tax issues associated with ecommerce.

In addition, he has authored articles in a variety of journals and publications relating to business information system structuring; legal perspectives on business data security management issues; FCC, FTC and other government regulation of online data and information systems; estate planning in the digital age; payment and tax structuring for online transactions; and broadband over power line (BPL) legal issues. Scott has given presentations on legal issues to a variety of business, legal, and other groups relating to various topics in information law, identity, privacy and data security; monetization and risk mitigation legal strategies for data collection and aggregation; legal issues of commercial interactions using virtual reality interfaces; emerging legal issues in virtual property; issues associated with cloud data storage and services; telecom tax; digital estate planning; nanotechnology; robotics; legal structuring and strategies for technical standards initiatives; gift card and stored value card systems. Prior to joining K&L Gates, Scott practiced with Simpson Thacher & Bartlett in New York City. Before attending law school, he worked as the production manager for a computer manufacturer in Rhode Island. Scott is a member of the bars of New York and Washington.

He received an LL.M., (taxation) from New York University in 1990, a J.D., from Georgetown University Law Center, 1985 (magna cum laude) and did his undergraduate work at Brown University.



DEBRA N. DIENER, CIPP/G, J.D., has over 30 years of expertise from serving in senior legal, policy, legislative and managerial positions in all three branches of the Federal Government. Before retiring, she served as the Senior Advisor and Director of Privacy Policy in the Privacy Office for the Department of Homeland Security (DHS). For over three years, Ms. Diener was a Co-chair of the Identity Management Subcommittee of OMB's CIO Council's Privacy Committee. In that role, she helped to spearhead the successful collaboration between the Federal Government and private sector organizations on privacy priorities, including the Government's innovative approach to identity management. Prior to DHS, Ms. Diener served with the Treasury Department in diverse senior positions with the Headquarters Office of General Counsel, the Financial Management Service (FMS) and the IRS. She played a lead role on domestic and international policy, legal, and regulatory matters in criminal justice/law enforcement, financial services, privacy, information protection and identity management. She also served as a counsel on the Crime and Criminal Justice Subcommittee, House Judiciary Committee, where she was instrumental in crafting significant legislation. Ms. Diener holds a B.A. in Political Science from Syracuse University; an M.A. in Political Science from the University of Pennsylvania; and a J.D. from the George Washington University. She is also a Certified Information Privacy Professional/ Government.



RAINER HOERBE is a contributor, architect and standards editor for the Austrian eGovernment federation and used to be lead developer for products used in the federation. In the European cross-border eHealth project epsOS he serves as security advisor. As a member of Kantara Initiative and ISO SC27 he is engaged in developing new models and standards in federated identity management.



HISHAM KASSAB, PH.D. is the founder and president of MOBILAPS, LLC. MOBILAPS is based in Silver Spring, MD, and specializes in mobile applications; geospatial technologies; and innovative applications for network appliances, including next-generation emergency notification technologies such as web-browser alerts and streaming video alerts. MOBILAPS has been funded by NSF, USDA, and the state of Maryland; and counts NASA and the Open Geospatial Consortium among its clients. Hisham received his B.S. in Electrical Engineering, M.S. in EECS, M.S. in Operations Research, and Ph.D. in EECS from MIT. His Ph.D. dissertation was in the field of wireless networks. After MIT, Hisham worked for several years in the strategy consulting industry, first working for the multinational Booz & Co.; and then joining TMNG, a boutique firm specializing in the ICT industry. In 2005, Hisham left the management consulting industry to launch MOBILAPS.



RL "BOB" MORGAN has worked locally, nationally, and internationally for over 20 years to design and deploy advanced identity management systems in support of higher education and research. He is an Identity and Access Management Architect for UW Information Technology at the University of Washington. He has been in this position since 1999; prior to that he was in a similar role at Stanford University. In this position he contributes to designing, implementing, and documenting identity management and distributed service infrastructure for the UW. Bob has been the Chair of the Middleware Architecture Council for Education (MACE), a US-based international group of identity management architects providing guidance for the Internet2 Middleware Initiative, since its inception in 1999. He has been a primary contributor to a number of Internet2-initiated projects, notably Shibboleth, a system for secure access to inter-institutional web resources. He was a co-founder in 2004 of the InCommon Federation, the leading trusted identity community for higher-education and research in the US, and serves as co-chair of the InCommon Technical Advisory Committee. He is also active in a variety of standards activities and cross-industry identity collaboration groups including IETF, OASIS, Identity Commons, the Kantara Initiative, the Open Identity Exchange (OIX), and REFEDS. In this role he has helped to develop the Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML) standards.



