Pacific Northwest
NATIONAL LABORATORY

PNNL-30538

Department of Energy Water Power Technologies Office Cyber Response & Recovery Flipbook

September 2021

Marie V Whyatt
Darlene E Thorsen
Ford E Powers
Mark A Watson
David McKinnon
Jordan D Seaman

U.S. DEPARTMENT OF ENERGY

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

DISCLAIMER

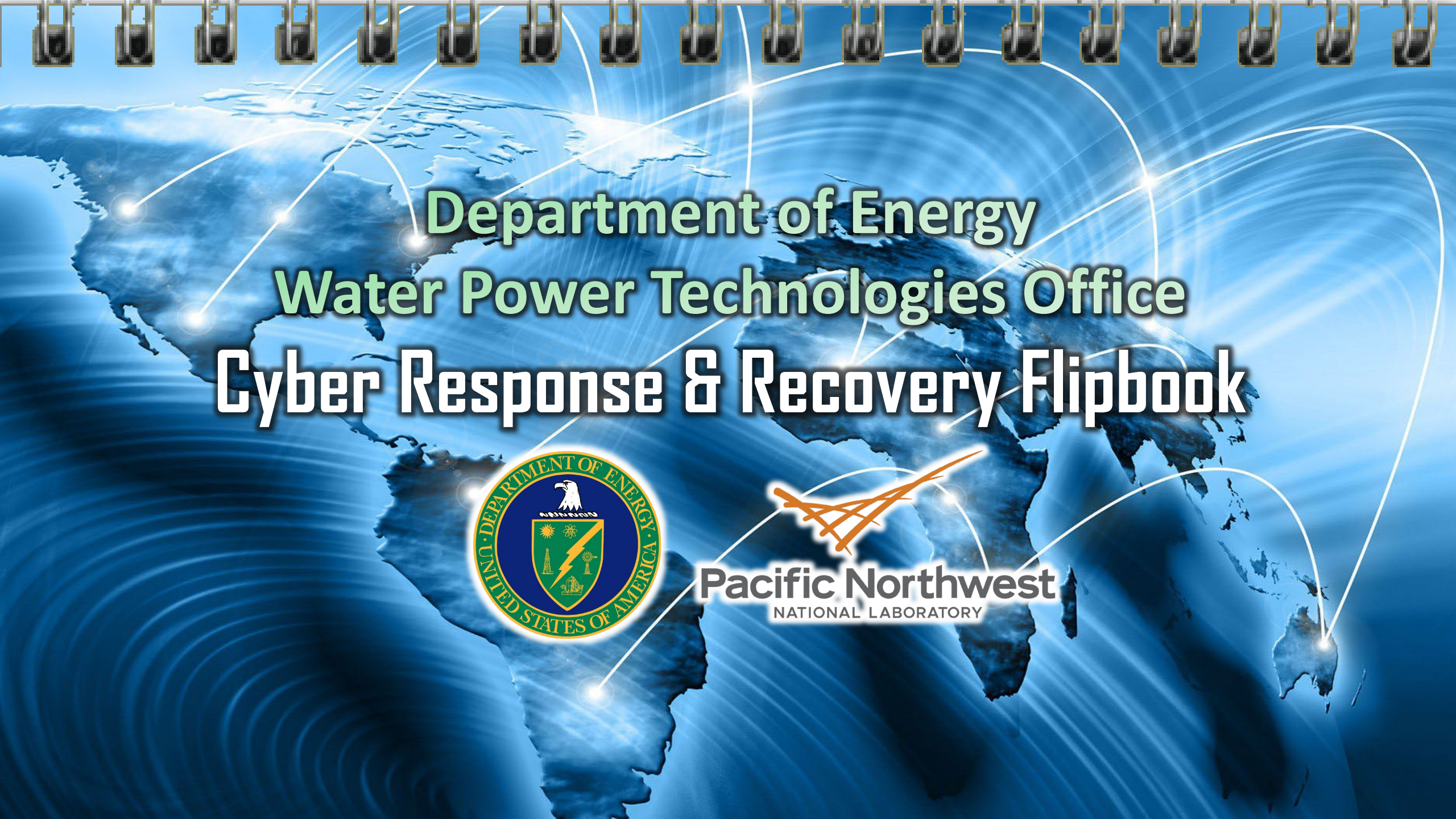
PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

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,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(9/2003)


Department of Energy
Water Power Technologies Office
Cyber Response & Recovery Flipbook
Pacific Northwest
NATIONAL LABORATORY

Intended Users

This flipbook is meant to assist a hydro facility staff member to quickly act to respond and recover from a cyber event - particularly at a small facility.

Intended Scope

The guidance provided in this publication is intended to address only the implementation and management of cybersecurity practices associated with information technology (IT) and operations technology (OT) 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 Hydropower 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.

Contents

Acronyms and Definitions

APPA	American Public Power Association
AHJ	Authority Having Jurisdiction
CIRT	Cyber Incident Response Team
CMA	Cyber Mutual Assistance
COP	Common Operating Picture
CTIIC	Cyber Threat Intelligence Integration Center
DB	Database
DHS	Department of Homeland Security
DOE	Department of Energy
EAP	Emergency Action Plan
E-ISAC	Electricity – Information Sharing and Analysis Center
EOC	Emergency Operations Center
ESCC	Electricity Subsector Coordinating Council
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
ICS	Industrial Control System (in context of OT)
ICS	Incident Command System (in context of NIMS)
IR	Incident Response
IRT	Incident Response Team
ISAC	Information Sharing and Analysis Center
JAA	Joint Action Agencies
JIS	Joint Information System
MAN	Mutual Aid Network
MAC	Multi-Agency Coordination
MS-ISAC	Multi-State – Information Sharing and Analysis Center
MIL	Maturity Indicator Level (MIL0, MIL1, MIL2, MIL3)
NIMS	National Incident Management System
MSEL	Master Scenario Events List (used in tabletop exercises)
NCCIC	National Cybersecurity and Communications Integration Center
NERC	North American Energy Reliability Corporation
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
R&R	Response and Recovery
RTLT	Resource Typing Library Tool (NIMS definitions online DB)
SLTT	State, Local, Tribal, and Territorial
US-CERT	United States – Computer Emergency Readiness Team
WPTO	Water Power Technology Office

Event:	an observable occurrence in a system or network
Adverse Event:	an event with negative consequences
Incident:	a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (including cyberattack)

What To Have Ready

Rapidly *and* ***Simultaneously***…

- Assemble initial teams (CIRT) · assign initial roles · do initial triage · take first actions to secure & make safe:

