Morgan Lewis

CYBERSECURITY POLICY CHANGES FROM THE BIDEN-HARRIS ADMINISTRATION

October 7, 2021

Presenters

Ezra Church

Kristin Hadgis

Dan Skees

Morgan Lewis

Agenda

- Ransomware Attacks and Current Developments
- Infrastructure Bill & Mandates for Owners and Operators of Pipelines
- Overarching Administration Efforts on Cybersecurity


Ransomware Attacks and Current Developments
Morgan Lewis

Ransomware Attacks – What Are They?

- The increase in ransomware attacks is the big news in privacy and cyber fields
- 700% increase in ransomware attacks for 2020, even more in 2021
- What are they?
  - Threat actor enters system and uses malware to encrypt the system to shut it down
  - Provides a ransom note demanding payment in cryptocurrency in exchange for the key needed to decrypt the system
  - Launched by organized criminal groups, typically located in Russia, China, or North Korea, with Darkside, Nightwalker, and Revil
  - Dual threat — exfiltration of sensitive data

Ransomware Attacks – What Is Causing Them?

- Change in business model — traditional attacks focused on exfiltration are more difficult to perpetrate and less lucrative.
  - Companies avoid storing sensitive data, use encryption, use multi-factor
  - Payment network has evolved with chip technology and other changes
  - Your data is already out there!
- Fueled by the rise in remote work and distraction due to COVID-19 over the last year, which has opened companies to more vulnerability.
  - Use of remote access tools, such as outdated VPNs and equipment, personal devices, unsecure Wi-Fi
  - Microsoft found that the level of overall cyber attacks reached an all-time high in the three months immediately after WHO announced that COVID-19 was a global pandemic in May 2020

Ransomware Attacks – How to Respond When They Occur?

- Convene the incident response team
- Outside counsel's role
- Outside cybersecurity expertise
- Insurance
- PR and crisis communications
- Contacting law enforcement
- Negotiating a ransom payment
- Data mining
- Notification obligations

Ransomware Attacks – Is It Alright to Pay?

- US Department of the Treasury's Office of Foreign Assets Control (OFAC) recently issued an updated advisory on potential sanctions risks for companies facilitating payments in connection with ransomware attacks.
- In September 2021, OFAC for the first time sanctioned a cryptocurrency exchange for its part in facilitating financial transactions for ransomware actors, and it will continue to impose sanctions on those who provide financial, material, or technological support for ransomware activities.
- Violations of OFAC regulations may result in civil penalties based on strict liability.
- OFAC strongly discourages companies from making ransomware payments and instead recommends focusing on strengthening defensive measures and reporting to/cooperating with authorities — actions that OFAC would consider to be "mitigating factors" in any related enforcement action.

Ransomware Attacks – How Can You Prevent Them?

- Focus on backups — ensure regular, complete, and segregated
- Know your system and endpoints — inventory and data map are critical
- Consider vulnerabilities created in remote work environment
- Maintain good, consistent cyber hygiene
  - Regular patches
  - Updated anti-virus
  - Authentication protocols (passwords and multi-factor)
- The buck stops with your incident response team and planning process

Infrastructure Bill & Mandates for Owners and Operators of Pipelines

Morgan Lewis

Infrastructure Bill

- State and Local Cybersecurity Improvement Act (section 70611 et seq.)
  - $1 billion in funds for grants to state, local, and tribal governments for enhancing their cybersecurity efforts, to be disbursed over four years
  - Develop and implement cybersecurity plan address imminent cyber risks
  - Includes DHS review of entity cybersecurity plans
- Cyber Response and Recovery Act (section 70601 et seq.)
  - Declaration of cyber emergency authority for DHS for critical US organizations, with $100 million to be disbursed over five years in responding to these incidents
- CISA to receive $35 million on sector risk management
- DHS Science and Technology Directorate to receive $150 million on cyber and tech research
- Funding for initial White House national cyber director office
- Note: Whether these initiatives pass and in what form very much remains to be seen

2021 Colonial Pipeline Incident

- Largest U.S. pipeline system for refined oil products
- Caused by ransomware attack on company computer systems
- Unknown IT/OT access; facts developing
  - Disconnected OT systems to silo ransomware in IT environment
- Effects:
  - Scattered gas shortages across the southeastern US
  - Gas price spikes
  - State of emergency declared by governors in multiple states
- Colonial paid $4.4 million to attackers

TSA Directives Stemming from Colonial Pipeline Incident

- Initial Security Directive: May 27, 2021 (Security Directive Pipeline-2021-01)
  - Non-publicly identifies "critical pipeline owners and operators"
  - Major components:
    - Pipeline owners and operators to report confirmed/potential cybersecurity incidents to CISA
    - Review current cybersecurity practices and identify gaps with steps to remediation within 30 days
      - List of security practices to use for evaluation publicly available
    - Appoint a primary and alternative Cybersecurity Coordinator available 24/7 to CISA and TSA
- Legal authority: 49 U.S.C. 114(*l*)(2)(A) – TSA Administrator can issue emergency regulations or security directives without typical APA notice and comment if "the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security"

TSA Directives Stemming from Colonial Pipeline Incident

- Second security directive: July 20, 2021
  - Directs owners and operators to:
    - Implement identified mitigation measures to protect against attacks on IT and OT systems (particularly against ransomware)
    - Develop and implement a contingency and recovery plan
    - Review the cybersecurity architecture design of their systems
- Content of directives and their legal obligations mostly not publicly available
  - Washington Post received a slightly redacted version in response to a FOIA request and published it


Overarching
Administration
Efforts on
Cybersecurity
Morgan Lewis

Executive Order 14017
Securing America's Critical Supply Chains

- February 2021 – President Biden signs Executive Order addressing vulnerabilities in the supply chains of critical national economic sectors
  - Protection of key industrial sectors from supply chain shocks and vulnerabilities, including sectors implicated in the administration's focus on combatting climate change
- Two main components
  1. 100-day review of supply chain risks impacting four key product categories:
     - semiconductors
     - critical minerals, like rare earth elements
     - pharmaceuticals
     - "high capacity" batteries, including electric vehicle batteries
  2. Long-term review of supply chains
     - defense industrial base
     - the public health and biological preparedness industrial base
     - information and communications technology (ICT) industrial base
     - supply chains for agricultural commodities and food production
     - transportation industrial base; and energy sector industrial base

DOE 100 Day Plan

- DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and electric utilities to advance technologies to shore up electric industrial control systems
  - Encourages owners and operators to implement measures or technology that enhance their detection, mitigation, and forensic capabilities;
  - Includes concrete milestones over the next 100 days for owners and operators to identify and deploy technologies and systems that enable near real time situational awareness and response capabilities in critical industrial control system (ICS) and operational technology (OT) networks;
  - Reinforces and enhances the cybersecurity posture of critical infrastructure information technology (IT) networks; and
  - Includes a voluntary industry effort to deploy technologies to increase visibility of threats in ICS and OT systems.

*Source: US Department of Energy

New Federal Cybersecurity Executive Order 14028
Executive Order on Improving the Nation's Cybersecurity

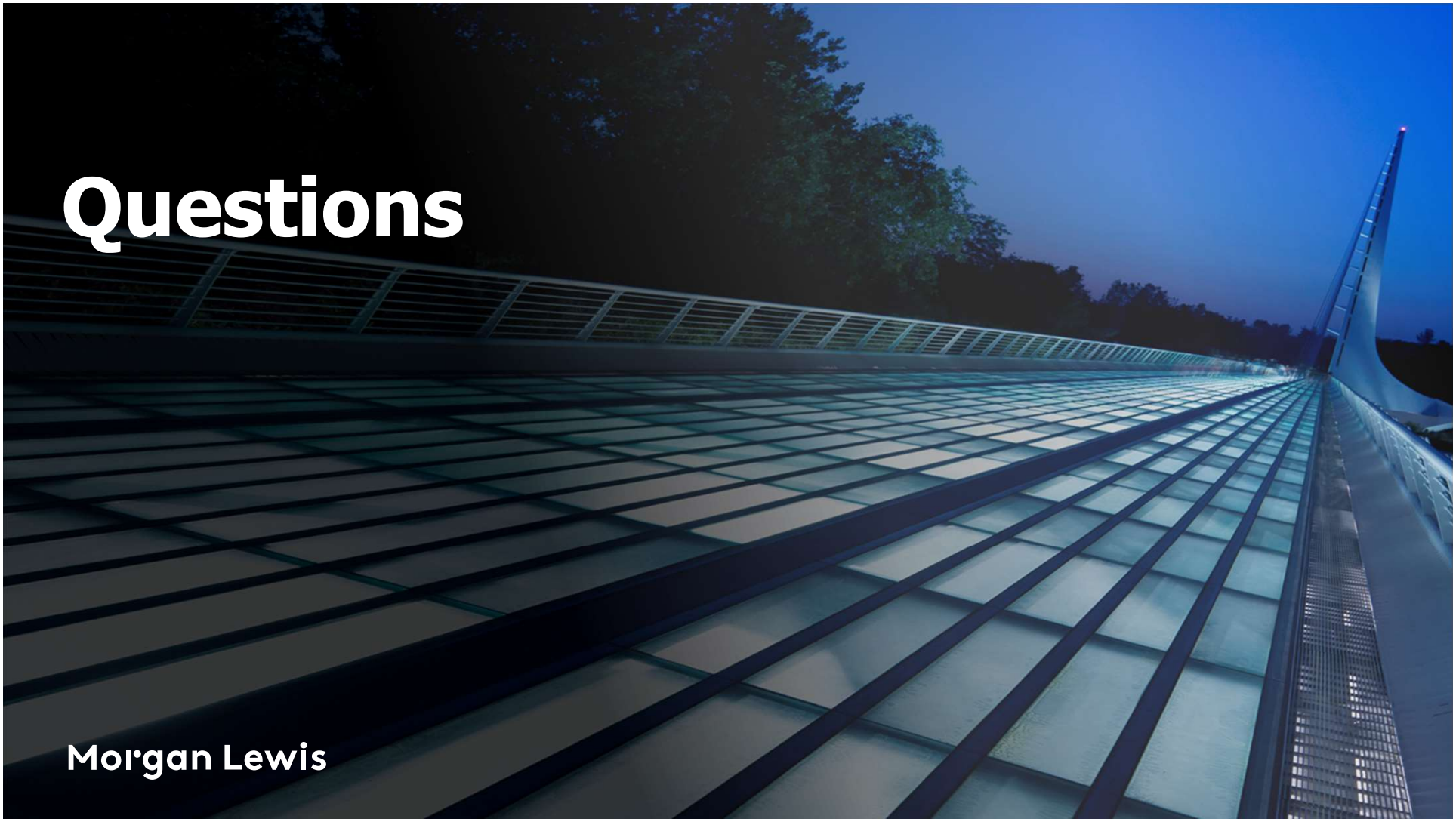
- Objective: Protect federal government networks and software supply chains against increasing threats of attacks from malicious actors and improve response capabilities
- Key features:
  - *Information Sharing:* Requires IT and communication government contractors to share information with agencies about cyber threats and to report cyber incidents
  - *Modernizing Cybersecurity*: Adoption of cloud networks and multifactor authentication
  - *Security Best Practices*: New security standards for software sold to the government to address vulnerabilities in software supply chains
  - *Cybersecurity Safety Review* Board: Co-chaired by government and private sector leads, to analyze significant cyber incidents and make recommendations.
  - *Cybersecurity incident response*: Agency playbook and government-wide endpoint detection and response.
  - *Logging*: Cybersecurity event log requirements for federal departments and agencies.

National Security Memorandum

- July 28, 2021: White House issues National Security Memorandum on "Improving Cybersecurity for Critical Infrastructure Control Systems"
  - CISA and NIST to jointly develop cybersecurity performance goals for critical infrastructure (focus on power, water, and transportation sectors)
  - Industrial Control System Cybersecurity Initiative established to develop technology to enhance the early identification of threats

Executive Order 13920
Securing the United States Bulk-Power System

- May 1, 2020: President Trump signs Executive Order 13920
  - Imposed restrictions on transactions involving "bulk-power system equipment" provided by entities controlled by foreign adversaries where the transaction would create an undue risk
  - DOE directed to develop regulations by late-2020
- December 17, 2020: DOE issues the "Prohibition Order" limiting some utilities acquisitions or installations of certain bulk-power system equipment
  - Targeted select equipment "manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China"
- January 20, 2021: President Biden suspends EO 13920 for 90 days
- April 20, 2021: DOE revokes Prohibition order
- RFI responses submitted by June 7, 2021; comments still under review


Questions
Morgan Lewis

Biography

Ezra D. Church
Philadelphia, PA
+1.215.963.5710
ezra.church@morganlewis.com

Ezra D. Church counsels and defends companies in privacy, cybersecurity, and other consumer protection matters. He helps clients manage data security and other crisis incidents and represents them in high-profile privacy and other class actions. Focused particularly on retail, ecommerce, and other consumer-facing firms, his practice is at the forefront of issues such as biometrics, artificial intelligence, location tracking, ad tech, and blockchain. Ezra is a Certified Information Privacy Professional (CIPP) and co-chair of the firm's Class Action Working Group.

Biography

Kristin M. Hadgis
Philadelphia, PA
+1.215.963.5563
kristin.hadgis@morganlewis.com

Kristin M. Hadgis counsels and defends retail and other consumer-facing companies in matters relating to privacy and cybersecurity, class actions, Attorney General investigations and enforcement actions, the California Consumer Privacy Act, consumer protection laws, retail operations, loyalty and gift card programs, and commercial disputes. Kristin also handles data security incident response crisis management, including any resulting litigation or government investigations.

Biography

Dan Skees
Washington, DC
+1.202.739.5834
daniel.skees@morganlewis.com

J. Daniel Skees represents electric utilities before the Federal Energy Regulatory Commission (FERC) and other agencies on rate, regulatory, and transaction matters. He handles rate and tariff proceedings, electric utility and holding company transactions, utility financing, electric markets and trading issues, reliability standards development and compliance, including cybersecurity requirements, administrative litigation, and transmission development. In handling appeals of FERC decisions, Dan has successfully represented clients before both the US Court of Appeals for the District of Columbia Circuit and the US Court of Appeals for the Fifth Circuit.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington

Morgan Lewis

THANK YOU