1.5.1.601– Hydropower Fleet Cybersecurity Response and Recovery Guide

Darlene Thorsen
Senior Cybersecurity Analyst
Pacific Northwest National Laboratory

Darlene.Thorsen@pnnl.gov

Marie Whyatt
Senior Cybersecurity Engineer
Marie.Whyatt@pnnl.gov

Project Overview

Project Summary

- This project built the Department of Energy (DOE) Water Power Technologies Office's (WPTO) Cyber Response & Recovery Flipbook. This handy tool assists plant operators in detecting anomalous cyber activities, defending against those adverse actions, and recovering quickly. It includes step by step actions to quickly recover the plant's operation and includes information on regulatory requirements, organizations that can assist, and websites that can be used in the recovery process.

.

Intended Outcomes

- An easy-to-use guide that color codes actions, defines actors for each action, and includes hyperlinks to appropriate websites to assist in recovering from a cyber incident on a hydropower plant.
- The tool aligns cybersecurity steps from the National Institute of Standards & Technology (NIST) Incident Handling Guide 800-61r2, to the steps in emergency response defined by Federal Emergency Management Agency (FEMA) 64 Federal Guidelines for Dam Safety: Emergency Action Planning for Dams. It also appropriately references other agencies and requirements throughout the recovery process.

Project Information

Principal Investigator(s)

- Marie Whyatt

Project Partners/Subs

- FEMA Dam Safety
- DOE Cybersecurity, Energy Security, and Emergency Response (CESER) Infrastructure Security and Energy Restoration (ISER) Division

Project Status

Completed

Project Duration

- Project Start Date: Sept 24, 2019
- Project End Date Sept 30, 2020

Total Costed (FY19–FY21)

- $300,000.

Project Objectives:

Relevance to WPTO Program Goal:

- Create cybersecurity tools and studies to articulate the cybersecurity target, risk, and recovery landscape
  - Awareness of the cybersecurity landscape for hydro by operators and policy makers.

A Cyber Incident on a Hydropower Plant can Affect a LOT!

A Hydropower Cyber Incident can affect:

- Public Safety
- Critical Infrastructure
- Energy distribution on the grid
- Cyber systems
- Unforeseen events

Multiple Organizations are Helping Mitigate Cyber Risks

Department of Homeland Security
CISA

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Department of Energy

CIS. Center for Internet Security®

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

DHS Federal Emergency Management Association

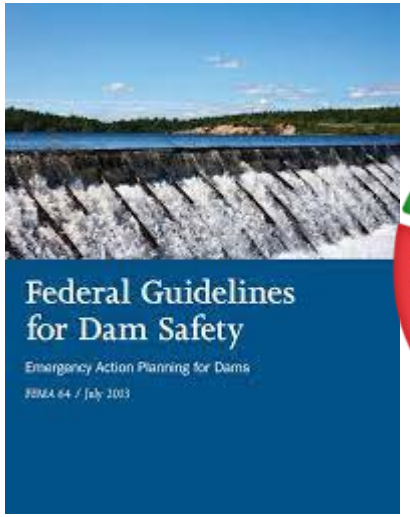
Federal Bureau of Investigation

Federal Energy Regulatory Commission

ESCC
Electricity Subsector Coordinating Council

FEMA NDSP
FEMA National Dam Safety Program

Which Tool to Use and When



FEMA 64 Federal Guidelines for Dam Safety

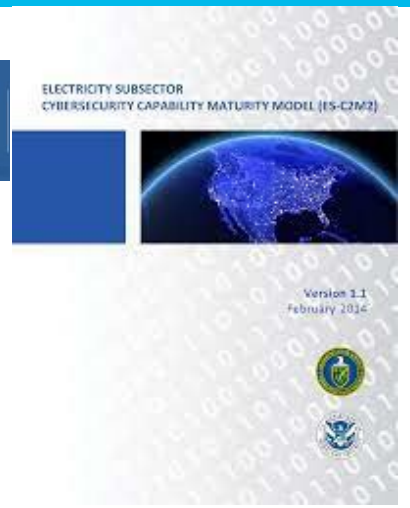
NIST Cybersecuritv Framework (CSF)

ESCC

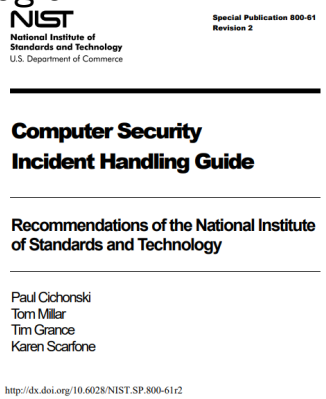
Electricity Subsector Coordinating Council

