Pacific Northwest
NATIONAL LABORATORY

PNNL-30593

Hydroelectric Cybersecurity Response and Recovery Overview

Technical Report

September 2020

Darlene E Thorsen
Marie V Wyatt
Mark Watson
A David McKinnon
Angela C Dalton
Jordan D Seaman

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

PNNL-30593

Hydroelectric Cybersecurity Response and Recovery Overview

Technical Report

September 2020

Darlene E Thorsen
Marie V Wyatt
Mark Watson
A David McKinnon
Angela C Dalton
Jordan D Seaman

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

Protecting hydroelectric plants from incidents that adversely impact their cyber-physical systems presents unique challenges due to the widely dispersed geographic locations and varied plant configurations as well as the relative nascent nature of the cyberattacks targeting these facilities. To help hydroelectric plants better respond to and mitigate cybersecurity incidents, this report documents the work by delivering a set of products broadly applicable to cybersecurity response and recovery (R&R) plan design. Delivered with this report are three additional products, including:

- Department of Energy Water Power Technologies Office Cyber Response & Recovery Flipbook to be used at hydroelectric plants to quickly respond to an anomalous event.
- A quick reference guide, *WPTO Response Alignment,* that lines up the cyber processes within the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide against the Emergency action planning steps in the *Federal Guidelines for Dam Safety: Emergency Action Planning for Dams (FEMA 64).* This guide is used as a reference to understand how a computer incident handling checklist aligns to an emergency action plan process.
- An overall hyperlinked list of publicly available hydroelectric plant references, *WPTO Resources: Dam Sector*, to be used by hydroelectric plants for additional guidance.

While these products are valuable to all types of hydroelectric plants, there is a focus on smaller plants that do not have resources to stand up a robust R&R process or team. This R&R plan integrates with the NIST Cybersecurity Framework and pertinent Department of Homeland Security emergency action planning information into a cohesive process guide to inform the development of an R&R process rather than developing novel guidance itself. The R&R process not only delineates plant operator actions in direct response to the incidents, but also offers recommendations to engage an internal cyber incidence response team and/or federal, state, and other agencies as the potential for incident escalation changes. By enabling hydroelectric plants to competently and effectively respond to and recover from cybersecurity incidents, this R&R plan makes an important contribution to the security and resiliency of the nation's critical infrastructure and energy. Hydroelectric plant owners are encouraged to tailor the R&R plan to account for their unique organizational and operational contexts to better manage the plants' future cyber-physical security and operational continuity.

Acknowledgments

The Pacific Northwest National Laboratory project team gratefully acknowledges the guidance and assistance provided by Dr. Mark Christian, U.S. Department of Energy (DOE) Water Power Technologies Office (WPTO) technology manager. We appreciate the guidance and extensive assistance from those we interviewed during this process to include the Federal Energy Regulatory Commission including Mr. Rui Li, Mr. Solomon Karchefsky, and Ms. Liza Velez; the DOE Cybersecurity, Energy Security, and Emergency Response office to include Mr. Fowad Muneer, Mr. Matthew Tarduogno, and Mr. Brian Marko; and the Washington State Grant County Public Utilities District to include Mr. Greg Keyes. We also presented our work for review to the following events: Portland Chapter of Women in Hydropower including Ms. Brenna Vaughn, the Northwest Hydroelectric Association's Annual Conference, and the Infrastructure Protection & Security Group of the Centre for Energy Advancement through Technological Innovation International including Mr. Don Burlack. We also thank Mr. Paul Boyd, Mr. James O'Brien, and Ms. Alison Colotelo of PNNL for their helpful input. The accuracy of the information and the views presented in this report are the responsibility of the authors and do not necessarily represent the opinion of the DOE WPTO or other individuals or organizations.

Special thanks to the American Public Power Association and its members, and to the Nexight group for their work, *Public Power Cyber Incident Response Playbook*. This report both provided technical reference and validation of the work in the DOE WPTO Cyber Response & Recovery Flipbook.

Acronyms and Abbreviations

BES	Bulk Electric System
CISA	Cybersecurity and Infrastructure Security Agency
CSF	Cybersecurity Framework
DHS	Department of Homeland Security
DOE	U.S. Department of Energy
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FSLTT	Federal, State, Local, Tribal, and Territorial Agencies
HSIN-CI	Homeland Security Information Network - Critical Infrastructure
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
OE	Office of Energy
R&R	Response and Recovery
SCADA	Supervisory Control And Data Acquisition
WPTO	Water Power Technologies Office

Contents

Figures

1.0 Introduction

As our nation's hydroelectric industry modernizes, the systems that control and maintain this critical infrastructure are correspondingly evolving. Hydroelectric plants that were previously controlled by physical systems have now been upgraded with electronic controls that manage the generators, turbines, penstocks, gates, and other components either remotely or on site. With this evolution, simple manual systems that were initially isolated and unconnected to other electronic systems are now fully integrated cyber-physical components that can be complex to recover if anomalous actions were to affect the plant.

With the integration of these systems, the cybersecurity guidance and frameworks to assist the hydroelectric industry have also expanded. Across all federal agencies, the Department of Homeland Security (DHS) serves as the Dams Sector-Specific Agency. The DHS Office of Infrastructure Protection leads a coordinated national program to reduce risks to the nation's critical infrastructure, including dams, posed by acts of terrorism. Under DHS, the Federal Emergency Management Agency (FEMA) administers the National Dam Safety Organization, which coordinates all federal dam safety programs and assists states in improving their dam safety regulatory programs. Additional cybersecurity guidance and frameworks through DHS, the National Dam Safety Organization, and the National Institute of Standards and Technology (NIST) are discussed in further detail below. Each of these organizations and many others have extensive information to assist the sector in the different facets of the incident response and recovery (R&R) process; however, depending on the organization, many of these resources are difficult to identify (e.g., location and accessibility) and difficult to understand how they might be applied during a cyber incident that affects the cyber systems, cyber-physical components of a plant, and safety-critical aspects of a facility. This work along with three additional hydroelectric plant R&R products stitch together these resources into an easier-to-understand process with linkages to appropriate external resources throughout the R&R process.

Three products this paper addresses:

- Department of Energy (DOE) Water Power Technologies Office (WPTO) Cyber Response & Recovery Flipbook to be used at hydroelectric plants to quickly respond to an anomalous event.
- A quick reference guide, *WPTO Response Alignment,* that lines up the cyber processes within the NIST Computer Security Incident Handling Guide against the Emergency action steps in the *Federal Guidelines for Dam Safety: Emergency Action Planning for Dams (FEMA 64)* to be used as a reference for hydroelectric owners and operators to understand how a computer incident handling checklist aligns to an emergency action plan process.
- An overall hyperlinked list of publicly available hydroelectric plant references, *WPTO Resources: Dam Sector*, to be used by hydroelectric plants for additional guidance.

Assembling these sources into a cohesive set of products becomes more critical as the expansion of inadvertent actions and nefarious actors threaten plants with a wide range of malicious activity. From a small event noticed by an operator, to an incident such as exfiltration of business sensitive data, to the degradation of system performance, to the threat of a crisis with the potential for devastating effects of a plant failure, a cyber attack can potentially impact business operations, energy generation, or the networked systems connected to a hydroelectric plant. As we experienced in 2013 when cyber criminals infiltrated a hydroelectric facility in Westchester County, NY, threat actors are poised to affect hydropower systems (York, 2016). In

this example the attack was not successful; however, even during small events that do not pose a risk to normal business operations, an operator needs to respond to and recover from the event appropriately. For all events and incidents, both successfully deterred and those not thwarted, a clear process flow with alignment to appropriate agencies and organizations can help a facility better respond to and recover from cyber attacks.

