Pacific Northwest
NATIONAL LABORATORY

PNNL-30540

WPTO Navigator

September 2022

Mark D Watson
Ford E Powers
Marie V Whyatt
Darlene E Thorsen

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

FEMA 64 Emergency Action Plan (EAP) Framework			NIST 800-61 Computer Security Incident Handling Guide			
EAP Steps	**EAP Role Responsibilities**	**EAP Actions**	**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.		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	**DHS FEMA** FEMA 64 – Federal Guidelines for Dam Safety: Emergency Action Planning for Dams FEMA P-1025 – Federal Guidelines for Dam Safety Risk Management Emergency Operations Planning: Dam Incident Planning Guide **DHS CISA** Dams Sector Crisis Management Handbook A Guide for Owners and Operators **FERC** Chapter VI Emergency Action Plans Time Sensitive EAP Initiative **Dam Safety Office (DSO) Example** Guidelines for Developing Dam Emergency Action Plans
Step 2: Notification and communication	**Dam Owner/Operator** 2. Notify other participating emergency management (Table B-1: Summary of EAP Responsibilities) **Dam Operator** 3. 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	**DHS FEMA** FEMA 64 – Federal Guidelines for Dam Safety: Emergency Action Planning for Dams Forms 205 and 205a FEMA P-1025 – Federal Guidelines for Dam Safety Risk Management **DHS CISA** Dams Sector Crisis Management Handbook A Guide for Owners and Operators **FERC** Chapter VI Emergency Action Plans Small/Low Impact Hydropower Projects **Dam Safety Office (DSO) Example** Guidelines for Developing Dam Emergency Action Plans
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	**DHS FEMA** FEMA 64 – Federal Guidelines for Dam Safety: Emergency Action Planning for Dams Emergency Operations Planning: Dam Incident Planning Guide **DHS CISA** Dams Sector Crisis Management Handbook A Guide for Owners and Operators 2015 **FERC** Chapter VI Emergency Action Plans **Dam Safety Office (DSO) Example** Guidelines for Developing Dam Emergency Action Plans
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.		7.3 If necessary, implement additional monitoring to look for future related activity	3.3.4 Eradication and Recovery	**DHS FEMA** FEMA 64 – Federal Guidelines for Dam Safety: Emergency Action Planning for Dams Emergency Operations Planning: Dam Incident Planning Guide **DHS CISA** Dams Sector Crisis Management Handbook A Guide for Owners and Operators 2015 **FERC** Chapter VI Emergency Action Plans **APPA** American Public Power Cyber Incident Response Playbook **Dam Safety Office (DSO) Example** Guidelines for Developing Dam Emergency Action Plans
	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