Cybersecurity Preparedness and Supply Chain Risk Management in the Electric Sector

American Public Power Association Legal & Regulatory Conference

October 8-11, 2017

Paul M. Tiao
Partner
Hunton & Williams LLP

Kevin W. Jones
Partner
Hunton & Williams LLP

Randall S. Parks
Partner
Hunton & Williams LLP

Roadmap

- Cyber Threat Landscape
- Cybersecurity Legal Framework
- Cybersecurity Preparedness Measures
- Recent FERC Developments on Supply Chain
- Supply Chain Contracting Issues and Suggestions

Notable Cyber Incidents

HEADLINES TODAY

- **Equifax** – theft of credit records
- **WannaCry and Notpetya** – worldwide ransomware attack
- **Yahoo!** – theft of account information
- **Democratic National Committee** – sensitive emails
- **Ukraine Power Company** – blackout
- **Hollywood Presbyterian Medical Center** – ransomware
- **OPM** – theft of background check data
- **Sony** – destructive malware, theft of IP, PII and emails
- **Blue Cross Blue Shield** – theft of PII and PHI
- **Sands Casino** – destructive malware
- **JPMorgan Chase** – theft of financial account Information
- **Target** – theft of credit card data
- **Saudi Aramco** – destructive malware
- **Top 50 U.S. Banks** – denial of service attacks

Cyber Attacks in the Energy Sector

2017

- Cyber attacks on Wolf Creek Nuclear facility and other energy companies
- Wannacry and NotPetya ransomware attacks

2016

- Crash Override attack on Ukraine power grid;
- Ransomware attacks on midwest utility company

2015 Cyber attack on Ukraine power grid

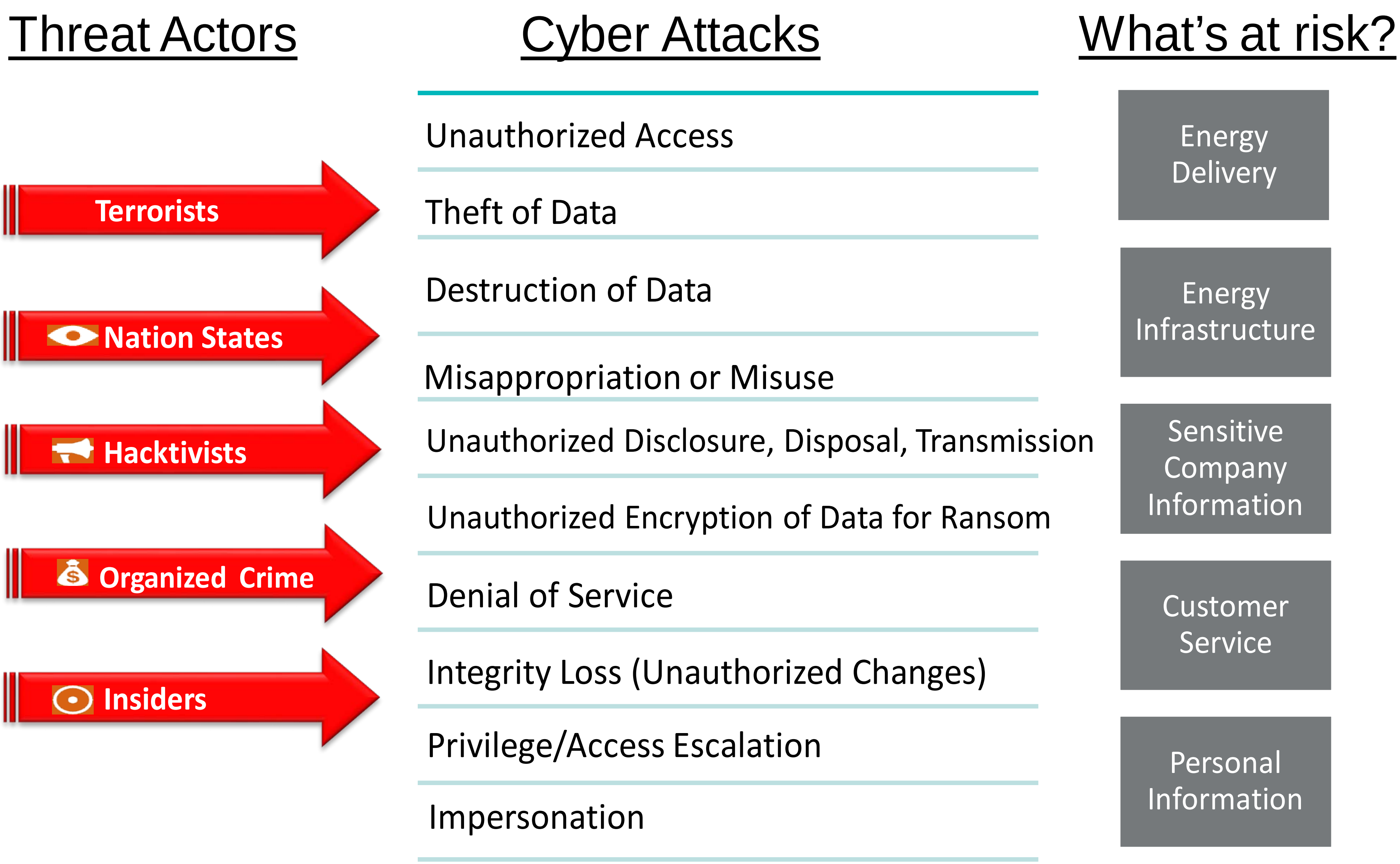
2014 Black Energy, Havex and Sandworm malware attacks on energy ICS

2013

- Iranian cyber attacks on control systems of oil and gas pipeline companies
- PRC cyber espionage targets 23 natural gas pipeline companies
- Researchers demonstrate ability to hack into control systems and turn oil well pumps on and off remotely, and access domestic pipeline sensors

2012 Destructive malware attacks on Saudi Aramco and Qatar RasGas

Cyber Threats



Threat Actors

- Terrorists
- Nation States
- Hacktivists
- Organized Crime
- Insiders

Cyber Attacks

- Unauthorized Access
- Theft of Data
- Destruction of Data
- Misappropriation or Misuse
- Unauthorized Disclosure, Disposal, Transmission
- Unauthorized Encryption of Data for Ransom
- Denial of Service
- Integrity Loss (Unauthorized Changes)
- Privilege/Access Escalation
- Impersonation

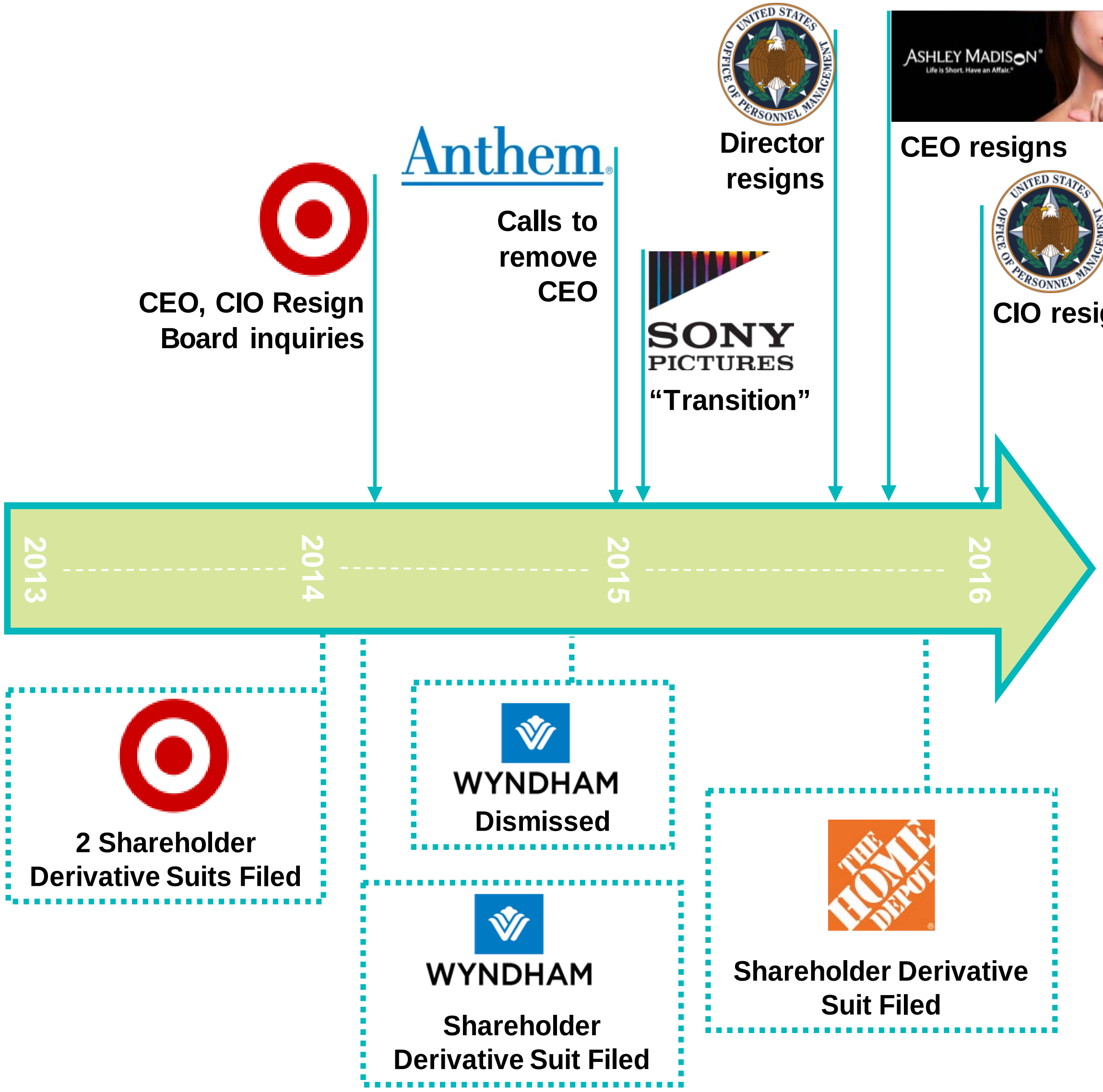
What's at risk?

- Energy Delivery
- Energy Infrastructure
- Sensitive Company Information
- Customer Service
- Personal Information

Harsh Realities at the Top

"There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again."

– FBI Director Robert Mueller, March 2012


2013
2014
2015
2016
Anthem
SONY PICTURES
ASHLEY MADISON
Life is Short. Have an Affair.
UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
WYNDHAM
THE HOME DEPOT

CEO, CIO Resign
Board inquiries

Calls to remove CEO

"Transition"

Director resigns

CEO resigns

CIO resigns

2 Shareholder Derivative Suits Filed

Dismissed

Shareholder Derivative Suit Filed

Shareholder Derivative Suit Filed

If you are a director or officer, you should be asking whether your company can withstand third party scrutiny after a breach.

– Kevin Mandia, Founder of Mandiant, October 2015

U.S. Regulatory Landscape

Federal Law

□ FTC Act

□ Gramm-Leach-Bliley

□ HIPAA/HITECH

□ NERC/FERC

□ SEC Reporting

□ Communications Act

□ ECPA/CFAA

□ SOX

□ DFARS

State Requirements

□ MA, NV, CA and progeny

□ Breach notification laws

□ Mini-FTC Acts

□ Disposal Laws

□ Surveillance Laws

Industry Standards

□ PCI DSS

□ ISO

□ NIST

□ COBIT

□ ISA/IEC

Recent Federal Cybersecurity Law

- Cybersecurity Information Sharing Act of 2015 (CISA)
  - Cyber threat indicators and defensive measures
  - Monitoring information systems, operating defensive measures, sharing information
  - Liability protection
  - Privacy protections - removal of personal information
  - Protection from FOIA disclosure
  - Limits on regulatory use
  - Source anonymization
- How CISA applies to private companies
  - ISACs
  - Sharing with other companies
  - Sharing with the US government

Overview of Preparedness Measures

- Systematically identify and catalogue sensitive data, networks, facilities
- Update cyber and physical security governance, policies, and procedures
- Assess regulatory compliance posture – NERC CIP, state regulations
- Work with IT vendors to deploy hardware and software tools that strengthen information security in operational and corporate networks
- Strengthen vendor management program

Overview of Preparedness Measures

- Improve access to current cyber threat data via info sharing programs
- Strengthen insider threat program – HR, management, IS, risk indicators
- Reduce financial exposure – cyber insurance, SAFETY Act
- Ensure frequent cyber and physical security training and awareness
- Update incident response plan and notification toolkit
- Conduct tabletop exercises

Supply Chain Security

Recent FERC Developments on Contracting Issues and Suggestions

FERC Order 829

HUNTON & WILLIAMS

- FERC issued Order 829 on July 21, 2016.

- Order 829 directed NERC to develop mandatory requirements for the protection of aspects of the supply chain that are within the control of responsible entities (*i.e.*, NERC-registered owners, operators, and users of the bulk power system)

- Consistent with the earlier NOPR, FERC directed NERC to develop a "forward-looking, objective-driven new or modified Reliability Standard to require each [responsible entity] to **develop and implement a plan** that includes **security controls** for **supply chain management** for industrial **control system hardware, software, and services** associated with **bulk electric system operations**"

- FERC stated that many concerns expressed by comments on the NOPR are addressed in the flexibility inherent in its directive

FERC Order 829

- The Reliability Standard was required to address the following security objectives in the context of addressing supply chain management risks:
  1. Software integrity and authenticity
  2. Vendor remote access
  3. Information system planning
  4. Vendor risk management and procurement controls
- The Reliability Standard was to require responsible entities to develop a plan to meet the four security objectives, while allowing flexibility as to how to meet the objectives
- The Reliability Standard was to require the responsible entity's CIP Senior Manager to review and approve the controls adopted to meet the security objectives at least every 15 months
- NERC was required to submit the Reliability Standard to FERC by Sept. 27, 2017

FERC Order 829

First Objective: Security Integrity and Authenticity

The Reliability Standard must address verification of:

1. The identify of the software publisher for all software and patches that are intended for use on BES Cyber Systems

2. The integrity of the software and patches before they are installed on the BES Cyber System environment

FERC Order 829

Second Objective: Vendor Remote Access to BES Cyber Systems

- The Reliability Standard must address responsible entities' logging and controlling all third-party (*i.e.*, vendor) initiated remote access sessions
- This objective covers both user-initiated and machine-to-machine vendor remote access

FERC Order 829

Third Objective: Information System Planning and Procurement

- The Reliability Standard must address how a responsible entity will include security considerations as part of its information system planning and system development life cycle process
- The Reliability Standard must address a responsible entity's CIP Senior Manager's identification and documentation of the risks of proposed information system planning and system development actions

FERC Order 829

Fourth Objective: Vendor Risk Management & Procurement Controls

- The Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations

- The Reliability Standard must address controls for the following topics:
  1. Vendor security event notification processes
  2. Vendor personnel termination notification for employees with access to remote and onsite systems
  3. Product/service vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords
  4. Coordinated incident response activities

NERC CIP-005-6, -010-3, & -013-1: Background

- NERC initially proposed to issue one new Reliability Standard (CIP-013-1), but ultimately proposed the issuance of two further new Reliability Standards (CIP-005-6 and CIP-010-3) to comply with the Order 829 directives

- Key Milestones in the development of the new Reliability Standards:

– Final NERC ballot	Concluded July 20, 2017
– NERC Board vote	Aug. 10, 2017
– Filed with FERC	Sept. 26, 2017

NERC CIP-005-6, -010-3, & -013-1: Responsible Entities

- The Reliability Standards will apply to the following types of entities:
  - Balancing Authority
  - Distribution Provider
  - Generator Operator
  - Generator Owner
  - Interchange Coordinator or Interchange Authority (CIP-005-6 and CIP-010-3 only)
  - Reliability Coordinator
  - Transmission Operator
  - Transmission Owner
- Facilities covered by the Reliability Standards:
  - All Bulk Electric System (BES) Facilities
  - Distribution Provider's applicable facilities

NERC CIP-005-6, -010-3, & -013-1: Framework

- Overview of new Reliability Standards:
  - CIP-013-1 requires Responsible Entities to **implement** processes to:
    - **Identify and assess cyber security risks** to the BES from vendor products and services in their planning activities for high and medium impact BES Cyber Systems
    - **Include specified security concepts** in their procurement activities for high and medium impact BES Cyber Systems
  - CIP-005-6 bolsters protections in the existing CIP-005 by addressing specific risks related to **vendor remote access**
  - CIP-010-3 augments existing CIP-010 protections in relation to risks associated with **software integrity and authenticity**

NERC CIP-013-1: Summary of Requirements

- Final draft of CIP-013-1 submitted to FERC proposes three requirements:

R1 **Develop** a supply chain cybersecurity **plan** addressing the security objectives of Order 829:

1. Software integrity and authenticity;
2. Vendor remote access;
3. Information system planning; and
4. Vendor risk management and procurement controls

R2 **Implement** the **plan**

– Does not require renegotiation of existing contracts

R3 **Reassess** security controls at least once every 15 months

– Review must include consideration of new risks and changes

NERC CIP-005-6: Summary of Requirements

- Final draft of CIP-005-6 submitted to FERC proposes two requirements:

R1 **Implement** documented process that ensures applicable systems meet the following requirements related to the **ESP**:

1. All applicable Cyber Assets with routable protocol network connections are within a **defined ESP**;
2. All external routable connectivity must be through an identified Electronic Access Points (**EAP**);
3. Require inbound and outbound **access permissions** for EAPs;
4. **Authentication** for dial-up connection with applicable Cyber Assets;
5. Capability to **detect** known or suspected **malicious communications** for inbound and outbound traffic

NERC CIP-005-6: Summary of Requirements

- Final draft of CIP-005-6 submitted to FERC proposes two requirements *(continued):*

R2 **Remote Access Management—Implement** documented process that ensures applicable systems meet the following requirements:

1. Interactive **remote access** must use:
   - an intermediate system so that Cyber Assets are not accessed directly;
   - Encryption terminating at an intermediate system; and
   - Multifactor authentication
2. Capability of **determining** active vendor remote access sessions, and of **terminating** such access sessions

NERC CIP-010-3: Summary of Requirements

- Final draft of CIP-010-3 submitted to FERC proposes four requirements:

R1 **Implement** documented process that includes the following:

1. **Develop** baseline configuration for operating systems, open-source applications, installed custom software, logical network access points, and security patches;
2. **Authorize** and document changes that deviate from the baseline;
3. For deviations, **update** the baseline as necessary within 30 days of completing the change;
4. **Determine** required cyber security controls prior to the change, verify that those controls are not adversely affected following the change, and document the results of the verification;
5. If technically feasible, **test changes** in a test environment prior to implementing the change, documenting the results; and
6. Prior to implementing the change, **verify** the **identity** of the software source and the **integrity** of the software when available

NERC CIP-010-3: Summary of Requirements

- Final draft of CIP-010-3 submitted to FERC proposes four requirements *(continued):*

R2 **Implement** documented process that monitors at least once every 35 days for changes to the baseline configuration

R3 **Implement** documented process that includes the following:

1. **Conduct** a paper or active vulnerability assessment at least once every 15 days;
2. **Perform** active vulnerability assessment at least once every 36 months and document the result;
3. Prior to adding a new applicable Cyber Asset to the production environment, **perform** an active vulnerability assessment of the asset; and
4. **Document** the results of each of the above and the plan to remediate or mitigate identified vulnerabilities

NERC CIP-010-3: Summary of Requirements

- Final draft of CIP-010-3 submitted to FERC proposes four requirements *(continued):*

  R4 **Implement** documented plans for Transient Cyber Assets and Removable Media that include requirements specified in an attachment to the Reliability Standard, which address the management, authorization, and mitigation of risks associated with Transient Cyber Assets managed by the Responsible Entity or by other parties

NERC Technical Guidance

- NERC Technical Reference on the Final Draft CIP-013-1 sets forth examples of controls that may satisfy the Reliability Standard requirements
- Examples of controls for **Software Integrity and Authenticity**:
  - Ensuring patches are from the original source before installation
  - Implementing server-side encryption keys that may be validated and regularly tested
  - Using third party certificates to validate the identity of the vendor
  - Requiring use of digital fingerprints and checksums

NERC Technical Guidance

- Examples of controls for **Vendor Remote Access**:
  - Using an operator-controlled, time limited (e.g. lock out, tag out) process for third-party remote access
  - Setting up alert and monitoring parameters on key attributes and thresholds such as number of failed log-in attempts
  - Logging and review procedures
  - Using jump hosts for access to protected networks
  - Changing default passwords
  - Monitoring and acting on advisories
  - Contract terms to support controls

NERC Technical Guidance

- Examples of controls for **Information System Planning**:
  - Screening criteria to determine high-risk systems or changes
  - Processes to assess third-party risks in planning, including
    - Gathering and review of information on vendor security processes
    - Engaging vendors in testing of potential vulnerabilities
    - Use of available tools for establishing vendor risk baseline
  - New system design processes to incorporate layered protections, security policy, architecture, and controls
  - Processes for coordination and approval involving appropriate IT security, supply chain, and legal personnel

NERC Technical Guidance

- Examples of controls for **Procurement Risk Management**:
  - Incorporate risk-assessment information in RFPs
  - Establish procurement review teams that include CIP personnel
  - Develop contract terms addressing the four security objectives
  - Require notification of security events that may impact the Responsible Entity
  - Require notification of transfer, reassignment, or termination of employees with remote or onsite access to BES Cyber Systems

Key Contractual Considerations

- Security Obligations
  - At very least, need to address the following:
    - Notification of security events that may impact the Responsible Entity
    - Notification of transfer, reassignment, or termination of employees with remote or onsite access
    - Disclosure of known vulnerabilities of the vendor
    - Coordination of response to vendor-related cyber security incidents
  - Security requirements, standards, policies
- Audit Rights and Reporting
  - Inspection rights
  - Third party audits and certifications
    - SOC reports
    - ISO certifications

Key Contractual Considerations

- Risk Allocation
  - Indemnification
    - Scope of obligation
    - Indemnification Procedures
  - Liability Limitations
    - Address exceptions to both direct damages cap **and** consequential damages waiver
  - Warranties
  - Force Majeure
    - Definition of “Force Majeure”

Key Contractual Considerations

- Termination Rights
  - Material breach vs. specific right
- Insurance
  - Type of insurance?
  - Who provides insurance?
- Subcontractors
  - Approval rights?
  - Vendor still primarily liable for acts of subs

Contractual Approaches

- What Approach Do I Take?
  - Update existing form agreements?
  - Checklists for responding to vendor paper?
  - Security Addendum?
  - All of the above?

- Approach will differ depending on type of Vendor
  - Software licensors vs. Service Providers

Paul Tiao

Partner, Global Privacy and Cybersecurity, Co-founder and Co-Chair of the Energy Sector Security Team and the Cyber and Physical Security Task Force

- Advises energy, transportation, communications and other critical infrastructure companies on risk management, incident response, investigations, litigation, regulations and legislation
- Served as Senior Counselor for Cybersecurity and Technology to the Director of the FBI

Kevin Jones

Partner, Energy and Infrastructure, Co-founder and Co-Chair of the Energy Sector Security Team and the Cyber and Physical Security Task Force

- Kevin advises energy sector clients and government entities on the development of energy infrastructure, energy regulation, and the design and operation of wholesale electricity markets

Randy Parks

Partner, Head of the Global Technology and Outsourcing practice

- Randy has negotiated and documented dozens of large-scale, complex commercial and technology transactions worth billions of dollars for multinational companies, including retailers, manufacturers and consumer products companies.

Questions?