For asset owners/operators, federal, state, local, tribal, territorial agencies (FSLTT), industry organizations, and commercial entities, an R&R process flow provides an overarching guide to assist during the potentially confusing process of ensuring unusual cyber events and incidents are handled and mitigated appropriately. A simple and easy-to-use process flow can help a hydroelectric organization during the highly fluid period of a cyber incident where effective and timely decisions have the potential to save human lives and critical infrastructure. This guidance also has the potential to be used in a similar fashion for navigation locks, levees, dikes, hurricane barriers, or industrial waste owners. This resource guidance can also be used to ensure that an organization knows reporting obligations during an event, what references are available and establishes a proposed integration of cyber R&R steps into the FEMA Emergency Action Plans.

1.1 Background and Significance

In 2019 hydroelectric plants were considered the second largest renewable energy resource in the United States and they continued to play a vital role in the nation's irrigation, flood control, recreation, and municipal water supply (EIA, 2020) (FERC, 2017). Given their importance in our nation's critical infrastructure, there is a large number of agencies, organizations, and commercial entities concerned for safe and reliable operation, the integration of energy generation into the larger energy grid, and hydroelectric's place as a critical infrastructure component (FERC, 2020). During a cyber attack on a hydroelectric plant, this broad community can include plant owners, regulatory agencies, the emergency response community, energy grid organizations, and FSLTT organizations who all have interest in the safety of the plant (FERC, 2020). Integrating all these organizational needs, their guidance, and which resource is referenced during a plant's recovery is a complex and confusing process for a hydroelectric organization.

While the nation's approximate 2,400 hydroelectric plants generate energy, they have a significant range of power generation capacities, ownership resources, and regulatory requirements that can affect how a plant responds to a cyber incident (DOE, 2020). For each grouping of plants, there are different laws, regulations, and guidance applied. While some might have the benefit of strong cybersecurity oversight or guidance, others might not have the resources to stand up a robust cybersecurity process or team. In order to be efficient, this R&R guidance will not repeat established cybersecurity policy, frameworks, or guidance, but will focus on linking existing guidance into a process flow to assist those organizations who have limited cybersecurity R&R expertise.

This R&R process addresses the cyber component of a facility and the recovery of key components of a digitally managed hydroelectric plant such as the turbine-generator power train and spill gates. Included with those steps are the available external notification and assistance opportunities appropriately integrated throughout. The common components of a hydroelectric plant include the dam, powerhouse, water conveyance mechanisms, mechanical systems, electrical systems, and controls, some of which can be managed manually or digitally. Electronically controlled plants can include supervisory control and data acquisition (SCADA) systems, analog and/or digital devices, an onsite control system and/or a distributed control

system that is managed off site, a human-machine interface, and a communication network that connects them all. There are many variants of these computerized systems and configurations; however, common among all of them are the computerized network and the cyber-physical components of the two primary elements of a hydroelectric plant: the water conveyance mechanisms and the turbine-generation powertrain. The other non-electronically controlled components (e.g., reservoir, tailrace, transmission lines, broader grid) are not within the scope of this work.

1.2 Structure of the Report

In order to ensure a robust R&R process for hydroelectric plants the team reviewed over 50 separate products published by FSLTT, hydroelectric sector organizations, industrial control systems organizations, cybersecurity organizations, and R&R experts. Section 3.1 describes the technical approach we used in identifying, characterizing, and evaluating R&R process tools, frameworks, and governmental guidance for three components of the hydroelectric plant recovery process: the cyber R&R, emergency response R&R, and the integration of the two. In Section 3.3 we report findings of the analysis and focus on providing additional details about the frameworks we chose to base our R&R process on. In Section 4.0 we illustrate the alignment between this guidance and the larger cyber incident recovery landscape. Namely this includes the *National Institute of Science and Technology (NIST) SP* 800-61r2 *Computer Security Incident Handling Guide* and *Federal Guidelines for Dam Safety: Emergency Action Planning for Dams (FEMA 64).* These documents provide guidance to understand how a computer incident handling checklist aligns to an emergency action plan process—both identify how the integration of a cybersecurity incident fits within the larger emergency response action plan. Finally in Section 5.0 we conclude by summarizing the findings and next steps.

2.0 Cybersecurity and Hydroelectric Plants

2.1 Overview of Hydroelectric Plants

Hydroelectric plants generate power by the flow of water through the turbine to spin a generator that produces electricity. While the plant has physical components that include civil works, reservoir, tailrace, roads, fish passage facilities, and transmission lines—which all play a part in an efficient plant—the cyber-physical key components of the turbine-generator power train and spill gates are of particular concern during a cyber attack. These two components are typically controlled by a SCADA system either using analog and/or digital network communication and are at risk of unauthorized alteration during a cyber attack. This R&R process flow specifically addresses only hydroelectric plants that are digitally controlled.

The boundary of the hydroelectric system included in this R&R process addresses all the components that control the cyber-physical components of a plant. For those plants that are remotely managed through wireless, internet, or satellite communication, or those managed on site, recovering from a cyber attack can mean recovering the computer systems as well as the SCADA systems in a cloud or remote location as graphically described in Figure 2.1.

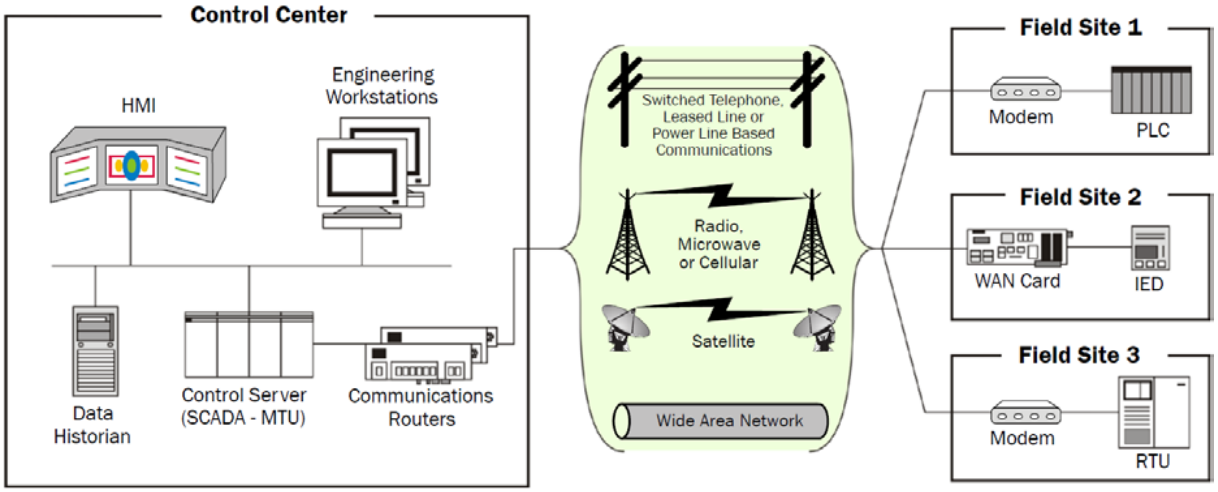

Figure 2.1. SCADA System General Layout (DHS Dam Safety, 2015)

For the nation's hydroelectric plant owners there are many variants of how they manage cybersecurity. In the case of larger plants, the resources available to protect and defend against a cyber attack can easily surpass the financial constraints of a smaller, less resourced plant.

Plants owned by FSLTTs or large commercial entities have requirements and regulations that provide some impetus to prepare for and respond to potential cyber attacks. Entities that are required to adhere to the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) cyber incident report, a DOE electronic disturbance event report, an Office of Energy (OE) 417 report, a Public Utility Commission requirement, or a Department of the Army U.S. Army Corps of Engineers Critical Infrastructure Cybersecurity Mandatory Center of Expertise regulation, can find cybersecurity R&R assistance in their regulatory or organizational requirements (NERC, 2018) (USACE, 2019) (DOE, 2018). However for smaller organizations with limited resources, there remains no clear R&R roadmap to guide recovery in the heat of the moment during a cyber incident.

