

# SESSION 11: Conclusions, Initiatives, Tasks, Schedules

(No slides used in session 11)

## Fort Worth Workshop Notes

### Session 1

“Deputizing public” – Really means education to have them help protect. They are familiar with the project; if they see something unusual they should report it.

Had tours in the past...not any more. Note surveillance if seen.

Offer rewards to public for information (i.e. “night out”).

Production vs. security: how reconcile them?

This is a key point for the committee work; security concerns cannot interfere with operations. Budgets cannot compete. Use team approach. Separate capital funding between organizations so there is no fight. Prioritizing between equipment vs. security... how do you separate budgets? – convince management that you need upgrades, well and fine; show that security upgrades help all facilities, hydro, fossil, etc.

Remote instrumentation (critical): paid for CCTV to help monitor instruments, so production can pay for security cameras.

Background checks for employees & vendors; how enforce them? – Is part of contract & hire firms to do it. How put all the plans together, i.e. bomb threat plan, fire plan, etc. Should it be in the EAP? – Depending on the condition, some responders need information, others do not. Coordinate with the responders...what they want is what should be in the plan. Hand-deliver the revised plans to responders to be sure they are using the correct ones.

How do you define THREAT? – What is the “design threat”? – Do not address airplane or swat threat; can’t be protected. Need to define what is credible. What is the realistic level of threat? Even if you cannot stop it, look for signs and education. Refine surveillance and try to see it. Be aware of what could happen if “x” occurs. If you get warning, you can prepare, but without warning you may not be able to handle it.

What is response vs. delay time? - It depends on the site; nearly immediate to several hours.

Boat closing & recreational closures – A reservoir was completely closed off (2 years), but found a way to issue permits (with security review) to allow “cleared” recreationalists into the reservoir. If something bad does occur from this it cannot be stopped, but they weighed the risk versus the benefits of allowing boating to continue.

Does it need a license amendment? Hopefully no...

If you have a recreational concern we need to know about it. FERC is being pressured to keep recreation on going. Notify your regional office IMMEDIATELY and let us work together to resolve it. We will explain it on a site-by-site basis.

Other agencies (i.e. USACE) can deny access as needed.

### Session 2

Some docs are public that should be CEII; how resolve that? – Initial burden was on licensees, FERC will identify when possible. If you find them accessible, let FERC know and we will pull them.

The Op Inspection Reports were provided to licensees. Now need to formally request them. The PFMA docs; are they handles the same? Do they need to be formally requested? - You can request it from the FERC engineer/inspector and they have authority to provide it can be a simple email. (But it still should be a request to them.) Get an eLibrary subscription to become aware that a document was issued, and then you know you can request it.

Can copies of classification guide be provided? - Process needed “original classification authority” can be given to a federal agency; maybe to a private organization on a “need to know” basis.

### Session 3

Tasks: Agencies need to coordinate better, therefore get Hydraulic Sub committee (maybe) together with USACE/USBR/FERC to form working group to unite response and studies. So, organize a group and agree on how to meet. We can’t wait for anyone else; we must do it for ourselves. Let’s assign people to work on this.

A dam in the NW had a situation, and their coordination with USBR on same river went very well.

Needed to obtain information “in the dark” and they were able to accomplish it. It took ground work, and it helped.

SCE is working with USBR and the exercise looks good so far.

#### Session 4

Penetration analysis: there are access portals for monitoring that allows professional hackers to be able to input signals. Need proper firewall protection.

Ask vendors if they off-shore help.

Automating powerhouses: is it feasible? – Always consider failure management (what do you do IF it fails). Need back-up/contingency.

Look at 1) procedures and 2) operator training (& career paths).

Powerhouses have been automated for a long time...esp. remote locations to reduce staff. Gaining more staff may not be feasible to reduce automation. Be sure operators are training to operate in manual if necessary. Establish local manual procedures.

SCADA is technical...is there a standard for an RFP? – Probably not a standard, but there are resources...NERC is working with labs for a white paper for categorizing all risk assessment methods there are (Bob Windus, BPA with RAMs...) Need to find them, review them and find the best fit for your site. See NERC site on web.

Is there a “simple tool” out there? Can a lay person do it, only a specialist, or form a dam sector work group to study this? We need a COMMON LANGUAGE. Therefore form a working group... There is so much guidance; can it be simplified.

Would the PFMA have picked up the Ralson Afterbay situation? – No, Steve does not think so. Part of the PFMA is to recognize potential failure modes in general. Therefore it is reasonable to assume that cyber should be considered in the PFMA process. Not even sure currently how/why it happened.

Is FERC thinking of getting additional expertise? – Best is to form a working group!

The cyber world advances very quickly. How can we predict what will happen in the near future, re. obsolescence and how to address replacing human skills/training/knowledge? – This should be on everyone’s mind...where are we going and when will it end. The news is that it will never end. We are at cusp of this advance; the pendulum will swing back and forth. Will see various kinds of audits: visits from regional and state regulators and local elements. We will see more certified products along with legacy products (aging). Hardware will probably be first to be certified (ISA, maybe ES-ISAC). We will see more experts coming in. Some colleges are addressing this situation now, so the experts will come out of the woods. You will see increased sensitivity of events that will occur. You will be expected to fix it, whether you can or not. Best advice: get out in front of it before it over-runs you.

“Reliability” may be a better word to use than “Security”. This may be more acceptable to management. It is our job.

Even the “new” products have faults; need patches, need better engineering, etc. Thinking that you have a new turn-key system will solve your problems is not the solution; your cyber people need to evaluate it constantly – Bruce thinks it will get better in ten years...

NERC cyber standards: What guidelines are available to remove physical/cyber access? Is there a timeliness factor? EX: you terminate a vendor’s previous access. When do you need to change it? – If deal with vendor access &/or fire an employee (for cause) = 24 hour change; if under more favorable conditions = 7 days. (Deals in the “personnel section” section CIP-007).

Need controls to see who is calling in; verify that they are legitimate.

#### Session 5

#### Session 6A

Session 6B

Session 6C

Session 6D

Session 7

Is the CD for FEC use only? – For all to use in an emergency. Will work together to make it; both FERC and licensee. Therefore it would be for the licensees' primary use...also we will provide training for how/why to use it. It was developed from learning about shortcomings in recent events. Also need training on how best to deal with media...and LOOK GOOD.

Need a liaison established in EOC for coordination. We will get comments from licensees prior to proceeding.

What can be done to quicken response time? – In a tabletop exercise, you can juggle time element better. Was there any media response for the Boundary Dam exercise? Public response? Also what's up with the robot? – Pend Oreille Co. had media coordination...media reps could not get to the dam; kept them controlled, but allowed them to see some chrome to keep them happy. For secondary devices, they were informed to look for them (cascade attacks); even if devices go off, look for more.

What was the FBI role (strategic or tactical); who was in charge? – FBI was good at not being seen; participated in initial explosion. Pend Oreille Co was in charge.

EAP training in the 1980's (?) showed that NOAA alerts were too broad. – NOAA radio has improved dramatically in last 10-15 years...is becoming MUCH more refined. This is the only way to wake up people in middle of night. We should use a suit of methods.

What is the format for the CD data? – Need to determine that.

What are customary budgets for security? – Walt: Heard 3-5% from USBR; non-recoverable. SCL thinking that it is 0.3% or so. Have some grant money, but hard to manage it...need it obvious, but need to refine it. Ed: Money always an issue; not eligible for reimbursement, would like it. Stood up big time after 9/11; time tends to reduce urgency; maybe have doubled expenditures; they have experienced a spike of surveillance and responded as needed. Display a visible security presence.

What types of inundation maps are best to use? – Should we use multiple break scenarios, i.e. just a spillway versus the whole dam...what is most useful to use? – Communicate info to the public: should be simple. Other concern is to keep it confidential so adversary does not get it; use design basis threat that is reasonable (not a nuclear bomb, but maybe something of lesser consequence); develop inundation scenarios in response to what is reasonably expected compared to 100-500 yr flood (for example). Send this info to local government and those who only need it. These are confidential (tactical response plan specified to assumed scenarios). This allows responders to communicate.

What is schedule to develop CD – A schedule is not specified. Need data collection (work group will assist it). Within 1 year?

What would SCL do differently in exercise planning? What did AAR show? – Aware of the planning that went into it (a lot), not too much expense. The counties were the drivers, SCL followed on. AAR was done; SCL has not implemented recommendations yet; but will. Have done significant security hardening. The food was good. Employees did a good job responding; good briefing...went well. Weapons made them nervous...need to control them very well.

Ed Laatsch: have been many dam exercises; are very beneficial – do them if you can.

Were the Boundary adversaries taken alive? – The hostage taker was as polite as possible, worrying about what SWAT would do to him. Several spare pants were available. Everyone in the control room is assumed to be an adversary (concealed a/o Stockholm Syndrome).

Education of all those people responding to an emergency is essential. Hold field trips for the orientation of what the critical infrastructure is; this provides a better response. Develop relationships beforehand. Also

helps with intelligence and threat dissemination.

## Session 8

Steve Jones: Inspectors would look at training materials re operators, etc. – Has not been done yet, will it? –

Gus: Yes we need to do that, is on our radar scope. Want to develop: coordination, operating manual, and recovery work groups. We will do that this afternoon and you will assist FERC develop them.

Do any use computerized maintenance programs (preventative maintenance programs)? – AEP: no, do not use; will initiate now through “Indus” (thermal plants already); are growing. Chelan: have “CMMS” and it has been helpful in programming tasks (schedules) & be sure maintenance is done. SCL: does have “Maximo” (?).

Dominion: does have a program, plus a database reminder (work items alarm).

Incentives to employees to participate in remote site training – Utilize local sheriff; put it in a good location they want to go to...keep them happy!

Process for pre-employment screening, recurring intervals, and old time employees (for security): - Legal battles are tough (only power management & those being promoted in WA). NERC is requiring that under 1300 for ~all disciplines.

Who wants to work on Operation/maintenance plans? (Work Group Formation): “Minimum things to put into a manual”

- Chelan Co (Dan Garrison)
- Judy Schneider (Consumers Energy)
- SCL may help
- NHA will canvas members
- Ask USBR
- City of Ann Arbor (Sumedh Bahl)
- Angela Froelich (City of Escondido)

## Session 9

Just know what you need to go through after an emergency; short term/long term. Do I recover?

There is a regulation for a recovery plan (1980's) (SC order from Commissioners – Charleston/Cooper River water supply).

We do not want anything elaborate...what is being used so far, and can this be used to provide guidance to others for their assistance. Can this be outlined out?

Avista has separate plans for various contingencies (is comprehensive, but not shown to FERC...stay low).

Do we need something formatted? Do not need additional regulations. – FERC does not want a formal outline, but “suggestions for what to include” (dependent on site conditions).

(This also applies to institutional knowledge retention.)

Still need to revisit the content of the EAP.

Can it be called a “response plan” instead of recovery plan?

Joe Kick: “Mitigate/Evaluate/Formalize Response.” It took 20 months to evaluate the Michigan failure.

The level of detail will be decided by the team; not set in concrete.

Cover dam/water/generation only, or each major feature? Keep it simple.

- Ernie, Wing and Gus
- Al Hancock
- Dave Ayres
- Bernie Rasmussen

## Session 10

Insurance; premiums are high...how set w/out RA? – The probability levels we want for dams (1/million...), any sort of averaging at this level is not effective, therefore they round up to larger probabilities they are used to. But those companies have provided data to such RAs and RAs are viewed as

positive, i.e. best practice.

As dam owner, what is relative cost versus PFMA? – (USBR), RAs range from couple thousands of dollars (if properly trained). 50k to \$100k for more fully realized study. It can be more for a larger facility. ASCE: need to target what you need to address...if ask for a car, you may get a Corvair (may be ok, but what do you want?) If you anticipate a highly-contentious situation, you need more detail.

Scope should be driven by level of defensibility required.

How can RA be plugged into regulatory framework? (need a bar to reach) – Martin thinks that there are levels of risk that are acceptable, i.e. safety goal associated with safety standards. It can be done, but what FERC does needs to be addressed. Don't deal w/ performance goal; deal with risk-based versus risk-informed; used as a guideline for political/economical/environmental realm. "Risk-informed regulation" for decision making based on risk. D. Bowles: we do not recommend throwing away traditional approaches, but rather put dams on common playing field that public can identify with.

USBR needed to establish a guideline for public protection (based on what others did previously); may change, but it allowed them to start.

How can another fed agency promote guidelines, either higher or lower than established by others? – Hard to say, but coordination is needed. Self-regulatory is different from outside regulation;

WORD FROM GUS: FERC had a training class for FERC (36 people sent). Need to decide when to use RA. We have consulted with USBR; we are learning and we are helping them straighten out. USACE is working towards RA too. Feds need to go through OMB for funding, so need to do similar things. We and licensees have been doing RA to some sort or another already. We have some projects that are not "up to standard" but we have used risk to allow an educated analysis to proceed. Even factors of safety are a form of RA... It will be a long way before we ask licensees to do RA. Pacific NW earthquakes are an issue to discuss. PMFs & PMPs are also changing, and risk may be appropriate. ICODS has a subcommittee on RA. Let's see what others are doing.

If a company does not meet standards, might FERC allow RA to adjust? – FERC may look at this in the future, but we will not ask licensee to do it. If licensee proposes this, we will entertain it.

USSD Conference: June in Salt Lake. Will have a Wed session of RA; Thursday will provide a management with risk. We will have PFMA, USBR performance program, potential failure modes, linking PFMA to instrumentation, collection of instrumentation data, benefits of auto instrumentation collection, special inspections, etc. PLUS, we will have status reports from the groups established here!!!!

END OF WORKSHOP