ESCC Mutual Assistance Program

Presidential Policy Directive United States Cyber Incident Coordination



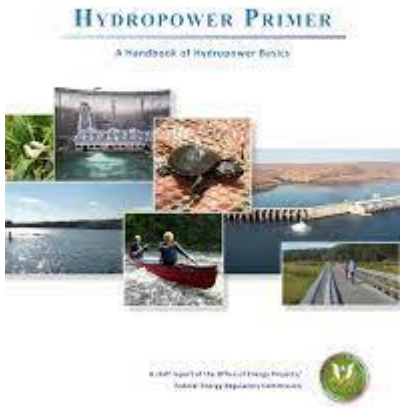
Electrical Sector-Cybersecurity Capability Maturity Model (ES-C2M2



NIST Computer Incident Handling Guide

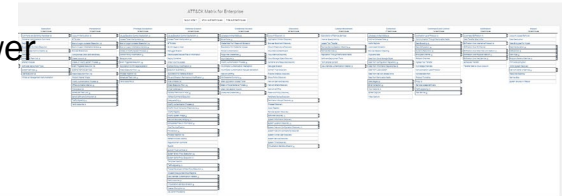
American Public Power Association

NERC CIP V5



FERC Hydropower Primer

CISA Incident Reporting

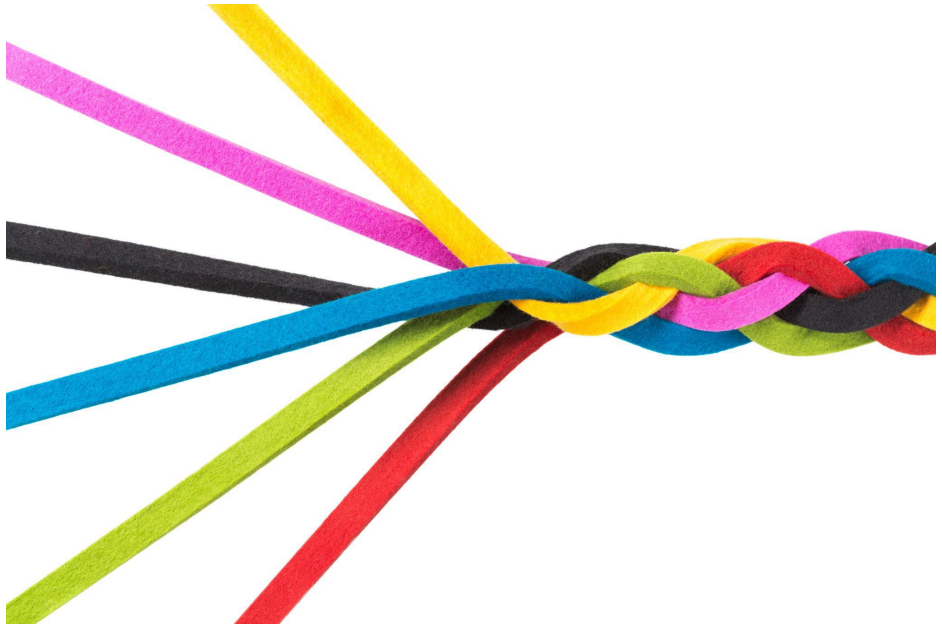


MITRE ATT&CK

Project Objectives: Approach

Approach:

- We integrated resources from:
  - Best practice cyber tools
  - Established emergency response recovery tools
  - Hydro policy resources
  - Energy sector industry assistance



- To deliver an easy step-by-step process for a hydropower operator to QUICKLY recover from a cyber incident.

Project Objectives: Expected Outputs and Intended Outcomes

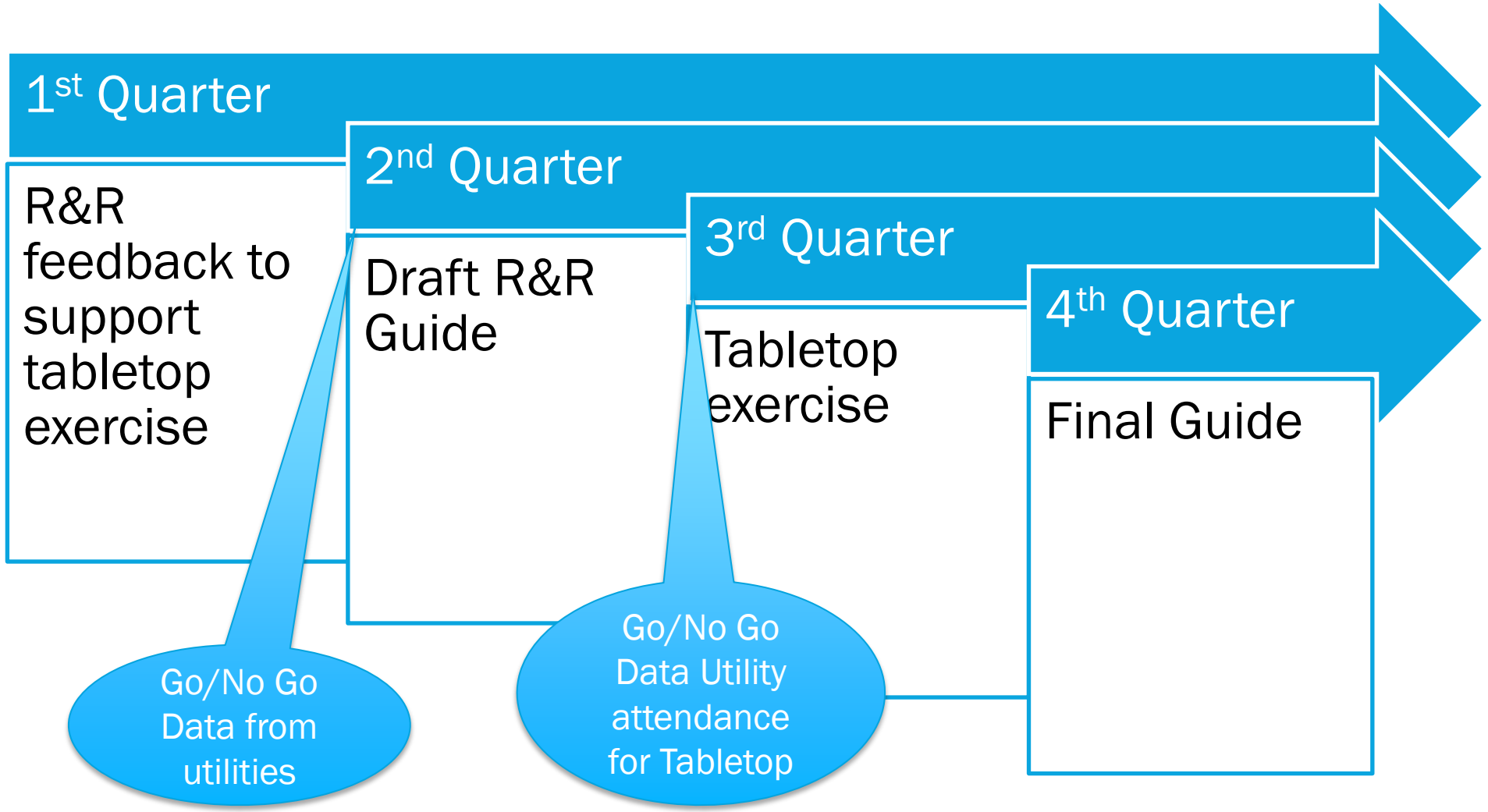
Outputs:

- An easy-to-use reference flip-book for hydropower plant operators to use during a cyber emergency.
- A hyperlinked reference library of online sources of cyber, emergency response, and regulatory requirements for the hydropower sector.
- An integration of NIST cyber recovery steps and the steps of FEMA 64 Federal Guidelines for Dam Safety: Emergency Action Planning for Dam Owners.
- A report detailing the project's research methods.

Outcomes:

- Common usage of the flip-book across small to moderate hydropower plants as they prepare to respond and recovery from a cyber incident.
- Engagement of common response and recovery language, risk measurements, and processes across federal agencies.

Project Timeline FY 2019



Project Budget

Total Project Budget – Award Information		
DOE	Cost-share	Total
$300K	$0K	$300K

FY19	FY20	FY21	Total Actual Costs FY19–FY21
Costed	Costed	Costed	Total Costed
$300K	$0K	$0K	$300K

- This project relied on assistance from hydropower plants and energy organizations. However, COVID occurred which transitioned the tabletop exercise to a telecom with Infrastructure Protection & Security Group of the Centre for Energy Advancement through Technological Innovation International.

End-User Engagement and Dissemination

- Presented the project efforts and organizational review to:
  - Northwest Hydroelectric Association's Annual Conference
  - Portland Chapter of Women in Hydropower
  - Infrastructure Protection & Security Group of the Centre for Energy Advancement through Technological Innovation International
- Presented the project efforts and validated the steps with:
  - Federal Energy Regulatory Commission (FERC)
  - Washington State Grant County Public Utilities District
  - DOE Cybersecurity, Energy Security, and Emergency Response (CESER)
- Validated industry need by engaging hydropower organizations.
- Validated alignment with cyber incident notification requirements and energy incident response requirements with ongoing federal engagement.
- Expected to exercise the tool in Clear Path X.

Performance: Accomplishments and Progress

- This effort brings all the complex resources together in a color-coded, easily referenced, and consistently formatted flip book for operators of hydropower plants.
  - As cyber attacks grow against critical infrastructure organizations, not all attacks will be deterred. It is critical to enhance how we respond to cyber incidents to minimize the loss and destruction, mitigate the weakness exploited by the attack, and restore the business quickly. (NIST 800.61r2)

Performance: Accomplishments and Progress (cont.)

Selected for the Office of Energy Efficiency & Renewable Energy Year End Success Story in 2020.

Future Work

- If funded, the tool will be validated and updated during the Department of Energy's Clear Path X exercise.

Q&A