As we just defined, financially resourced plants with larger generation, and those owned by FSLTTs probably have some cybersecurity guidance available. Of those remaining, about 10% of the total number are owned by federal organizations, while public owned plants comprise about 24% of all plants. This leaves the largest percentage of 63% to investor owned utilities and independent power producers. Though this group has the greatest number of plants numerically, they only produce 25% of the nation's capacity and are within the group of 1,640 plants that generate less than 10MW (DOE, 2016). It is these organizations, the smaller producers, the less resourced, and those that might not have extensive cyber experience that can use some assistance in efficiently responding to and recovering from a cyber incident, and which is the target user for this paper.

2.2 Overview of Hydroelectric Plant Cybersecurity

Within electronic systems an abnormal process can signal a cyber attack; however, deciphering when something is unusual and the effects of a nefarious actor can be difficult to pinpoint. In this area we rely on NIST, which defines "event" as any observable occurrence in an information system. Events can include a firewall that is misconfigured and is blocking network traffic, or a turbine that is unresponsive to operator controls. These types of events occur often and are most likely remedied by simple computer management methods.

However, for a more adverse cyber event, NIST's Special Publication Computer Security Incident Handling Guide defines an "adverse event" as having negative consequences that can trigger a cyber incident (NIST, 2012). Examples of these kinds of adverse events include unauthorized access that installs malware which will likely result in a negative consequence. However, an adverse event does not include unauthorized access that does not necessarily result in negative consequences but is still concerning to a plant operator. For these events NIST uses the term *incident* which is a "violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." The combination of both an adverse event (one that causes harm) and a security incident (a violation of policies or standard security practices) is how this work defines the initiation of a cyber attack.

During the lifecycle of a cyber attack, a threat actor goes through several steps prior to causing or affecting the safe and reliable operation of a hydroelectric plant. Lockheed Martin defined these steps as the "kill chain", referenced in Figure 2.2, to separate activities in preparation for, during, and after a nefarious actor's inappropriate use of electronic systems (Lockheed Martin, 2011). The adversary's steps include preparing for an attack, exploiting their vulnerabilities, and maintaining ongoing or long-term access to a system. Throughout this kill chain lifecycle, a plant operator can detect anomalous activity, defend against that activity, and recover from the effects of any unauthorized actions on their electronic systems. Irrespective of when a hydroelectric plant notices a cyber attack, this work will assist an operator in initiating a response.

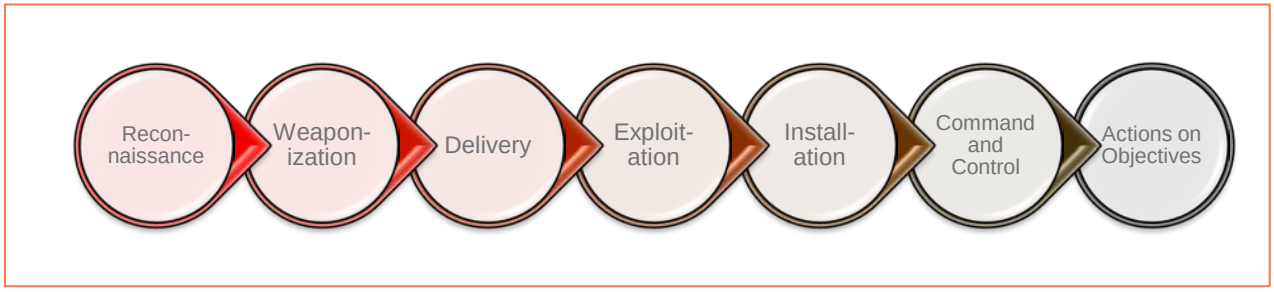

Figure 2.2. Lockheed Martin Kill Chain

3.0 Resource Evaluation

This section includes a review of available industry experts and guidance, and federally available resources to determine a process flow applicable for hydroelectric plants across the United States.

3.1 Resource Overview

During the development of the R&R guidance, the team relied heavily on industry member interviews, site visits, meetings with industry groups, and extensive analysis of existing and emerging cybersecurity policies, guidance, and industry group informational resources. For this work we met with federal organizations to include the Federal Energy Regulatory Commission (FERC) Division of Dam Safety and Inspections and DOE's Cybersecurity, Energy Security, and Emergency Response office as well as international and U.S. based industry organizations, working groups, and conferences to vet both the concept and proposed process flow.

During this process we reviewed over 62 publicly available resources addressing cybersecurity R&R guidance, emergency response, plant safety, and those that merged the three concentrations. A list of those resources can be found in Appendix A. We found that there are three main components of responding to and recovering from a cyber event for a hydroelectric plant: 1) those that focus on the safety critical aspect of the recovery process; 2) those that focus on the emergency that could be caused by a plant degradation or failure; and 3) those that focus on the cyber or electronic system recovery process.

During this review process we found that for the 52% of federally owned plants including the U.S. Army Corps of Engineers, Bureau of Reclamation, Tennessee Valley Authority, Bureau of Indian Affairs, and the International Boundary and Water Commission, these plants are required to follow the NIST criteria to mitigate cybersecurity risks based on the 2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (Office of Inspector General, 2018). In addition, they rely on their agencies' charters and applicable federal laws and treaties to provide guidance as the Foundation for Water & Energy Education and FERC defines (FWEE, 2020) (FERC, 2017).

The remainder, or non-federally owned, 2,500-plus plants fall under FERC regulation and must adhere to other pertinent federal laws and regulations (FERC, 2017). Within this group the NERC CIP applies cybersecurity controls to appropriate Bulk Electric System (BES) facilities, dams, and water facilities (Dressel, 2014). Smaller plants, those that operate at voltages of less than 100 kV, are not subject to NERC CIP requirements. We found little regulation requiring small, non-BES plants to address cybersecurity or a cyber incident. Though these plants might not have the requirement to formalize an R&R process, they remain a critical risk for our nation due to the integrated nature of our energy grid and the safety critical physical component of the dam within the surrounding community (DHS Dam Safety, 2015).

For these non-federal, non-NERC CIP requirement hydroelectric plants, an R&R process flow will assist an operator in quickly responding to a cyber event while being cognizant of the availability of external assistance if the need arises.

3.2 Resource Groupings

Due to the extensive set of resources available, the team binned resources into general groupings based on the intent of the author or organization. Though somewhat vague in description, we defined four general areas of concerns for these documents: 1) those concerned about the safety of the physical plant itself and its operations; 2) those concerned about the FSLTTs organized emergency response; 3) those concerned about the computer or cyber components of a plant; and 4) resources we found that integrated two or more of the concerns into Other Resources. We address each grouping below. In addition, we provide a number of pertinent resources in Appendix A.

3.2.1 Safety Critical Resources

In the first area of concern we looked at federal guidance. The DHS Office of Infrastructure Protection is primarily responsible for dam critical infrastructure protection since it is designated as the dam sector-specific agency under the Presidential Policy Directive 21 (CISA, 2015). From this office we evaluated their website, Homeland Security Information Network - Critical Infrastructure (HSIN-CI) Dams Portal. This website contains a number of sensitive documents and has numerous unclassified publications, 11 of which are referenced in Appendix A (CISA, 2020).

In addition to the secure website HSIN-CI, the Office of Infrastructure Protection also has publicly available documents that discuss the dam sector, securing the dam, and information on a cyber incident that causes the degradation or failure of the plant operation. The primary resource we used was the sector-specific plan that defines key security and resilience concerns including cyber (DHS , 2020). In addition we reviewed the many resources contained on the HSIN-CI Dams Portal, most specifically a series of Dam Sector handbooks that are Official Use Only (Dam Safety, 2020). These documents define the public-private partnership, improve information sharing, and assist the sector in improving the resiliency of a dam (DHS, 2015).

Though these documents were extensive, we primarily used them as background information in the event of a cyber incident harming the operations of a hydroelectric plant.

