VENABLE® LLP

Cyber Sticks and Carrots: How the NIST Cybersecurity Framework, Incentives, and the SAFETY Act Affect You

SEPTEMBER 25, 2013

WASHINGTON, DC

VENABLE LLP

Agenda

Cyber Sticks and Carrots

- Introduction
- The Cybersecurity Framework, Incentives, and Liability
- The SAFETY Act: an Already Available Incentive
- Secretary Lute's Remarks

VENABLE® LLP

The Cybersecurity Framework, Incentives, and Liability

SEPTEMBER 25, 2013

WASHINGTON, DC

VENABLE® LLP

EO 13636: Improving Critical Infrastructure Cybersecurity

- Directs to NIST to develop a Cybersecurity Framework “to reduce cyber risks to critical infrastructure”
- Directs DHS to establish a voluntary program to support adoption of the Framework by owners and operators of Critical Infrastructure
- Directs DHS to coordinate establishment of a set of incentives to promote participation in this program

VENABLE® LLP

Incentives

- DHS, Treasury, Commerce reports
- White House list of incentives
- Discussion at Dallas workshop
  - adoption, improvement, or hybrid?

VENABLE® LLP

Tort/Contract Liability

- potential liability abounds
- administration's emphasis on insurance
- legislation?

VENABLE® LLP

The SAFETY Act:

an Already Available Incentive

SEPTEMBER 25, 2013

WASHINGTON, DC

VENABLE LLP

The SAFETY Act

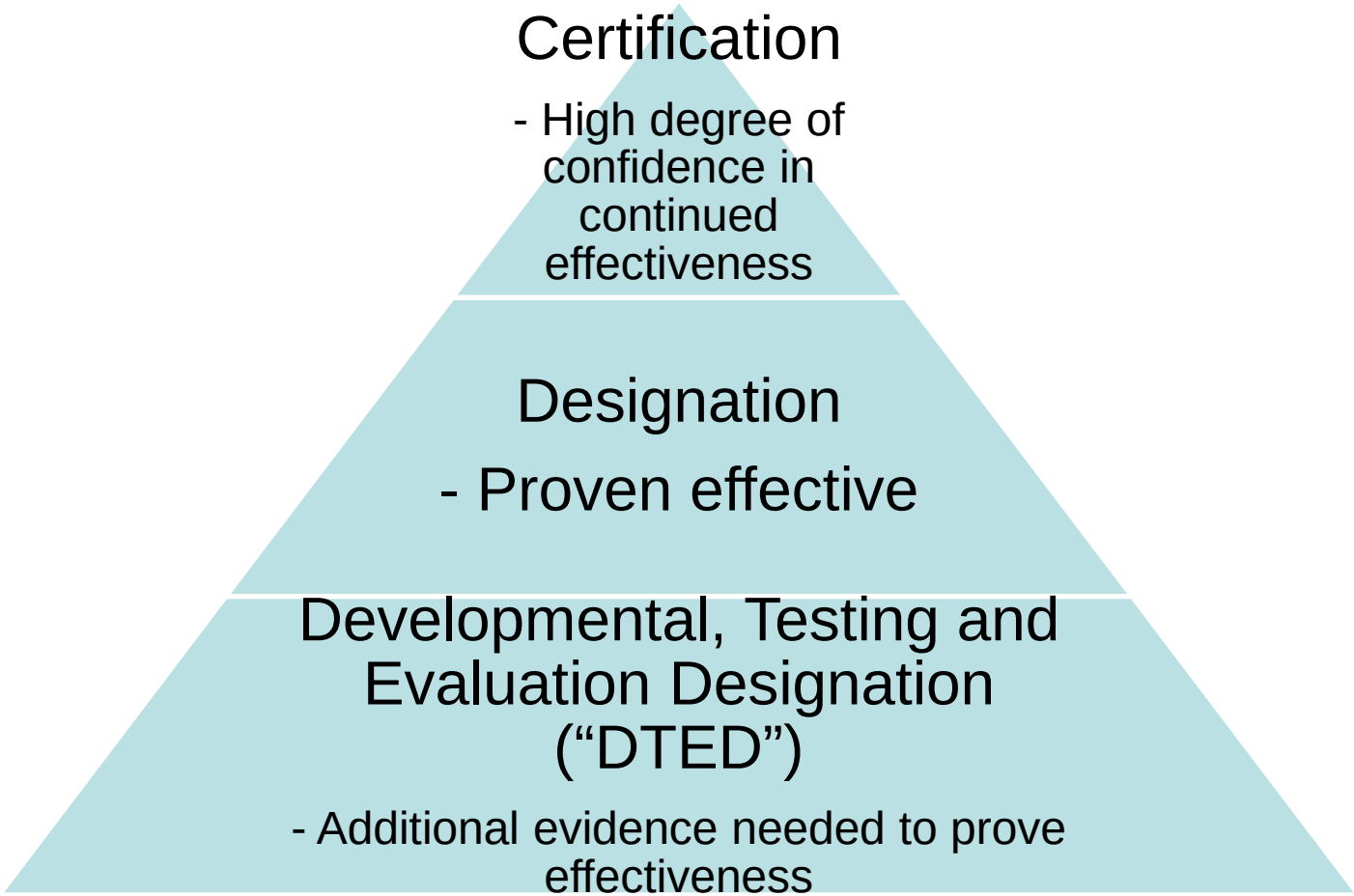
- The SAFETY Act (Support Anti-Terrorism by Fostering Effective Technologies Act)
  - Enacted as part of the Homeland Security Act of 2002, Public Law 107-296 (Title VIII, Subtitle G, Secs. 861-65)
  - Implementing regulation at 6 C.F.R. Part 25
- Intended to encourage the development and deployment of anti-terrorism technologies by creating systems of "risk" and "litigation management"
- Technologies include:
  - Products, devices, equipment
  - Services – both supporting and standalone services
  - Cyber-related items
    - Information technologies and networks
    - Integrated Systems

VENABLE LLP

Scope of the Act

- Applies to an "act of terrorism," which may include cyber terrorism
- An "act of terrorism" is defined by DHS as:
  - Unlawful
  - Causes harm, including financial harm, to a person, property, or entity, in the United States…; and
  - Uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States
- Includes attacks committed by domestic terrorists
- May include attacks on foreign soil, if harm is to a person, property or entity in the United States

Levels of SAFETY Act Protection



VENABLE® LLP

Benefits of Protections

Certification	- All the benefits of Designation - Government Contractor Defense
Designation	- Liability cap at a pre-determined insurance level - Exclusive jurisdiction in Federal court - Consolidation of claims - No joint and several liability for noneconomic damages - Bar on noneconomic damages unless plaintiff suffers physical harm - No punitive damages and prejudgment interest - Plaintiff's recovery reduced by collateral sources
DTED	- Same as Designation, but for a shorter duration (3 yrs)

Obtaining SAFETY Act Protections

The Applicant's Role

Internal Assessment of Technology
- Document
-Enhance

Prepare Application

Submit Application to OSAI

OSAI/DHS's Process

Completeness Review (30 days)

Technical & Economic Review / Requests for Information

DHS Decision

OSAI/DHS Review Time = 120 days (total)

VENABLE® LLP

Questions?

Upcoming Events

- **CyberMaryland 2013, Wednesday, October 9, Baltimore, MD:**

Michael Baader

Partner, Venable LLP

"Trends & Hot Issues in Mergers and Acquisitions"

Track A (moderator)

1:30-2:15 pm ET

Dismas Locaria

Partner, Venable LLP

"Building an Effective Cyber Risk Culture: An Overview of Cybersecurity Insurance & the Support Anti-Terrorism by Fostering Effective Technologies Act ('SAFETY Act')"

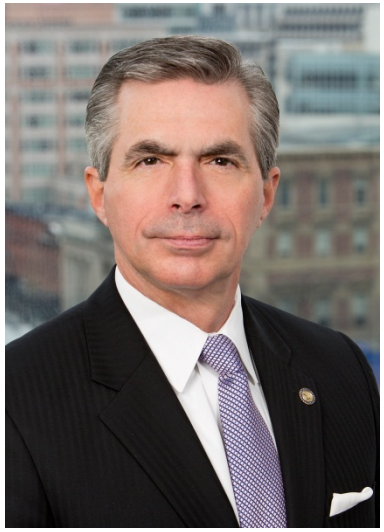
Track B (speaker)

1:30 p.m.-2:15 pm. ET

Please click here for more information and to register.

Upcoming Events

- **Cyber Security Finance Forum 2013, October 21-22, Washington, D.C.**



Jamie Barnett
Rear Admiral (Ret.)
Partner, Venable LLP

Sessions Include:

- The Cyber State of Play: Understanding the Digital Threat
- Defining the Federal Cyber Agenda
- Technology Panel: Which Technologies are Grabbing Center Stage in the Cyber Security Space?

Please click here for more information and to register.

