Increasing the Value Proposition:
Export and Cyber Compliance

October 11, 2018
1:00 PM – 2:00 PM ET

The Connecticut Hydrogen Fuel Cell Coalition is a proud member of FCHEA
House Keeping

All participants are in “Listen-Only” mode. Select “Use Mic & Speakers” to avoid toll charges and use your computer’s VOIP capabilities. Or select “Use Telephone” and enter your PIN onto your phone keypad.

Submit your questions at any time by typing in the Chat Box, selecting “Organizer”, and hitting Send.

This webinar is being recorded
You will find the presentations and a recording of this webinar at:

fchea.org/events/
neesc.org/events/past-events/

The Connecticut Hydrogen Fuel Cell Coalition is a proud member of FCHEA
About NEESC

• Regional Industry Cluster
• New England States, NY, and NJ
• Hydrogen, Fuel Cell, and Battery Technologies
• Businesses, Government, Service Providers, Academia
• State Roadmaps, Regional Fleet Plans, White Papers
• NEESC is administered by CCAT & Regional Partners

WWW.NEESC.ORG

The Connecticut Hydrogen Fuel Cell Coalition is a proud member of FCHEA
Today’s Moderator

Jennifer Gangi
Director of Communications and Outreach
Fuel Cell and Hydrogen Energy Association
jgangi@fchea.org

The Connecticut Hydrogen Fuel Cell Coalition is a proud member of FCHEA
About the Fuel Cell and Hydrogen Energy Association (FCHEA)

- FCHEA represents the leading companies and organizations that are advancing innovative, clean, safe, and reliable energy technologies.

- FCHEA drives support and provides a consistent industry voice to regulators and policymakers. Our educational efforts promote the environmental and economic benefits of fuel cell and hydrogen energy technologies.
Today’s Presenters

Natalie Real, **CCAT**

Greg Bugbee, **Novus Insight**

The Connecticut Hydrogen Fuel Cell Coalition is a proud member of FCHEA
Natalie Real, CCAT

Chief Administrative Officer & In-House Counsel

The Connecticut Hydrogen Fuel Cell Coalition is a proud member of FCHEA
Greg Bugbee, Novus Insight

CTO and Security Specialist

The Connecticut Hydrogen Fuel Cell Coalition is a proud member of FCHEA
CYBERSECURITY AND EXPORT CONTROL

exportcyber.ccat.us
CCAT Overview

CCAT is a dynamic and innovative applied technology organization that leads regional and national partnerships that assist global companies and the manufacturing supply chain across industry sectors to drive advancements, efficiencies and adoption of leading edge technologies.

**Mission**

Develop direct and concise strategies to advance applied technologies that drive innovative processes and value driven solutions to businesses.

**Vision**

To lead the advancement of applied technologies in manufacturing and committing to the adoption of technology developments and processes to enhance the capabilities of businesses.
Who Regulates

- **Department of Commerce (DoC)**
  - Bureau of Industry and Security
    - *Export Administration Regulations (EAR)*

- **Department of State (DOS)**
  - Directorate of Defense Trade Controls
    - *International Traffic in Arms Regulations (ITAR)*

- **Department of Treasury (DOTR)**
  - Office of Foreign Asset Control
What is Regulated

**DOC**
- Dual Use Commodities
- Software
- Data

**DOS**
- Defense Articles and Services
- Software
- Data

**DOTR**
- Embargoes
- People
- Companies

**EAR**

**ITAR**

Dual Use

Commodities

Data

Software

Companies
Essence of an Export
Transfer of an item, technology, or data to a foreign person

Examples:

**Authorized Export**
- Controlled item to foreign national with license
- Internal disclosure of controlled data to foreign national under a technology agreement
- Shipment of uncontrolled part that includes controlled technical drawings properly executed under a license authorization

**Unauthorized Export**
- Uncontrolled item to embargoed country
- Uncontrolled data to denied party
- Controlled data to foreign person without license
- Providing defense related services to foreign national without license
- Controlled shipment to foreign country without license
Costs of Non-Compliance

- Civil Penalties
- License application denial
- Jail time
- Criminal Penalties
- Debarment
- Business Reputation
- Export Violations
Enforcement Actions

2017 BIS Criminal Convictions
- Months of imprisonment
- 31 convictions

2017 BIS Criminal Fines
- $692M
- 31 convictions

2017 BIS Forfeitures
- $166M
- Value of goods forfeited

2017 BIS Administrative Penalties
- 52 cases

2018 DDTC Order
- Imposed on ONE company; $15M civil penalty and $15M suspended upon condition the funds will be used to implement a compliance program

Call me direct: Natalie Real, CCAT - 860.282.4204 | nreal@ccat.us | www.ccat.us
Reducing Your Risk
Strategy to Mitigate Internal Risks of Unauthorized Disclosure of Controlled Information

**Policies & Procedures**
01 Culture of compliance starts with Management commitment

**Digital Protection Requirements**
03 Cybersecurity

**Education**
02 Company wide training

**Physical Protection**
04 Facility Security
Export Management and Compliance Program

Management Commitment
Written policies and procedures
Ongoing training and awareness
Recordkeeping
Cyber Security
Internal audits
Responsive and transparent corrective actions
Incident Reporting

Export Compliance
Security vs. Compliance

Are you Secure and Compliant?

Greg Bugbee, CISSP
Chief Technology Officer

novusinsight.com
About Novus

40-employee, wholly-owned subsidiary of CCAT

Provider of IT, security and data services
  • Managed IT support
  • IT infrastructure hosting
  • Private cloud management
  • Cybersecurity services
  • Technology and security assessments
  • Strategic IT planning
  • Custom application development
COMPLIANCE DOES NOT EQUAL SECURITY

**Compliance:** A one-time, point-in-time demonstration that your organization meets the *minimum* requirements outlined by compliance standards.

**Security:** A framework consisting of policies, processes, and technical controls that defines how your organization stores, processes, consumes and distributes information in a way that verifiably protects it. This framework is strictly adhered to and part of the organization’s culture.

*Security will always lead to compliance.*
*Compliance will not always lead to security.*
Threat and Risk Landscape

“Compliant” companies are attacked and breached constantly.

- Target
- Equifax
- Facebook

Non-Compliance can result in:

- Regulatory fines
- Lost contracts

Lack of Security can result in:

- Lawsuits
- Brand reputation loss
- Theft of information
What Is Your Current Security Posture?

1. Not compliant with any standards, nor secure
2. Secure in a limited way, but not compliant with standards
3. Compliant with standards, but not very secure in reality
4. Secure and compliant
Think about compliance differently:

• Compliance standards are point-in-time and updated infrequently. They cannot keep pace with the changing threat landscape.

• Compliance should not be something you achieve primarily to satisfy an audit.

• Compliance is an opportunity to get things right, to implement an adaptable framework that keeps information and systems safe.
What is a Security Framework?

An information security framework is a series of documented, agreed and understood policies, procedures, and processes that define how information is managed in a business with the goal of lowering risk and vulnerability, and increasing confidence.

Security frameworks must be customized to meet business objectives and tailored to outline specific security controls and regulatory requirements. *This is your plan and not just a copy and paste of compliance standards.*
How Do I Build A Secure Framework?

1. Inventory Your Data
   • What type of data do I have?
   • Where is it stored?
   • Who has access?
   • How is data backed up? Do backup and recovery plans & controls align with my business processes?

2. Classify Your Data
   • Define appropriate categories
   • Label with tags

3. Govern Your Data
   • What are the policies and procedures for handling data?
   • What are the incident response procedures?
   • Are there retention policies and how are they enforced?
   • Are there validated, comprehensive audit logs that are easy to produce?
Basic Secure Framework Technical Controls

1. Data Loss Prevention
   • Controls the access of information based on classification

2. Network segmentation
   • Builds a wall around protected information

3. Encryption
   • Protects information at rest, in transit, and in use

4. Multi-factor authentication
   • Adds a second layer of authentication to account credentials

5. Identity and access management
   • Who has access?
   • To what data?
   • From where?

6. End-user training
   • Relevant training that is regularly validated and documented
Takeaway Points

• The Security Framework becomes a set of guidelines governing operations.

• When a system change is made, reference the framework and ask, “Is this change going to impact my security framework?” If yes, “can I accept the risk?”

• Question everything against your Security Framework. If you are not questioning vendors, customers, employees, etc., you are putting yourself at risk.

• Constantly assess your vulnerabilities and risk. Don’t rely on compliance standards to maintain security.
What are your Risks?
Lobby/Reception

Risks:
- Tours
- Unverified Visitors
- Contractors

Mitigation:
- “Clean” Tour Route
- Visitor verification system
- Badges
Human Resources

Risks:
- Hiring practices
- Misunderstanding of job assignment
- Travel

Mitigation:
- Employee verification
- Training
- Travel Policies
Information Technology

Risks:
- Unsecure networks
- Un-encrypted drives
- Lack of employee training
- Thumb drives/Flash drives
- Remote access to machines

Mitigation:
- Cybersecurity requirements (NIST 800-171)
- Implement a secure framework
- Employee training
Information Technology

NIST First 15

| 3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). |
| 3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. |
| 3.1.20 | Verify and control/limit connections to and use of external information systems. |
| 3.1.22 | Control information posted or processed on publicly accessible information systems. |
| 3.5.1 | Identify information system users, processes acting on behalf of users, or devices. |
| 3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. |
| 3.8.3 | Sanitize or destroy information system media containing CUI before disposal or release for reuse. |
| 3.10.1 | Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. |
| 3.10.3 | Escort visitors and monitor visitor activity. |
| 3.10.4 | Maintain audit logs of physical access. |
| 3.10.5 | Control and manage physical access devices. |
| 3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. |
| 3.13.5 | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. |
| 3.14.2 | Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. |
| 3.14.4 | Update malicious code protection mechanisms when new releases are available. |
| 3.14.5 | Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. |
Sales Department

Risks:
- Unauthorized transfer of controlled information
- Improper marking
- Misunderstanding of products
- Lack of knowledge of end use or end user

Mitigation:
- Export due diligence
- Implement standard markings
- Develop Product Matrix
Engineering/Quality Inspection

Risks:
- Drawings
- Unfettered access
- Unauthorized transfer of data
- Part Integrity

Mitigation:
- Document markings
- Transfer via secure network
- Red Zone designation
Shop Floor

Risks:
- Customer Access
- Equipment Maintenance
- Part Integrity
- Tours

Mitigation:
- Visitor Management
- Red Zone Designation
- Limit remote machine access
Shipping/Receiving

Risks:
- Receipt of unmarked items
- Driver access
- Improperly marked shipments
- Unverified freight forwarder
- Diversion/Unauthorized in-transit shipments

Mitigation:
- Export Due Diligence
- Visitor Management
- Zone Designation
Risks:
- External communications
- Disclosure of IP
- Disclosure of controlled information
- Trade Shows

Mitigation:
- Centralized POC for external communications
- Training
- Management review
C-Level

Risks:
- Systemic violations
- Significant fines
- Jail time
- Disclosure of company or customer IP
- Loss of Government contracts

Mitigation:
- Culture of compliance
- Dollars for training
- Increased leadership responsibility for compliance
- Ability to hire the right people
For more information:

Natalie J. Real
nreal@ccat.us
860-282-4204

Exportcyber.ccat.us

Greg Bugbee
bugbee@novusinsight.com
860-282-4200 x7041

Novusinsight.com
Questions
Thank you

Natalie J. Real, Esq.
Chief Administrative Officer, CCAT
Direct - (860) 282-4204
nreal@ccat.us

Greg Bugbee, CISSP
Chief Technology Officer, Novus Insight, Inc.
Direct - 860.282.4200 x704
gbugbee@novusinsight.com

The Connecticut Hydrogen Fuel Cell Coalition is a proud member of FCHEA