3.2.2 Emergency Resources

Closely related to the safety of a dam, FEMA is concerned about an emergency involving a dam. This office “coordinates the Federal response to disasters and for providing Federal guidance to State, local, Tribal, and Territorial emergency management authorities for all foreseeable emergencies” (FEMA, 2013). In the event of a failure or degradation of a dam, FEMA gives guidance on who to call, how the recovery of an event is handled, and who is in charge.

We used the guidance from this agency, specifically *Guidelines for Dam Safety, the Emergency Action Planning for Dams FEMA’s 64* (FEMA, 2013), to build out the steps an operator goes through if a plant were to require outside assistance (FEMA, 2013).

3.2.3 Cybersecurity Recovery

There are two aspects of cybersecurity response we considered for a hydroelectric plant R&R process. Primarily we looked to the DHS Cybersecurity and Infrastructure Security Agency (CISA) office whose role is to defend against cyber attacks based on the Presidential Policy

Directive 41 (The White House, 2016). A key mission of this directive is to support a national response involving a cyber component. For the technical aspects of how to respond to and recover from a cyber incident on a computer system, we looked to NIST for guidance (DHS, 2020).

We also looked at the National Cyber Incident Response Plan that describes a national approach to cyber incidents (CISA, 2020). This document, closely related to the FEMA 64 guidance in emergency response, integrates FSLTT and the private sector in responding to cyber incidents. This document applies to significant cyber incidents that are "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people" (CISA, 2020).

We looked to resources from NIST, which has been defined in Executive Order 13800 to be used to mitigate risks to our nation's critical infrastructure (Whitehouse, 2017). NIST provides a variety of cybersecurity guidance that could be of assistance to hydroelectric plants during an R&R process. Some include the *Cybersecurity Framework* (CSF), the *Guide for Cybersecurity Event Recovery, Cybersecurity Framework Smart Grid Profile*, and the *Computer Security Incident Handling Guide* among others (NIST, 2020).

We reviewed several NIST documents to assess the alignment of guidance against the R&R process a plant would experience. While the CSF has included "Response" and "Recovery" within its core, the objectives do not align with the intent of an R&R process for a hydroelectric plant in the middle of a cyber event. The CSF has five concurrent and continuous functions that "provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk" (NIST, 2020). Those functions are Identify, Protect, Detect, Respond, and Recover. These functions are intended to manage risk prior to a cyber event but do not assist an operator in responding to nor recovering from a cyber incident that is occurring in real time.

Another document within the NIST library is the *Guide for Cybersecurity Event Recovery,* which addresses comprehensive recovery planning for a cyber incident (NIST, 2016). It focuses on proactively preparing for a cyber event to assist in the planning and testing of recovery scenarios. This document, like the CSF, does not address the steps necessary to recover from an event in the heat of the moment.

The last major document we reviewed was the *NIST 800-61r2 Computer Security Incident Handling Guide*, which is intended to guide the reader in performing an incident response and directly aligns to the intent of responding and recovering during an incident (NIST, 2012). The phases within this document, Preparation, Detection and Analysis, Containment Eradication & Recovery, and Post-Incident Activity, clearly address the steps an operator could use during the cyber component of recovering from a cyber event. We used these phases to provide the foundation of R&R for an operator. We will discuss the processes of NIST 800-61r2 in more detail in later sections of this report.

3.2.4 Other Resources

Other resources we used address the notification requirements for state, local, tribal, or territorial organizations and others. We included the OE 417 reporting requirements, FERC dam safety officer notification requirement, and Bureau of Reclamation notifications pulled from appropriate websites and in some cases validated by the responsible office.

In addition, we found some industry and other resources that gave differing perspectives of cyber in energy generation, dam safety, and emergency response. We found the American Public Power Association's Cyber Incident Response Playbook to be the most helpful in the multitude of considerations a plant would address during a cyber incident (APPA, 2019). We also used DOE's Chapter 2 State of Hydropower in the United States, NERC CIP information, the National Governors Association's State Cyber Disruption Response Plans, and the Washington State Department of Ecology Dam Safety Office's dam emergency planning and response references (DOE, 2016) (NERC, 2018) (National Governers Association) (NERC, 2018) (State of Washington, 2020).

The additional references we reviewed ensured that externally required notifications were addressed in the process flow, and that our flow aligned to sector organizations and was reasonable to propose to the hydroelectric sector for an R&R process flow.

3.3 Integrated Framework

After an extensive review of these documents, we started the processes within our R&R with the recovery of the cyber component and applying emergency actions from FEMA 64 as the event warrants. We used NIST 800-61r2 as the foundational set of steps as the event is observed and classified as an incident. As the R&R expands into emergency actions and outside assistance, if necessary, we integrate into an emergency action plan process based on *FEMA's 64 Guidelines for Dam Safety, the Emergency Action Planning for Dams*.

If an observable occurrence in a system or network were to be noticed as we describe in Section 2.2, the operator would initially focus on the cyber components to determine if the event is unusual or the effects of a nefarious actor. To assist an operator in this aspect of recovery we used the phases within the *NIST 800-61r2 Computer Security Incident Handling Guide* to provide the process steps in aligning an operator's R&R of the cyber components of a plant. Once the event rises to an adverse event (an event with negative consequences) or to an incident level (violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices), the operator might need to address the steps defined in *FEMA's 64 Guidelines for Dam Safety, the Emergency Action Planning for Dams*.

The steps an operator goes through to respond to and recover from any event, incident, or crisis are generalized in Figure 3.1. In this graphic, the foundation of an R&R flow is the continuous normal business process while the yellow star denotes an unusual event occurring during normal business process. Once an observable event occurs, the operator would refer to the WPTO R&R guide for the initial actions to determine if the event rises to the level of an incident. If the event is found to be quickly resolvable, the operator returns to normal business process after a set of post-event activities. If the event is found to be an incident as defined in NIST 800-61r2, the operator would refer to the WPTO R&R guide for escalation steps to either respond to the incident or determine if the incident rises to a crisis state which requires outside assistance. If the former, the operator would recover from the incident; while if the latter, the operator would follow crisis state steps found in the WPTO R&R guide. For both, the operator will need to follow post-incident activities to completely recover from a cyber incident.