VENABLE® LLP

contact information

Jamie Barnett, Rear Admiral (Ret.), Partner
jbarnett@Venable.com
t 202.344.4695

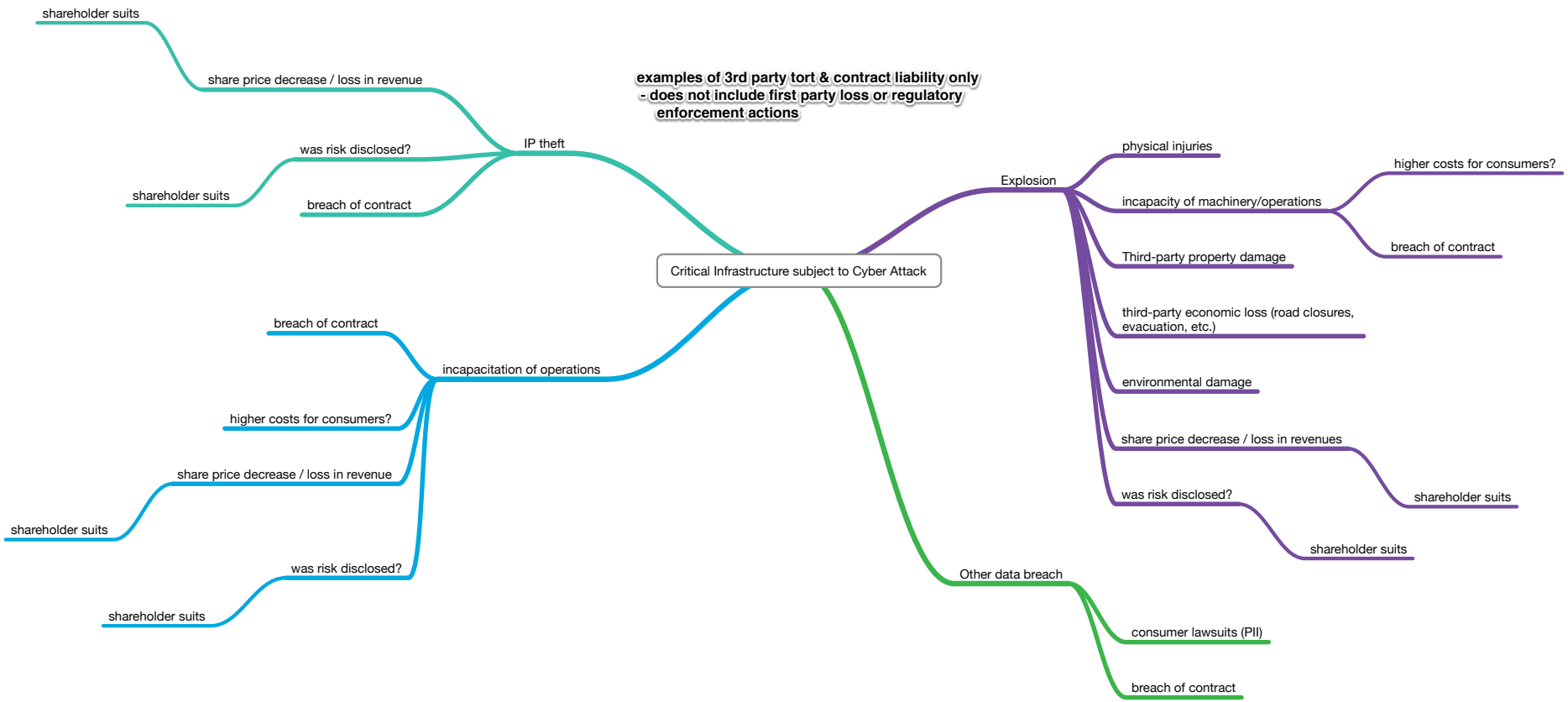
Dismas Locaria, Partner
dlocaria@Venable.com
t 202.344.8013

Jason R. Wool, Associate
jwool@Venable.com
t 202.344.4511

www.Venable.com

Incentive	DHS	TRSRY	Comm.	WH*	Notes
Insurance	X	X	X	X	Commerce recommends engaging insurance companies. "This collaboration . . . could serve as a basis for creating underwriting practices that promote the adoption of cyber risk-reducing measures and risk-based pricing. This collaboration could also foster a competitive cyber insurance market." Commerce at 2. "Direct government involvement may not be necessary and could, in fact, impede the development of a private market." Treasury at 6. DHS second tier; category "Bundled Insurance Requirements, Liability Protections, and Legal Benefits." DHS echoed Treasury comment (above), but concluded that "nonetheless, market-based incentives like insurance can be encouraged via government policy, including policy that promotes sustained stakeholder dialogue about enhancing their viability." Further, DHS encourages bundling with liability protection, i.e., that "owners and operators carry insurance in order to receive . . . liability protections." DHS at 18. WH: "The goal of this collaboration would be to build underwriting practices that promote the adoption of the cyber-reducing measures and risk-based pricing and foster a competitive cyber insurance market."
Tort liability reduction, etc.	X	X	X	X	Commerce recommends studying the effectiveness of this incentive. "This study should include a review of tort cases against critical infrastructure owners and operators and an assessment of mechanisms (e.g., insurance or statutory liability limitations) that have the potential to reduce or transfer their tort liability if a cyber incident causes damage despite the owner or operator's adoption and implementation of some or all of the standards, procedures, and other measures that comprise the Framework." Commerce at 2. Treasury "recommends further study of whether adopting the Framework through the voluntary program could serve as a standard of conduct for, or minimum acceptable level of, systems integrity and precautions . . . [a] court may find that joking the voluntary program, implementing the Framework or, at the very least, some of its practices, satisfies a duty of care in a civil lawsuit. Alternatively, legislation could establish a statutory defense. Such a defense could take several forms. For example, it could take the form of a safe harbor, which could present a partial or complete defense from liability. Alternatively, it could take the form of a rebuttable presumption that a critical infrastructure entity has taken sufficient action under the circumstances. In ether case, it is important to note that extending liability protection could also introduce moral hazard [.]" DHS second tier; category "Bundled Insurance Requirements, Liability Protections, and Legal Benefits;" DHS: "reduce liability in exchange for improved cybersecurity or increased liability for the consequences of poor security; full indemnity, higher burden of proofs, or limited penalties; case consolidations; case transfers to a single federal court; creation of a federal legal privilege that also preempts State litigation discovery law and applies to owners and operators that undertake cybersecurity self-assessments so that those assessments would not be discoverable in subsequent litigation and/or used as evidence in court." WH pointed to need for more information to determine "if legislation to reduce liability on Program participants may appropriately encourage" a broader range of participants. WH listed reduced tort liability, limited indemnity, lower burdens of proof, or the creation of a Federal legal privilege that preempts state disclosure laws.
Consider participation as a criterion for NSTIC Pilot and other Commerce Grants			X		
Consider cybersecurity as an "appropriately weighted criteria for evaluating federal grant applicants"	X	X	X	X	DHS first tier
Identify candidates for regulatory streamlining	X		X	X	"Once NIST has published the first version of the Framework and the Program is operational, the Administration, independent agencies, and Congress should use this information to inform discussions of specific regulatory streamlining proposals." Commerce at 2. DHS third tier; "create unified compliance model for similar requirements and eliminate overlaps among existing laws (e.g., SOX, HIPAA, GLB; international law); reduce audit burden; prioritized permitting.
Explore a Fast-Track Patent Pilot for cybersecurity			X		
Government procurement considerations	X		X		Commerce recommends studying the effectiveness of this incentive. DHS second tier

Use of Tax Incentives	X	X	X		"There was little consensus among respondents to the NOI on whether or which kinds of tax incentives might be effective. In Commerce's analysis, it would be difficult to ensure that tax incentives are sufficient to encourage participation in the Program and do not impose undue costs on the federal government." Commerce at 3. "Tax incentives are difficult to target specifically at cybersecurity activities, and harder still to target at cybersecurity investments that firms would not otherwise make. Ultimately, adoption of a tax incentive would come at the expense of foregone revenue for the government or reallocation of existing fiscal obligations." Treasury at 6. DHS second tier
Public Recognition	X		X	X	Commerce recommends studying the effectiveness of this incentive. DHS third tier
Technical Assistance	X	X	X	X	Commerce recommends studying the effectiveness of this incentive. DHS third tier WH: Not limited to technical assistance, but a "range of government programs in which participating in the Voluntary Program could be a consideration in expediting existing government service delivery." Notably, "**[a]gencies currently have the authority to act in these areas without further legislation.**"
Expedited security clearances	X	X	X		Commerce determined that the EO already provided for this; DHS removed from consideration due to overlap with existing efforts to provide expedited clearances.
Enhance Information Usage Capabilities		X			
Rate Recovery	X			X	DHS first tier WH identified need for further dialogue with federal, state, and local regulators and sector specific agencies on whether the regulatory agencies that set utility rates should consider allowing utilities recovery for cybersecurity investments related to complying with the Framework.
Subsidies	X				DHS second tier
Information Sharing	X				DHS removed from consideration due to section 4 of EO, which would provide information sharing independently of adoption of the Framework.
Security Disclosure	X				Actually a "stick"; "require public notification of disclosures to encourage owners and operators to take care to avoid breaches; preemption of state notice requirements."
= recommended against					*"While these reports do not represent final Administration policy, they do offer an initial examination of how the critical infrastructure community could be incentivized to adopt the cybersecurity Framework as envisioned in the Executive Order."


