FERC Security Program Requirements and Cyber Brief

March 14, 2018

FERC Security Program Requirements and Cyber Brief

Presentation to begin at 1:35

Introduction

- D2SI Security Team
  - *Nadim Kaade, Liza Velez, and Justin Smith*
- Cyber Security Specialist
  - *Barry Kuehnle*
- DHS Special Guests

Discussion Points

- Ground rules
- DHS NCCIC Brief
- Documentation Labeling Guidelines
- Annual Security Compliance Certification Letter Template
- Field Documents – (Request for Additional Info)
- Revision 3A/3B
- Lessons Learned - 2017 Season
- Cyber Security (Barry)
- Licensee Expectation – 2018 Season
- 2018 DHS Information Sharing Drill
- Homeland Security Information Network (HSIN)
- Suspicious Activity Reporting (SARs)
- UAS at Critical Infrastructure
- Good Physical Security Practices
- Regional Office Security SMEs
- Final Thoughts

Ground Rules

- DHS ICS-CERT – 1-hr including Q&A
- FERC – 30mins with time for Q&A
- Type questions into WebEx at presentation's end

Department of Homeland Security

National Cyber Security and Communications Integration Center

Documentation Labelling

- Guidelines for the Protection of Sensitive Information
- CEII documents should be labeled on each page as:
  - Header only: **CUI//CEII**
- Privileged documents should be labeled on each page as:
  - Header only: **CUI//PRIV**
- Security Documents (SP, VA/SA, IERRR) should be labeled as:
  - Header: **CUI//CEII/PRIV**
  - Footer: **Security Sensitive Material**
- Cybersecurity Documents should be labeled as:
  - Header: **CUI//CEII/PRIV**
  - Footer: **Security Sensitive Material**

Annual Security Compliance Certification Letter Template

DRAFT Rev. – March 1, 2018

Annual Security Compliance Certification – FERC Security Program for Hydropower Projects:

Dear Mr./Ms. (Licensee),

As you are aware, the Division of Dam Safety and Inspections (D2SI) requires licensees/exemptees with Security Group 1 & 2 dams to annually certify compliance with FERC's Security Program for Hydropower Projects. With the implementation of Revision 3A, which largely incorporated Cyber Security into the Program, licensees/exemptees (regardless of security group if interconnected) that fall under the guidelines, must be in compliance for applicable cyber security measures.

As a reminder, by the end of each year, you are required to submit the annual security compliance certification letter to your designated Regional Office **via hard copy** through commercial mail carrier services (e.g. USPS/UPS/FedEx/etc.). For appropriate handling of documentation, the Division of Dam Safety and Inspections, Office of Energy Projects adheres to the FERC Guidelines for the Protection of Sensitive Information. Please note that any submission which contains **security sensitive material** including the annual security compliance certification letter, should be labeled as shown below:

Header:

CUI//CEII/PRIV

Footer:

Security Sensitive Material
Do Not Release

Attached is an annual security compliance certification letter template for your reference.

We appreciate your cooperation and your continued efforts in keeping your project secure.

Refer to the link below for additional guidance on the FERC's Hydropower Security Program:

http://www.ferc.gov/industries/hydropower/safety/guidelines/security.asp

Sincerely,

Attachment 1: Template - Annual Security Compliance Certification Letter

Security Sensitive Material

DO NOT E-FILE!

DO NOT E-FILE!

DO NOT E-FILE!

CUI//CEII/PRIV

Attachment 1

Company Name
Company Address

December 31, 20XX

Regional Engineer
FERC D2SI Regional Office
Address

Re: Annual FERC D2SI Security Compliance Certification for (List out Projects/Dams (name, number/s (dam numbers included – e.g. Any Dam 1, 0999-01-01; Any Dam 2, 0999-02-01; etc.) 20XX.

Dear Regional Engineer:

We are certifying compliance to the FERC Security Program for Hydropower Projects Revision 3A for the referenced projects above.