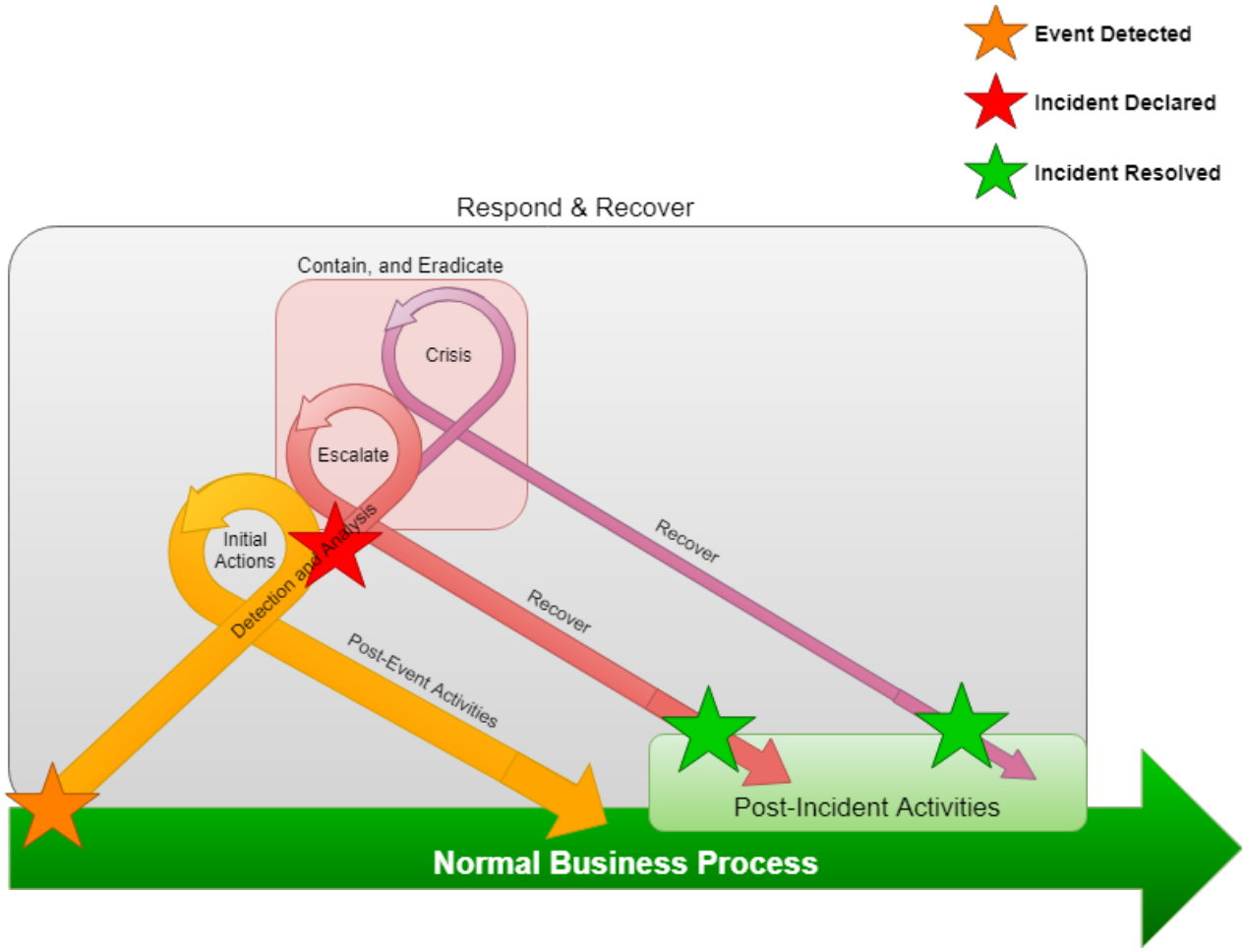

Figure 3.1. R&R Process Flow

The three aspects of recovery—safety critical, emergency management, and cyber combined—provided the baseline used to define the steps within our process. These steps resulted in three products

- A flipbook, *The Department of Energy Water Power Technologies Office Cyber Response & Recovery Flipbook*, to be used at a hydroelectric plant to quickly respond to an anomalous event.
- A quick reference guide, *WPTO Response Alignment,* that lines up the cyber processes within the NIST Computer Security Incident Handling Guide against the emergency action steps found in *Federal Guidelines for Dam Safety: Emergency Action Planning for Dams*. This alignment is to be used as a reference if the plant wants to understand how a computer incident handling checklist aligns to an emergency action plan process.
- An overall hyperlinked list of publicly available hydroelectric plant references, *WPTO Resources: Dam Sector*, to be used for additional guidance.

These products all rely on guidance from NIST, specifically NIST Special Publication 800-61r2 for the cybersecurity process flows (NIST, 2012). This guide covers the following steps:

- Preparation – Serves as a preparation handbook for a hydroelectric plant in defining an incident R&R plan for their specific needs. This phase includes establishing an R&R

capability to include people, processes, and technology that will assist an organization in preventing and deterring attack vectors as well as establishing the policies and procedures necessary for a strong and competent team prepared to respond to a cyber incident.

- Detection and Analysis – Lists the steps in detection and analysis of an event for a hydroelectric plant to apply to their specific situation and configuration. This effort defines the need of an organization to apply appropriately resourced tools, technologies, and teams prepared to respond quickly and reliably against cyber attacks. Also included are external technical sources.
- Containment, Eradication, and Recovery – Defines the strategy a plant may apply for a cyber incident on their system.
- Post-Incident Activity – Defines best practices a plant might take to improve detection, eradication, and recovery from a cyber incident.

These process flows established our foundation guiding an operator through the necessary details to respond to and recovery from a cyber incident on a computerized system. However, if the event causes disruption to the safe and reliable operation of the physical components of the dam, we relied on the guidance within FEMA 64 and the National Incident Management System (NIMS) to provide a systematic, “proactive approach to guide all levels of governmental, nongovernmental, and private-sector organizations to work seamlessly to respond” (FEMA, 2013).

Within our flipbook the team established a framework to assist an operator in quickly navigating the recovery process. The flipbook starts with a high-level flow color-coded page where the operator can quickly decipher the section they need to locate. Peach color sections are Initial Emergency Actions, gray are R&R Actions, green are Demobilize and Deescalate actions, red are Escalation, and purple are Crisis State actions. Within each action section, the flipbook is further separated into four subsections. The first addresses the operator’s actions; those inputs, events, and outputs that describe the details. The second subsection covers the roles that describe the responsibilities and authorities involved in each action. The third subsection is the processes that occur within each action section. The fourth subsection describes external publicly available resources for the operator to reference if more information or guidance is needed.

Given our alignment with national directives, established regulations, and policies, this proposed R&R process flow is squarely within the compliance requirements of existing regulations and polices. It will be compatible with and complementary to the current regulatory framework.

3.4 Caveats or Limitations

This work attempts to generalize the needs of smaller hydroelectric plants and is not completely representative of the diversity of hydroelectric plants. Therefore, modification and tailoring would be necessary to both build specific steps required by any state, local, tribal, territorial, or ownership requirement and integrate specific points of contacts not addressed in the R&R process flow separately delivered. As the team reviewed the multitude of FSLTT regulations and guidance, the scientific and industry papers on R&R, and the FEMA guidance, the integration of computer system R&R processes need to include safety physical dependencies as well. As such, this work is a new effort and is a living document that should be updated as new technologies and cyber dynamics change over time.

4.0 Response and Recovery Plan

4.1 Key Assumptions

Though the work is focused on the digitally controlled hydroelectric plant, the team understands that the two cyber-physical controlled components—the turbine-generator powertrain and the spillway gates—continue to retain the option of manual controls. This aspect of a recovery process during safety critical events ensures that if the electronic or digital systems are not able to recover, the plant has the option to recover or safely stop the two components through a manual process.

4.2 Impact Severity

During the R&R process there are two routes for recovering from a cyber incident affecting the safe and reliable operation of a hydroelectric plant: the cyber or system recovery and the physical recovery of the plant itself. They determine the level of risk a cyber event has to system and business operations, compliance requirements, and other aspects. Knowing the severity or impact to the plant helps an operator manage the event appropriately and use consistent language to articulate the event. On the cyber side, CISA has established an incident scoring system to assess impacts of a cyber event (DHS CISA, 2017).

These evaluation techniques provide a complete picture for plant owners, operators, and interested parties in establishing the level of response necessary to mitigate adverse effects of a cyber incident. The priority levels in CISA's scoring system, which is not intended to be the complete answer, focuses on weighted arithmetic measuring categories to include impacts, activities, and characterizations to establish priority levels. The categories include the following:

- Functional Impact
- Observed Activity
- Location of Observed Activity
- Actor Characterization
- Information Impact
- Recoverability
- Cross-Sector Dependency
- Potential Impact

On the physical response side, FEMA has developed FEMA 333, *Federal Guidelines for Dam Safety: Hazard Potential Classification System for Dams*, to establish a hazard potential classification system (FEMA, 2004). This guidance focuses on how the physical plant effects the loss of human life, economic losses, environmental damage, and lifeline disruption.

The combination of CISA and FEMA systems provides a more robust evaluation of a cyber event. However these two scoring systems are distinctly different. In order to assist owners and operators the team proposes that the DHS consider integrating CISA's scoring system for cyber events into FEMA's Hazard Potential Classification System and address this in the upcoming release of the National Cyber Incident Response Plan (DHS, 2016).