examples of 3rd party tort & contract liability only - does not include first party loss or regulatory enforcement actions
Critical Infrastructure subject to Cyber Attack
IP theft
shareholder suits
share price decrease / loss in revenue
was risk disclosed?
shareholder suits
breach of contract
incapacitation of operations
breach of contract
higher costs for consumers?
share price decrease / loss in revenue
shareholder suits
was risk disclosed?
shareholder suits
Explosion
physical injuries
incapacity of machinery/operations
higher costs for consumers?
breach of contract
Third-party property damage
third-party economic loss (road closures, evacuation, etc.)
environmental damage
share price decrease / loss in revenues
shareholder suits
was risk disclosed?
shareholder suits
Other data breach
consumer lawsuits (PII)
breach of contract

VENABLE LLP

the SAFETY Act

SAFETY ACT ATTORNEY QUICK FACTS

Cross-discipline team of over 15 attorneys experienced in SAFETY Act and related security and cybersecurity matters

Our Team Includes:

- Former Chief, Public Safety and Homeland Security Bureau, Federal Communications Commission
- A licensed U.S. Customs broker
- Former Counsel, DC Council, Committee on Consumer and Regulatory Affairs
- Authors of LexisNexis®' *The Homeland Security Deskbook: Private Sector Impacts of the Defense Against Terrorism*

HONORS AND AWARDS

Recognized by *Chambers USA*

TOP RANKED CHAMBERS USA 2013 Leading Firm

Previous Winners of the *Chambers USA* Award for Excellence

Ranked among the nation's top firms, Technology: Data Protection & Privacy, in *Legal 500*

The LEGAL 500 UNITED STATES LEADING FIRM 2013

Previously, Two of the "Top 25 Privacy Experts" – *Computerworld*

Attorneys with top rankings by

Chambers USA
Legal 500

THE SAFETY ACT

how to protect your company from terrorism liability, including risks from cyber terrorism, and gain valuable business benefits

The SAFETY Act's benefits to your company

When Congress passed the Homeland Security Act of 2002, it sought to encourage the development and deployment of anti-terrorism products and services, including those for cybersecurity, through the "Support Anti-terrorism by Fostering Effective Technologies Act of 2002" (SAFETY Act). Thus, if your business manufactures and/or sells anti-terrorism technologies, or is one that develops and implements its own cyber or physical security program, the SAFETY Act may be an important risk mitigation tool for you. The SAFETY Act's framework can also provide added benefits to your customers. Therefore, the SAFETY Act not only protects your company from potential liability, but can also make you a more attractive provider to potential customers.

The SAFETY Act provides two primary levels of protection—Designation and Certification. Technologies and security programs that satisfy the "Designation"-level requirements receive many risk management protections, including liability caps, exclusive jurisdiction in federal court, bars against punitive damages and prejudgment interest, to name a few.

Technologies and security programs with the higher level of protection—"Certification"—receive all the benefits of Designation, with the added benefit of *complete immunity from third-party liability arising from an Act of Terrorism*. These benefits apply not only to sellers/suppliers of the covered technology and businesses with covered security programs, but also to their customers. In other words, end-users receive total third-party liability immunity from harm and damages arising from Acts of Terrorism for implementing a SAFETY Act Designated or Certified service or program, along with the downstream benefit of differentiating your organization in the marketplace. With these significant protections, SAFETY Act awardees can also often negotiate reductions to their insurance premiums, thus directly reducing your company's overhead expenses.

Additional information on the SAFETY Act can be found at www.safetyact.gov.

How Venable can help

To limit your liability from cyber terrorism through the SAFETY Act, your company must undergo an extensive application and review process, in which the technology or security program is evaluated according to key criteria. Venable attorneys have significant experience in obtaining and maintaining the SAFETY Act's protections, including:

- Determining the appropriate cyber and physical security benchmark for your company;
- Analyzing your company's cyber and physical security programs against the benchmark;
- Strengthening your cyber and physical security program to meet and/or exceed the benchmark;
- Memorializing your cyber and physical security program and its efficacy to a written SAFETY Act application;
- Responding to DHS's requests for information;
- Liaising with DHS and its SAFETY Act evaluators;
- Maintaining SAFETY Act protections, including preparing modifications to technology descriptions; and,
- Seeking renewal of SAFETY Act protections.

In addition to Venable's experience in navigating the SAFETY Act process, our attorneys can also advise your company on the legal nuances of protections received and modifications to your operations to maximize protection benefits and minimize other areas of exposure.

Contact our SAFETY Act Team members below for more information on how Venable can help your business benefit from the protections offered by the SAFETY Act.

Dismas Locaria | DLocaria@Venable.com | 202.344.8013

Dismas (Diz) Locaria is a member of the firm's Government Contracts Group. Mr. Locaria's practice focuses on assisting government contractors in all aspects of working with the Federal government. Mr. Locaria also represents and counsels clients with regard to the peculiarities of the Homeland Security Act of 2002, including obtaining and maintaining SAFETY Act protections. In fact, Mr. Locaria has assisted several clients in receiving SAFETY Act Designation, as well as Certification, the highest level of protection afforded under the Act. Mr. Locaria also assists clients in maximizing the benefits of their SAFETY Act protection, including negotiating reductions in insurance premiums, obtaining first-party waivers of claims, and the preparation of marketing materials. Mr. Locaria is a recognized speaker and author on the topic of the SAFETY Act and is a co-author of and contributor to Venable's *Homeland Security Desk Book*.

Lindsay Meyer | LBMeyer@Venable.com | 202.344.4829

For over twenty-five years, Ms. Meyer has provided International Trade and Customs advice at Venable, where she co-chairs Venable's International Practice based in Washington, DC. Ms. Meyer concentrates on all aspects of International Trade and Customs matters. She regularly advises companies on their compliance with import and export control laws and regulations, and appears before numerous regulatory authorities such as U.S. Customs and Border Protection (CBP),the International Trade Commission (ITC), the Commerce Department's Bureau of Industry and Security (BIS), the State Department's Directorate of Defense Trade Controls (DDTC), the Treasury Department's Office of Foreign Assets Control (OFAC), and the Committee on Foreign Investment in the United States (CFIUS). Ms. Meyer has extensive experience counseling on compliance with supply-chain security programs, including Customs-Trade Partnership Against Terrorism (C-TPAT), the Importer Self Assessment (ISA) Program and other cross-border trade controls regulated by CBP, BIS, DDTC and OFAC. She actively assists companies in their registration, classification, license and authorization needs for imports, exports, re-exports and deemed exports. She guides companies through internal Import and Export Control Assessments and formal investigations, helps develop tailored compliance policies and procedures, and conducts training on trade laws and regulations affecting business operations. Ms. Meyer is a co-author of Venable's *Homeland Security Desk Book*.

Brian Zimmet | BMZimmet@Venable.com | 202.344.4510

Brian Zimmet is a partner in Venable's energy practice group with a broad range of experience in federal regulation and restructuring of the electric utility industry. In recent years, Mr. Zimmet's practice has focused on the regulation of reliability matters by the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and regional entities pursuant to FPA Section 215, with a particular focus on cybersecurity regulation of electric utilities. Mr. Zimmet is an expert on the cybersecurity (CIP) standards applicable to electric utilities, and has provided compliance counsel and related representation to electric utilities in audits, investigations and enforcement proceedings related to CIP matters. Mr. Zimmet also has followed closely the ongoing efforts by the National Institute of Standards and Technology (NIST) to develop a comprehensive Cybersecurity Framework applicable to owners and operators of critical infrastructure, and has been involved in counseling clients on the potential impact of that developing framework on their businesses.

Jason Wool | JRWool@Venable.com | 202.344.4511

Jason Wool's practice focuses on electric and other utility regulation at the state and federal levels. Mr. Wool has specifically focused much of his career on advising Independent System Operators and Regional Transmission Organizations on reliability compliance as well as a variety of other issues before the FERC. Through his work advising clients on the NERC Critical Infrastructure Protection (CIP) Reliability Standards, as well as tracking and participating in the Cybersecurity Framework development process coordinated by the NIST pursuant to Executive Order 13636, Improving Critical Infrastructure Cybersecurity, Mr. Wool has gained significant experience with cybersecurity regulation and policy. Mr. Wool has also personally attended and participated in each of NIST's workshops on the Cybersecurity Framework.

Andrew Bigart | AEBigart@Venable.com | 202.344.4323

Andrew Bigart is an associate in Venable's Regulatory Practice Group with a focus on international trade and business counseling. Mr. Bigart assists clients with ongoing regulatory compliance matters, civil and criminal investigations, and litigation before the Department of Justice, the Department of Homeland Security, the Department of Commerce, the Department of the Treasury, CFIUS, and various other federal and state agencies and courts. Mr. Bigart has significant experience in counseling clients on complying with federal laws governing international trade, including the Foreign Corrupt Practices Act and U.S. export controls. His work also includes counseling clients on the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act).

July 2013

Please contact any of the authors below if you have questions regarding this alert.

Authors:

Michael J. Baader
mjbaader@Venable.com
410.244.7708

Jamie Barnett, Rear Admiral (Ret.)
jbarnett@Venable.com
202.344.4695

Dismas Locaria
dlocaria@Venable.com
202.344.8013

Anthony J. Rosso
ajrosso@Venable.com
410.244.7543

Brian M. Zimmet
bmzimmet@Venable.com
202.344.4510

Keir X. Bancroft
kxbancroft@Venable.com
202.344.4826

Jason R. Wool
jrwool@Venable.com
202.344.4511

NIST Holds Third Workshop on Cybersecurity Framework Development, Identifies Greatest-Risk Critical Infrastructure

On July 10-12, 2013 in San Diego, the National Institute of Standards and Technology ("NIST") held its third workshop on critical infrastructure cybersecurity pursuant to President Obama's February Executive Order, which requires NIST to promulgate a Cybersecurity Framework within one year of the Order's issuance. In addition, on July 19, 2012, the Department of Homeland Security ("DHS") was obligated under the Executive Order to identify critical infrastructure at greatest risk. The Secretary of DHS will confidentially notify owners and operators of critical infrastructure regarding this identification and will provide the basis for the determination. Owners and operators may request reconsideration of "greatest risk" determinations, however a process for such appeals has not been publically released.