AKIKO ORITA, PH.D. is an assistant professor at Keio University in Japan. She is conducting research projects related in social media, identity and anonymity and users' behavior. She got her M.A. in Media and Governance at Keio University, then served as a research associate working as an assistant of Prof. Jun Murai to establish national IT strategy in Japan. Dr. Orita stood for the Diet election in 2002 as an

official candidate appealing for individual control for privacy. After earned her Ph.D. in Media and Governance at Keio University in 2007, she served as an assistant professor at Chuo Graduate School of Strategic Management, then moved to Keio University. In 2010, Dr.Orita was a member of national, high-level regulation reformation committee of IT strategic headquarters in Japan, Dr.Orita also has an experience as a visiting assistant professor at Kennesaw State University in Georgia in 2011 teaching at Computer Science and Information Systems Department.



THOMAS J. SMEDINGHOFF is a partner in the Privacy & Data Protection practice group in the Chicago office of Edwards Wildman Palmer LLP. His practice focuses on the developing field of information law and electronic business activities, with an emphasis on electronic transactions, identity management, data security, privacy, and corporate information governance issues. Mr. Smedinghoff has been actively involved in developing e-business, e-signature, data security, and information legal policy both in the U.S. and globally. He currently serves as chair of the Identity Management Legal Task Force of the American Bar Association (ABA) Section of Business Law, and co-chair of its Cyber Security Committee.

Previously, he was chair of the ABA Section of Science & Technology Law (1999-2000), chair of the ABA Electronic Commerce Division (1995-2003), and chair of the International Policy Committee (2008-2011). He is also a member of the U.S. Delegation to the United Nations Commission on International Trade Law (UNCITRAL), where he participates in the Working Group on Electronic Commerce and helped to negotiate the international e-commerce treaty titled the “United Nations Convention on the Use of Electronic Communications in International Contracts” and the UNCITRAL “Model Law on Electronic Signatures.” He was also the ABA Advisor to the Uniform Law Commission Committee to Implement the UN E-Commerce Convention (2008 – 2010), and served as an ABA Advisor to the Uniform Law Commission committee that drafted the Uniform Electronic Transactions Act. Mr. Smedinghoff is the author of the book titled INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE, (IT Governance Publishing, 2008). He is also the editor and primary author of the e-commerce book titled ONLINE LAW: THE LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET (Addison Wesley, 1996), as well as numerous articles on electronic transactions, identity, privacy, and data security law issues.



JUDITH SPENCER is the Chair, CertiPath Policy Management Authority. She manages the CertiPath Bridge Certification Authority, which provides the federated trust environment for the Aerospace-Defense community. In addition, she represents the CertiPath community stakeholders in activities related to NSTIC. Previously, Ms. Spencer was employed by the U.S. General Services Administration building cross-organizational consensus on matters related to identity management. She was Chair of the Federal PKI Policy Authority, and Co-Chair of the Federal Identity, Credential and Access Management Subcommittee, assisting the Federal community in implementing HSPD-12 and setting government-wide goals for identity management.



HAL WARREN has more than 18 years of experience in Internet technology development specializing in social networking tools and web delivery of commercial content. Currently Mr. Warren is working to use emerging trusted identity to build stronger peer circles for scientists and to create better semantics in scholarly publishing. Mr. Warren also serves as president of the OpenID Society. He graduated with a B.A. in philosophy from the University of Tennessee.

CONTRIBUTING EDITOR



SAM ECKLAND is an associate at McBee Strategic Consulting, provides research, policy analysis, and communications guidance for clients and in the emerging growth, energy, and cyber security sectors. Sam's previous work with Open Identity Exchange included working as a Policy Analyst and Project Coordinator for the OIX response to the National Strategy for Trusted Identities in Cyberspace (NSTIC) Notice of Inquiry: NSTIC Governance Structure. Sam has also held positions with McBee Strategic's Capital Markets Group, the Office of Rep. Betsy Markey (D-CO), and with the US Climate Action Network. Sam graduated from Northwestern University with a BA in Classics & Environmental Policy and Culture.