4.3 R&R Flow Diagram

This work describes the process in delivering four products:

- This overview plan discussing the work.
- An R&R process flow flipbook intended to be stored on site for an operator to quickly respond to and recover from a cyber attack.
- A simple overview of the process flow aligned to FEMA 64 guidance and to the NIST 800-61r2 Computer Security Incident Handling Guide (FEMA, 2013) (NIST, 2012).
- An overall hyperlinked list of publicly available hydroelectric plant references, *WPTO Resources: Dam Sector*, to be used by a plant for additional guidance.

4.4 Application and Validation

We see the application of this R&R flow, in a flipbook format, as a handy on-site reference tool for operators attempting to respond to a hydroelectric plant cyber incident. During an abnormal event the flipbook can assist an operator in quickly reviewing actions, processes, and expected outputs during the initial emergency occurring in a facility.

This flipbook guidance is intended to address only the implementation and management of cybersecurity practices associated with information and operational technology assets and the environments in which they operate. This guidance is not intended to replace or subsume other cybersecurity-related activities, programs, processes, or approaches that Hydroelectric Sector organizations have implemented or intend to implement, including any cybersecurity activities associated with legislation, regulations, policies, programmatic initiatives, or mission and business requirements. Compliance requirements are not altered in any way by this model. Additionally, this guidance is not part of any regulatory framework and is not intended for regulatory use. Rather, the guidance in this publication is intended to complement a comprehensive enterprise cybersecurity program.

The second deliverable, the WPTO Response alignment hyperlinked document, aligns the FEMA 64 emergency action steps to the NIST 800-61 Computer Security Incident Handling Guide. This tool will also assist the plant owner, operators, and staff with the integration of cybersecurity recovery steps into the FEMA 64’s Emergency Action Plan process for an R&R process.

Though this work is new and correlates two resources in a unique way, the process flow can now be reviewed by others across the hydroelectric community for validation and ongoing updates. Constant review by those who implement this R&R flow and organizations who integrate with hydroelectric plants during cyber events will ensure continued improvement for this R&R flow.

5.0 Conclusion

Response and recovery tools can be efficiently integrated and accessible during a fast moving and confusing cyber event if they are integrated into a comprehensive cyber and plant recovery program. A robust R&R strategy for hydroelectric systems must include both an emergency action plan to recover the plant and a cyber program for operators to recover the system services the plant relies on. For an effective organization, the integration of the two will reduce confusion, enable coordination between emergency responders and the cybersecurity community, and ensure a structured response to minimize effects of breakdowns caused by a cyber incident.

In addition to the R&R tool, this work has focused on suggested resources to grow cybersecurity capabilities for hydroelectric plant operators to include the American Public Power Association Public Power Cyber Incident Response Playbook, the MITRE ATT&CK® Matrix and threat actor mitigations, the Electricity Subsector Coordinating Council Cyber Mutual Assistance, and two popular cyber organizations, (ISC)², and SANS Institute (MITRE, 2020) (ISC², 2020) (SANS, 2020) (ESCC, 2020).

6.0 References

APPA. (2019, August). *Public Power Cyber Incident Response Playbook.* Retrieved from publicpower.org: https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf

Bristow, M. (2020, 09 24). (CS)2AI ONLINE: Control System Security Incident Handling in the Fog of War. ((CS)2AI, Interviewer)

CISA. (2015, March). *Sector-Specific Agencies*. Retrieved from CISA: https://www.cisa.gov/sector-specific-agencies

CISA. (2020). *Homeland Security Information Network - Critical Infrastructure (HSIN-CI) Dams Portal*. Retrieved from Cybersecurity& Insfrastructure Security Agency: https://www.cisa.gov/hsin-dams-portal

CISA. (2020). *The National Cyber Incident Response Plan (NCIRP)*. Retrieved from US-CERT.CISA.gov: https://us-cert.cisa.gov/ncirp

Congress. (2019). *Dam Safety: Federal Programs and Authorities.* Washington DC: Congressional Research Service . Retrieved from https://fas.org/sgp/crs/homesec/IF10606.pdf

Dam Safety. (2020). *Emergency Action Planning*. Retrieved from damsafety.org: https://damsafety.org/dam-owners/emergency-action-planning

DHS . (2020). *HSIN-CI Dams Portal.* Retrieved from cisa.gov: https://www.cisa.gov/hsin-dams-portal

DHS. (2011). *Presidential Policy Directive / PPD-8: National Preparedness*. Retrieved from DHS.gov: https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

DHS. (2012, April). *National Infrastructure Protection Plan Dam Sector.* Retrieved from NPPD Dam Sector Snapshot: https://www.dhs.gov/xlibrary/assets/nppd/nppd-dams-sector-snapshot-508.pdf

DHS. (2015). *Dams Sector-Specific Plan.* Retrieved from cisa.gov: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf

DHS. (2016, December). *National Cyber Incident Response Plan.* Retrieved from US-CERT.CISA.gov: https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

DHS. (2020). *DHS ROLE IN CYBER INCIDENT RESPONSE*. Retrieved from CISA.gov: https://www.cisa.gov/sites/default/files/publications/DHS%20Cyber%20Incident%20Response%20Fact%20Sheet%20v15%20-%20508%20Compliant.pdf

DHS CISA. (2017, March). *CISA Cyber Incident Scoring System* . Retrieved from US-CERT.CISA.gov: https://us-cert.cisa.gov/CISA-Cyber-Incident-Scoring-System

DHS Dam Safety. (2015). *DHS Dam Sector Roadmap To Secure Control Systems In The Dams Sector 2015.* Retrieved from damsafety.org: https://damsafety.org/sites/default/files/files/DHS%20Dam%20Sector%20Roadmap%20To%20Secure%20Control%20Systems%20In%20The%20Dams%20Sector%202015.pdf

DOE. (2016). Chapter 2: State of Hydropower in the United States. In U. D. Energy. Washington DC: U.S. Department of Energy. Retrieved from https://documents.pub/document/hydropower-vision-chapter-2-state-of-hydropower-in-the-united-.html

DOE. (2016, December 30). *Hydropower Vision Chapter 2: State of Hydropower in the United States.* Retrieved from documents.pub: https://documents.pub/document/hydropower-vision-chapter-2-state-of-hydropower-in-the-united-.html

DOE. (2018, 05). *Department of Energy Office of Cybersecurity, Energy Security, & Emergency Response.* Retrieved from Energy.Gov: https://www.oe.netl.doe.gov/oe417.aspx

DOE. (2020, 09). *Types of Hydropower Plants.* Retrieved from Energy.gov: https://www.energy.gov/eere/water/types-hydropower-plants

Dressel, A. (2014). NERC CIP Version 5: Impact to Hydro Owners and Operators. *Hydroreview*, 1. Retrieved from Hydroreview.com: https://www.hydroreview.com/2014/07/21/nerc-cip-version-5-impact-to-hydro-owners-and-operators/#gref

EIA. (2020, March 30). *Hydropower Explained*. Retrieved from U.S. Energy Information Administration : https://www.eia.gov/energyexplained/hydropower/#:~:text=Hydropower%20was%20one%20of%20the,annual%20U.S.%20renewable%20electricity%20generation.