NIST will host a final Cybersecurity Framework workshop on September 11-13, 2013 at the University of Texas at Dallas before issuing the preliminary Cybersecurity Framework for public comment on October 10, 2013. In particular, owners and operators of greatest-risk critical infrastructure, as well as any other entities wishing to take advantage of potential incentives for adopting the Framework, may wish to participate in this final stage of piecing together the preliminary Framework. Venable will also continue to cover the Framework development process.

Risk Management Approach

Prior to the Workshop, NIST released a Draft Outline of the Framework along with two companion documents: a Draft Outline core and a Draft Outline compendium. NIST created these documents using comments from stakeholders submitted in response to NIST's Request for Information issued in February 2013 regarding current cybersecurity practices as well as the outputs of NIST's prior workshop in Pittsburgh in May of 2013.

The Draft Outline's risk management approach is divided into five key functions: Know, Prevent, Detect, Respond, and Recover, defined as follows.

Know - Gaining the institutional understanding to identify what systems need to be protected, assess priority in light of organizational mission, and manage processes to achieve cost effective risk management goals.

Prevent - Categories of management, technical, and operational activities that enable the organization to decide on the appropriate outcome-based actions to ensure adequate protection against threats to business systems that support critical infrastructure components.

Detect - Activities that identify (through ongoing monitoring or other means of observation) the presence of undesirable cyber risk events, and the processes to assess the potential impact of those events.

Respond - Specific risk management decisions and activities enacted based upon previously implemented planning (from the Prevent function) relative to estimated impact.

Recover - Categories of management, technical, and operational activities that restore services that have previously been impaired through an undesirable cybersecurity risk event.

Each function will be structurally divided into categories and subcategories, which are logical subdivisions of functions and categories, respectively. Examples of potential categories could include "know the enterprise assets and systems" and "implement risk monitoring and detection," while examples of the more granular sub-categories could include "inventory hardware assets" and "restrict and protect remote

access." Both categories and subcategories may be paired with so-called "informative references" to existing standards, practices, and guidelines, which are collected in the Draft Compendium, in order to provide detailed guidance on effective practices specific to the category or sub-category in question.

The objectives of the third workshop were to discuss the Draft Outline, generate content for the preliminary Framework (i.e. add categories, subcategories, and informative references to each of the five functions), and discuss specific topics that inform the preliminary Framework. NIST plans to release a first draft of the preliminary Framework in August, in advance of the final workshop in Dallas on September 11-13.

Framework Implementation Levels

The Draft Outline also includes Framework Implementation Levels ("FILs"), which express, by role, the characteristics of the level of maturity of an organization for each function, category, and subcategory. FILs are provided for officials at three levels – senior executives, business process managers, and operations managers – as well as for, currently, three levels of organizational maturity, i.e. FIL 1, FIL 2, and FIL 3.

DHS Performance Goals

At the workshop, DHS also revealed its draft performance goals, which are required under section 7(d) of the Executive Order. DHS emphasized that the performance goals are not designed to measure implementation of the Framework and that they focus on "the direction we want to move in" as a nation, not individual entities.

The performance goals currently consist of "vision" and "strategic performance goal" statements, as well as "primary performance goals" ("PPGs") and "supporting performance goals" ("SPGs"). The proposed performance goals are as follows.

Vision - The American People will have a high level of confidence that essential services and products[1] will continue to be delivered to critical customers[2] in the face of most cyber incidents.

Strategic Performance Goal - Organizations mitigate the consequences of cyber threats and vulnerabilities to their business functions, and to national economic security, public health, and safety, through enterprise risk management and the appropriate mix of prevention, detection, response, and resilience measures.

PPG 1 - During and following a cyber incident, essential services and products continue to be delivered with a high degree of reliability, resiliency, safety, and integrity.

PPG 2 - Intellectual property and personal information are protected to maintain the confidentiality of proprietary information and ensure privacy and civil liberties.

SPG 1 - Capabilities are built and sustained to prevent, detect, respond to, recover, and learn from cyber incidents as part of an ongoing enterprise risk management process.

SPG 2 - Functions critical to the delivery of essential services and products are sustained, or otherwise rapidly restored, over the course of a cyber incident.

SPG 3 - Preparedness and resilience are continuously improved based on lessons learned from incidents, exercises, and other activities.

DHS emphasized that the performance goals are a work in progress. DHS's Framework Collaboration Working Group meets every Wednesday to discuss the performance goals and other Framework-related issues, and membership is open to stakeholders. Entities interested in joining or providing feedback to DHS can email EO-PPDTaskForce@hq.dhs.gov.

Venable will continue to follow closely NIST's progress on the development of the Cybersecurity Framework, including the remaining workshop and issuance of the preliminary Framework for public comment. With just one workshop left before the preliminary Cybersecurity Framework is released for public comment, readers may have questions about the impact the Cybersecurity Framework will have on their respective businesses. Venable's attorneys are well-positioned to answer any such questions, having participated in and attended all relevant meetings conducted by NIST since the Executive Order was released in February.

Venable LLP offers a broad array of legal services to a variety of different players within the cybersecurity

arena. Our attorneys are adept at understanding complex client issues and tapping into the extensive experience of our many practice areas including privacy and data security, e-commerce, intellectual property, government contracting, telecommunications, energy, and corporate.

If you have any questions concerning this alert, please contact any of the listed authors.

[1] The terms “essential services and products” is currently defined as “those services and products upon which security, national economic security, national public health or safety, or any combination of those matters is dependent.”

[2] The term “critical customer” is currently defined as “a recipient of essential services and products who, in turn, provides or produces essential services and products.”

If you have friends or colleagues who would find this alert useful, please invite them to subscribe at www.Venable.com/subscriptioncenter.

CALIFORNIA DELAWARE MARYLAND NEW YORK VIRGINIA WASHINGTON, DC

1.888.VENABLE | www.Venable.com

VENABLE LLP

cybersecurity alert

September 2013

Please contact any of the authors below if you have questions regarding this alert.

Authors:

Michael J. Baader
mjbaader@Venable.com
410.244.7708

Jamie Barnett, Rear Admiral (Ret.)
jbarnett@Venable.com
202.344.4695

Dismas Locaria
dlocaria@Venable.com
202.344.8013

Anthony J. Rosso
ajrosso@Venable.com
410.244.7543

Brian M. Zimmet
bmzimmet@Venable.com
202.344.4510

Keir X. Bancroft
kxbancroft@Venable.com
202.344.4826

Jason R. Wool
jrwool@Venable.com
202.344.4511

NIST Releases Draft Preliminary Cybersecurity Framework in Advance of Dallas Workshop

On August 28, 2013, the National Institute of Standards and Technology (NIST) released the **first publically available draft** of the preliminary Cybersecurity Framework, which is being developed at the direction of President Obama's February **Executive Order** on critical infrastructure cybersecurity. The Executive Order requires NIST to issue a preliminary draft of the Framework by October 10, 2013.

In anticipation of that deadline, and to give stakeholders an opportunity to participate in the revision of the draft, NIST will host a fourth and final workshop on September 11-13, 2013 at the University of Texas at Dallas before issuing the preliminary Cybersecurity Framework for public comment.

Venable has attended all of NIST's workshops on the Framework and will be in attendance in Dallas to continue providing coverage on the Framework development process to its clients.

In addition, Venable will host a **live presentation and webinar**, *Cyber Sticks and Carrots: How the NIST Cybersecurity Framework, Incentives, and the SAFETY Act Affect You*, on September 25, 2013. Former Deputy Secretary of Homeland Security Jane Holl Lute will give the keynote speech.

Overview of Draft Framework

The draft preliminary Framework largely reflects the characteristics originally set forth in the **Draft Outline of the Framework** released prior to NIST's **July 10-12 workshop** in San Diego. Specifically, the draft retains the outline's proposed structure, consisting of five "core functions" – Know, Prevent, Detect, Respond, and Recover – each of which is divided into categories and subcategories.

At the subcategory level, specific tasks are enumerated alongside selected suggestions for achieving those tasks using existing cybersecurity standards, *i.e.* so-called "Informative References." The listed Informative References, which include well-known standards such as ISA 99, COBIT, the ISO/IEC 27000 series, and NIST's own SP 800-53, are not exhaustive, and entities "are free to implement other standards, guidelines, and practices."

Framework Implementation Tiers and Profiles

One notable change from the draft outline is the replacement of the maturity indicators known as Framework Implementation Levels with Framework Implementation Tiers. The Tiers still reflect an implementing organization's respective maturity under the Framework, measured from zero to four for each core function. Whereas the Framework Implementation Levels were proposed to define specific levels of maturity for each category and subcategory for various roles in an organization, the Framework Implementation Tiers are defined generally and are not role specific, greatly simplifying the measurement of an organization's implementation of the Framework.