  Initial Emergency Actions [pages 10]
  References [starts on page 50]

- Record event information

  Initial Emergency Actions · Resources [page 19] · FEMA 64 "*Example Dam Emergency Incident Log*" (link)
  Appendix [page 54] - Lists · Forms · Logs

- Notify (internally) · prepare to notify externally

  Initial Emergency Actions · Resources [page 19] · FEMA 64 *"Example Notification Flowchart"* (link)
  Initial Emergency Actions · Resources [page 19] · FEMA 64 "*Table F-1: Examples of Notification Information by Emergency Level*" (link)
  Appendix [page 61]

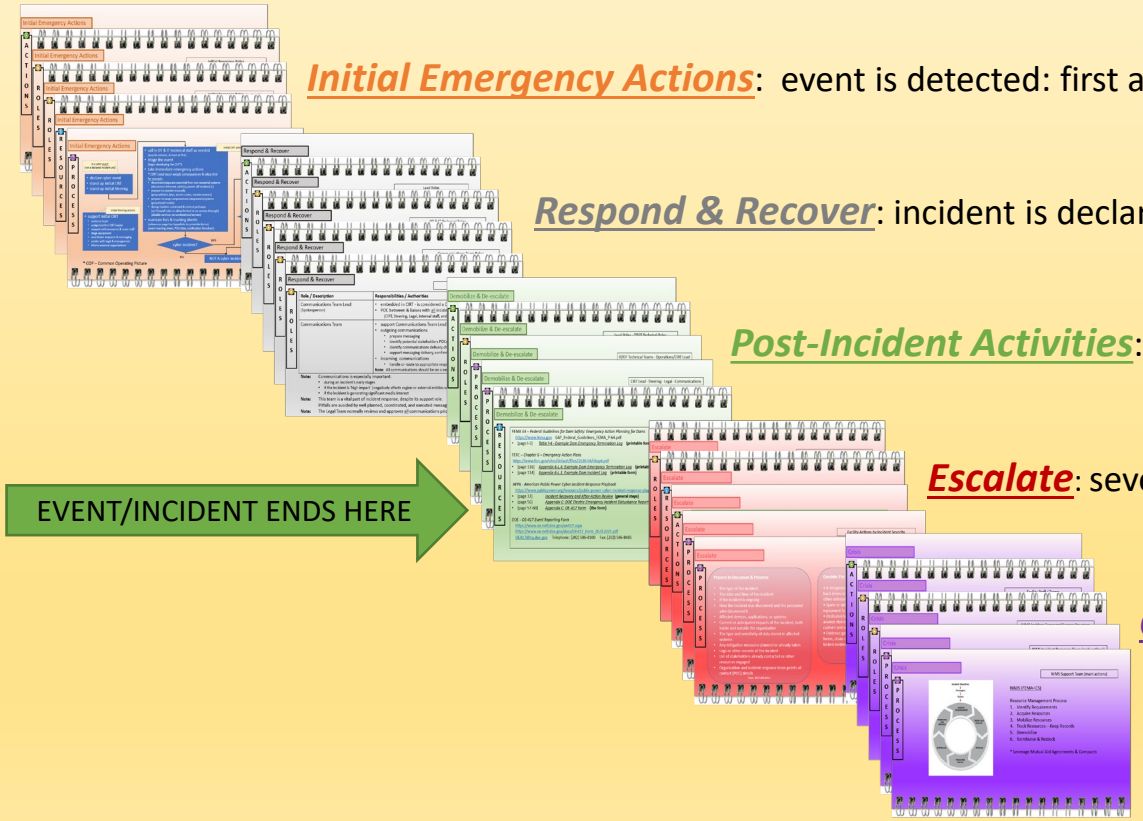
Since a hydro facility can be held liable for failure to apply due diligence, having a plan and sticking to it unless it clearly isn't working is the best policy.
A major flaw in R&R plans is that people don't know their role or who to call, the most vocal member ends up leading but often doesn't know what to do.

R&R - The Five States

EVENT STARTS HERE

1. ***Initial Emergency Actions***
2. ***Respond & Recover***
3. ***Post-Incident Activities***
4. ***Escalate***
5. ***Crisis***

This flipbook is organized into 5 distinct ***states*** describing the major stages of a cyber event or incident. They align closely with NIST 800-61r2.



Initial Emergency Actions: event is detected: first actions · stand-up initial teams · assign roles · halt damage · make safe · do initial triage

Respond & Recover: incident is declared: isolate & eradicate · fortify teams · secure resources · take actions · monitor closely

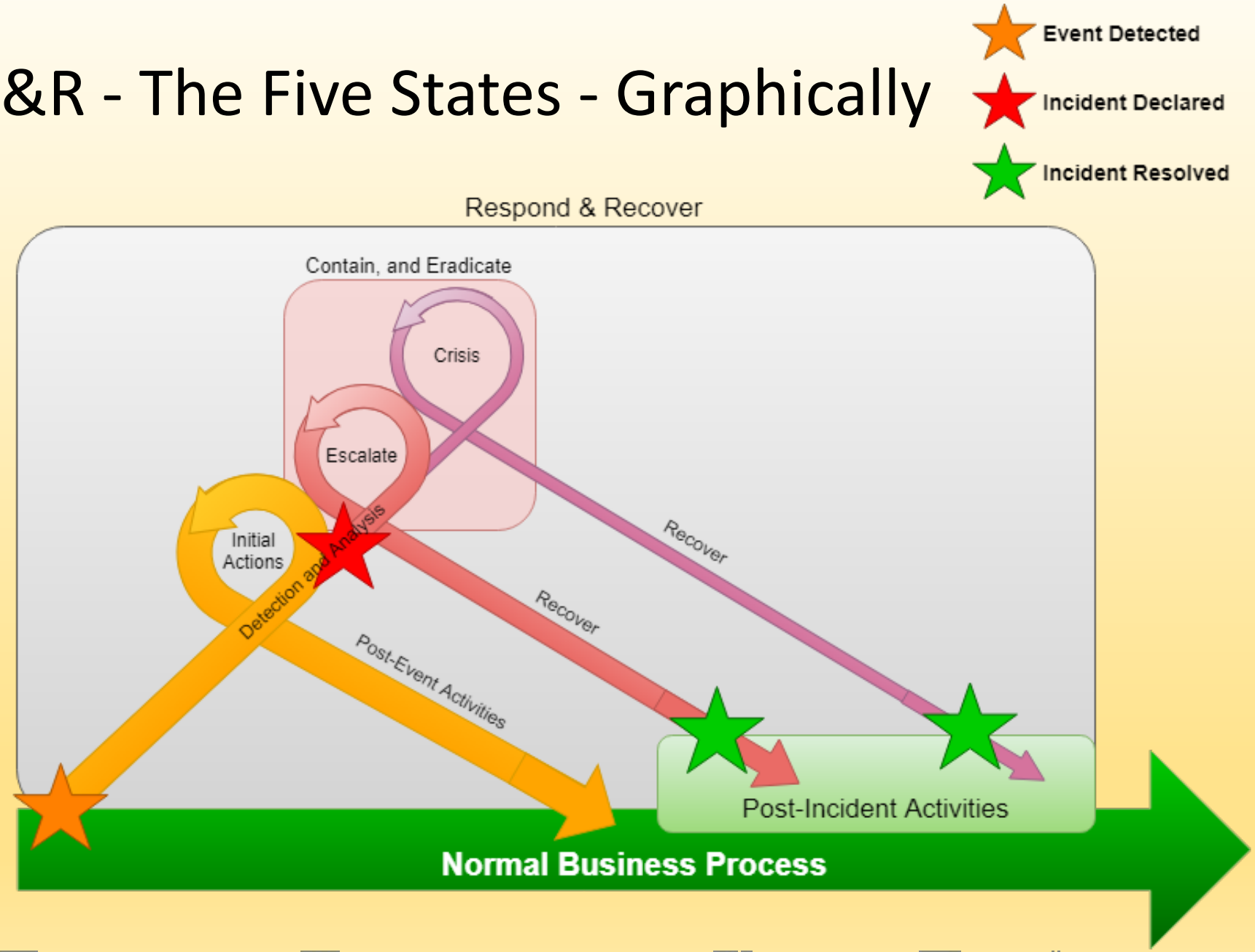
Post-Incident Activities: incident resolved: stand-down · post-incident activities

