Recent Cybersecurity Developments

NAESB Update Meeting

August 26, 2021

ARDUA STRATEGIES Inc.

Annie McIntyre
President
amcintyre@arduastrategies.com

Big Considerations for 2021

- Increased awareness of the Threat Landscape and the OT-IT bridge
- Competitive-driven vs regulated security
- New directives are taking a more 'applied' focus
- Industry response is strong – creating natural 'categories' of response
- Flexibility is required….

The only thing certain in 2021 is CHANGE

ARDUA STRATEGIES Inc.

Compliance Landscape Pre-2021

- In Critical Infrastructure, the regulation of cybersecurity focused mainly in two areas:
  - Bulk electricity – NERC CIP
  - Pipeline security information handling – 49 CFR Part 1520

- In addition to these, the following federal guidelines and industry standards comprised the compliance landscape
  - National Institute of Standards and Technology (NIST) Cybersecurity Framework
  - National Institute of Standards and Technology (NIST) Guide to Industrial Control Systems (ICS) Security 800-82
  - Transportation Security Administration (TSA) 2021 Cybersecurity Guidelines
  - Transportation Security Administration 2011 Smart Security Practices
  - International Electrotechnical Commission (IEC) 62443 Security for Industrial Automation and Control Systems (IACS) Standards Series
  - American Petroleum Institute 1164 Pipeline SCADA Security

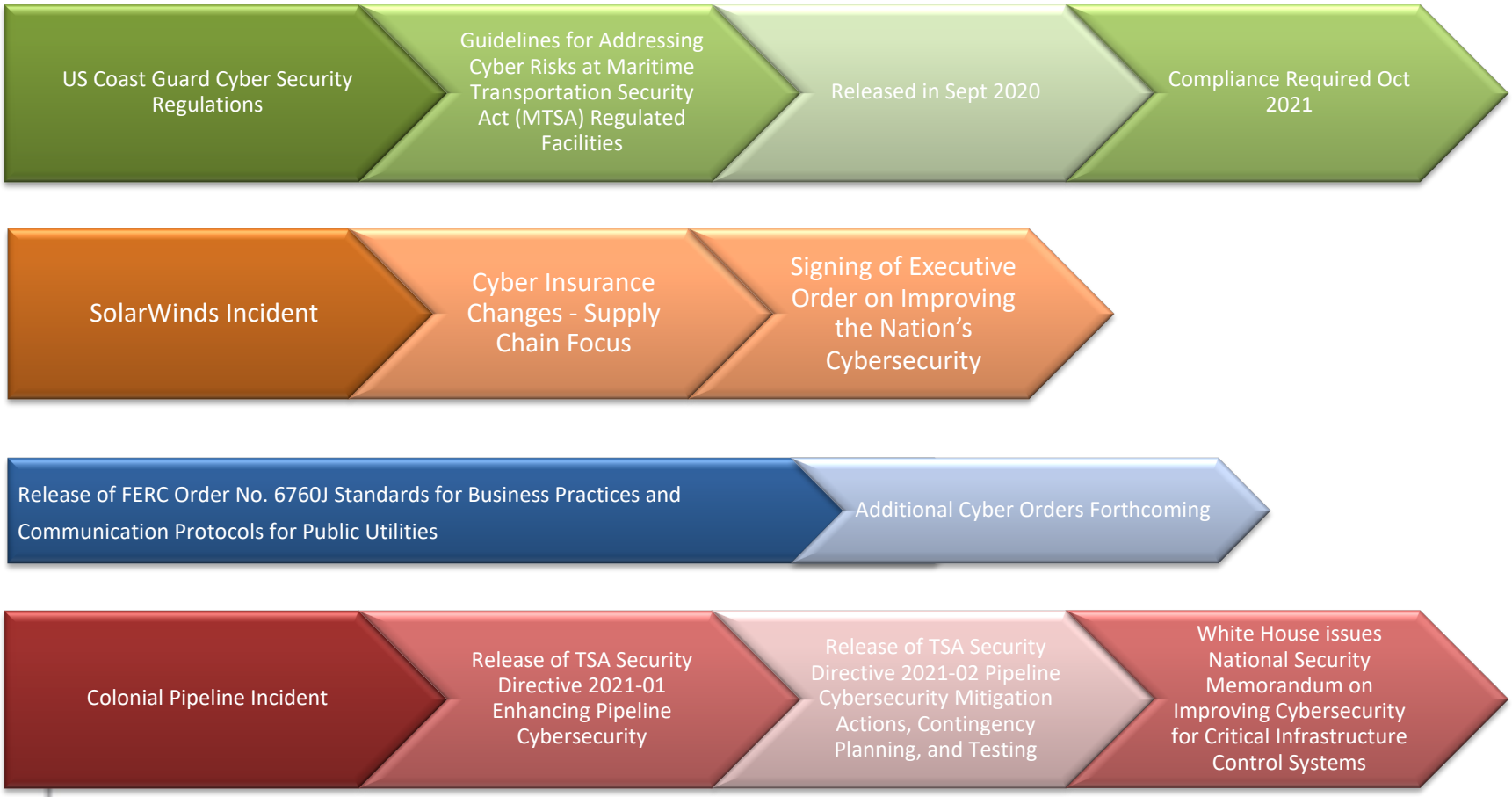
ARDUA STRATEGIES Inc.

2021 Events

- SolarWinds Incident
  - Cyberinsurance Changes – new supply chain focus
  - Signing of Executive Order on Improving the Nation's Cybersecurity
  - Release of FERC Order No. 676-J, Standards for Business Practices and Communication Protocols for Public Utilities
- Colonial Pipeline Incident
  - Release of TSA Security Directive 2021-01 Enhancing Pipeline Cybersecurity
  - Release of TSA Security Directive 2021-02 Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing
  - White House issues National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems
  - US Coast Guard NVIC 01-20 Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities take effect (Oct 2021)
  - API 1164 v3 Released

ARDUA STRATEGIES Inc.

2021 Motivators



ARDUA STRATEGIES Inc.

Review of New Regulations and Directives

- US Coast Guard Port NVIC 01-20 - Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities
  - Addresses control system environments at ports
  - Points to compliance with
    - National Institute of Standards and Technology (NIST) Cybersecurity Framework
    - National Institute of Standards and Technology (NIST) Guide to Industrial Control Systems (ICS) Security 800-82
  - Released in 2020, ports must be compliant Oct 1, 2021

ARDUA STRATEGIES Inc.

Review of New Regulations and Directives

- TSA 2021-01 Security Directive: Enhancing Pipeline Cybersecurity
  - DHS **critical** pipelines must adhere to Section 7 (cyber) of the 2018 Cybersecurity Guidelines as well as reporting changes released in April 2021
  - Critical pipelines have 30 days to respond to DHS with compliance plans (June 30)
  - **Non-critical** pipelines are encouraged to meet the TSA 2018 Cybersecurity Guidelines
- TSA 2021-02 Security Directive: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing
  - Sensitive Security Information (SSI)
  - DHS **critical** pipelines must adhere to the detailed technical metrics in the Directive
  - 25 pages, very specific technical mitigations with aggressive timelines
  - Effective July 26

ARDUA STRATEGIES Inc.

Path Forward

- Where do we go from here?
- Near-term and long-term considerations
- Return on investment
- Preparedness vs Reaction

ARDUA STRATEGIES Inc.