A new feature of the draft preliminary Framework is the introduction of Framework Profiles, which make use of the simplified maturity measurement facilitated by the Framework Implementation Tiers. The draft instructs adopting organizations to calculate both their current Profile – consisting of the Tier ratings for each of the core functions – as well as their target Profile, *i.e.* the set of Framework Implementation Tiers that an organization determines it should have based on its assessment of its own cyber-risk. In addition to assisting entities to achieve the right level of risk mitigation by identifying gaps, the Framework Profile concept is intended to assist entities in communicating with one another about cyber-risk.

Areas of Improvement

In addition to providing further detail on the contents of the Cybersecurity Framework, the draft also describes several "areas for improvement" for which "[c]ollaboration and cooperation must increase...to further understanding and/or the development of new or revised standards." The initially identified areas are as follows:

- Authentication;
- Automated indicator sharing;
- Conformity assessment;
- Data analytics;
- International aspects, impacts, and alignment;
- Privacy; and
- Supply chains and interdependencies.

Venable Webinar

The upcoming webinar will take place shortly after the conclusion of NIST's final workshop and will provide a holistic overview of the currently known information on the Framework and the voluntary program to adopt it that will be established by the Department of Homeland Security (DHS). In addition to featuring a keynote speech from Secretary Lute, the President and CEO of the Council on Cybersecurity and former deputy secretary of DHS, the webinar will also feature presentations by Venable's own cybersecurity practitioners who will provide key insights and industry updates. The following questions will be addressed:

- What has happened since the Executive Order?
- How will the Cybersecurity Framework affect you?
- What is ahead in regulatory and voluntary measures?
- What steps can you take now?

The webinar will also include a review of the potential incentives for adoption of the Framework and the currently available protections available under the SAFETY Act, which can be utilized in conjunction with the Framework or another set of cybersecurity standards or guidelines to substantially reduce liability arising from Acts of Terror. **Registration is still open for the event**.

Venable will continue to closely follow NIST's progress on the development of the Cybersecurity Framework, including the remaining workshop and issuance of the preliminary Framework for public comment. With just one workshop remaining before the preliminary Cybersecurity Framework is released for public comment, readers may have questions regarding the impact that the Cybersecurity Framework will have on their respective businesses. Venable's attorneys are well-positioned to answer any such questions having participated in and attended all relevant meetings conducted by NIST since the Executive Order was released in February.

Venable LLP offers a broad array of legal services to a variety of different players within the cybersecurity arena. Our attorneys are adept at understanding complex client issues and tapping into the extensive experience of our many practice areas including privacy and data security, e-commerce, intellectual property, government contracting, telecommunications, energy, and corporate.

If you have any questions concerning this alert, please contact any of the authors.

Please contact any of the authors below if you have questions regarding this alert.

Authors:

Michael J. Baader
mjbaader@Venable.com
410.244.7708

Jamie Barnett, Rear Admiral (Ret.)
jbarnett@Venable.com
202.344.4695

Dismas Locaria
dlocaria@Venable.com
202.344.8013

Anthony J. Rosso
ajrosso@Venable.com
410.244.7543

Brian M. Zimmet
bmzimmet@Venable.com
202.344.4510

Keir X. Bancroft
kxbancroft@Venable.com
202.344.4826

Jason R. Wool
jrwool@Venable.com
202.344.4511

Upcoming Events

CyberMaryland 2013
October 9, 2013
Baltimore, MD

Mike Baader will moderate the Track A panel titled "Trends & Hot Issues in Mergers and Acquisitions" from 1:30 – 2:15 pm ET. **Dismas Locaria** will speak on the Track B panel, "Building an Effective Cyber Risk Culture: An Overview of Cybersecurity Insurance & Support Anti-Terrorism by Fostering Effective Technologies Act ('Safety Act')."

NIST Holds Fourth Workshop on Cybersecurity Framework

On September 11-13, 2013, the National Institute of Standards and Technology (NIST) held its fourth and – for now – final workshop on the preliminary Cybersecurity Framework. The Framework is being developed pursuant to President Obama's February **Executive Order** (EO) on critical infrastructure cybersecurity. NIST released a **draft** of the preliminary Framework **prior to the workshop**.

Because much of the drafting of the preliminary Framework had been completed, discussion largely focused on how to promote executive engagement on issues relating to cybersecurity, implementation of the Framework, and what participation in the Department of Homeland Security (DHS) voluntary program would look like. Officials also attempted to address head-on the widespread concern that the Framework would be used to impose additional regulation on the 16 critical infrastructure sectors.

Venable has attended all of NIST's workshops on the Framework and will host a **live presentation and webinar**, *Cyber Sticks and Carrots: How the NIST Cybersecurity Framework, Incentives, and the SAFETY Act Affect You*, on September 25, 2013. Former Deputy Secretary of Homeland Security Jane Holl Lute will give the keynote speech.

Significance of Critical Infrastructure Again Emphasized

Dr. Patrick Gallagher, acting Deputy Secretary of Commerce and Director of NIST, kicked off the workshop by reiterating the relationship of cybersecurity to national security. Recalling the events of September 11, 2001 – exactly 12 years prior to the date of the conference – Gallagher re-emphasized the central mission of the EO and the Cybersecurity Framework, *i.e.* the protection of our nation's most critical infrastructure, which, he noted, is defined in the EO as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." A number of panelists also alluded to this core mission, particularly with regard to industrial control systems, which affect "tangible assets" and can even affect personal safety.

Cyber-Risk as Business Risk

NIST representatives emphasized that the message for senior executives at firms that own or operate critical infrastructure is that cyber-risk must be understood as, and managed like, any other form of corporate risk. They noted that senior executives must understand that decisions concerning cyber-risk management will affect their corporations in the marketplace, in terms of maintaining and growing customer base, reducing costs, increasing revenue, protecting corporate reputation, and more. Similarly, stakeholders repeatedly stated that, in order to promote adoption of the Cybersecurity Framework, NIST must sell the concept of cyber-risk management – not the Framework itself.

Implementation

Many participants expressed concern that the draft preliminary Framework lacks specific guidance with regard to implementation and requested that NIST issue further instructions for potential adopters regarding how to use the Framework. Others worried that the process of mapping existing cybersecurity practices to the categories and sub-categories set forth in the draft would be onerous. With these concerns in mind, a number of stakeholders recommended that the sector-specific agencies responsible for the 16 critical infrastructure sectors be tasked with providing guidance and advice on implementation of the Framework specific to each sector and/or sub-sector. Some participants even suggested that each

from 1:30-2:15 pm ET.

Click here for more information.

Cyber Security Finance Forum (CSFF) 2013
October 21-22, 2013
Washington, DC

Jamie Barnett will speak at the 3rd Annual CSFF, the most comprehensive and definitive source of cyber security information, bringing together industry leaders, advisors, investors and government officials. This conference will debate, discuss and deliver answers to the key challenges of cybersecurity, equipping you with guidance and contacts to drive your business ahead.

Click here for more information.

sector should have its own specific maturity model instead of the standardized tier/profile system utilized in the draft preliminary Framework.

Concerns About Regulation

Stakeholders repeatedly voiced concern that the Framework, though nominally voluntary, would be used to increase the regulation of critical infrastructure. In response to these concerns, which have been voiced throughout the NIST stakeholder process, Andy Ozment of the National Security Staff spoke about the Administration's commitment to a voluntary approach to increasing the cybersecurity of Critical Infrastructure as a "preferred path." However, he also implied that continued reliance on a voluntary approach would depend on the quality of the Framework crafted by the NIST stakeholders as well as the level of adoption of the Framework following its finalization.

"The Administration is not pushing for new regulations...[but in those sectors that are already regulated,] those regulatory agencies have an existing mandate to protect the public and therefore they will necessarily consider the role of the framework in addressing that responsibility, and the EO specifically calls on regulators to look at the framework when they are considering that responsibility." The latter statement appears to be a reference to section 10 of the EO. Further, Ozment stated that the administration has "consistently supported the full range of executive and legislative actions that we need to protect our critical infrastructure" and that "voluntary success here could reduce the drive towards greater regulation elsewhere."

Publication and Next Steps

The preliminary Cybersecurity Framework will be issued on October 10, 2013, and will be subject to a 45-day public comment period. NIST has stated that it will hold additional workshops in the future concerning the Framework, but it has not provided any specifics at this time.

Venable Webinar

The upcoming webinar will take place on September 25, 2013, and will provide a holistic overview of the currently known information on the Framework and the voluntary program to adopt it that will be established by DHS. In addition to featuring a keynote speech from Secretary Lute, the President and CEO of the Council on Cybersecurity and former Deputy Secretary of DHS, the webinar will also feature presentations by Venable's own cybersecurity practitioners, who will provide key insights and industry updates.

The webinar will also include a review of the potential incentives for adoption of the Framework and the currently available protections available under the SAFETY Act, which can be utilized in conjunction with the Framework or another set of cybersecurity standards or guidelines to substantially reduce liability arising from acts of terror. **Registration is still open for the event**.

Venable will continue to closely follow NIST's progress on the development of the Cybersecurity Framework, including the issuance of the preliminary Framework for public comment. With the publication of the preliminary Framework due in less than a month, readers may have questions regarding the impact that the Cybersecurity Framework will have on their respective businesses. Venable's attorneys are well-positioned to answer any such questions, having participated in and attended all relevant meetings conducted by NIST since the Executive Order was released in February.

