North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

NATF-RF-SERC Special Webinar: Identifying and Managing Potential Compromise of Network Interface Cards

October 22, 2020

SERC

RELIABILITY FIRST

Open Distribution

Welcome and Agenda Overview

Slides posted on https://www.natf.net/industry-initiatives/supply-chain-industry-coordination/all-resources

- Policies and Open Meeting Reminder
- Webinar Logistics
- Opening Comments: Overview of NATF-ERO Collaboration Pilot
- NATF Supplier Cyber Security Assessment Model – How Entity Mitigation Fits In
- NERC/FERC Joint Staff White Paper on Supply Chain Vendor Identification
- Regional Perspectives on Responding to Supply Chain Compromise Risk
- NATF Member Perspectives and Experiences

Policies and Open Meeting Reminder

- Policies – General Statement
  - Obey **antitrust laws and guidelines**
    - Avoid conduct that unreasonably restrains competition
  - Respect **intellectual property**
    - Secure permissions for any sharing or use of others' intellectual property

- Open Meeting Reminder
  - Participants are reminded that this webinar is public. The access information was posted on the NATF public website, as well as the NERC, RF, and SERC websites and has been widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Webinar Logistics

Lee Underwood (NATF)

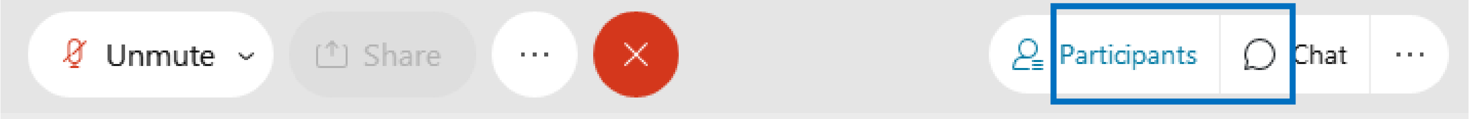
Director, Practices

Webinar Logistics

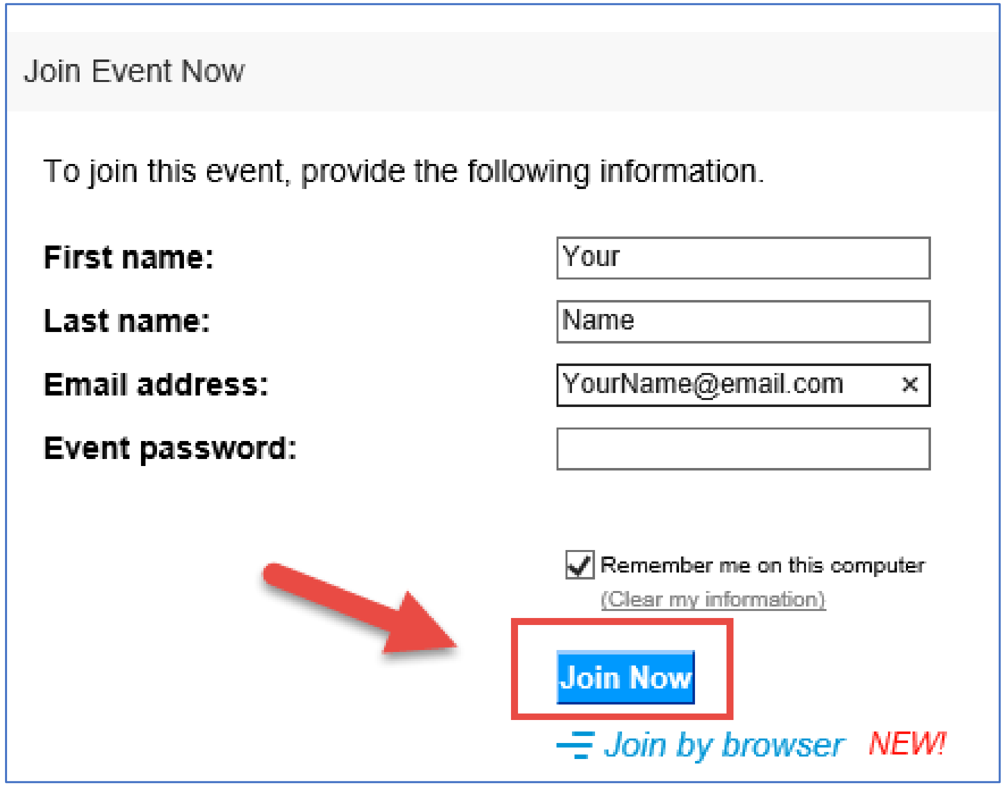
- All attendee lines are muted
- Use the raise hand feature if you’d like to ask a question or provide a comment
  - We’ll acknowledge you and unmute your line
- We may not be able to answer questions submitted via the Q&A

Raising Your Hand

If you joined using the desktop application (the Join Now button):



Participant list

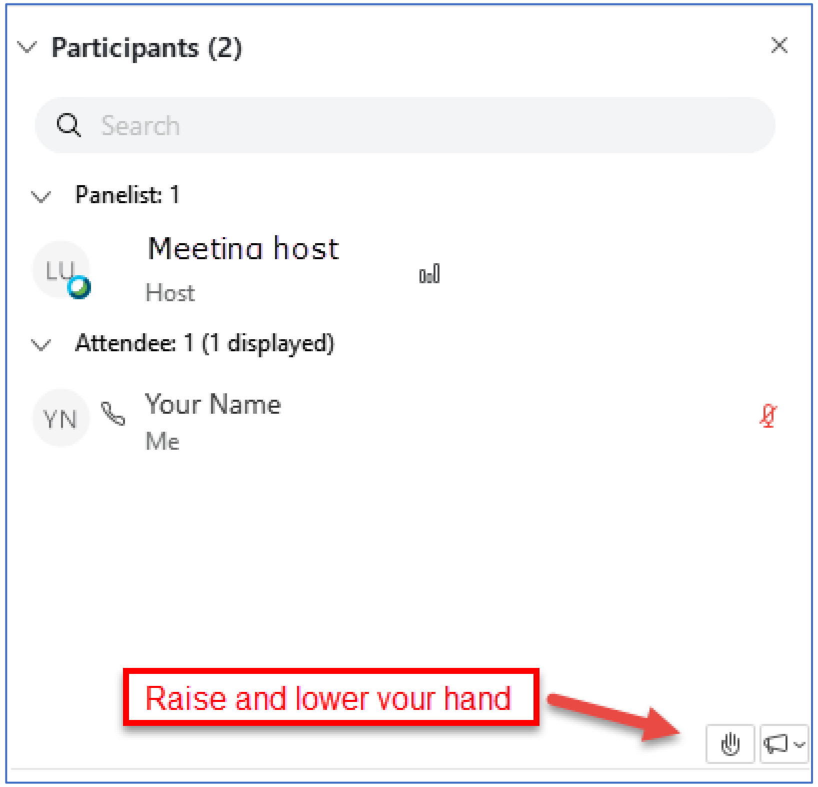


Join Event Now

To join this event, provide the following information.

