VENABLE® LLP

# The NIST Cybersecurity Framework: What You Need to Know

FEBRUARY 19, 2014

VENABLE® LLP

# AGENDA

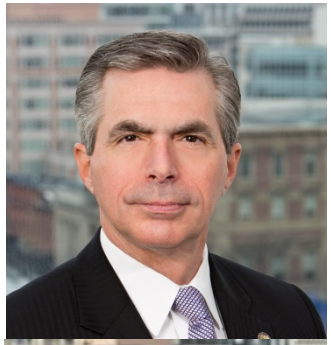
How Will the Cybersecurity Framework Affect You?

- Opening Remarks — Jamie Barnett
- Cybersecurity Framework Overview — Jason Wool
- Analysis, Impact and Next Steps — Larry Clinton
- The Privacy Aspect — Stu Ingis
- Your questions and discussions

## NOTES

1. Program is being recorded
2. Phone lines muted; chat function for questions
3. Recording and slides will be available

# Our Attorney Panelists from Venable



## Jamie Barnett

Rear Admiral USN (Ret), Telecom Co-Chair
Former Chief FCC Public Safety & Homeland Security
Led voluntary cyber initiatives at the FCC

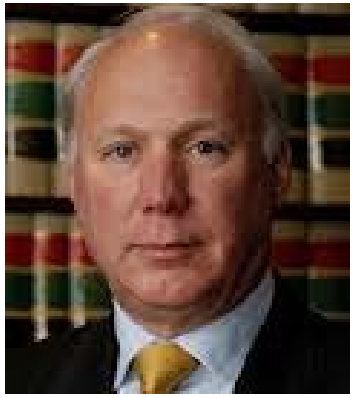
## Jason Wool

Focuses on electrical and other utility regulation and especially cybersecurity regulations
Participated in all NIST cybersecurity workshops

## Stu Ingis

Nationally recognized attorney on privacy and Internet
Co-leads Venable's privacy and data breach practice
Ranked as first tier privacy attorney in *Legal 500*, *Chambers USA* and *ComputerWorld* magazine

# Our Special Guest Speaker



## Larry Clinton

President and CEO of Internet Security Alliance (ISA), a multi-sector trade association from virtually all critical industry sectors

- Author of numerous articles on cybersecurity
- Testified before Congress, both House and Senate
- Led ISA in development of the Cybersecurity “Social Contract”
- Promotes market-based incentives for adoption of best practices
- Former Legislative Director for Hon. Rick Boucher
- Former Vice President at US Telecom
- Taught at the University of Illinois

# The Cybersecurity Framework

- Will your company be exposed to liability if the Framework is not adopted or is imperfectly implemented?
- Does the Framework establish a de facto standard of care, and if so, will this standard of care extend beyond critical infrastructure?
- Is the Framework cost effective and has adoption been properly incentivized?
- Will agencies base regulations on the Framework?
- What are the ramifications of the Framework's statements on privacy and how will they be harmonized with NIST's upcoming efforts to develop technical privacy standards?

VENABLE LLP

# EO 13636: Improving Critical Infrastructure Cybersecurity

- Directs NIST to develop a Cybersecurity Framework "to reduce cyber risks to critical infrastructure." § 7(a)
- Directs DHS to establish a voluntary program to support adoption of the Framework by owners and operators of Critical Infrastructure. § 8(a)
- Directs DHS to coordinate establishment of a set of incentives to promote participation in this program. § 8(d)

VENABLE® LLP

# Final Framework

- Released February 12, 2014
- DHS' "Critical Infrastructure Cyber Community ($C^3$) Voluntary Program" launched the same day
- Version 1.0 – will be updated
  - First by NIST
  - Then…?

VENABLE® LLP

# Basics of the Cybersecurity Framework

- Leverages existing cybersecurity best practices (ISO 27001/2, SP800-53, COBIT, ISA 99, etc.)
- Controls divided into five “core functions”
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- Each function has categories, sub-categories, and informative references
- Tiers represent how orgs view and respond to risk; profiles facilitate customization and improvement

VENABLE LLP

# Notable Changes from Prelim. Version

- Removal of separate privacy appendix; integration of methodology into the body of the Framework
- Increased focus on business case for cyber risk management ("bottom line," "overinvestment," "business needs," "economies of scale")
- Increased focus on flexibility
- Tweaking of subcategories
  - Removal of IP-specific control
  - Removal of "PII" control
  - Addition of language on network segregation