Venable LLP offers a broad array of legal services to a variety of different players within the cybersecurity arena. Our attorneys are adept at understanding complex client issues and tapping into the extensive experience of our many practice areas including privacy and data security, e-commerce, intellectual property, government contracting, telecommunications, energy, and corporate.

If you have any questions concerning this alert, please contact any of the authors.

Jane Holl Lute

President and Chief Executive Officer
Council on CyberSecurity

Jane Holl Lute is the President and Chief Executive Officer of the Council on CyberSecurity, responsible for the overall direction and activities of the organization. Ms. Lute most recently served as Deputy Secretary for the Department of Homeland Security (DHS). As the Department's chief operating officer, Ms. Lute was responsible for the day-to-day management of the Department's efforts to prevent terrorism and enhance security, secure and manage the nation's borders, administer and enforce U.S. immigration laws, strengthen national resilience in the face of disasters, and ensure the nation's cybersecurity. From 2003-2009 Ms. Lute served as Assistant Secretary-General of the United Nations (UN) responsible for comprehensive on-the-ground support to UN peace operations worldwide, including rapid-response efforts in support of development and humanitarian operations and crises. Ms. Lute also served as Assistant Secretary-General for Peacebuilding, responsible for coordinating efforts on behalf of the Secretary General to build sustainable peace in countries emerging from violent conflict.

Prior to joining the UN, Ms. Lute was executive vice-president and chief operating officer of the United Nations Foundation and the Better World Fund and worked with David A. Hamburg, former president of the Carnegie Corporation of New York and Cyrus Vance, former U.S. Secretary of State, on the Carnegie Commission on Preventing Deadly Conflict, a global initiative that pioneered the cause of conflict prevention.

Ms. Lute served on the National Security Council staff under both President George H.W. Bush and President William Jefferson Clinton and had a distinguished career in the United States Army, including service in the Gulf during Operation Desert Storm. She has a Ph.D. in political science from Stanford University and a J.D. from Georgetown University.

The Council on CyberSecurity (the Council) is an independent, not-for-profit organization with a global scope, committed to an open and secure Internet. Drawing together acknowledged experts from the fields of technology, business, education, science, and the public sector, the Council aims to fill a persistent void for practitioner and policymaker alike – that is, to provide an independent, authoritative platform to identify, validate, promote and sustain the global adoption of best practice in all dimensions of cybersecurity. In so doing, best practice will become common practice. More information is available at www.counciloncybersecurity.org.

VENABLE LLP

our people

Jamie Barnett, Rear Admiral (Ret.)

Partner — *Washington, DC Office*

T 202.344.4695 F 202.344.8300 jbarnett@Venable.com

Admiral Barnett is Co-Chair of Venable's Telecommunications Group and a partner in the firm's Cybersecurity Practice. He has a rare combination of experience in cybersecurity, national defense, homeland security, emergency communications, public safety communications and technology policy. This experience is invaluable to clients in the financial services, transportation, telecommunications and utilities industries as well as other critical infrastructures.

Admiral Barnett has had a distinguished career in the public and private sector. A surface warfare officer, he has over 30 years of experience in the United States Navy and Navy Reserve, rising to the rank of Rear Admiral and serving as Deputy Commander, Navy Expeditionary Combat Command and Director of Naval Education and Training in the Pentagon. Among other personal awards, he has received four Legion of Merit medals.

In addition to his military service, Admiral Barnett served as the Chief of the Public Safety and Homeland Security Bureau of the Federal Communications Commission where he executed major cybersecurity initiatives. As Chief of the Bureau, Admiral Barnett also led major rulemakings and projects in public safety broadband, emergency alerting and Next Generation 9-1-1, working closely with industry and government stakeholders. He has also testified before Congress and is a noted speaker on cybersecurity.

For nearly 20 years, Admiral Barnett worked as an attorney in private practice. He represented cities, counties, school districts, law enforcement agencies and development authorities in the board room and in state and federal court advising on a range of topics including constitutional law, governmental liability, personnel and employment law, education and school law, policy development, legislation, procurement, and ethics.

Prior to joining Venable, Admiral Barnett served as Senior Vice President for National Security Policy at the Potomac Institute for Public Policy, a premier not-for-profit science and technology policy research institution in the Washington, DC area. He remains a Senior Fellow of Potomac Institute.

AREAS OF PRACTICE

Regulatory

Communications

Homeland Security

Privacy and Data Security

Technology Transactions and Outsourcing

Domain Names and Cyber Protection

INDUSTRIES

Cybersecurity

GOVERNMENT EXPERIENCE

Chief, Public Safety and Homeland Security Bureau, Federal Communications Commission

Rear Admiral, United States Navy

BAR ADMISSIONS

District of Columbia

Mississippi

EDUCATION

J.D., University of Mississippi School of Law, 1984

Chairman of the Moot Court Board

PUBLICATIONS

- September 2013, NIST Holds Fourth Workshop on Cybersecurity Framework, Cybersecurity Alert
- September 2013, NIST Releases Draft Preliminary Cybersecurity Framework in Advance of Dallas Workshop, Cybersecurity Alert
- July 2013, NIST Holds Third Workshop on Cybersecurity Framework Development, Identifies Greatest-Risk Critical Infrastructure, Cybersecurity Alert
- July 17, 2013, Tough Standards, Diversity are Military Assets, *Stars & Stripes*
- June 2013, NIST Holds Three-Day, Stakeholder-Driven Workshop on Executive

Dean Parham Williams Outstanding Student

National Director of the ABA's National Appellate competition

B.A., University of Mississippi, 1976

Order Cybersecurity Framework Development, Cybersecurity Alert

- April 9, 2013, NIST Holds First Workshop on Executive Order Cybersecurity Framework, Cybersecurity Alert
- March 20, 2013, Hurricane Warnings for the New Public Safety Communications Network, *Roll Call*
- March 2013, NIST Issues Request for Information, Begins Developing Cybersecurity Framework Under Recent Executive Order, Cybersecurity Alert
- February 2013, NIST Seeking Comments on Revised Standards for FISMA Compliance, Cybersecurity Alert
- February 2013, Executive Order Opens Consultative Processes to Draft Cybersecurity Framework for Critical Infrastructure, Cybersecurity Alert

SPEAKING ENGAGEMENTS

- October 21, 2013 - October 22, 2013, "Bringing the Government and the Cyber Industry Together," Cyber Security Finance Forum 2013
- September 25, 2013, Cyber Sticks and Carrots – How the NIST Cybersecurity Framework, Incentives, and the SAFETY Act Affect You
- September 10, 2013, "Cybersecurity: Addressing One of the Primary Obstacles to Consumer Acceptance of Mobile Payments" at Law Seminars International's Conference on Mobile Payments
- August 16, 2013, "The Growing Cyber Threat" at the Industry Council for Emergency Response Technologies Annual Meeting
- July 16, 2013, "Mobile Technology and Public Safety" for the Brookings Institution
- June 21, 2013, "Policymakers Roundtable" at the Utilities Telecom Council's 700 MHz Workshop
- May 14, 2013, "Cybersecurity and the Arrival of the Mobile Payments Era" at the Annual Meeting of the Merchant Acquirer's Committee
- April 30, 2013, 2013 Electronic Transactions Association's Annual Meeting and Expo
- April 23, 2013, "How the Cybersecurity Executive Order Impacts You" at the National Security Institute's IMPACT 2013 Conference
- April 17, 2013, "What is FirstNet? An Overview of the Nationwide Public Safety Broadband Project" at the Competitive Carriers Association Global Expo Conference
- April 4, 2013, "Global Challenges to Telecommunications Law & Policy in an Age of Austerity" for Catholic University Law School
- April 1, 2013, "The World on a Plate: How Food Shapes Civilization" at a Chef Jose Andres Course Discussion
- March 14, 2013, "Oversight of FirstNet and Emergency Communications" at a House Subcommittee on Communications and Technology Hearing
- March 11, 2013, Cybersecurity Executive Order – A Briefing
- February 27, 2013, "Emergency Management" at the AFCEA Homeland Security Conference
- February 21, 2013, "Cyber and Supply Chain Policy Issues" at the National Defense Industrial Association Manufacturing Division Meeting
- February 14, 2013, "No Cells in Cells" at a Congressional Briefing
- February 12, 2013, "Securing the International Telecommunications Supply Chain" for the FCBA International Telecommunications Committee

VENABLE LLP

our people

Dismas Locaria

Partner — *Washington, DC Office*

T 202.344.8013 F 202.344.8300 dlocaria@Venable.com

AREAS OF PRACTICE

Government Contracts

Homeland Security

INDUSTRIES

Cybersecurity

Government Contractors

Nonprofit Organizations and Associations

BAR ADMISSIONS

District of Columbia

Maryland

EDUCATION

J.D., *with honors*, University of Maryland School of Law, 2003

Articles Editor, *Maryland Law Review*

B.A., *magna cum laude*, San Francisco State University, 1999

Dismas (Diz) Locaria is a member of the firm's Government Contracts Group. Mr. Locaria's practice focuses on assisting government contractors in all aspects of working with the Federal government. Mr. Locaria has extensive experience assisting clients with regulatory and contract/grant term counseling, compliance (including ethics and integrity compliance), responsibility matters, such as suspension, debarment and other contracting/grant exclusions, small business matters and GSA Federal Supply Schedule contracting. Mr. Locaria also represents and counsels clients with the peculiarities of the Homeland Security Act, including obtaining and maintaining SAFETY Act protections.

Government Contract and Grant Counseling and Compliance: Mr. Locaria has a wealth of knowledge regarding applicable contract (*e.g.*, the Federal Acquisition Regulation) and grant (*e.g.*, OMB Circular A-110 and A-122) regulations, including the application of these regulations to both prime contractors/grant recipients and subcontractors/subgrantees. This knowledge has enabled Mr. Locaria to assist both for-profit and nonprofit organizations with meeting the requirements for becoming a federal contractor or grantee, interpreting the implication of regulatory, contract and grant term to clients' work and operations, evaluating and advising contractors and grantees on intellectual property issues and contract modifications, among many other issues.

Mr. Locaria also assists clients with their efforts to remain compliant with the myriad of applicable regulations and requirements. This includes providing training on relevant regulations and contract and grant terms, as well as federal ethics laws and practices, conducting internal audits and investigations, making improvement and/or remedial recommendations, implementing such recommendations, making appropriate disclosures to cognizant federal and state agencies, and defending clients during federal and state audits and investigations.

As a result of Mr. Locaria's deep understanding of government contractor/grant compliance matters, Mr. Locaria is often involved in business formation, merger and acquisition and related business matters to provide expertise and advice on the implication of such activity on a client's existing and future contracts/grants.

Suspension and Debarment: Mr. Locaria represents clients in suspension and debarment matters, as well as other eligibility and responsibility issues raised by federal and state agencies. In this capacity, Mr. Locaria has represented clients before all the various defense agencies (*e.g.*, Army, Navy, Air Force, Defense Logistics Agency (DLA)), as well as various civilian agencies, such as the General Services Administration, the Department of Homeland Security, as well as DHS's sub-agency, Immigration and Customs Enforcement (ICE), the Environmental Protection Agency (EPA), Health and Human Services, Housing and Urban Development, as well as several others.

Some of the suspension- and debarment-related matters Mr. Locaria and the Venable team successfully resolved included:

- Representing a national manufacturing company with a host of Clean Air Act, Clean Water Act, OSHA, and civil and criminal violations to avoid discretionary suspension or debarment. Mr. Locaria and his Venable colleagues were able to secure a voluntary exclusion for certain segments of the company while the matter was under review. Ultimately, Venable was able to reinstate those facilities subject to a statutory ineligibility, the entities under the voluntary exclusion were reinstated and the entire company entered into a compliance agreement with EPA. The company recently completed its time under the compliance agreement without incident and has maintained full contracting authority.

- Assisting a nonprofit, quasi-governmental mass-transit entity with resolving a statutory ineligibility with EPA and restoring the entity to full grant eligibility within a matter of days following its conviction.

- Representing an international company convicted on several counts of fraud and false statements before DLA regarding its present responsibility and contracting future with DoD. Ultimately, Mr. Locaria and his Venable colleagues were able to secure a compliance agreement for the company, which allowed it to continue to contract with the DoD and other federal agencies. This also required liaising with other agencies, such as GSA, which issued a show cause letter to the company for the same bases of debarment as DLA.

- Representing a multi-national company before the Maritime Administration to demonstrate that despite various criminal violations implicating the company's integrity and ethical business practices, such company was in fact presently responsible. Ultimately, Mr. Locaria and his Venable colleagues were able to secure a compliance agreement for the company to allow it to fully contract with and received subsidies and other assistance from the federal government. This matter also involved a statutory ineligibility issue related to a Clean Water Act violation that was handled before EPA.

- Representing several entities, individuals, small businesses and non-profits before ICE for immigration-related convictions. In each instance, Mr. Locaria and his Venable colleagues were able to convince ICE that no action was necessary to protect the public interest.

Small Business Matters: Mr. Locaria has extensive experience working with small businesses to determine their size status, 8(a) and other socio-economic statuses, including analyzing affiliation issues. Mr. Locaria represents clients in both the prosecution and defense of small business size protests before the Small Business Administration and the Office of Hearing and Appeals.

GSA Federal Supply Schedule Contracting: Mr. Locaria is also well-versed in assisting clients with GSA Federal Supply Schedule matters, in particular advising clients on how best to structure proposals to avoid price reduction clause (PRC) issues, and addressing PRC, Trade Agreements Act and other compliance matters post-award.

Homeland Security and the SAFETY Act: Mr. Locaria represents a number of clients in homeland security-related matters including drafting guidelines for various companies' information handling, such as Sensitive Security Information, or in harnessing all the benefits of the SAFETY Act. In fact, Mr. Locaria has assisted several clients in receiving SAFETY Act Certification, the highest level of protection afforded under the Act. Mr. Locaria has published on the topic of the SAFETY Act and is a co-author and contributor to Venable's Homeland Security Desk Book.

ACTIVITIES

Mr. Locaria actively participates in the American Bar Association as a vice chair of the Section of Public Contract Law Committee on Debarment and Suspension.

PUBLICATIONS

"Frankel v. Board of Regents of the University of Maryland System - In the Name of Equality: The Proper Expansion of Maryland's Heightened Rational Basis Standard," 61 MD L. REV. 847 (2002).

- September 2013, NIST Holds Fourth Workshop on Cybersecurity Framework, Cybersecurity Alert
- September 2013, NIST Releases Draft Preliminary Cybersecurity Framework in Advance of Dallas Workshop, Cybersecurity Alert
- August 2013, Federal Grant & Contract News for Nonprofits - August 2013
- August 2013, The SUSPEND Act: Fixing What Isn't Broken in the Federal Government's Suspension and Debarment System, Government Contracts Update
- August 5, 2013, NIST's Proposed Cybersecurity Research and Development Center, *Westlaw Journal Government Contract*
- July 2013, Federal Grant & Contract News for Nonprofits - July 2013
- July 2013, NIST Holds Third Workshop on Cybersecurity Framework Development, Identifies Greatest-Risk Critical Infrastructure, Cybersecurity Alert
- July 2013, New SBA Regulations Focus on Small Business Size and Status Integrity, Government Contracts Update
- June 2013, Federal Grant & Contract News for Nonprofits - June 2013
- June 2013, NIST Holds Three-Day, Stakeholder-Driven Workshop on Executive Order Cybersecurity Framework Development, Cybersecurity Alert
- May 2013, Federal Grant & Contract News for Nonprofits - May 2013
- May 28, 2013, Reducing Risks of Operating in Conflict Zones Through Better Contract Drafting, *Westlaw Journal*
- May 2013, NIST Revises Security and Privacy Controls Before Public Meeting, Cybersecurity Alert
- April 2013, Federal Grant & Contract News for Nonprofits - April 2013
- April 24, 2013, SAFETY Act: A Cybersecurity Win-Win For Gov't, Industry, *Law360*
- April 9, 2013, NIST Holds First Workshop on Executive Order Cybersecurity Framework, Cybersecurity Alert
- March 2013, Federal Grant & Contract News for Nonprofits - March 2013
- March 2013, NIST Issues Request for Information, Begins Developing Cybersecurity Framework Under Recent Executive Order, Cybersecurity Alert
- February 2013, Federal Grant & Contract News for Nonprofits - February 2013
- February 2013, NIST Seeking Comments on Revised Standards for FISMA Compliance, Cybersecurity Alert
- February 2013, Maryland Cybersecurity-Related Legislative Developments, Cybersecurity Alert
- February 2013, Executive Order Opens Consultative Processes to Draft Cybersecurity Framework for Critical Infrastructure, Cybersecurity Alert
- February 12, 2013, The Top Ten Federal Grant and Contract Pitfalls for Nonprofits
- January 2013, What You Need to Know About the Proposed Maryland Investment Tax Credit for Cybersecurity, Cybersecurity Alert
- January 2013, Federal Grant & Contract News for Nonprofits - January 2013
- December 2012, Record Civil False Claims Act Recoveries: The Implications for Nonprofits
- December 2012, Record Civil False Claims Act Recoveries Point to Increased Whistleblower Cases in 2013, *Law360*
- November 9, 2012, Crucial Legal Issues in the Recovery from Hurricane Sandy
- August 7, 2012, Lessons from the *Agility Defense* Case: Severing Affiliation with a Suspended Contractor, Government Contracts Update
- July 13, 2012, Suspension & Debarment: New Trends and the Continuing Due

Process Debate, Government Contracts Update

- April 2012, DoD Fast-Track Acquisition Process Promises New Opportunities for Contractors, Cybersecurity Alert
- April 2012, Housing Counseling Agencies: Tips to Avoid Government Scrutiny
- January 2012, The Public Disclosure of Contractor Information on FAPIIS is Here to Stay, Government Contracts Update
- January 18, 2012, New IT Security Requirements For GSA Contractors, *Law360*
- January 2012, GSA Requires IT Contractors to Create and Implement IT Security Plans: This May Only Be the Beginning, Government Contracts Update
- January 10, 2012, Pitfalls for Nonprofits that Receive Federal Funds: Lessons Learned from ACORN
- December 13, 2011, Pitfalls for Nonprofits that Receive Federal Funds: Lessons Learned from ACORN
- December 2011, House Intelligence Committee Announces Cybersecurity Legislation: Path Forward Uncertain, Cybersecurity Alert
- October 18, 2011, A Roadmap To The U.S. Government Contracts Market, *Law360*
- July 2011, Proposed DFARS Rule Would Impose New Protection and Reporting Requirements on Defense Contractors, Government Contracts Update
- October 26, 2010, "GTSI's Suspension Shows That Contractors Should Ensure Accurate Representations Concerning Small Business Matters", *Federal Contracts Report*
- October 2010, The Small Business Administration Flexes its Muscle: Contractors Should Ensure Accurate and Appropriate Representations and Teaming Arrangements, Government Contracts Update
- June 2010, Government Contractors Toolkit - Selling to the Federal Government
- March 2010, Contractors Can Challenge the Government's In-Sourcing Efforts
- December 2009, The GSA Schedules: How to "Get on Schedule" and Broaden Your Business, *Originally published in the December 2009 issue of Contract Management magazine, © 2009, the National Contract Management Association*
- November 18, 2009, Proposed Rules Issued For Prevention of Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, Government Contracts Update
- August 27, 2009, New OMB Guidance Further Signals the Sea Change in Government Contracting, Government Contracts Update
- July 13, 2009, The Federal False Claims Act - What Does It Mean for Nonprofit Organizations?
- May 29, 2009, The Federal Government Provides Significant Opportunities for Asset Managers Looking to Expand Their Business, Financial Services Alert
- March 2009, Suspension and Debarment: New Developments and Future Challenges, *Contract Management*
- February 24, 2009, Increased Oversight of Government Contracts, Government Contracts Update
- February 3, 2009, GSA Proposes Several Significant Changes to its Federal Supply Schedule Contracting Program, Government Contracts Update
- October 2008, The National Defense Authorization Act for FY09's Clean Contracting Act Mandates Significant Changes in Federal Acquisitions, Government Contracts Update
- August 8, 2008, 2007 Year in Review: Analysis of Significant Federal Circuit Government Contracts Decisions
- July 31, 2008, Department of Justice Updated Guidance on Seeking Waivers of Attorney-Client Privilege May Not Go Far Enough, Government Contracts Update
- July 23, 2008, GAO'S New Bid Protest Jurisdiction May Aim to Foster Competition but Leaves Many Questions Unanswered, Government Contracts Update
- March 2008, 2008 DoD Authorization Bill Adds Relief and Complexity to DoD's Procurement of Specialty Metals, Government Contracts Update

- October 2007, Court of Federal Claims Makes Unusual Request for FTC Opinion on OCI Issue, Government Contracts Update
- August 31, 2007, 2006 Year In Review: Analysis of Significant Federal Circuit Government Contracts Decisions, *Public Contract Law Journal*
- June 2007, The U.S. Supreme Court Narrows Relators' Ability to Pursue Qui Tam Claims, Government Contracts Update
- January 2007, New Department of Justice Guidance on Circumstances in Which Prosecutors Should Seek Access to Privileged Information Does Not Eliminate Many Concerns, Government Contracts Update
- September 7, 2006, Homeland Security Deskbook: Private Sector Impacts of the War Against Terrorism
- Fall 2006, Final SAFETY Act Rule Resolves Some Questions, Generates Others, and Creates Important Procurement Linkage to the SAFETY Act, *Procurement Lawyer*
- August 2006, Administrative Remedies: Contractors Should be Concerned With Losing More Than Just Dollars in a Civil Suit, Government Contracts Update
- May 12, 2006, Possible Changes on the Horizon for Berry Amendment, *Northern Virginia Technology Council B2G Committee Legal Updates*
- April 2006, Possible Changes on the Horizon for the Berry Amendment, Government Contracts Update
- April 2005, Former 8(A) Business Not Liable for Warranty and Upgrade Services, Government Contracts Update
- December 2004, SBA Issues Final Rules For Subcontracting Assistance Program, Government Contracts Update
- September 2004, Reliance on Government Estimates, Government Contracts Update
- May 2004, Critical Infrastructure Information Act, Government Contracts Update

SPEAKING ENGAGEMENTS

- October 9, 2013, CyberMaryland 2013
- October 1, 2013, "Federal Contracting Options: Subcontracting/Teaming/Joint Ventures" for the 2013 GovConnects Fall Educational Series
- September 25, 2013, Cyber Sticks and Carrots – How the NIST Cybersecurity Framework, Incentives, and the SAFETY Act Affect You
- September 19, 2013, Time to Update Your Internal Controls – Take Steps Now to Limit Liability from Severe Civil and Criminal Penalties
- April 17, 2013, Government Contracts Symposium
- March 11, 2013, Cybersecurity Executive Order – A Briefing
- February 20, 2013, Government Contracting Group Breakfast: "Subcontract Compliance and Reporting Issues from Both Sides of the Table" for the Center Club
- February 12, 2013, The Top Ten Federal Grant and Contract Pitfalls for Nonprofits
- January 31, 2013, State of the Government Services Market: Preparing for Change
- October 11, 2012, "The New World of Debarment and Suspension Actions," WMACCA Government Contractors Forum
- September 30, 2012 - October 3, 2012, Association of Corporate Counsel (ACC) 2012 Annual Meeting
- September 13, 2012, "Ethics and Compliance for Federal Contractors in an Increasingly Scrutinizing World," NCMA Webinar
- August 9, 2012, "GSA Schedules: Federal Contracting Made Easy," NCMA Webinar
- March 19, 2012, "Ethics and Compliance for Small Businesses," Cyber Incubator at UMBC
- March 4, 2012 - March 6, 2012, International Restaurant and Foodservice Show of New York
- February 15, 2012, "What You Don't Know Can Hurt You – Compliance Basics in the New Age, and a Few Timeless Ideas" for the National Contract Management Association (NCMA)

- December 13, 2011, Legal Quick Hit: "Pitfalls for Nonprofits that Receive Federal Funds: Lessons Learned from ACORN" for the Association of Corporate Counsel's Nonprofit Organizations Committee
- June 7, 2011, "Ensuring Compliance with Small Business Set-Aside Requirements: Lessons for Small and Large Businesses" for SC&H Group
- December 7, 2010, "Ensuring Compliance in a Post-GTSI Environment: Lessons for Small and Large Businesses," hosted by Venable LLP
- July 14, 2009, Legal Quick Hit: "The Federal False Claims Act - What Does It Mean for Nonprofit Organizations?"
- September 4, 2008, National Contract Management Association, NOVA Chapter - Monthly Meeting
- January 17, 2008, National Contract Management Association: Greater Johnstown Chapter's Dinner Meeting
- November 1, 2007, Northern Virginia Chapter of the National Contract Management Association (NCMA)

VENABLE LLP

our people

Jason R. Wool

Associate — *Washington, DC Office*

T 202.344.4511 F 202.344.8300 jrwool@Venable.com

Jason Wool's practice focuses on electric and other utility regulation at the state and federal levels. Mr. Wool has specifically focused much of his career on advising ISOs and RTOs on reliability compliance as well as a variety of other issues before the Federal Energy Regulatory Commission (FERC).

Through his work advising clients on the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards, Mr. Wool has gained significant experience with cybersecurity regulation and policy.

AREAS OF PRACTICE

Energy

Regulatory

INDUSTRIES

Cybersecurity

BAR ADMISSIONS

District of Columbia

New York

Virginia

EDUCATION

J.D., William and Mary School of Law, 2009

B.A., Haverford College, 2004

MEMBERSHIPS

Energy Bar Association

REPRESENTATIVE CLIENTS

Mr. Wool has advised investor-owned utilities, renewable energy developers, Regional Transmission Organizations, Independent System Operators, electric cooperatives and government agencies on a variety of regulatory issues.

HONORS

Recipient, Legal Skills Scholars Award, William & Mary School of Law, 2009

PUBLICATIONS

- September 2013, NIST Holds Fourth Workshop on Cybersecurity Framework, Cybersecurity Alert
- September 2013, NIST Releases Draft Preliminary Cybersecurity Framework in Advance of Dallas Workshop, Cybersecurity Alert
- July 2013, NIST Holds Third Workshop on Cybersecurity Framework Development, Identifies Greatest-Risk Critical Infrastructure, Cybersecurity Alert
- June 2013, NIST Holds Three-Day, Stakeholder-Driven Workshop on Executive Order Cybersecurity Framework Development, Cybersecurity Alert
- May 2013, NIST Revises Security and Privacy Controls Before Public Meeting, Cybersecurity Alert
- April 9, 2013, NIST Holds First Workshop on Executive Order Cybersecurity Framework, Cybersecurity Alert
- March 2013, NIST Issues Request for Information, Begins Developing Cybersecurity Framework Under Recent Executive Order, Cybersecurity Alert
- February 2013, NIST Seeking Comments on Revised Standards for FISMA Compliance, Cybersecurity Alert
- February 2013, Executive Order Opens Consultative Processes to Draft Cybersecurity Framework for Critical Infrastructure, Cybersecurity Alert
- January 11, 2013, Cybersecurity Regulation: 5 Issues for Companies, *Wall Street*

Journal Market Watch

- 2011, Protecting the Nation's Essential Services – Recent Developments: Water, *Recent Developments in Public Utility, Communications and Transportation Industries*

SPEAKING ENGAGEMENTS

- September 25, 2013, Cyber Sticks and Carrots – How the NIST Cybersecurity Framework, Incentives, and the SAFETY Act Affect You
- May 16, 2013 - May 17, 2013, Virginia Bar Association's National Regulatory Conference 2013