First name:	Your
Last name:	Name
Email address:	YourName@email.com
Event password:	

☑ Remember me on this computer
(Clear my information)



Participants (2)

Panelist: 1

Meeting host
Host

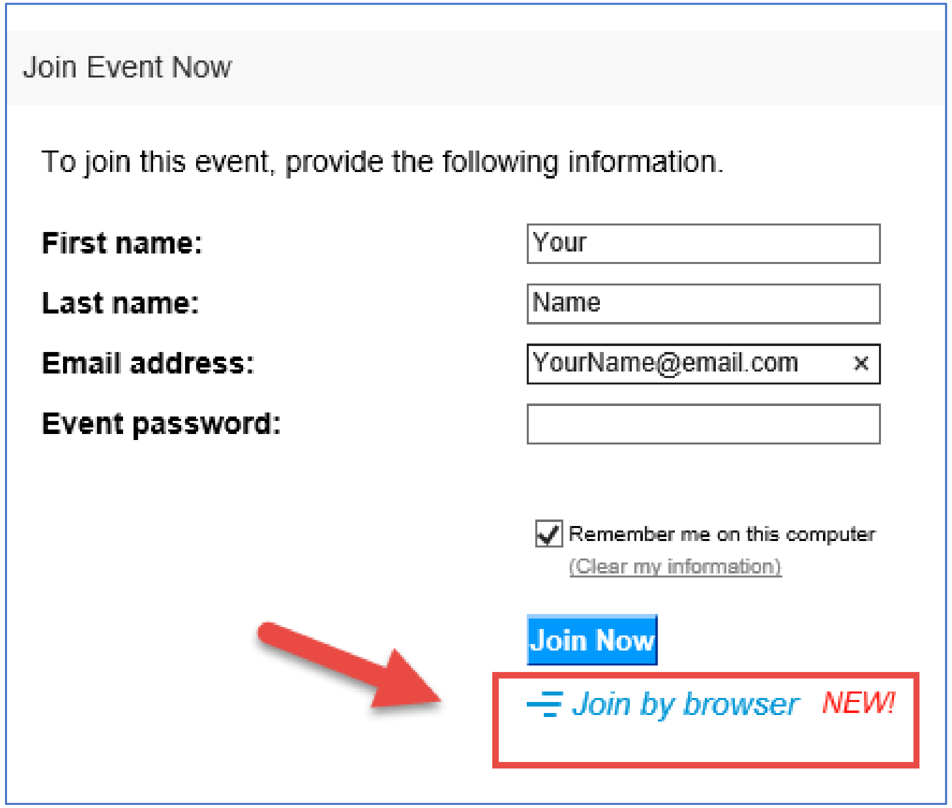
Attendee: 1 (1 displayed)

Your Name
Me

Raise and lower your hand

Raising Your Hand

If you joined by browser:

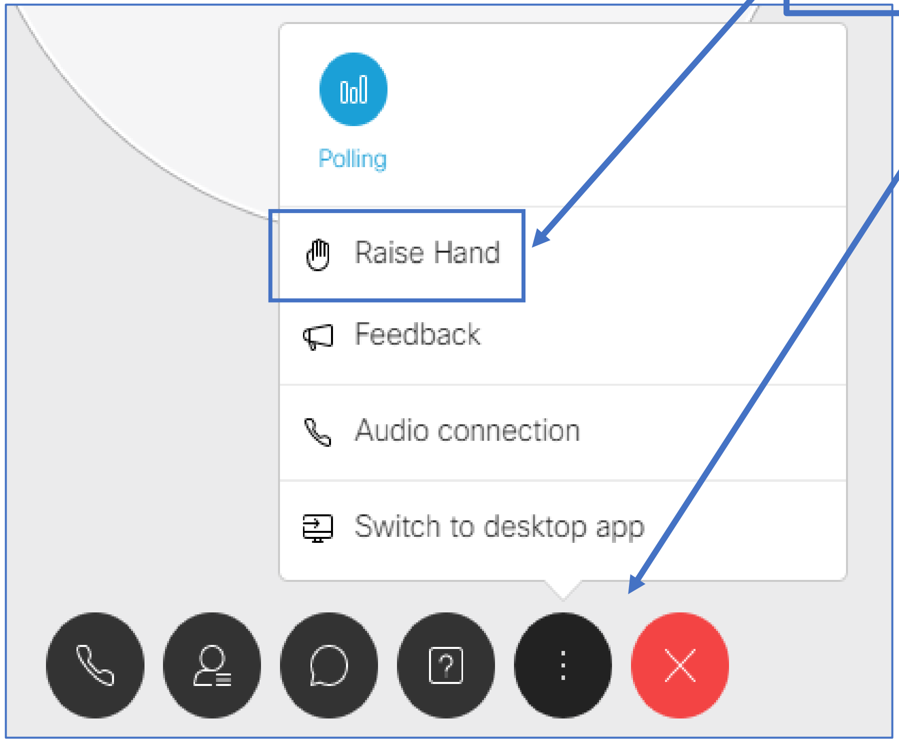


Join Event Now

To join this event, provide the following information.

First name:	Your
Last name:	Name
Email address:	YourName@email.com ×
Event password:	

☑ Remember me on this computer
(Clear my information)



Raise Hand

Opening Comments: Overview of NATF-ERO Collaboration Pilot

Tom Galloway (NATF)