Each security group 1 and 2 dam has its own site specific: security plan (including the Internal Emergency Response and Rapid Recovery); vulnerability assessment (applies to Group 1 dams) security assessment (applies to group 1 and 2 dams for physical security; and group 3 dams for physical security to protect cyber assets); and cyber security requirements.

- The Security Plan for (state project/dam number) XXXX-XX-XX were reviewed and updated on XX-XX-XXXX (annual update - date should be consistent with the actual security plan).
- The Internal Emergency Response and Rapid Recovery (Group 1) for (state project/dam number) XXXX-XX-XX was/were reviewed and updated on XX-XX-XXXX (annual update - date should be consistent with the actual IERRR within the security plan).
- The Internal Emergency Response (Group 2) for (state project/dam number) XXXX-XX-XX were reviewed and updated on XX-XX-XXXX (annual update - date should be consistent with the actual IER within the security plan).
- The Vulnerability Assessment (Group 1) for (state project/dam number) XXXX-XX-XX was last re-evaluated/re-printed on XX-XX-XXXX (re-print required every 5 years). The VA was/were reviewed and updated on XX-XX-XXXX (annual update - date should be consistent with the actual date of the vulnerability assessment).
- The Security Assessment (Group 2 and/or 3 for cyber assets) for (state project/dam number) XXXX-XX-XX was last re-evaluated/re-printed on XX-XX-XXXX (re-print required every 10 years). The SA was/were reviewed and updated on XX-XX-XXXX (annual update - date should be consistent with the actual date of the security assessment).
- The security plan (Group 1) for (state project/dam number) XXXX-XX-XX was last exercised on XX-XX-XXXX (required every 5 years).

Security Sensitive Material

Field Documents

1. Complete Security Checklists (physical and cyber)
2. Provide physical security checklists to engineer
3. Provide cyber asset spreadsheet, if necessary
4. Have VA, SA, SP, IERRR, Cyber Security Checklist available for review
5. Provide 2017 Annual Certification letter for review

Revision 3A/3B Changes

- *March 2018* – New document labelling in effect – Guidelines for Protection of Sensitive Information
- New Sec. Cert. Letter Template (due 12/31 – do not e-File)
- Request for additional information (checklist/spreadsheet)

Reminder

Physical Security

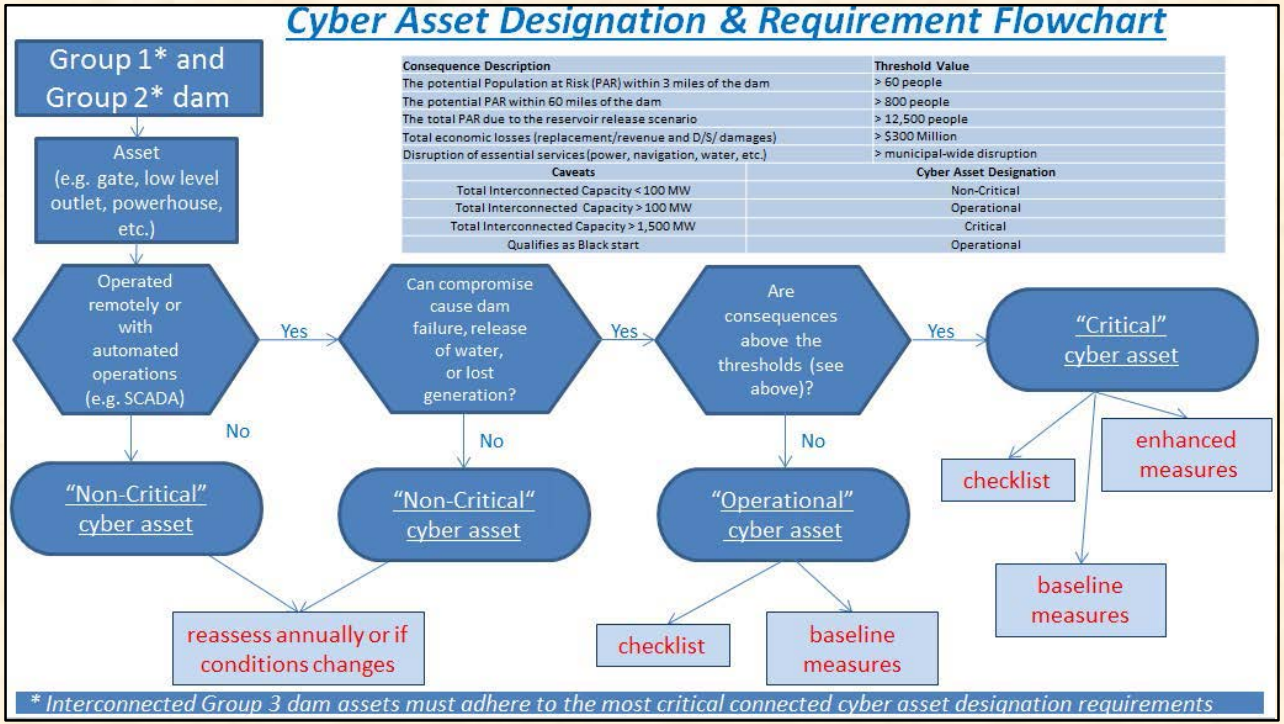
- Group 1, 2 dams:
  - National Terrorism Advisory System (Normal, Elevated, Imminent)
  - SP requirements (annual update – revision sheet)
- Group 1 dams:
  - VA requirements (5 year re-evaluation/reprint, annual update)
  - Evaluate 5 DBT for each critical asset
- Group 2 dams:
  - SA requirements (10 year re-evaluation/reprint, annual update)
  - Use of generic threat to baseline assess security