ESCC. (2020). *Cyber Mutual Assistance.* Retrieved from Electricity Subsector Coordinating Council: https://www.electricitysubsector.org/cma

FEMA. (2004). *Hazard Potential Classification System for Dams (FEMA 333).* Jessup, Maryland: FEMA. Retrieved from https://www.fema.gov/media-library-data/20130726-1516-20490-7951/fema-333.pdf

FEMA. (2013, July). *Federal Guidelines for Dam Safety -Emergency Action Planning for Dams.* Retrieved from FEMA.gov: https://www.fema.gov/media-library-data/5b20db599c212f77fd5e85d256f471a3/EAP+Federal+Guidelines_FEMA+P-64.pdf

FEMA. (2013, July). *Federal Guidelines for Dam Safety FEMA 64.* Retrieved from damsafety.org: https://damsafety.org/sites/default/files/FEMA%20Federal%20Guidelines%20EAP%20P-64-2013.pdf

FEMA. (2013, July). *Homeland Security Digital LIbrary.* Retrieved from Center for Homeland Defense and Security: https://www.hsdl.org/?abstract&did=743802

FERC. (2017, February). *Hydropower Primer A Handbook of Hydropower Basics.* Retrieved from FERC.gov: https://www.ferc.gov/sites/default/files/2020-05/hydropower-primer.pdf

FERC. (2020, 05). Retrieved from FERC.Gov: https://www.ferc.gov/sites/default/files/2020-05/hydro-guide.pdf

FERC. (2020, May). *Hydropower Licencsing Get Involved A Guide for the Public.* Retrieved from FERC.gov: https://www.ferc.gov/sites/default/files/2020-05/hydro-guide.pdf

FWEE. (2020). *How Hydroelectric Projects Are Regulated.* Retrieved from Foundation for Water & Energy Education: https://fwee.org/nw-hydro-tours/how-the-northwest-hydro-system-works/how-hydroelectric-projects-are-regulated/

ISC². (2020). *ISC² Resource Center.* Retrieved from ISC²: https://www.isc2.org/Resource-Center

Lockheed Martin. (2011). *The Cyber Kill Chain®.* Retrieved from Lockheed Martine.com: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

MITRE. (2020). *MITRE ATT&CK®.* Retrieved from Attack.mitre.org: https://attack.mitre.org/

National Governers Association. (n.d.). *State Cyber Distruption Response Plans.* Retrieved from NGA.org: https://www.nga.org/wp-content/uploads/2019/04/IssueBrief_MG.pdf

NERC. (2018, July). *CIP-008-6 - Cyber Security - Incident Reporting and Response Planning.* Retrieved from NERC.com: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf

NIST. (2012, August). *Computer Security Incident Handling Guide.* Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from nvlpubs.nist.gov: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST. (2016, December). *NIST Special Publication 800-184.* Retrieved from Guide for Cybersecurity Event Recovery: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

NIST. (2020). *COMPUTER SECURITY RESOURCE CENTER.* Retrieved from csrc/nist.gov: https://csrc.nist.gov/publications

NIST. (2020). *Cybersecurity Framework*. Retrieved from NIST.gov: https://www.nist.gov/cyberframework

Office of Inspector General. (2018, June). *U.S. Bureau of Reclamation Selected Hydropower Dams at Increased Risk from Insider Threats.* Retrieved from Oversight.gov: https://www.oversight.gov/sites/default/files/oig-reports/FinalEvaluation_ICSDams_Public.pdf

SANS. (2020). *SANS Institute.* Retrieved from sans.org: https://www.sans.org/

State of Washington. (2020). *Emergency Planning & Response.* Retrieved from Department of Ecology State of Washington: https://ecology.wa.gov/Water-Shorelines/Water-supply/Dams/Emergency-planning-response

The White House. (2016, 07 26). *Presidential Policy Directive -- United States Cyber Incident Coordination.* Retrieved from obamawhitehouse.archives.gov: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan - December 2016.* Retrieved from us-cert.cisa.gov: https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

USACE. (2019, January 31). *Publications USACE.* Retrieved from Department of Army USACE: https://www.publications.usace.army.mil/Portals/76/Users/182/86/2486/ER%2025-1-113.pdf?ver=CWGVBUsmJ4bMuJ3kSM2L-A%3d%3d

Whitehouse. (2017, May 11). *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Retrieved from whitehouse.gov: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

York, S. o. (2016, March 24). Statement from Governor Andrew M. Cuomo on Cyber Attack Charges Announced By U.S. Attorney General Loretta Lynch and FBI Director James Comey Involving the Bowman Avenue Dam in Westchester County. New York, NY. Retrieved from https://www.governor.ny.gov/news/statement-governor-andrew-m-cuomo-cyber-attack-charges-announced-us-attorney-general-loretta

Appendix A – R&R Resources

List of R&R resources used to support this report (with hyperlinks).

DHS

CISA

- Dams Sector Consequence-Based Top Screen (CTS) methodology (2017)
- US-CERT Federal Incident Notification Guidelines (2017)
- Dams Sector Cybersecurity Framework Implementation Guidance (2015)
- Homeland Security Information Network – Critical Infrastructure (HSIN-CI) Dams Portal

C2M2

- Dams Sector Cybersecurity Framework Implementation Guide (2020)
- Dams Sector Cybersecurity Capability Maturity Model Version 1.0 (2016)

FEMA

- National Response Framework (2019)
- Emergency Operations Planning: Dam Incident Planning Guide (2019)
- National Incident Management System (NIMS) (2017)
- National Mitigation Framework: Critical Tasks for Operational Coordination (2016)
- Federal Guidelines for Dam Safety Risk Management (P-1025) (2015)
- Federal Guidelines for Dam Safety: Emergency Action Planning for Dam Owners (FEMA 64) 2013)
- Living with Dams: Know Your Risks (FEMA P-956) (2013)
- Federal Guidelines for Inundation Mapping of Flood Risks Associated with Dam Incidents and Failures (FEMA P-946) (2013)
- Strategic Plan for the National Dam Safety Program (P-916) (2012)
- Emergency Preparedness Guidelines for Levees: A Guide for Owners and Operators (2012)
- Emergency Action Planning for State Regulated High Hazard Potential Dams (FEMA 608) (2007)
- Federal Guidelines for Dam Safety (FEMA 93) (2004)
- Federal Guidelines for Dam Safety: Hazard Potential Classification System for Dams (FEMA 333) (2004)
- Federal Guidelines for Dam Safety: Glossary of Terms (FEMA P-148) (2004)
- ADSO/FEMA Specialty Workshop on Risk Assessment for Dams (2001)
- Dam Safety Technical Manuals and Guides

Dams Sector

- Dams Sector Landscape (2019)
- (FOUO) Dams Sector Protective Measures Handbook (2017)
- Dams Sector Cybersecurity Program Guidance (2016)
- Dams Sector Security Guidelines (2015)
- Roadmap to Secure Control Systems in the Dams Sector November (2015)
- Dams Sector Crisis Management Handbook A Guide for Owners and Operators (2015)
- Dams Sector-Specific Plan (2015)
- (FOUO) Dams Sector Security Awareness Handbook (2015)
- Dams Sector: Charters and Membership
- Emergency Action Planning
- Decision Support System for Water Infrastructure Security (DSS-WISE)

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

- NIST Cybersecurity Framework v1.1, Framework for Improving Critical Infrastructure Cybersecurity (2018)
- NIST SP 800-184 Guide for Cybersecurity Event Recovery (2016)
- NIST SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security (2015)
- NIST SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops (2013)
- NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide (2012)
- NIST SP 800-92, Guide to Computer Security Log Management (2006)

DoD	USACE	USACE Best Practices in Dam and Levee Safety Risk Analysis, Ver. 1.4 (2019) USACE EC 1110-2-6074, Guidance for Emergency Action Plans, Incident Management and Reporting, and Inundation Maps for Dams and Levee Systems (2018) USACE Dam Safety Program
FERC		FERC Notification Process in Response to an Incident at a FERC Hydro Facility FERC Division of Dam Safety and Inspections, Security Program for Hydropower Projects, Revision 3A (2016) FERC Chapter VI Emergency Action Plans (2015) Dam Safety and Inspections | Potential Failure Modes (PFMs) FERC Time Sensitive EAP Initiative FERC Dam Safety and Inspections
DOI	USBR	Appurtenant Structures for Dams (Spillways and Outlet Works) Design Standard (DS14): Chapter 3: General Spillway Design Considerations (2014) Dam Safety Public Protection Guidelines (2011)
DOE	FFRDC	Current State-of-Practice in Dam Safety Risk Assessment
Other	SLTT	Dam Safety Office (DSO) Dam Emergency Planning & Response (2020) State Cyber Disruption Response Plans (2019) Dam Safety Office (DSO) ECY 070-37 Dam Safety - Simplified Emergency Action Plan Form (2016) Dam Safety Office (DSO) Guidelines for Developing Dam Emergency Action Plans (2013)
	Utility	'Risk ownership' and mitigation are key to safety culture, Risk-Based Use Cases (2020) Power Production, Quarterly Commission Update: Hierarchy of Reliability Documentation (2019)
	Industry	APPA Cyber Incident Response Playbook (2019) CIP-008-6 Cyber Security — Incident Reporting and Response Planning CIP-009-5 Cyber Security — Recovery Plans for BES Cyber Systems
	Academia	CERIAS Tech Report 2014-01, Mapping Dams Sector Cyber-Security Vulnerabilities (2014)