VENABLE® LLP

# Impact on Business

- Implementation of Framework is left to entity's discretion, but some expectations are made explicit:
  - "[O]rganizations responsible for Critical Infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk."
  - In performing a self-assessment, an "organization may determine that it has opportunities to (or needs to) improve."
- Security concerns must be managed in a manner commensurate with risk

VENABLE® LLP

# Incentives

- For now, technical assistance via $C^3$
- Federal financial incentives not close to fruition in near term
  - DHS/White House have stated that safety is its own incentive
  - Expectation is that market-based "incentives" will develop organically (better access to insurance, trustmark-like certifications, etc.)
- Legislation needed to expand availability of liability protections (SAFETY Act)

# Liability Concerns

- Some have identified potential for emerging tort liability for commercially unreasonable cybersecurity practices based on the Framework
  - Key is risk management – not implementing the entire Framework in all cases
  - Every entity will have different needs and interests
- Could serve as basis for regulations or enforcement actions (section 10 of EO)

VENABLE® LLP

# Other Concerns

- What does adoption mean? Will there be certification/audit requirements to qualify for incentives in the future?
- How will insurers make use of the Framework? An upcoming *Request for Information* will help answer this.
- Availability of quality incentives, especially liability limitation


Larry Clinton

President & CEO
Internet Security Alliance

lclinton@isalliance.org

703-907-7028

202-236-0001

**www.isalliance.org**

# BACKGROUND

- 2008: ISA published "Cyber Security Social Contract" Advising Government to use industry standards and practices with voluntary adoption motivated by incentives
- 2012: President Obama issues Executive Order calling for a Framework of Cybersecurity best practices & standards with voluntary adoption via market incentives

# ISA view

- Entire process including NIST and new NIPP as well as incentive development and enhanced information sharing program are ground-breaking and major steps in the right direction

- Much better than EU model which adheres to outdated regulatory notion for addressing cybersecurity

# *Framework is an Olympian Achievement*

- But we have just passed the prelims now on to the medal round – much more work to do
- Cybersecurity is a competition – not like consumer product safety – problem is NOT faulty design, the system is under attack
- The Cyber Attack team is getting much better all the time – "APT" now showing up everywhere – even Target

# Expectations for the Framework

- Not a panacea
- Will it be clear for executives?
- Needs to be understood as a beginning not an end
- Is it a standard of care?
- Do we know what complying/adopting/using will mean?

# *Big Question : How do we promote Use?*

- Main problem is not lack of information or standards – it's the cost
- Can good companies keep up?
- Incentives all favor the bad guys
- Plus there are economic incentives to be insecure
- Risk management means how much security you can afford to buy

# EO Strategy

- Framework should be cost effective
- Voluntary adoption should be motivated by incentives
- More work to be done, but a wide range of incentives is being considered
- ISA has proposed "Beta Testing" the Framework – as we would in the private sector to develop metrics to show cost effectiveness and need for incentives


Larry Clinton

President & CEO
Internet Security Alliance

lclinton@isalliance.org

703-907-7028

202-236-0001

**www.isalliance.org**

VENABLE® LLP

# Privacy and Civil Liberties Methodology

- Origin: Executive Order 13636 - 7(c)
  - "Framework shall include methodologies to…protect individual privacy and civil liberties."
- First Take: Appendix B of Preliminary Framework
  - FIPPs-based controls mapped to Framework Core
- Revision: Industry concerns over scope and details
- Final Methodology: Mostly reflects industry input

VENABLE LLP

# Future and Direction of the Framework

- NIST continues to convene and coordinate
  - Informal comments accepted until formal notice issued
  - Workshop ~6 months from release – forum for stakeholders
  - "Privacy Engineering Workshop:" April 9-10, 2014
    - Develop technical privacy standards and best practices
    - Resurrection of Appendix B and FIPPs-based privacy controls?
- Framework as a "living document"
  - Evolution driven by feedback on implementation
  - "Areas for improvement:" authentication, data analytics, international, privacy standards, etc.
- Long-term planning – transfer of governance to NGO

VENABLE® LLP

# Contact Information


Jamie Barnett
JBarnett@Venable.com
t 202.344.4695

Stu Ingis
SIngis@Venable.com
t 202.344.4613

Jason Wool
JWool@Venable.com
t 202.344.4511

Larry Clinton
Internet Security Alliance
LClinton@ISAlliance.org
t 703.907.7028


www.Venable.com