Reminder

Cyber Security

- “Baseline” or “Enhanced” cyber security measures implemented.
- Request for Extension was due by June 2017.
- Review annually for changes in connectivity.
- Keep your inventory up-to-date!

Updated Cyber Asset Designation Flowchart – Rev 3B



Consequence Description	Threshold Value
The potential Population at Risk (PAR) within 3 miles of the dam	> 60 people
The potential PAR within 60 miles of the dam	> 800 people
The total PAR due to the reservoir release scenario	> 12,500 people
Total economic losses (replacement/revenue and D/S/ damages)	> $300 Million
Disruption of essential services (power, navigation, water, etc.)	> municipal-wide disruption

Caveats	Cyber Asset Designation
Total Interconnected Capacity < 100 MW	Non-Critical
Total Interconnected Capacity > 100 MW	Operational
Total Interconnected Capacity > 1,500 MW	Critical
Qualifies as Black start	Operational

*Use this flowchart to determine whether or not you have cyber assets at your facility.

Lessons Learned – 2017 Season

- Security Documentation – Should be Prescriptive rather than Descriptive
- Complete Cyber Checklists and Cyber Asset Spreadsheet
- If NERC, Cyber Assets must be NERC regulated, not NERC criteria (unless medium/high impact criteria)
- Interconnected Facilities (Group 1, 2, and 3)
- DHS Protective Security Advisor (PSA) assessments would still need to fulfill FERC requirements
- Describe rationale for NC/Operational/Critical

OER Public Report

(Barry Kuehnle)

- https://www.ferc.gov/media/news-releases/2017/2017-4/10-06-17.asp

Licensee Expectation – 2018 Season

- Baseline/Enhanced Cyber Security Measures Fully Implemented
- FERC Hydro Security Checklist (v5)
  - Continue to complete and provide checklist (hard copy) to FERC Inspector
- NERC/D2SI assets
  - Have NERC documents and audit results/recommendations available for review
- Updated Security Documentation for Current Year

2018 DHS Information Sharing Drill

- Date: February 6 – 7, 2018, Hot Wash February 8, 2018
- Participation through HSIN and FERC
- Good number of Participation – 37 Licensees
- Strengths – Realistic (scenarios, delivery time, number of injects were appropriate, good response back from licensees)
- Weaknesses – System malfunction (HSIN, video clips), emergency teleconferences should’ve been conducted earlier
- Group 1 dams to gain credit – state on annual security compliance certification letter