Appendix B – Alignment of the Two Primary R&R Guides

Alignment of the two primary resources used to define the steps in the WPTO R&R Guide

FEMA

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

FEMA 64 Emergency Action Plan (EAP) Framework			NIST 800-61 Computer Security Incident Handling Guide			
EAP Stages	**EAP Role Responsibilities (Answers Who)**	**EAP Actions (Decisions)**	**NIST 800-61 Response Lifecycle**	**NIST 800-61 Incident Handling Checklist**	**NIST 800-61 Section**	**References**
Step 1: Incident detection, evaluation, and emergency level determination	**Dam Owner** 1. Verify and assess emergency conditions (Table B-1: Summary of EAP Responsibilities) **Dam Operator** 1. Detect/confirm incident at dam 2. Determine emergency level (Table B-2: Summary of the Dam Owner's Responsibilities) **Engineering Manager** 1. Support onsite Operator and Operations Command Center on emergency level (Table B-2: Summary of the Dam Owner's Responsibilities) **Dam Owner/Operator & Emergency Management Authorities** Dam owner will categorize the condition of incident into one of the established emergency levels based on the severity of the initiating condition or triggering events.	An unusual condition or incident is detected and confirmed? Determine the number of emergency levels required for each dam on a case-by-case basis - High flow - Non-failure - Potential failure - Imminent failure The EAP should describe how each emergency level applies to the particular dam.	Detection & Analysis	1. Determine whether an incident has occurred 1.1 Analyze the precursors and indicators 1.2 Look for correlating information 1.3 Perform research (e.g., search engines, knowledge base) As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	3.2.1 Identify attack vectors 3.2.2 Signs of an Incident 3.2.3 Sources of Precursors and Indicators Table 3-1. Common Sources of Precursors and Indicators 3.2.4 Incident Analysis Perform Initial Analysis 3.2.5 Incident Documentation	
Step 2: Notification and communication	**Dam Owner/Operator** 2. Notify other participating emergency management (Table B-1: Summary of EAP Responsibilities) **Dam Operator** 2. Make calls on Notification Flowchart Notify notifications are made in accordance with the EAP's Notification Flowchart(s) (Table B-2: Summary of the Dam Owner's Responsibilities) **Dam Owner/Operator & Emergency Management Authorities** 2. Notify other participating emergency management agencies, provide any information that will assist in the declaration of public emergency decision by emergency management authorities. (Table B-1: Summary of EAP Responsibilities) **Engineering Manager** 2. Make calls on notification flow chart (Table B-2: Summary of the Dam Owner's Responsibilities) **Senior Management** 1. Make calls on notification flow chart (Table B-2: Summary of the Dam Owner's Responsibilities) **Dam Owner/Operator** Make periodic status reports to the affected emergency authorities and other stakeholders in accordance with the Notification Flowcharts and associated procedures **Dam Operator** 6. Provide regular status reports to senior management **Engineering Manager** 7. Provide regular status reports to senior management (Table B-2: Summary of the Dam Owner's Responsibilities) **Senior Management** 2. Initiate periodic status report conference calls with dam site, command center, engineering, and public relations (Table B-2: Summary of the Dam Owner's Responsibilities)	1. During this step, the dam owner should provide any information that will assist in that decision. An early decision and declaration are critical to maximizing available response time. Dam owners will contact: - Engineer/management staff/public affairs officer - Local emergency authorities or 911 centers - State dam safety program representatives - Other regulatory authorities - Upstream and downstream dam owners Local emergency management authorities will contact: - Other local responders such as police or fire - State emergency management authorities - Affected residents and businesses - Appropriate NWS WFO	Detection & Analysis	2. Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	3.2.6 Incident Prioritization Table 3-2. Functional Impact Categories Table 3-3. Information Impact Categories 3.2.7 Incident Notification	
Step 3: Emergency Actions	**Dam Owner/Operator** Act to save the dam and minimize impacts to life, property, and the environment (Table B-2: Summary of the Dam Owner's Responsibilities) **Dam Owner/Operator** 3. Take corrective action at facility (Table B-1: Summary of EAP Responsibilities) **Engineering Manager** 3. Determine emergency operation and construction procedures (Table B-2: Summary of the Dam Owner's Responsibilities) **Senior Management** 3. Provide regular status reports to County Emergency Operations Center (Table B-2: Summary of the Dam Owner's Responsibilities) **Dam Operator** 4. Coordinate with Command Center and Engineering on gate operations and emergency procedures (Table B-2: Summary of the Dam Owner's Responsibilities) **Engineering Manager** 4. Coordinate with Operator and Command Center on gate operations and emergency procedures (Table B-2: Summary of the Dam Owner's Responsibilities) **Senior Management** 4. Coordinate with upper management(Table B-2: Summary of the Dam Owner's Responsibilities) **Engineering Manager** 5. Dispatch engineers and construction crews as necessary (Table B-2: Summary of the Dam Owner's Responsibilities) **Engineering Manager** 6. Dispatch engineer as technical liaison to County Emergency Operations Center (Table B-2: Summary of the Dam Owner's Responsibilities) **Dam Operator** 5. Implement gate operations and other emergency procedures (Table B-2: Summary of the Dam Owner's Responsibilities)	Continuous process of taking actions, assessing the status of the situation, and keeping others informed through communication channels established during the initial notifications.	Containment Eradication & Recovery	4. Acquire, preserve, secure, and document evidence 5. Contain the incident 6. Eradicate the incident 6.1 Identify and mitigate all vulnerabilities that were exploited 6.2 Remove malware, inappropriate materials, and other components 6.3 If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (Step 5) and eradicate (Step 6) the incident for them 7. Recover from the incident 7.1 Return affected systems to an operationally ready state 7.2 Confirm that the affected systems are functioning normally	3.2.6 Incident Prioritization Table 3-2. Functional Impact Categories Table 3-3. Information Impact Categories 3.2.7 Incident Notification	
Step 4: Termination and follow-up	**Dam Owner/Operator or Dam Safety Expert** 4. Declare termination of emergency at facility (Table B-1: Summary of EAP Responsibilities) **Senior Management** 5. Coordinate with public relations staff at County and technical liaison at County Emergency Operations Center (Table B-2: Summary of the Dam Owner's Responsibilities)	Responsible for notifying the authorities that the condition of the dam has been stabilized. Government officials are responsible for declaring an end to the public emergency response.	Containment Eradication & Recovery	7.3 If necessary, implement additional monitoring to look for future related activity	3.3.4 Eradication and Recovery	
	Dam Owner/Operator or Dam Safety Expert & Emergency Management Authorities Create an After Action Report (AAR) **Dam Owner/Operator or Dam Safety Expert** 5. Update EAP on at least an annual basis (Table B-1: Summary of EAP Responsibilities) **Dam Owner/Operator** The results of the after-action review should be documented in an After Action Report (AAR) and used as a basis for revising the EAP.		Post-Incident Activity	8. Create a follow-up report 9. Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	3.4.1 Lessons Learned	

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov