FERC Security Program Requirements and Cyber Brief

March 8, 2017

Introduction

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

Discussion Points

1. Ground rules
2. DHS ICS-CERT Brief
3. Pre-Inspection Notification
4. Reminder Revision 3A
   A. History
   B. Physical Security - Minor Changes
   C. Cyber Security - Major changes
5. Lessons Learned - 2016 Season
6. Licensee Expectation - 2017 Season
7. Suspicious Activity Reporting (SARs)
8. Drones/UAS/UAV
9. Physical Security Considerations
10. Final Thoughts

Ground Rules

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

Department of Homeland Security

Industrial Control System -

Cyber Emergency Response Team

Pre-Inspection Notification

1. Complete Checklists
2. Discuss Checklists and Cyber Assets
3. Have VA, SA, SP, IERRR available
4. Provide 2016 Annual Certification letter

Reminder Revision 3A

History

- April 2015 – *Email about the draft and open comment period*
- August 2015 – *Posted Revision 3 on ferc.gov*
- September 2015 – *Notification to Licensees/Exemptees and email checklist*
- January 2016 – *Revision 3 in effect*
- March 2016 – *Revision 3A, FAQs and Cyber Security Checklist posted to ferc.gov*
- April 2016 – *Mass Mailing Completed*
- May 2016 – *FERC Security Program Webinar*
- December 2016 – *Cyber Security Checklist Should be Completed*
- December 2017 – *Cyber Security Measures Implemented*

Reminder Revision 3A

Physical Security – Minor Changes

- Group 1, 2 dams:
  - *New NTAS, National Terrorism Advisory System*
  - *SP requirements*
- Group 1 dams:
  - *VA requirements*
  - *Evaluate 5 DBT for each critical asset*
- Group 2 dams:
  - *SA requirements*
  - *Use of generic threat to baseline assess security*

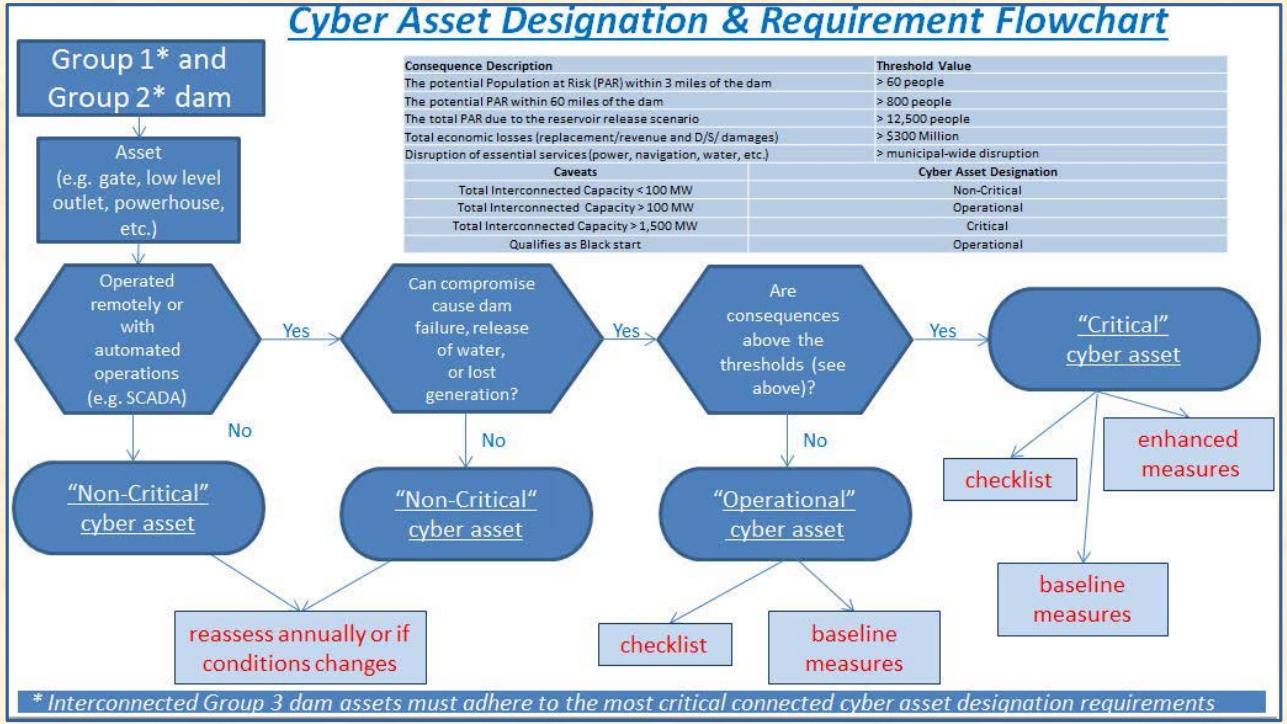
Reminder Revision 3A

Cyber Security – Major Changes

- All Group 1 & 2s determine cyber assets
- Complete the checklist, look for gaps
- “Enhanced” and/or “Baseline” measures implemented

Reminder Revision 3A

Cyber Security – Major Changes



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 – 2016 Season

- Form 3 – provide rationale
- Powerhouse Consequences - not just generation
- Cyber Asset Inventory – Licensee/Exemptee vs FERC
- If NERC–CIP → document
- USACE & BOR Projects
- Powerhouses not operated by the Licensee/Exemptee
- Group 3 Dams – MW > 100 or Black Start Capability
- Interconnected Facilities (Group 1, 2, and 3)

Licensee Expectation – 2017 Season

- Form 3 Cyber Security Checklist
- Identify all cyber assets including justifications for designations
- Address all gaps
- FERC Hydro Security Checklist (v5)
- NERC/D2SI assets
  - *Identify cyber assets (non-critical, operational, critical)*
  - *Provide NERC audit results/recommendations*
- Implement cyber & physical security measures – NLT December 2017
- EOT request hardcopy – 6 months prior (e.g. by June 2017)

Suspicious Activity Report (SAR)

- Report All Suspicious Activities (physical and cyber) to Local, State, and Federal Law Enforcement
- Evaluate physical protection of cyber systems as well
- 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

Drones/UAS/UAV

- What is the Threat*?
  - *Weaponized or Smuggling Payloads*
  - *Prohibited Surveillance and Reconnaissance*
  - *Intellectual Property Theft*
  - *Intentional Disruption or Harassment*
- Why is this **Important** for Critical Infrastructure*?
  - *Increased purchases for commercial/recreational use of drones will increase potential threats*
  - *Physical and operational characteristics of drones can often evade detection*
  - *Creates challenges for critical infrastructure community*
- What You Can Do*?
  - *Implement legally approved counter-UAS technology*
  - *Contact FAA to consider UAS restrictions near facilities*
  - *Update SP for UAS security and response strategies*
  - *Report potential threats to local law enforcement*

*As modified from DHS website.

Drones/UAS/UAV

- Helpful Resources/Contact information
  - https://www.dhs.gov/uas-ci
  - https://www.faa.gov/uas/
  - uashelp@faa.gov (email address)
  - https://www.faa.gov/uas/resources/uas_regulations_policy/media/Pages-from-PLAW-114publ190.pdf, (Page 7, Petition for Restricted Air Space – Still in the Works)
  - No Drone Zone Tool Kit

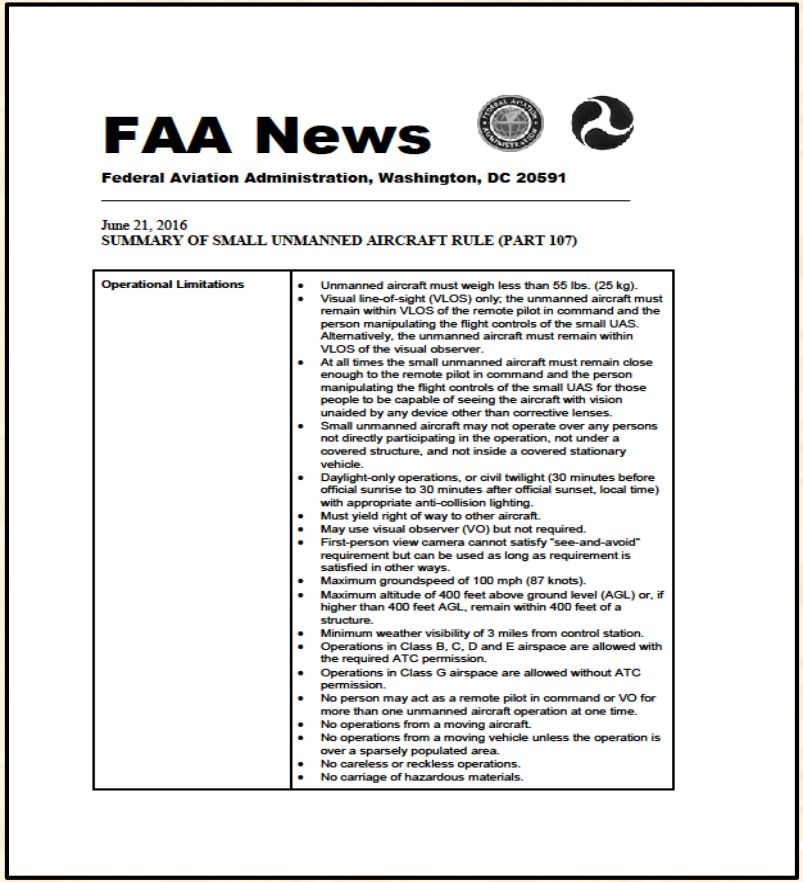
    https://www.faa.gov/uas/where_to_fly/no_drone_zone/

*No Drone Zone Tool Kit can be posted around your facility as a deterrent, however, the only way to prosecute is if the drone lands or takes off on your property (coordinate with local law enforcement). There are currently no air space regulations for critical infrastructure.

Drones/UAS/UAV

- Helpful Resources Continued
  - Summary of Small Unmanned Aircraft Rule (Part 107)

  FAA News (Link to Part 107)



FAA News

Federal Aviation Administration, Washington, DC 20591

June 21, 2016

SUMMARY OF SMALL UNMANNED AIRCRAFT RULE (PART 107)

Operational Limitations	• Unmanned aircraft must weigh less than 55 lbs. (25 kg). • Visual line-of-sight (VLOS) only; the unmanned aircraft must remain within VLOS of the remote pilot in command and the person manipulating the flight controls of the small UAS. Alternatively, the unmanned aircraft must remain within VLOS of the visual observer. • At all times the small unmanned aircraft must remain close enough to the remote pilot in command and the person manipulating the flight controls of the small UAS for those people to be capable of seeing the aircraft with vision unaided by any device other than corrective lenses. • Small unmanned aircraft may not operate over any persons not directly participating in the operation, not under a covered structure, and not inside a covered stationary vehicle. • Daylight-only operations, or civil twilight (30 minutes before official sunrise to 30 minutes after official sunset, local time) with appropriate anti-collision lighting. • Must yield right of way to other aircraft. • May use visual observer (VO) but not required. • First-person view camera cannot satisfy "see-and-avoid" requirement but can be used as long as requirement is satisfied in other ways. • Maximum groundspeed of 100 mph (87 knots). • Maximum altitude of 400 feet above ground level (AGL) or, if higher than 400 feet AGL, remain within 400 feet of a structure. • Minimum weather visibility of 3 miles from control station. • Operations in Class B, C, D and E airspace are allowed with the required ATC permission. • Operations in Class G airspace are allowed without ATC permission. • No person may act as a remote pilot in command or VO for more than one unmanned aircraft operation at one time. • No operations from a moving aircraft. • No operations from a moving vehicle unless the operation is over a sparsely populated area. • No careless or reckless operations. • No carriage of hazardous materials.

Physical Security Considerations

- 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.)

Physical Security Considerations

- 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 powerhouse)
  - Boat barriers – public safety & line of demarcation
  - Controlled access to spillway/intake gate or powerhouse

Final Thoughts

- 2017 Inspection
  - Complete checklists beforehand
  - Discuss cyber assets
  - Have all documentation available for review
- Compliant with Revision 3A by Dec. 31, 2017
- Report Suspicious Activity
- Stay informed about the FAA and Drones/UAS/UAV
- Consider Physical Security Measures
- Do Not E-File any Security Related Material, including certification letter

Questions?

Please complete the Survey!

(end of presentation)