Suspicious Activity Report (SAR)

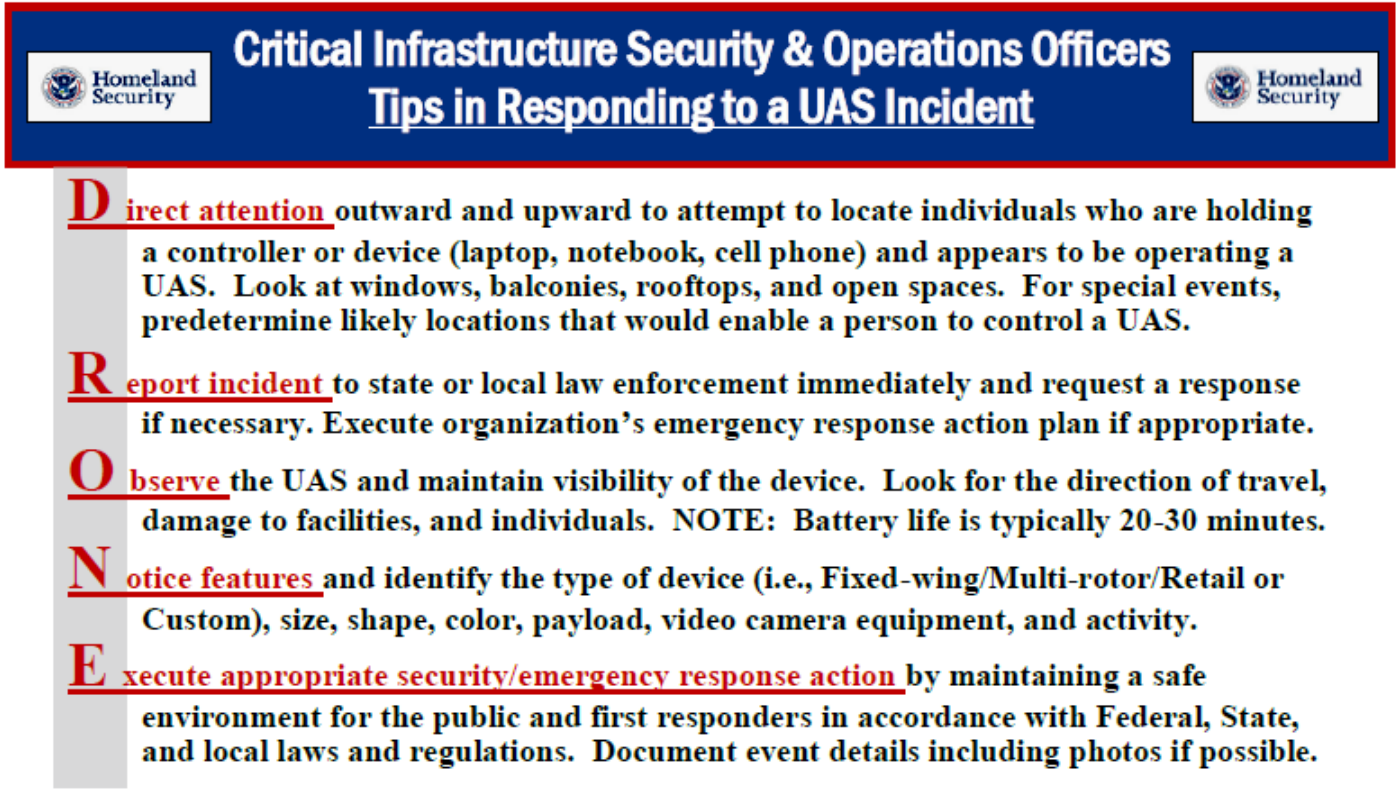
- Report All Suspicious Activities (physical and cyber) to Local, State, and Federal Law Enforcement
- Evaluate physical protection of cyber systems, also
- Complete FERC SAR form and email to your Project Engineer http://www.ferc.gov/industries/hydropower/safety/guidelines/security/security.pdf (pages 58 - 61)
- Keep track of all SARs (track history and trend)
- Report to HSIN (account required – optional, FERC can report for you)

Suspicious Activity Report (SAR)

HSIN Account Request

- Send email request to damsportal@hq.dhs.gov
- DHS will send instructions with application form
- Once approved, gain access to:
  - Free online training
  - Free security guidelines (physical and cyber)
  - Access to all SARs
  - Access to Threat Bulletins
  - Access to Information Sharing Drill

UAS at Critical Infrastructure



UAS at Critical Infrastructure

Category	Range	Payload
Retail Quadcopter 	Up to 3 Miles	0-2 lbs.
Retail or Custom Multi-rotor 	3—10 Miles	3-15 lbs.
Commercial Applications 	Varies	15-30 lbs.

INCIDENT REPORTING *QUICK* TIPS*

- Identify Operator and Witnesses *(Name & Contact Info)*
- Type of Incident *(Commercial, Hobby, Public/Governmental)*
- Type of Device (s) and UAS Registration Number
- Event Location and Incident Details *(Date, Time, and Place)*
- Evidence Collection *(Photos, Video, Device (s)*

** Always follow state and local laws and regulations.*

Homeland Security

UAS QUICK REFERENCE TIPS

https://www.dhs.gov/sites/default/files/publications/uas-ci-drone-pocket-card-112017-508.pdf

Good Physical Security Practices

- At the perimeter
  - ❑ Fence line minimum 6 ft. w/1 ft. top guard facing 45 degrees outward (industry standard)
  - ❑ No large gaps you can slip through
  - ❑ Tension wire is present & intact
  - ❑ No trees overhang or are growing into fence
  - ❑ Foliage is 10’ offset on both sides of fence
  - ❑ Gate openings can’t be pushed to create gap
  - ❑ Fence hardware intact (tact welded, etc.)

- Around the powerhouse
  - ❑ Cracked doors, windows, & roll-up bays should be protected (summer heat)
  - ❑ PLCs should have pass code or physically protected
  - ❑ Hinges inside or tack welds are best
  - ❑ Cameras/sensors inside and out
  - ❑ Roof access should be protected (locked) from inside
  - ❑ All wires should be in conduits and junction boxes locked
  - ❑ No gap to pick lock/deadbolt (susceptible to shimming, jimmying, prying, etc.)

Good Physical Security Practices

- At the spillway gates
  - Controls to motors locked
  - Power source protected
  - Maintenance hatch locked
- At all access points (e.g. road leading to dam)
  - Access Control (e.g. gates, locks, card readers, turnstiles, escorted access, etc.)
  - Cameras and/or sensors
  - Controlled access for ATVs, dirt bikes, etc.
  - Additional measures to be deployed at increased threat levels (e.g. jersey barriers, armed guards, law enforcement, etc.)
  - Pedestrian vs. vehicular traffic controlled
- Waterside of the dam (and PH) – almost always the most vulnerable
  - Boat barriers – public safety & line of demarcation
  - Controlled access to spillway/intake gate or powerhouse

Final Thoughts

- Licensee Expectations
  - Baseline/Enhanced Measures Implemented by Dec 2017
  - Complete Physical Security Checklist
  - Complete Cyber Asset Designation Spreadsheet, if necessary
  - Security Documents to be more prescriptive (DO NOT E-FILE)
- HSIN Accounts
  - Report Suspicious activity to local, state, and federal law enforcement agencies
- Document Labelling
  - CUI//CEII, CUI//PRIV, CUI//CEII/PRIV (alphabetical order)
- Group 1 participants in DHS exercise
  - State on annual security compliance
  - Remove any security info from an EAP exercise submittal

Questions?

Please complete the Survey!

(end of presentation)