President and CEO

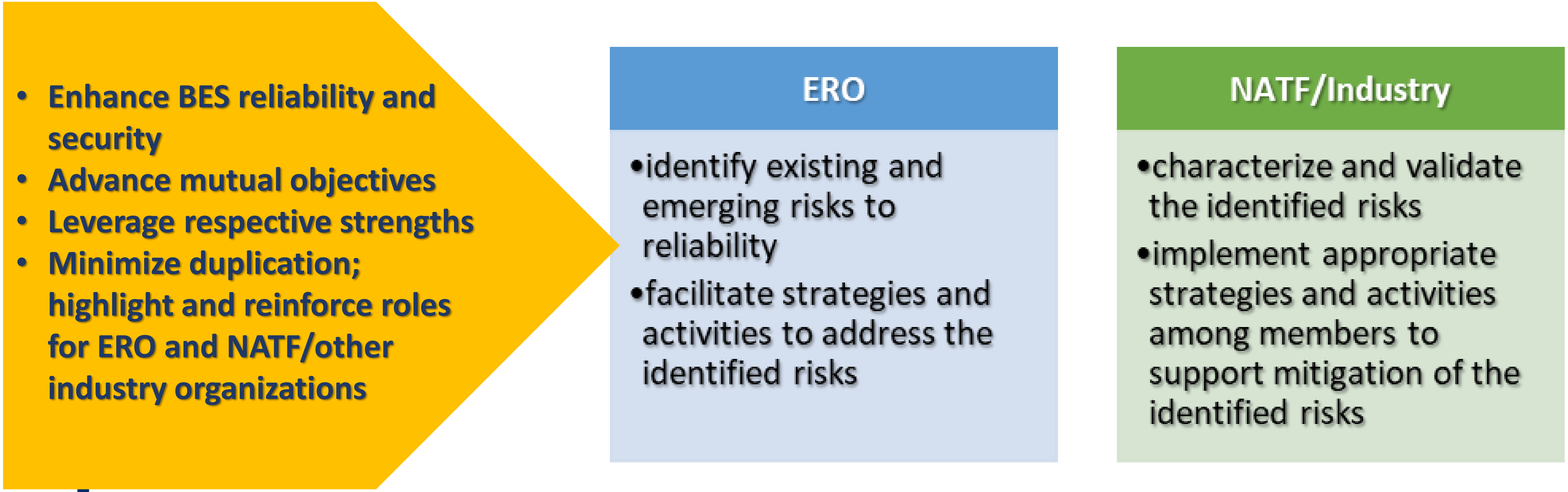
Pilot Collaboration Background

- NATF-NERC Memorandum of Understanding (MOU)
  - Original 2010; Revised 2013
  - Updated March 2019 – increased focus on collaboration
- Issues, and opportunity for collaboration, raised in NATF-NERC leadership meetings
- Discussed with NERC and regional CEOs (May 2019)
- Agreed to pilot collaborative activities with RF and SERC

Intent: Create repeatable model for collaboration on other topics

NATF-ERO Collaboration Model

The NATF is working with the ReliabilityFirst (RF) and SERC regions and NERC to pilot a collaboration model



- Enhance BES reliability and security
- Advance mutual objectives
- Leverage respective strengths
- Minimize duplication; highlight and reinforce roles for ERO and NATF/other industry organizations

ERO

- identify existing and emerging risks to reliability
- facilitate strategies and activities to address the identified risks

NATF/Industry

- characterize and validate the identified risks
- implement appropriate strategies and activities among members to support mitigation of the identified risks

Supply Chain Pilot Topics and Objectives

Conduct Regional Workshops on Entity Mitigation Practices for Supply Chain Risks

- Objectives for workshops:
  - Focus on security
    - Not compliance/standards
    - Not procurement or supplier evaluation/risk assessment
  - How entity action to reduce risk fits in supplier assessment model
  - Create awareness of entity actions, controls, and practices to detect, prevent, and correct risk introduced via supply chain

The NATF Supplier Cyber Security Assessment Model – How Entity Mitigation Fits In

Ken Keels (NATF)

Director, Initiatives

North American Transmission FORUM

Open Distribution

NATF Supply Chain Key Resources Available to Industry

NATF Public Website: Supply Chain Industry Coordination Page

- Provides information and resources

Supplier Cyber Security Assessment Model

- Model for assessing suppliers' cyber security practices

NATF Criteria

- 60 Criteria for suppliers' supply chain cyber security practices
- 24 Organization Information considerations

Energy Sector Supply Chain Risk Questionnaire

- 223 cyber security questions
- 20 general information questions

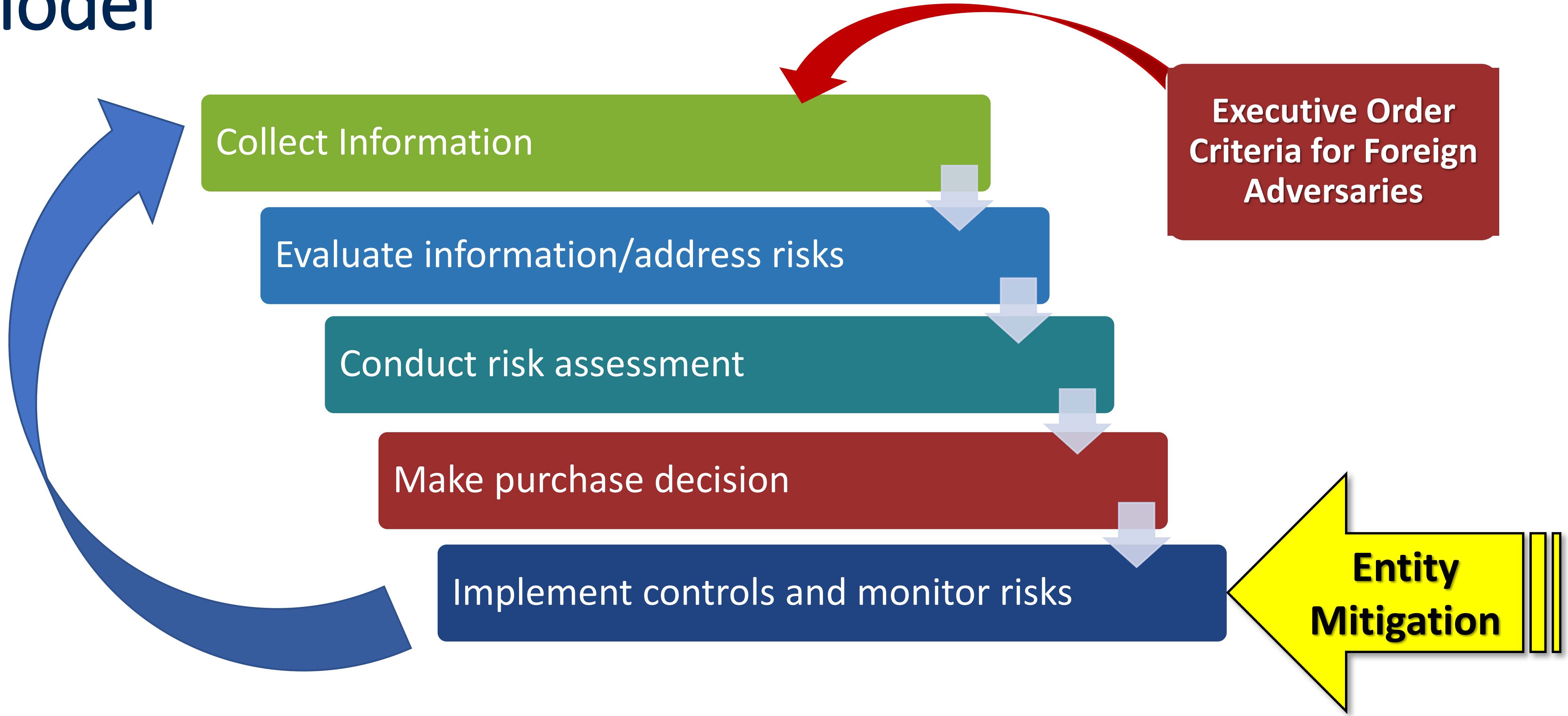
Revision Process for Criteria and Questionnaire

- Intake and consideration of industry input/comments for periodic modification
- Refining the Criteria and Questionnaire for industry convergence

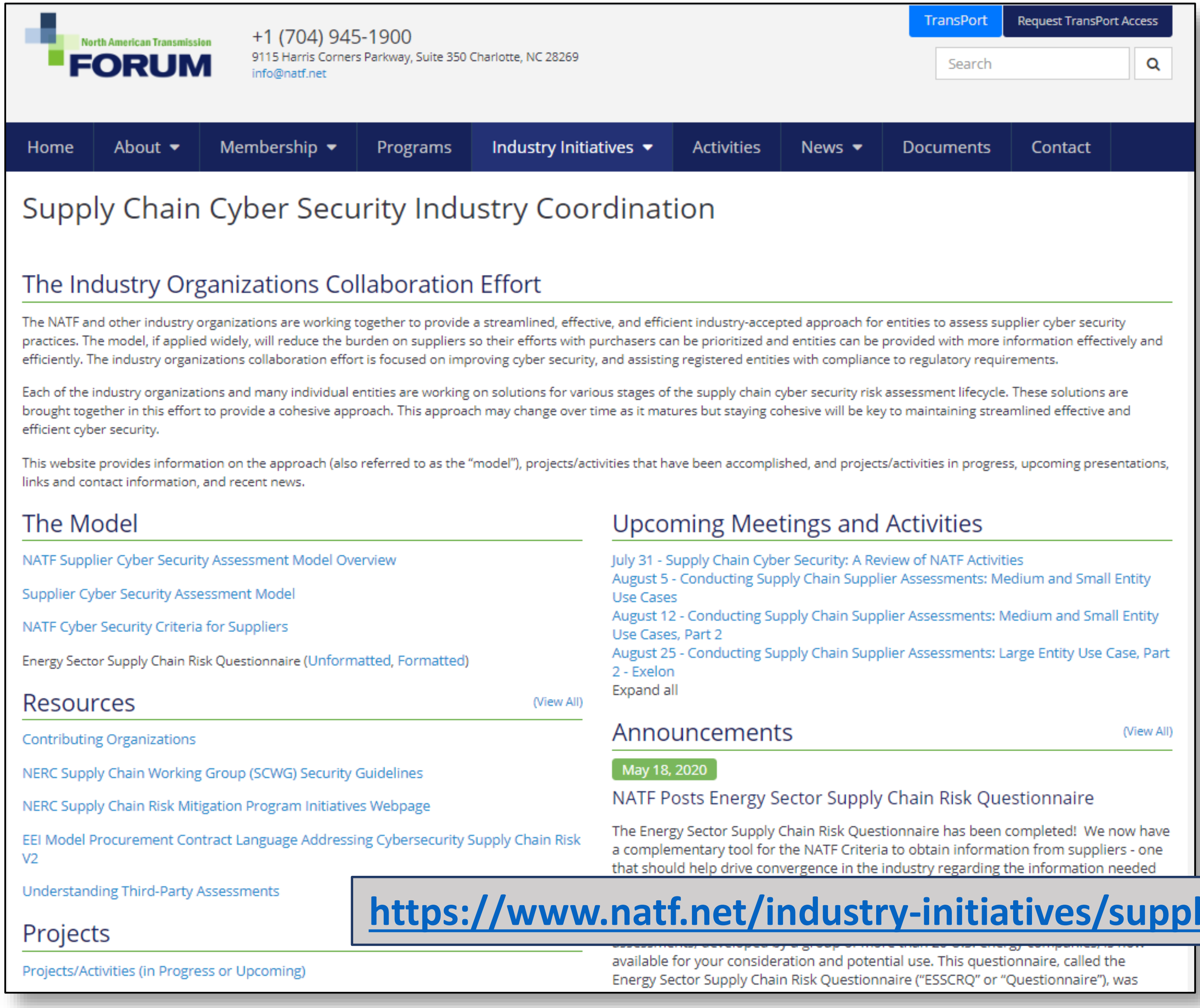
EEI Procurement Language

- Sample contract language to mitigate risk and provide assurances of supplier performance

NATF Supplier Cyber Security Assessment Model


Collect Information
Evaluate information/address risks
Conduct risk assessment
Make purchase decision
Implement controls and monitor risks
Executive Order Criteria for Foreign Adversaries
Entity Mitigation

NATF-hosted Industry Organizations Web Page



North American Transmission FORUM

+1 (704) 945-1900
9115 Harris Corners Parkway, Suite 350 Charlotte, NC 28269
info@natf.net

Supply Chain Cyber Security Industry Coordination

The Industry Organizations Collaboration Effort

The NATF and other industry organizations are working together to provide a streamlined, effective, and efficient industry-accepted approach for entities to assess supplier cyber security practices. The model, if applied widely, will reduce the burden on suppliers so their efforts with purchasers can be prioritized and entities can be provided with more information effectively and efficiently. The industry organizations collaboration effort is focused on improving cyber security, and assisting registered entities with compliance to regulatory requirements.

Each of the industry organizations and many individual entities are working on solutions for various stages of the supply chain cyber security risk assessment lifecycle. These solutions are brought together in this effort to provide a cohesive approach. This approach may change over time as it matures but staying cohesive will be key to maintaining streamlined effective and efficient cyber security.

This website provides information on the approach (also referred to as the "model"), projects/activities that have been accomplished, and projects/activities in progress, upcoming presentations, links and contact information, and recent news.

The Model

NATF Supplier Cyber Security Assessment Model Overview

Supplier Cyber Security Assessment Model

NATF Cyber Security Criteria for Suppliers

Energy Sector Supply Chain Risk Questionnaire (Unformatted, Formatted)

Resources

(View All)

Contributing Organizations

NERC Supply Chain Working Group (SCWG) Security Guidelines

NERC Supply Chain Risk Mitigation Program Initiatives Webpage

EEI Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk V2

Understanding Third-Party Assessments

Projects

Projects/Activities (in Progress or Upcoming)

Upcoming Meetings and Activities

July 31 - Supply Chain Cyber Security: A Review of NATF Activities
August 5 - Conducting Supply Chain Supplier Assessments: Medium and Small Entity Use Cases
August 12 - Conducting Supply Chain Supplier Assessments: Medium and Small Entity Use Cases, Part 2
August 25 - Conducting Supply Chain Supplier Assessments: Large Entity Use Case, Part 2 - Exelon
Expand all

Announcements

(View All)

May 18, 2020

NATF Posts Energy Sector Supply Chain Risk Questionnaire

The Energy Sector Supply Chain Risk Questionnaire has been completed! We now have a complementary tool for the NATF Criteria to obtain information from suppliers - one that should help drive convergence in the industry regarding the information needed

available for your consideration and potential use. This questionnaire, called the Energy Sector Supply Chain Risk Questionnaire ("ESSCRQ" or "Questionnaire"), was

https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

NERC/FERC Joint Staff White Paper on Supply Chain Vendor Identification

Lonnie Ratliff (NERC)
Senior Manager, Cyber and Physical Security Assurance

Barry Kuehnle (FERC)
CIP Senior Advisor

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Joint White Paper Supply Chain Vendor Identification

Lonnie J Ratliff, Senior Manager, Cyber and Physical Security Assurance
Barry Kuehnle, FERC
NATF Webinar
October 22, 2020

RELIABILITY | RESILIENCE | SECURITY

Topics

- Purpose
- Specific Vendors?
- Why Network Interface Controllers?
- Methods of discovery
- Key Takeaways

Purpose

- Mitigate supply chain risk on Bulk Electric System (BES)
- Previous Supply Chain Alert
- BES relies on networking and telecommunications equipment
- Non-Invasive techniques for discovery
- Overarching Supply Chain Awareness

Why specific vendors?

- 2012 House Permanent Select Committee on Intelligence Report
  - Recommended US government agencies and federal contractors against using Huawei or ZTE equipment
  - Encouraged private sector to exclude such equipment as well
- 2013 GAO assessed potential security risk of foreign manufactured equipment in communications networks
  - *"[a] potential enemy or criminal group has a number of ways to potentially exploit vulnerabilities in the communications equipment supply chain, such as placing malicious code in the components that could compromise the security and resilience of the networks."*
- Defense Innovation Board highlights threats posed by China and other nation-state adversaries
  - *"evidence of backdoors or security vulnerabilities have been discovered in a variety of devices globally"*

Why specific vendors? (cont)

- Hauwei, ZTE, and their subsidiaries have recently gained the largest market share of networking vendors globally.
- Portion of this market share dominance stems from embedded Huawei or ZTE components in equipment produced by otherwise unrelated vendor

Network Interface Controllers?

- Network Connectivity
  - The electric sector uses networking and telecommunications equipment to operate the Bulk Power System.
  - Rebranded hardware
- Low-level position in a computer system
  - Bypassing host-based firewall / IDS / IPS
- Great backdoor opportunity
- Large-scale deployment
  - Impact many devices at one time

Techniques for Discovery

- White paper has four:
  - NMAP Passive ARP
  - List ARP Cache Table
  - DHCP Client Table
  - Port Mirroring
- Registered Entities may have other methods
- Use caution on whatever method you select
  - Use ***EXPERIENCED*** Network and/or Cyber Security staff

Discovery of foreign vendors DOES NOT confirm malicious activity in the network. Actions should be taken to determine if the device or component exhibits malicious activity.

Key Take-Aways

- Testbed or development networks often is a representative of production
- ARP Cache tables are your friend.
- IDS Signatures can be used to detect specific MAC Addresses
- Use the tools that you may have deployed.
  - Health monitoring tools
  - Vulnerability Assessment tools
- Virtual Machine addresses may be difficult to properly identify
- Additional cyber asset components could be used to install backdoor.
- Understand the supply chain risk, and mitigate.

References

- Joint Staff White Paper on Supply Chain Vendor Identification
  - https://www.nerc.com/pa/comp/CAOneStopShop/Joint%20Staff%20White%20Paper%20on%20Supply%20Chain_07312020.pdf
- GAO, Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment
  - https://www.gao.gov/assets/660/654763.pdf
- Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE
  - https://fas.org/irp/congress/2012_rpt/huawei.pdf
- The 5G Ecosystem: Risks and Opportunities for DoD, Defense Innovation Board
  - https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF

Regional Perspectives on Responding to Supply Chain Compromise Risk

Scott Pelfrey (ReliabilityFirst)
Principal Technical Auditor

Bill Peterson (SERC)
Manager, Outreach & Training

NIC Risks, Mitigations & Remediations

Scott Pelfrey – Principal Technical Auditor
ReliabilityFirst

October 22, 2020

Agenda Topics

- Follow-On w/FERC-NERC White Paper
- Risks – or why should I be worried
- Potential controls/mitigations/remediations to address Vulnerabilities
- Awareness

Associated Risks

Major Risks

- **Identified NICs from Huawei or ZTE**
  - Compromised – Immediate or future?
  - Self-Discovery (proactive)
  - Vendor Identified (reactive)
- **Attack Vector?**
  - Dragos report (*North American Electric Cyber Threat Perspective – January 2020*) supply chain already being targeted
  - Successful attack from “trustworthy” supplied, OEMs, and MSPs can bypass security stack over trusted connections.
- **Allowance for authenticated lateral movement within the trust-zone**

Other Risks

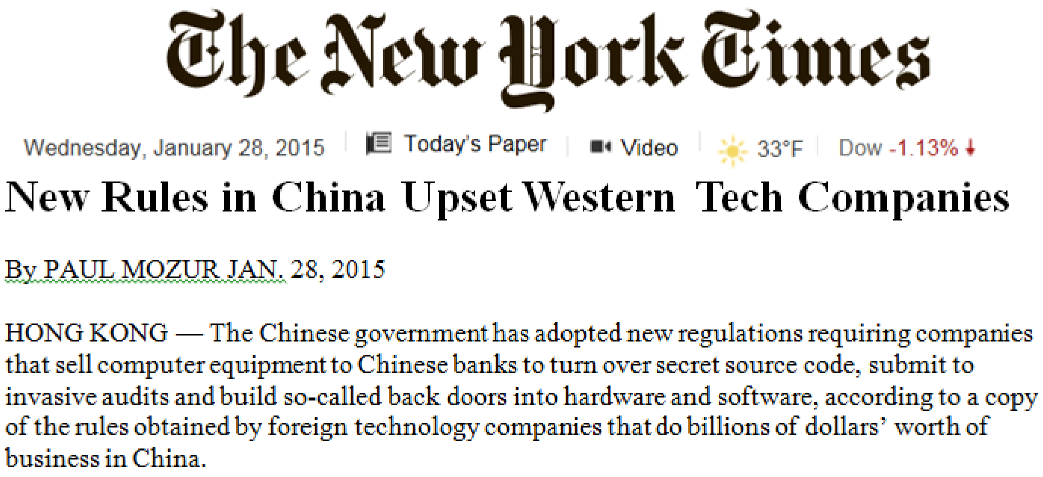
- **Other manufacturers of NICs from China?**
- **Other components – (GPU, CPU)**
- **Vendor pushback**
- **Complexity of Task (especially in larger organizations)**
- **Confusion around next steps**

