NATF™
North American Transmission Forum

Supplier Sharing Call

February 21, 2024

Open Distribution for Supply Chain Materials

Presentations are provided with the presenters' permission for distribution. The NATF makes no and hereby disclaims all representations or warranties, either express or implied, relating to the content, including as to the accuracy or completeness of the information. No liability is assumed by the NATF for any damages arising directly or indirectly from the content or by the use or application thereof. Use of the content constitutes agreement to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use. Further, no liability is assumed for infringement by any presentation materials, artwork, or photographs used in presentations not developed by NATF.

Guidelines for this Call for NATF Members

- This is an open call
- Some participants on this call are not employees of NATF member companies
    - Do not share confidential information
    - Avoid conduct that unreasonably restrains competition
    - Adhere to your organization’s standards of conduct
    - Do not share intellectual property unless authorized

Guidelines for this Call

- This call is not recorded
- Slides for the call will be available on the NATF public website at: Supplier Sharing Calls (natf.net)

Please Participate

- Raise your hand
    - We will unmute you
    - Make sure you are identified in the participant list
- Put a question or comment in the chat
- Put a question or comment in the Q&A

If you put a question or comment in the chat or Q&A but want to remain anonymous, please open with your request

Tom Galloway

NATF President and CEO

Opening Remarks

Tom Galloway,

NATF President and CEO

Purpose of the NATF Supplier Sharing Activities

- Provide an opportunity for suppliers to talk about cyber security issues and practices ranging from
  - How establish a security program to
  - In-depth discussions on a specific technical challenge
- Leverage knowledge from lessons learned
- Share information
- Calls will be limited to suppliers unless otherwise noted

Contributing Organizations

- Aspen Technology / OSI
- Hitachi Energy
- International Society of Automation (ISA)
- National Electrical Manufacturers Association (NEMA)
- Schneider Electric
- Schweitzer Engineering Laboratories (SEL)
- Siemens
- Siemens Energy
- US Chamber of Commerce
- With support from:
  - Nebraska Public Power District
  - Southern Company
  - North American Transmission Forum (NATF)

On this call

- Aspen Technology / OSI – Peter Escobar, VP, Research and Development
- International Society of Automation (ISA) – Andre Ristaino, Managing Director, Global Consortia and Conformity Assessment Programs
- Schneider Electric – Michael Pyle, Director of Product Cyber Security
- Schweitzer Engineering Laboratories (SEL) – Frank Harrill, VP Security
- Siemens Industry – Andy Turke, Cyber Security Officer
- Siemens Energy – Christopher Fitzhugh, Industrial Control Systems Security Consultant, North America
- US Chamber of Commerce – Heath Knakmuhs, VP and Policy Counsel
- LG&E and KU Energy – Tony Hall, Manager, CIP and Federal Regulatory Compliance
- Southern Company – Jennifer Couch, Manager, Transmission EMS Compliance

Agenda and Today's Presenters

- Geo-Political Threats/Incidents
  - Peter Escobar, VP, Product Security, Aspen Technology / OSI
- Incident Response Plans
  - Frank Harrill, VP, Security, Schweitzer Engineering (SEL)
  - Michael Pyle, Director of Product Cyber Security, Schneider Electric
  - Andy Turke, Cyber Security Officer, Siemens Industry
- Resources and Information
  - Christopher Fitzhugh, Industrial Control Systems Security Consultant, North America, Siemens Energy

Geopolitical Threats

Peter Escobar

VP, Research and Development, Aspen Technology

FBI Director Christopher Wray keynote address at Munich Security Conference on February 15, 2024

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-038A

February 7, 2024

Australian Government Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

National Cyber Security Centre PART OF THE GCSB

National Cyber Security Centre a part of GCHQ

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

The FBI, NSA, and CISA assess that People’s Republic of China state sponsored cyber actors are seeking to preposition themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.

CISA Identified Nation State Threat Actors

Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA

- Chinese actors - engages in malicious cyber activities to pursue its national interests including infiltrating critical infrastructure networks.
- Russian actors - engages in malicious cyber activities to enable cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries.
- North Korean actors - employ malicious cyber activity to collect intelligence, conduct attacks, and generate revenue.
- Iran actors - increasingly sophisticated cyber capabilities to suppress certain social and political activity, and to harm regional and international adversaries.

Past Examples

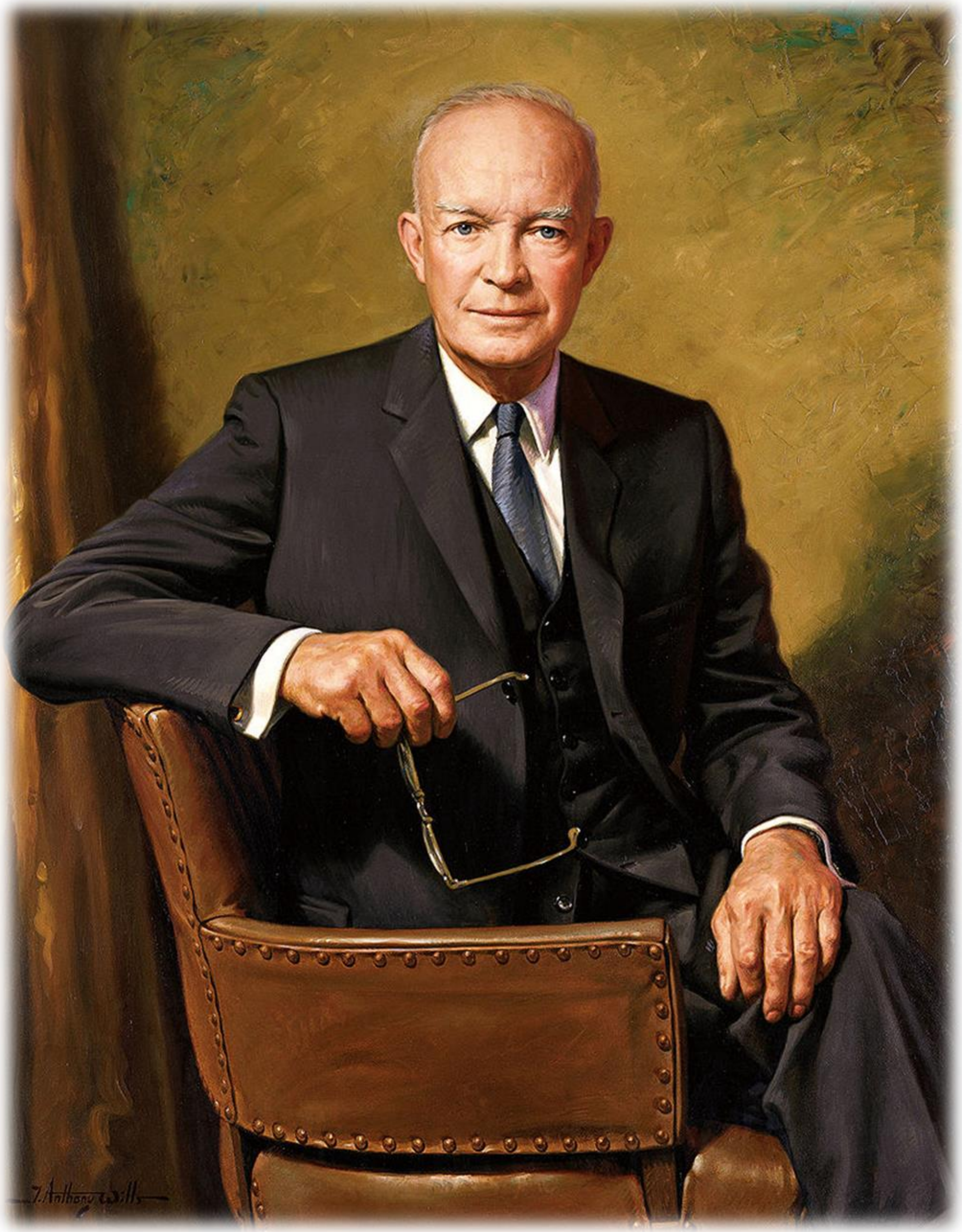
- Microsoft posted report April 2023
  - Iran linked group APT35 (Mint Sandstorm)
  - Targeted U.S. seaports, energy companies, transit systems, major gas and electric utilities between 2021-2022.
  - Cyberespionage and theft of sensitive data
- Colonial Pipeline 2021
  - Russian Attack leading to "Shields Up"
  - CISA published additional lessons in 2023
- Ukraine Power Grid In 2015 - Sandworm

Incident Response Plans

Frank Harrill,
VP, Security Schweitzer Engineering (SEL)

and

Michael Pyle,
Director of Product Cyber Security Schneider Electric



Plans are worthless, but planning is everything. There is a very great distinction because when you are planning for an emergency you must start with this one thing: the very definition of "emergency" is that it is unexpected, therefore it is not going to happen the way you are planning.

From a speech to the National Defense Executive Reserve Conference in Washington, D.C. (November 14, 1957) ; in *Public Papers of the Presidents of the United States, Dwight D. Eisenhower, 1957*, National Archives and Records Service, Government Printing Office, p. 818

Key Aspects of Cyber Incident Response Plans

A well-structured incident response plan is critical for effectively mitigating cybersecurity threats and minimizing potential damage.

- Well defined process
  - Categorize based on type of asset impacted Establish an incident response team with clearly defined roles and responsibilities.
  - Specify in terms of roles, skills, and domain specific knowledge.
- Identify and prioritize critical assets and systems, tune the plan for both internal systems and offers compromised at customer sites.
- Develop a communication plan for both internal and external stakeholders:
  - Executive Committee, Possibly the Board
  - Regulatory authorities
  - Impacted Customers
  - Media holding statement
  - Customer Support
  - Company at large
- Regularly conduct training and simulation exercises to ensure preparedness.

Key Aspects of Cyber Incident Response Plans

Implementation – Following The Plan

Detection and Analysis:

- Implement robust monitoring tools for network and system activity.
- Define thresholds for unusual behavior or security alerts.
- Establish procedures for analyzing potential security incidents promptly.

Containment, Eradication, and Recovery:

- Time is of the essence - Upon detection of an incident, isolate affected systems to prevent further damage.
- Identify the source and nature of the incident and take steps to eradicate the threat.
- Prepare and provide an initial communication and holding statement to key stakeholders, including those impacted, e.g., people, customers, organizations.
- Develop and document recovery procedures to restore affected systems and data.

Communicate to stake-holders & regulatory, prepare initial customer communications

Key Aspects of Cyber Incident Response Plans

Follow-Thru

Post-Incident Activity:

- Conduct a thorough review of the incident, documenting all actions and outcomes.
- Analyze root causes and identify areas for improvement in the incident response plan.
- Update the plan based on lessons learned and implement necessary changes.
- Implement identified improvements to your defenses and processes.

Communication and Reporting:

- Finalize communication with regulatory bodies, relevant stakeholders, including employees, customers.
- Prepare detailed incident reports, including the impact assessment and remediation actions taken and provide to relevant stakeholders and regulatory agencies as appropriate.

Resources and Information

Christopher Fitzhugh

Industrial Control Systems Security Consultant, North America, Siemens Energy

Resources and Information

- https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf
- https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf
- https://www.cisa.gov/sites/default/files/publications/enhanced-cybersecurity-services-fact-sheet-052021-508_1.pdf
- https://www.fbi.gov/investigate/cyber/partnerships
- JOINT-GUIDANCE-IDENTIFYING-AND-MITIGATING-LOTL.PDF (defense.gov)
- Industrial Cybersecurity Technology for ICS/OT Asset Visibility | Dragos
- https://redcanary.com/
- Incident response planning: When to call in the lawyers (redcanary.com)

Resources and Information (cont.)

- The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years | CISA
- Danish energy sector hit by a wave of coordinated cyberattacks - Help Net Security
- S21sec_Thales_ThreatLandscapeReport_2023_EN

Questions?

Comments?

Upcoming Calls

- April 17
- June 19
- Special Webinar – date TBD

  Watch for a NATF Special Webinar on updated mappings for NATF Criteria and Questionnaire to security frameworks!

Frank Harrill

VP, Security, SEL

Closing Remarks

Frank Harrill
VP, Security Schweitzer Engineering (SEL)

Thank you for attending!

supplychain@natf.net

dearley@natf.net

vagnew@natf.net