Hilltop Electric Cooperative (HEC)

- **HEC has 100+ Cyber Assets…**
  - Procured from reputable US company (Dell, HP, IBM, etc.)
  - Faithful supplier for 10+ years
  - MSP for cycled hardware and software updates every 3 years
  - Assets in both protected and corporate environments
- **HEC performs MAC address sweep**
- **Finds 15% of NICs are Huawei (MAC 28:e5:b0)**
- **Finds 40% of NICs are not expected (MAC D8:12:65** Chongqing Fugui Electronics Co.,Ltd.)

Issues

- NYT reports in Jan 2015 on China requirement for computer equipment
- Vendor knowledge - yes/no/maybe
- Need to determine communications capabilities (SOC, NOC)
- Status of current environment – Confidentiality, Integrity, Availability
- Next steps – verification / replacement / mitigation



The New York Times

Wednesday, January 28, 2015 | Today's Paper | Video | 33°F | Dow -1.13%

New Rules in China Upset Western Tech Companies

By PAUL MOZUR JAN. 28, 2015

HONG KONG — The Chinese government has adopted new regulations requiring companies that sell computer equipment to Chinese banks to turn over secret source code, submit to invasive audits and build so-called back doors into hardware and software, according to a copy of the rules obtained by foreign technology companies that do billions of dollars' worth of business in China.

Mitigation / Remediation (1)

- **Determine what the vendor knows and if any assistance**
- **Monitor, Monitor, Monitor**
  - Must have a very good understanding of traffic to monitor (baseline connections and traffic)
- **Determine risk of Cyber Asset**
  - HVAC may be less risky that EMS Operator Console
- **Determine Impact a compromised Cyber Asset has in your Environment**
- **Determine additional Security Controls / Internal Controls to add**

Mitigation / Remediation (2)

- **Increase NOC, SOC capabilities (personnel, network monitoring, firmware installs, firewall updates, etc.)**

- **Whitelisting (Firewall ACLs / subnets)**
    - Can be difficult to correctly implement – tread carefully!

- **Continue Risk Assessments**
    - Monitor government/member communities (NATF/FERC/NERC/Regions)

- **Determine Final Disposition**
    - Replacement? Monitoring? Internal Controls?

- **Plan for worst case - CSIRP (Assume compromise if discovered)**

Conclusion

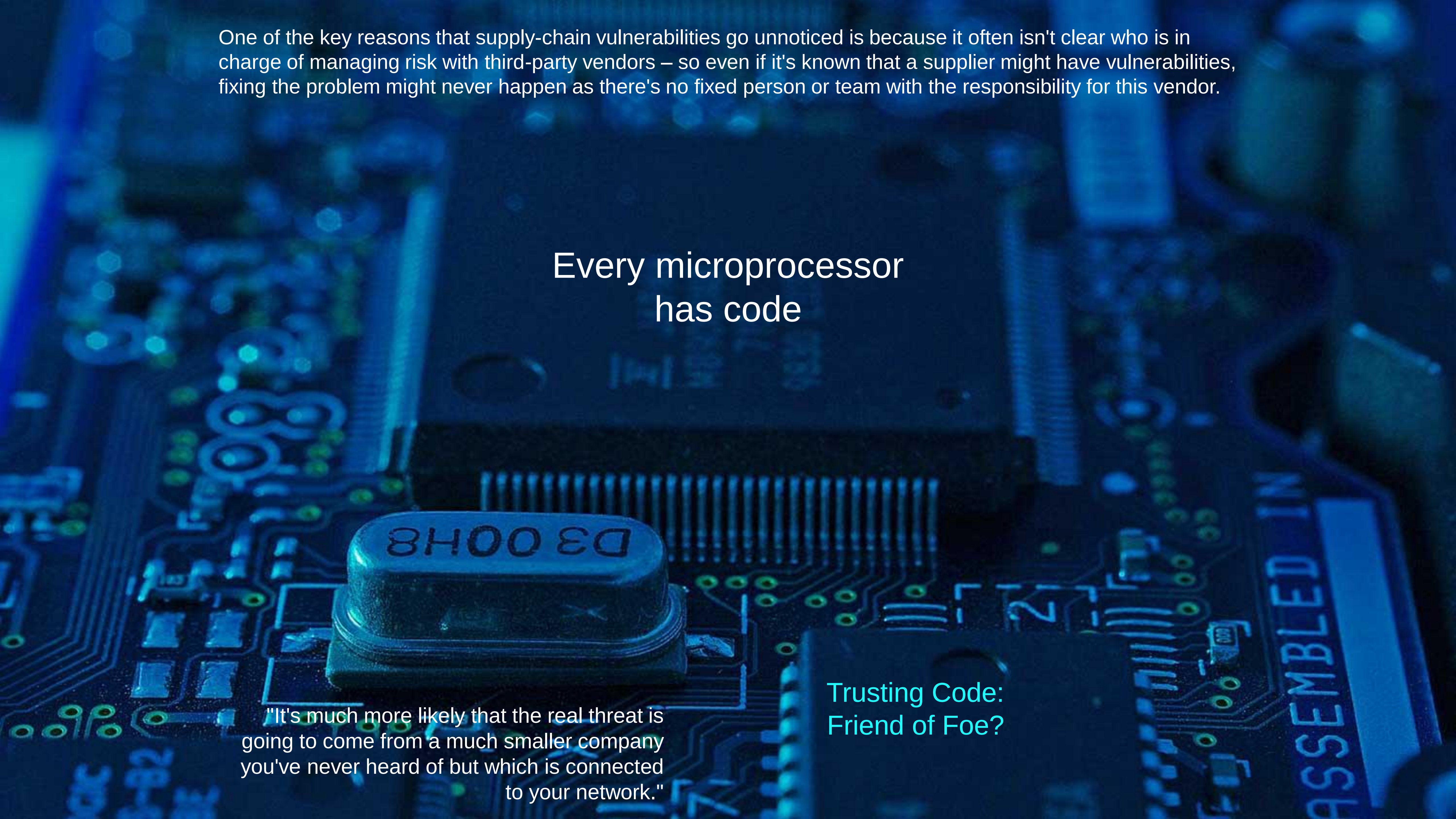
- **FERC/NERC/Regions acknowledge complexity and difficulty you face**
- **Process is time consuming and labor intensive**
  - May be able to identify easily, but mitigation/remediation will not be easy
- **Review/monitoring of traffic patterns are a given – entity MUST know what communications are required**
- **Review of connections to internet should be closely scrutinized and strict limits imposed**
- **Don’t forget to put lessons learned back into Supply Chain review and CSIRP**

Supply Chain Risks

October 22, 2020

One of the key reasons that supply-chain vulnerabilities go unnoticed is because it often isn't clear who is in charge of managing risk with third-party vendors – so even if it's known that a supplier might have vulnerabilities, fixing the problem might never happen as there's no fixed person or team with the responsibility for this vendor.

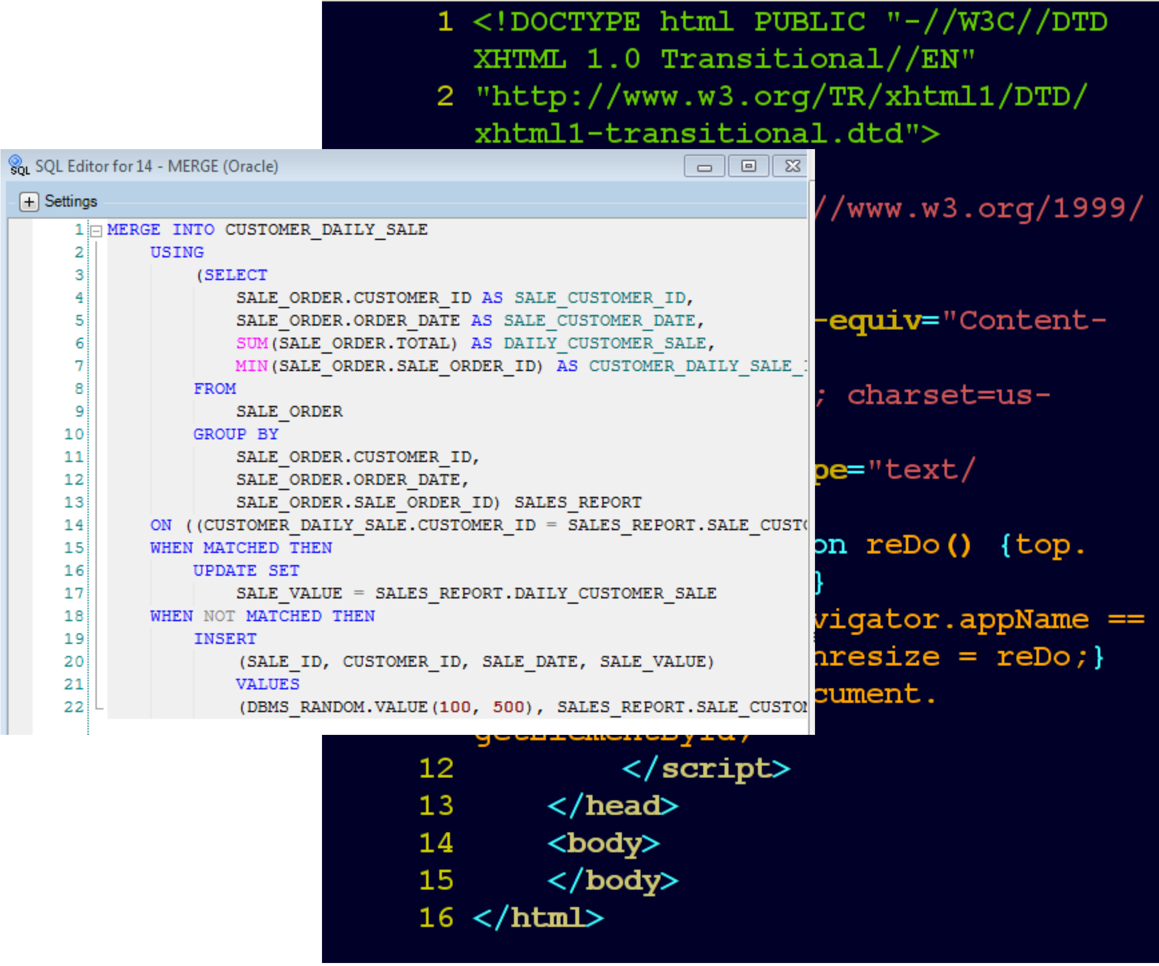
Every microprocessor has code



"It's much more likely that the real threat is going to come from a much smaller company you've never heard of but which is connected to your network."

Trusting Code:
Friend of Foe?

If you have code…



SQL Editor for 14 - MERGE (Oracle)

```
MERGE INTO CUSTOMER_DAILY_SALE
    USING
        (SELECT
            SALE_ORDER.CUSTOMER_ID AS SALE_CUSTOMER_ID,
            SALE_ORDER.ORDER_DATE AS SALE_CUSTOMER_DATE,
            SUM(SALE_ORDER.TOTAL) AS DAILY_CUSTOMER_SALE,
            MIN(SALE_ORDER.SALE_ORDER_ID) AS CUSTOMER_DAILY_SALE_I
        FROM
            SALE_ORDER
        GROUP BY
            SALE_ORDER.CUSTOMER_ID,
            SALE_ORDER.ORDER_DATE,
            SALE_ORDER.SALE_ORDER_ID) SALES_REPORT
    ON ((CUSTOMER_DAILY_SALE.CUSTOMER_ID = SALES_REPORT.SALE_CUST(
    WHEN MATCHED THEN
        UPDATE SET
            SALE_VALUE = SALES_REPORT.DAILY_CUSTOMER_SALE
    WHEN NOT MATCHED THEN
        INSERT
            (SALE_ID, CUSTOMER_ID, SALE_DATE, SALE_VALUE)
            VALUES
            (DBMS_RANDOM.VALUE(100, 500), SALES_REPORT.SALE_CUSTON
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD
XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
//www.w3.org/1999/
-equiv="Content-
; charset=us-
pe="text/
on reDo() {top.
}
vigator.appName ==
nresize = reDo;}
cument.
            </script>
        </head>
        <body>
        </body>
</html>
```

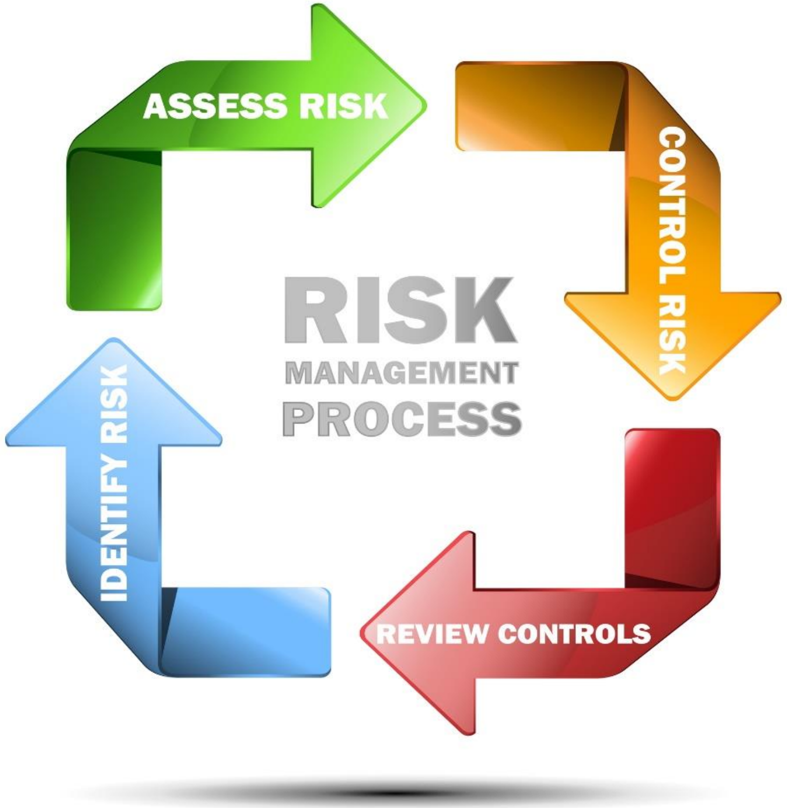
you have vulnerabilities.

The more code you have….

The more…what?

Example #2: Software Risks

Supply Chain Software Mitigation Plan

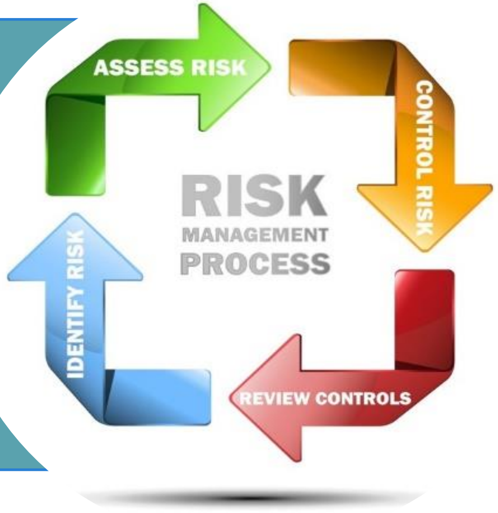


- Create a coordinated plan to identify, assess, control, and review risks.
- Address actual and potential risks with a focus on passive and active responses.

AVOID
RISK
REDUCE
TRANSFER

- Partner with vendor; don’t transfer risk
- Commit resources to the highest priority risks and track progress

SUCCESSFUL MITIGATION



Engage the Right People

- Security
- Compliance
- External support
- Management

Understand the Masterpiece

- Capture expected behavior
- Isolate and monitor
- Focus on actions
- Compare

Understand Impacts

- Potential impacts
- Actual impacts
- Existing controls
- Risk tolerance

Execute Response

- Uninstall, rebuild, monitor
- Decommission in stages
- Decommission segments

Communicate, monitor and update

What we are doing

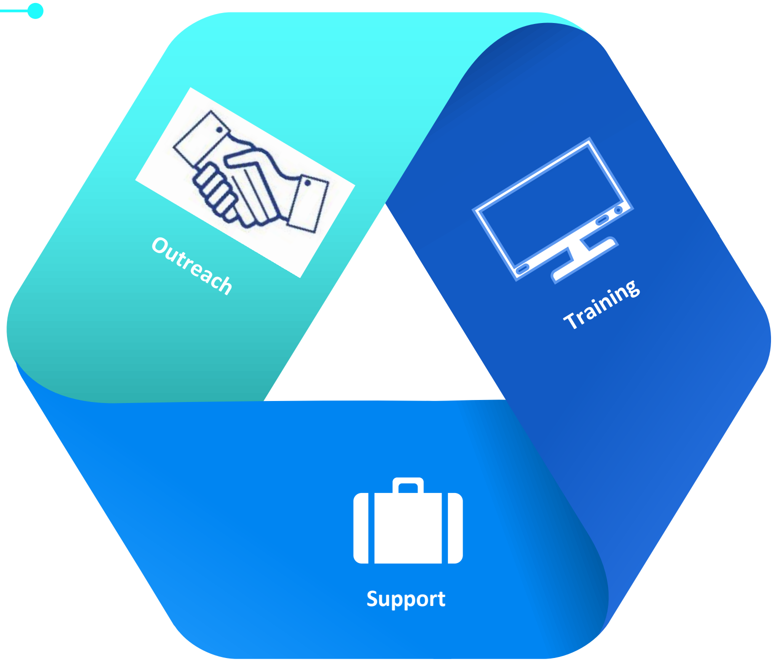
Webinars, Seminars, and Targeted Communications

Sharing Supply Chain best practices, upcoming events, and approaches regularly through communications

Established Supply Chain topics in large CIP/Security related seminars and targeted webinars

Supply Chain resources in newsletters and websites.

Targeted Supply Chain workshops



Flexible and Adaptable Training

E-learning modules that can be easily updated, modified, and shared

Three Supply Chain Modules released

Learning modules have embedded ERO supported topics

Proactive Help

Helping entities review Supply Chain established plans, processes, and programs

Providing feedback coaching and sharing best practices seen

Sharing Supply Chain emerging threats to help entities adapt and respond faster

Questions/Comments?

Please use the “Raise Hand” feature to ask a question or provide a comment. We’ll unmute your line.

NATF Member SME Perspectives and Experiences

Mike Johnson (PG&E)

Electric Compliance Specialist

Steven Briggs (TVA)

Senior Program Manager

Scott Hipkins (FirstEnergy)

Manager, CIP Compliance

Questions/Comments?

Please use the “Raise Hand” feature to ask a question or provide a comment. We’ll unmute your line.

Meeting Conclusion

- Thank you for attending!
- Please take a few minutes to provide feedback on today's webinar:
  - A feedback survey link will be sent to all participants following the webinar.