EVENT/INCIDENT ENDS HERE

Escalate: severity rises · coalesce full teams · enact full response

Crisis: facility resources are overwhelmed · call in external help

R&R - The Five States - Graphically



Each State's Four Page Types

Each ***state*** has four different page types:

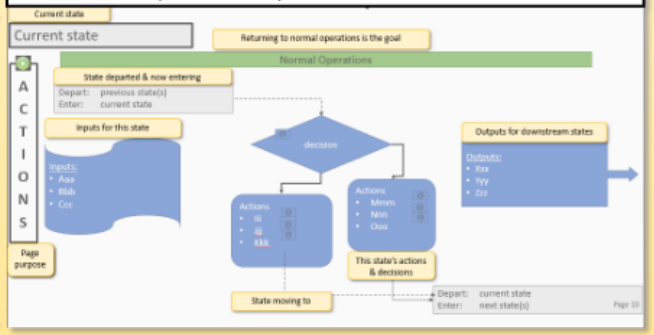
- ***actions*** (what happens)
- ***roles*** (who does what)
- ***process*** (how)
- ***resources*** (with what)

Type of slide

Description of type

ACTIONS

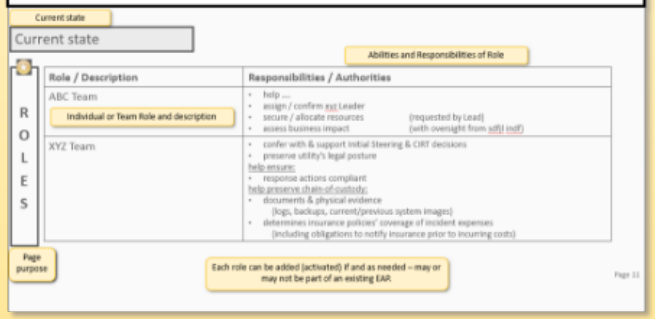
The **"What Happens"**
Inputs and outputs for the current state



Example of slide

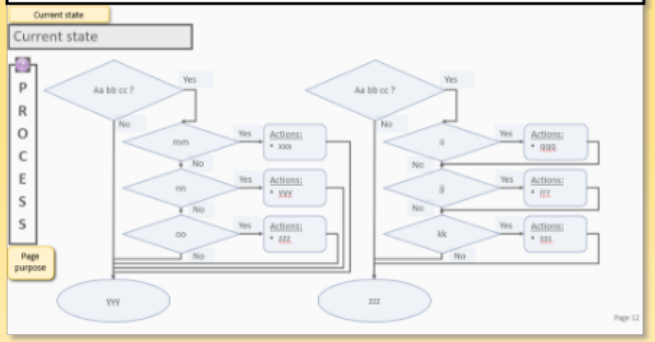
ROLES

The **"Who Does What"**
Roles correlated to actions



PROCESS

The **"How"**
Actions explained in great detail



RESOURCES

The **"With What"**
Resources for current state

ACTIONS Example

Current state

Current state

Reminds that return to normal operations is the goal

Normal Operations

A C T I O N S

State departed & now entering

Depart: previous state(s)
Enter: current state

Inputs for this state

Inputs:
- Aaa
- Bbb
- Ccc

decision

This state's decisions & actions

Actions
- Iii
- Jjj
- Kkk

Actions
- Mmm
- Nnn
- Ooo

Outputs for downstream states

Outputs:
- Xxx
- Yyy
- Zzz

Page purpose

State(s) moved to from this one

Depart: current state
Enter: next state(s)

State moving to

ROLES Example

A state's roles and responsibilities often span several pages.

Current state

Current state

ROLES

Abilities and Responsibilities of Role

Role / Description	Responsibilities / Authorities
ABC Team Individual or Team Role and description	• help …. • assign / confirm xyz Leader • secure / allocate resources (requested by Lead) • assess business impact (with oversight from sdfjl indf)
XYZ Team	• confer with & support Initial Steering Team & CIRT decisions • preserve utility's legal posture help ensure: • response actions compliant help preserve chain-of-custody: • documents & physical evidence (logs, backups, current/previous system images) • determines insurance policies' coverage of incident expenses (including obligations to notify insurance prior to incurring costs)

Page purpose

Each role can be added (activated) if and as needed – may or may not be part of an existing EAP.

Current state

PROCESS Example

Current state

PROCESS

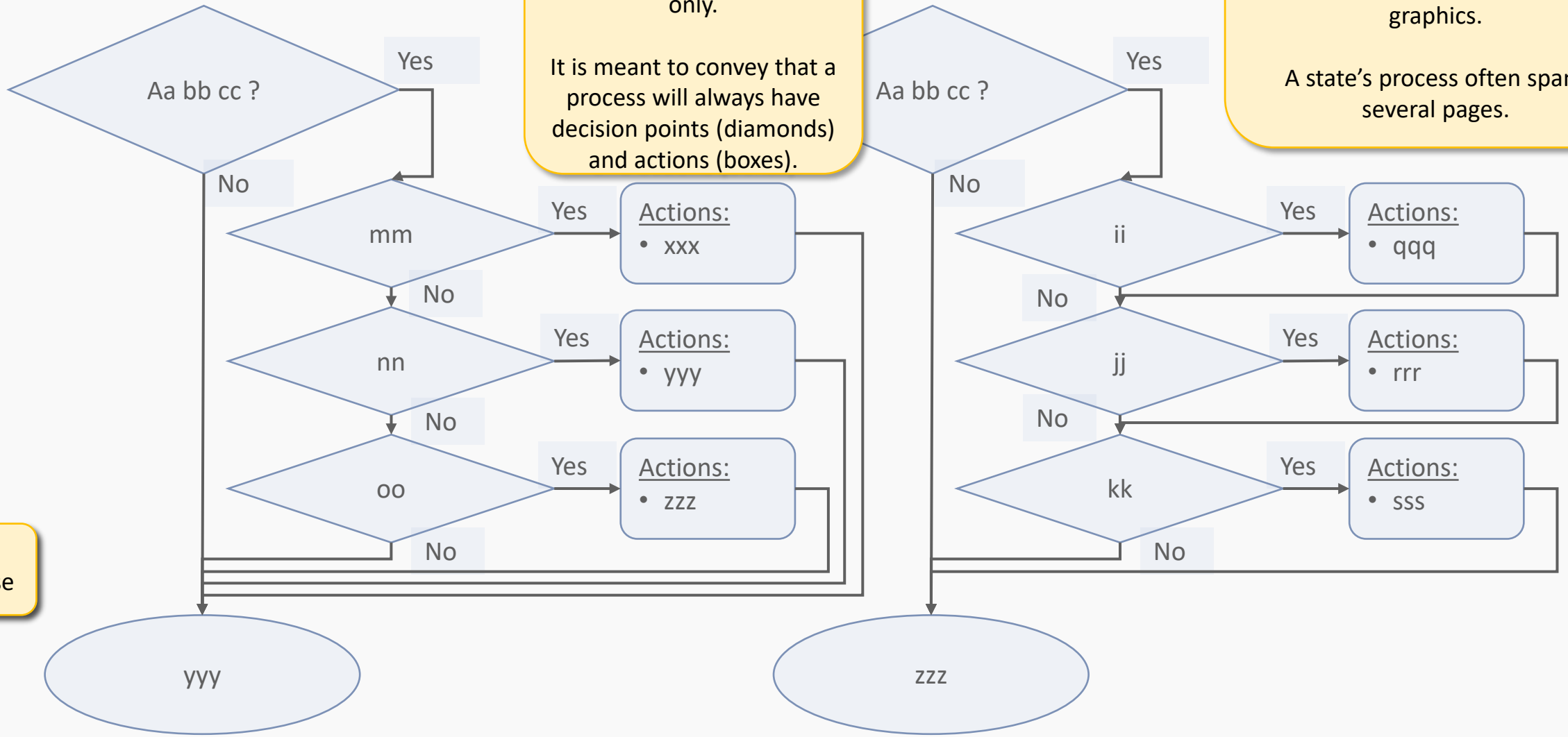
Page purpose

This flowchart is notional only.

It is meant to convey that a process will always have decision points (diamonds) and actions (boxes).

A state's process may be represented by a flowchart as shown here, or by textual descriptions and sometimes graphics.

A state's process often spans several pages.



RESOURCES Example

Current state

Current state

References

RESOURCES

FEMA 64 – *Federal Guidelines for Dam Safety: Emergency Action Planning for Dams*
https://www.fema.gov/ EAP_Federal_Guidelines_FEMA_P-64.pdf

- [Appendix A] *Form : Forms …* (**fillable form**)
- [Appendix B] *Table : Summary of ….* (**responsibilities by job role**)

DOE - *OE-417 Event Reporting Form*
https://www.oe.netl.doe.gov/oe417.aspx

Relevant hyperlinks

FERC – *Chapter 6 – Emergency Action Plans*
https://www.ferc.gov/sites/default/files/2020-04/chap6.pdf

- [page 97] *Appendix 6-F.2: Licensee Responsibilities Summary* **(Roles & Responsibilities, for FERC licensees)**

A state's resources often spans several pages.

These resources and additional ones are gathered at the end in Resources and Supplemental Information.

QR codes for hyperlinks

Page purpose

Initial Emergency Actions

(START HERE)

Initial Emergency Actions

ACTIONS

Normal Operations

Depart: normal operations
Enter: initial emergency actions

Event detected/reported

Inputs:
- SMEs & POCs
- System documentation
- Official Ops
  - Common practice
- Unofficial OPs
  - Unconventional / creative

- Halt destruction & make safe
- Stand up Initial CIRT & Initial Steering Team
- Activate EAP* (if one exists)
- Conduct initial triage
- Determine threat

Outputs:
- Emergency actions
- Event artifacts
- Initial assessment
- Event classification

cyber incident?

yes

Depart: initial emergency actions
Enter: respond & recover

no

Depart: initial emergency actions
Enter: Post-Incident Activities

* Emergency Action Plan (EAP) – may be part of Disaster Recovery Plan.

Initial Emergency Actions

Initial Response Roles

ROLES

Role / Description	Responsibilities / Authorities
Initial CIRT Lead (assigned by Initial Steering Team) (declares a cybersecurity event or incident which is then confirmed by the Steering Team) & **Initial CIRT Technical Staff** (Cyber Incident Response Team) (a.k.a. First Response CIRT)	**A small team of about 1-3 staff** *Smaller teams are agile and flexible if roles are clear.* (whose focus is technical response and who may fill several roles) **Main Purpose:** • Act immediately to triage a cyber event (actions happen in first minutes/hours) • Determine if a cyber incident occurred (often only a misunderstanding, not an actual incident) • Hand off initial facts to Full CIRT (only if incident declared, then team may join Full CIRT) • Participate in post-incident lessons learned / after-action **Initial CIRT Lead** (has working knowledge of facility systems, especially operational systems) (has capable cybersecurity skills) (has good IT/OT relationships & communications skills) • Stand-up & lead Initial CIRT (embedded with & leads CIRT Staff) • Assess response actions impacts (direct team's response actions) • Acquire resources & extra staff (most efficient if Steering handles) • Communicate decision impacts to Initial Steering Team • Coordinate IT technical & OT operations staff • Declare a cybersecurity incident (Initial Steering Team confirms) **Initial CIRT Technical Staff** (often 1-2 staff, called in as needed) • Determine situation & threat (the event's initial triage) • Enact initial responses (halt damage & make safe)

NOTE: Each role can be added (activated) if and as needed – may or may not be part of an existing EAP.

Initial Emergency Actions

Initial Response Roles (continued)

ROLES

Role / Description	Responsibilities / Authorities
Initial Steering Team (may be one person)	• Help coalesce Initial CIRT • Assign / confirm CIRT Leader • Secure / allocate resources (often as requested by CIRT Lead / Staff) • Assess business impact (with management / business office / legal input) • Determine point to engage external support • Authorize contracting with outside agencies • Communicate with outside agency officials
General Counsel (legal)	• Confer with & support Initial Steering Team & CIRT decisions • Preserve utility's legal posture • Assess legal consequences from incident & responses • Determine regulatory & contractual obligations <u>Help ensure:</u> • Response actions are compliant • Local regulations are followed (state/local/tribal/territorial) • Federal regulations are followed • Required disclosures are made <u>Help preserve chain-of-custody:</u> • Documents & physical evidence (logs, backups, current/previous system images) • Determines insurance policies' coverage of incident expenses (including obligations to notify insurance prior to incurring costs)

NOTE: Each role can be added (activated) if and as needed – may or may not be part of an existing EAP.

Initial Emergency Actions

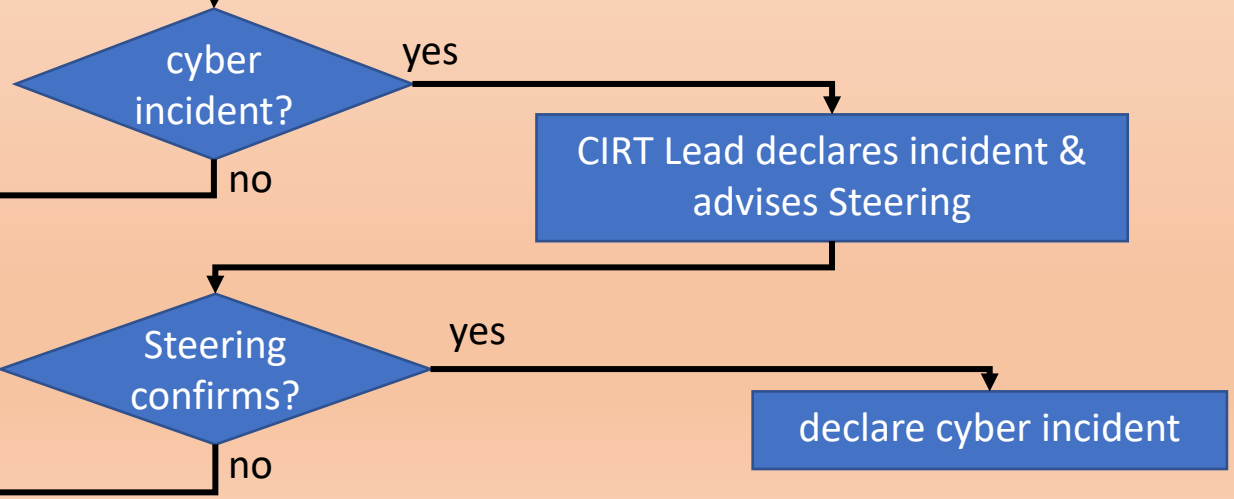
PROCESS

Initial CIRT actions
(is a cyber event not a declared incident yet)

- Declare cyber event
- Stand-up Initial CIRT
- Stand-up Initial Steering Team
- Call in OT & IT technical staff as needed
  (may be remote, at least at first)
- Triage the event
  (begin developing the COP*)
- Take immediate emergency actions
  (CIRT Lead must weigh consequences & okay first)
- Maintain lists & tracking sheets
  (references page has hyperlinks to printable forms)
  (event tracking sheet, POCs lists, notification flowchart)

Initial Steering Team actions

- support Initial CIRT
  - Coalesce team
  - Assign/confirm CIRT leader
  - Support with resources & more staff
  - Stage equipment
  - Coordinate response & messaging
  - Confer with legal & management
  - Inform external organizations



* COP – Common Operating Picture

Initial Emergency Actions

RESOURCES

FEMA 64 – *Federal Guidelines for Dam Safety: Emergency Action Planning for Dams*

https://www.fema.gov/ EAP_Federal_Guidelines_FEMA_P-64.pdf

- [page II-6] *e. EAP Response Process* **(expands on 4 major steps, is for writing an EAP but helpful nonetheless)**
- [page II-6 - II-8] *Step 1: Incident Detection, Evaluation, and Emergency Level Determination* **(4 emergency categories)**
- [Appendix B] *Table B-1: Summary of EAP Responsibilities* (**responsibilities upstream & downstream**)
- [Appendix B] *Table B-2: Summary of the Dam Owner's Responsibilities* (**responsibilities by job role**)
- [Appendix C] *Example Notification Flowchart* (**call sequence**) reproduced in References section
- [Appendix F] *Table F-1: Examples of Notification Information by Emergency Level* (**what to include in messaging**)
- [Appendix G] *Table G-1: Example Emergency Level – Potential Failure* (**dam emergencies with descriptions & actions**)
- [Appendix I] *Table I-1: Example Dam Emergency Incident Log* (**fillable form**)
- [Appendix I] *Table I-2: Example Record of Plan Holders* (**fillable form**)
- [Appendix I] *Table I-4: Example Dam Emergency Termination Log* (**fillable form**)

FEMA

FERC – *Chapter 6 – Emergency Action Plans*

https://www.ferc.gov/sites/default/files/2020-04/chap6.pdf

- [page 97] *Appendix 6-F.2: Licensee Responsibilities Summary* **(Roles & Responsibilities, for FERC licensees, useful for all)**

FERC

Respond & Recover

Respond & Recover

ACTIONS

Depart: initial emergency actions
Enter: respond & recover

- Actively monitor (COP*)
- Continue R&R activities
- Continue support & messaging

Threat change?

no

yes

- Determine targets & severity
- Update COP & evaluate

State change?

no

yes

Inputs:
- Facility equipment status
- Policies (facility/SLTT/federal)

Outputs:
- Threat status communiques
- Required notifications / alerts
- Voluntary notifications / alerts

Depart: respond & recover
Enter: post-incident Activities

~~Depart: respond & recover~~ **(continue R&R)**
Enter: escalate

~~Depart: respond & recover~~ **(continue R&R)**
Enter: crisis

* COP – Common Operating Picture

Respond & Recover

Lead Roles

ROLES

Role / Description	Responsibilities / Authorities
Initial or Full CIRT – Team Lead	• Manage cyber incident start to finish (has working knowledge of facility systems & capable cybersecurity skills) • Direct response procedures • Declare incident threat level & threat changes • Notify/liaise with Steering Team & senior management
Steering Team Lead	• Assess business impact (with SME input) • Secure/allocate resources • Determine point to engage external support • Authorize contracting with outside agencies • Authorize communications (messaging) with outside agency officials
Initial or Full CIRT – Operations Lead (IT/OT Liaison)	• Assess possible impacts to facility control systems (has working knowledge of operations systems) • Direct response actions affecting operations systems • Communicate impacts of decision to CIRT Team Lead • Coordinate IT technical response & OT operation staff (has good IT/OT relationships & communications skills)

NOTE: Each role can be added (activated) if and as needed – may or may not be part of an existing EAP.

NOTE: Situational awareness is vital. Remaining vigilant and actively monitoring is part of each CIRT member's job.

Respond & Recover

OT & IT Technical Roles

ROLES

Role / Description	Responsibilities / Authorities
OT Technical CIRT staff (general) & **IT Technical CIRT staff** (general)	• Investigate cyber incident, perform or support needed analysis (has technical understanding of utility's OT or IT networks, respectively) • Identify appropriate actions & execute (confirms actions with Operations Lead wherever prudent) • Contain & eradicate (core response & recovery actions) (under direction from Operations Lead & sometimes CIRT Lead)
OT & IT Technical CIRT Network Managers	• Secure network devices & communications pathways (may restrict/block network data flow, power down network devices) • Conduct supporting analysis on IT networks or OT networks (has technical understanding of utility's IT or OT networks)
OT & IT Technical CIRT Application/DB Administrators	• Secure databases & systems that contain OT or IT data (may restrict access, backup/image systems, prepare to restore from backup) • Detect abnormal access/behavior (understands normal/baseline operation)
OT & IT Technical CIRT System Administrators	• Secure workstations & servers (may restrict access, disable services, backup/image, restore from backup) • Analyze compromised workstations/servers (understands IT or OT installed applications and data)

Respond & Recover

Communications Team Roles

ROLES

Role / Description	Responsibilities / Authorities
Communications Team Lead (Spokesperson)	• Embedded in CIRT - is considered a CIRT role • POC between & liaises with <u>all</u> incident teams (CIRT, Steering, Legal, internal staff, and external entities)

Communications Team	• Support Communications Team Lead
	• Handle outgoing communications
	  • Prepare messaging
	  • Identify potential stakeholders POCs (external and internal)
	  • Identify communications delivery channels
	  • Support messaging delivery, confirm receipt
	• Handle incoming communications
	  • Handle or route to appropriate responder
	Note: All communications should be on a need-to-know basis

Note: Communications is especially important:
- during an incident's early stages
- if the incident is 'high impact' (negatively affects region or external entities widely or severely)
- if the incident is generating significant media interest

Note: This team is a vital part of incident response, despite its support role.
Pitfalls are avoided by well planned, coordinated, and executed messaging.

Note: The Legal Team normally reviews and approves <u>all</u> communications prior to release.

Legal Team Roles

ROLES

Role / Description	Responsibilities / Authorities
General Counsel / Legal Team	• Work in parallel with Initial/Full CIRT Teams • Preserve utility's legal posture • Assess legal consequences from incident & responses • Determine regulatory & contractual obligations <u>Ensure:</u> • Response actions are compliant • Local regulations are followed (state/local/tribal/territorial) • Federal regulations are followed • Required disclosures are made <u>Preserve chain-of-custody:</u> • Documents & physical evidence (logs, backups, current/previous system images) • Determine insurance policies' coverage of incident expenses (including obligations to notify insurance prior to incurring costs)

Legal Team Roles (continued)

ROLES

Role / Description	Responsibilities / Authorities

General Counsel / Legal Team (continued)	• Issues legal holds for relevant records
	• Retains external expertise
	(in consultation with business office and CIRT & Steering Teams)
	• Prepares legal agreements with 3rd parties assisting with incident:
	  • Non-disclosure agreements (NDA)
	  • Information sharing agreements
	
	<u>Assists Communications Team:</u>
	• Help develop communication plan (internal and external)
	• Help choose appropriate spokesperson
	(usually facility staff member)
	• Help business office develop government relations/notifications plan
	
	Note: Legal counsel normally reviews and approves <u>all</u> communications

Respond & Recover

PROCESS

Four Fundamental Steps

Step 1: Emergency level determination — CATEGORIZE (most EAPs have 4)
- Event detected (reported by anyone)
- Initial triage done (by Initial CIRT & Initial Steering Team)
- Elevated to incident (by CIRT Lead, confirmed by Steering Lead)

Step 2: Notification and communication
- Provide Incident Information to:
  - Local emergency management
  - Non-CIRT facility staff & sister facilities
  - Appropriate oversight agency (normally one of: FERC/USACE/DNR/SLTT)

Step 3: Emergency actions
- Monitor incident, maintain COP*, detect changes, re-evaluate threat level (actions are undertaken by CIRT Lead / Operations Lead / OT & IT Teams)

Step 4: End-of-emergency declaration
- Declared by CIRT Lead & confirmed by Steering Lead
- Communications Team sends concluding messaging
- CIRT staff conduct after-action, collect lessons learned, update response plan
- Legal Team prepares for aftermath (with Business Office involvement)

Response & Recovery actions are many and varied. There are too many variations to include a fully-functional flowchart.

Instead the general steps are given here with links to a more complete process on the Resources page.

The assumption is a team of level-headed technical staff with practical-minded leaders can understand and act.

* COP – Common Operating Picture

Respond & Recover

PROCESS

Steering Lead & Team:

- Support all teams
  - Acquire & distribute resources
  - Oversight of all activities
- Determine when and if to stand up Full CIRT

from: NIST 800-82r2

Response & Recovery is supported by each of these three teams working together.

The general activities and steps are given here.
The Resources page has links to documents with greater details.

The assumption is a team of level-headed technical staff with practical-minded leaders can understand and act.

IT Technical Team / Management:

- Execute the Business Continuity Plan (BCP)
  (less severe: may be called Operational Recovery Plan)
  (more severe: may be called Disaster Recovery Plan)
  (often in Recovery Time Objectives RTO section)
  - IT systems recovery
    (keep computer & communication systems useable)
  - IT systems data recovery
    (databases, files, logs, information about processes)

from: NIST 800-82r2

Communications Lead & Team:

(with guidance from Steering & Legal Teams)

- Prepare messaging
  - Emergency management authorities
    (who decide if/when to declare public emergency)
  - Facility staff (internal non-CIRT staff)
  - Sister facilities (external non-CIRT staff)
  - FERC regional office (if FERC licensee)
  - USACE (if USACE facility)
  - Dept of Natural Resources (if DNR facility)
  - SLTT (if not FERC/USACE/DNR)
- Identify recipient POCs & means of delivery
- Send messaging & confirm receipt

Respond & Recover

RESOURCES

FEMA 64 – *Federal Guidelines for Dam Safety: Emergency Action Planning for Dams*

NOTE: *FEMA 64 is written for response & recovery from physical damage, but much is translatable to response & recovery from cyberattack damage*

https://www.fema.gov EAP_Federal_Guidelines_FEMA_P-64.pdf

- [page II-6] *e. EAP Response Process* **(expands on 4 major steps, is for writing an EAP but helpful nonetheless)**
- [page II-6 – II-8] *Step 1: Incident Detection, Evaluation, and Emergency Level Determination* **(4 emergency categories)**
- [Appendix D] *Table D-1: Sample Guidance Table for Determining Emergency Level* **(for 'sabotage' substitute cyberattack)**
- [page II-9] *Step 2: Notification and Communication* **(overview of how & when described in 3rd & 4th paragraphs)**
- [Appendix C] *Example Notification Flowchart* (**call sequence**) reproduced in References section
- [Appendix F] *Table F-1: Examples of Notification Information by Emergency Level* **(what to include in messaging)**
- [page II-9] *Step 3: Emergency Actions* **(overviewed in 2 paragraphs)**
- [Appendix G] *Table G-1: Example Emergency Level* **(conditions, descriptions, actions; 'sabotage' substitute cyberattack)**

FEMA

FERC – *Chapter 6 – Emergency Action Plans*

https://www.ferc.gov/sites/default/files/2020-04/chap6.pdf

- [page 102] *Appendix 6-H.1: Sample Guidance Table for Determining Emergency Level* **(similar to FEMA 64)**
- [page 110-112] *Table 6-K.1: Example Emergency Level – Potential Failure* **(especially 'sabotage and miscellaneous issues')**
- [page 99] *Appendix G: Example Notification Flowchart* **(meant as example, can serve as a guide)**
- [page 106] *Table 6-J.1: Emergency Notification Information and Messages* **(by severity level, key information to say)**
- [page 107-108] *Example Pre-Scripted Notification Messages* **(by severity level, actual scripts to say)**
- [page 114] *Appendix 6-L.1: Dam Emergency Incident Log* **(printable form)**

FERC

Post-Incident Activities

(FINISH HERE)

Post-Incident Activities

ACTIONS

Normal Operations

Depart: initial actions · monitor · escalate
Enter: Post-Incident Activities

Inputs:
- Stand-down approved

- Stand-down CIRT & Steering Teams
- Notify/assist involved external entities of stand-down
- Complete required/voluntary logging/reporting
- Complete messaging/awareness/communications
- Transmit artifacts to agencies as required/recommended
- Conduct lessons learned & complete after-action report
- Legal Team & Management prepare for after-issues

Incident closure

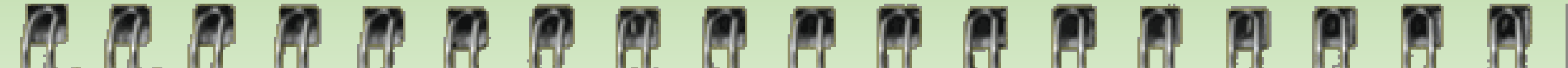
Outputs:
- Logs
- Notifications
- Lessons learned
- Reports submittals

Depart: Post-Incident Activities
Enter: normal operations/steady state

Post-Incident Activities

ROLES

Role / Description	Responsibilities / Authorities
CIRT – Team Lead	• Declare incident response & recovery complete • Notify Steering Team & senior management • Participate in lessons learned / after action (helps organize)
Steering Team (with Management coordination) (guided by Policy Rules from facility SOP's)	• Authorize return to recovered/normal operations • Authorize notification of external agency officials • Authorize internal & external messaging as needed • Replenish resources • Assess business impact (with Business Office) • Participate in lessons learned / after action (helps organize)
Communications	• Complete internal/external notifications & messaging • Participate in lessons learned / after action
Operations Lead (IT/OT Liaison)	• Coordinate IT & OT as they return to normal operations • Notify CIRT Lead when ready to declare end-of-emergency • Participate in lessons learned / after action



Post-Incident Activities

Legal Team · Communications Team Roles

ROLES

Role / Description	Responsibilities / Authorities
OT Technical CIRT (general)	• Return OT assets to normal operations • Revoke temporary accesses given to emergency responders • Participate in lessons learned / after action
IT Technical CIRT (general)	• Return IT assets to normal operations • Revoke temporary accesses given to emergency responders • Participate in lessons learned / after action
Communications Team	• Release messaging when authorized • Ensure all involved entities notified appropriately • Participate in lessons learned / after action
General Counsel / Legal Team	• Participate in lessons learned / after action <u>Prepare for after-events:</u> • Respond to inquiries from law enforcement and regulatory agencies • Lead proactive litigation if any (bringing action) • Lead reactive litigation if any (responding to lawsuit)

Post-Incident Activities

IT/OT Technical Teams · Operations/CIRT Lead

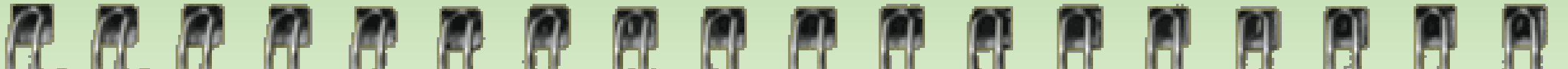
PROCESS

IT Technical Team
- Verify IT systems sufficiently restored
- Notify Operations Lead IT is recovered

OT Technical Team
- Verify OT assets sufficiently restored
- Notify Operations Lead OT is recovered

Operations Lead (IT/OT Liaison)
- Verify operations sufficiently restored
- Notify CIRT Lead ready to declare incident concluded

CIRT Lead
- Declare incident concluded / end of emergency
  (with Steering & Legal Team concurrence if/as needed)
  (likely is outside agency's responsibility if serious incident)
- Stand-down emergency staff & operations
  - EOC
  - Extra physical security / onsite dam monitoring
- Complete Emergency Termination Log



Post-Incident Activities

CIRT Lead · Steering · Legal · Communications

PROCESS

CIRT Lead · Steering · Legal

- Authorize declaration that incident has concluded
  (minimal effort for small incidents, larger effort for severe)
- Assist external entities with concluding emergency
  - Conclude emergency evacuation
- Authorize external & internal messaging
- Check if must file DOE OE-417
- Conduct after-action review
  (with all involved internal staff, possibly some external)
  - Review incident records & logs
  - Identify lessons learned & needed improvements
  - Update Risk Register using incident details
  - Update Threat Profile using incident details
  - Update EAP Incident Response / Disaster Recovery Plans (as applicable)
  - Write After Action Report (AAR)
- Plan to replenish resources

Communications

- Release external & internal messaging
- Notify chain-of-command (including alternates)
- Complete downstream notifications
- Complete public awareness communications

Post-Incident Activities

RESOURCES

FEMA 64 – *Federal Guidelines for Dam Safety: Emergency Action Planning for Dams*
https://www.fema.gov EAP_Federal_Guidelines_FEMA_P-64.pdf
- [page I-3] *Table I-4 - Example Dam Emergency Termination Log* **(printable form)**

FERC – *Chapter 6 – Emergency Action Plans*
https://www.ferc.gov/sites/default/files/2020-04/chap6.pdf
- [page 116] *Appendix 6-L.4: Example Dam Emergency Termination Log* **(printable form)**
- [page 114] *Appendix 6-L.1: Example Dam Incident Log* **(printable form)**

APPA - *American Public Power Cyber Incident Response Playbook*
https://www.publicpower.org/resource/public-power-cyber-incident-response-playbook **(requires registration)**
- [page 32] *Incident Recovery and After-Action Review* **(general steps)**
- [page 56] *Appendix C: DOE Electric Emergency Incident Disturbance Report* **(list of conditions triggering OE-417)**
- [page 57-60] *Appendix C: OE-417 Form* **(the form)**

DOE - *OE-417 Event Reporting Form*
https://www.oe.netl.doe.gov/oe417.aspx
https://www.oe.netl.doe.gov/docs/OE417_Form_05312021.pdf
OE417@hq.doe.gov Telephone: (202) 586-8100 Fax: (202) 586-8485

FEMA

FERC

APPA

OE

OE417 form

Escalate

Escalate

ACTIONS

Depart: any other state
Enter: escalate

Inputs:
- Threat assessment
- Contingency* plan (800-83r2)
- SLTT resources

Actions:
- Activate contingency* plan (if exists)
- Acquire staff & resources (as needed)

Support Actions:
- Stand-up Full CIRT
- Stand-up Full Steering Team
- Stand-up Communications Team
- Stand-up Legal Team

Outputs:
- Continued Operations
- Response/Recovery Status
- Investigation Artifacts
- Notifications/Messaging

Simultaneously: respond & recover

Depart: escalate
Enter: post-incident activities

Simultaneously: respond & recover

Depart: escalate
Enter: crisis

* a.k.a. Emergency Action Plan (EAP). May be part of Disaster Recovery Plan.

Escalate

Lead Roles

ROLES

Role / Description	Responsibilities / Authorities
Full CIRT – Team Lead	• Manage cyber incident start to finish (has working knowledge of facility systems & capable cybersecurity skills) • Direct response procedures • Declare incident threat level & threat changes • Notify/liaise with Steering Team & senior management
Full Steering Team / Management	• Assess business impact (with SME input) • Secure/allocate resources • Determine point to engage external support • Authorize contracting with outside agencies • Communicate with outside agency officials
Full CIRT – Operations Lead (IT/OT Liaison)	• Assess possible impacts to facility control systems (has working knowledge of operations systems) • Direct response actions affecting operations systems • Communicate impacts of decision to CIRT Team Lead • Coordinate IT technical response & OT operation staff (has good IT/OT relationships & communications skills)

NOTE: Each role can be added (activated) if and as needed – may or may not be part of an existing EAP.

NOTE: Situational awareness is vital. Remaining vigilant and actively monitoring is part of <u>each</u> CIRT member's job.

Escalate

OT & IT Technical Roles

ROLES

Role / Description	Responsibilities / Authorities
OT Technical CIRT staff (general) & **IT Technical CIRT staff** (general)	• Investigate cyber incident, perform or support needed analysis (has technical understanding of utility's OT or IT networks, respectively) • Identify appropriate actions & execute (confirms actions with Operations Lead wherever prudent) • Contain & eradicate (core response & recovery actions) (under direction from Operations Lead & sometimes CIRT Lead)
OT & IT Technical CIRT Network Managers	• Secure network devices & communications pathways (may restrict/block network data flow, power down network devices) • Conduct supporting analysis on IT networks or OT networks (has technical understanding of utility's IT or OT networks)
OT & IT Technical CIRT Application/DB Administrators	• Secure databases & systems that contain OT or IT data (may restrict access, backup/image systems, prepare to restore from backup) • Detect abnormal access/behavior (understands normal/baseline operation)
OT & IT Technical CIRT System Administrators	• Secure workstations & servers (may restrict access, disable services, backup/image, restore from backup) • Analyze compromised workstations/servers (understands IT or OT installed applications and data)

Escalate

Communications Team Roles

ROLES

Role / Description	Responsibilities / Authorities
Communications Team Lead (Spokesperson)	• Embedded in CIRT - is considered a CIRT role • POC between & liaises with <u>all</u> incident teams (CIRT, Steering, Legal, internal staff, and external entities)

Communications Team	• Support Communications Team Lead
	• Handle outgoing communications
	  • Prepare messaging
	  • Identify potential stakeholders POCs (external and internal)
	  • Identify communications delivery channels
	  • Support messaging delivery, confirm receipt
	• Handle incoming communications
	  • Handle or route to appropriate responder
	Note: All communications should be on a need-to-know basis

Note: Communications is especially important:
- during an incident's early stages
- if the incident is 'high impact' (negatively affects region or external entities widely or severely)
- if the incident is generating significant media interest

Note: This team is a vital part of incident response, despite its support role.
Pitfalls are avoided by well planned, coordinated, and executed messaging.

Note: The Legal Team normally reviews and approves <u>all</u> communications prior to release.

Legal Team Roles

ROLES

Role / Description	Responsibilities / Authorities
General Counsel / Legal Team	• Work in parallel with Initial/Full CIRT Teams • Preserve utility's legal posture • Assess legal consequences from incident & responses • Determine regulatory & contractual obligations <u>Ensure:</u> • Response actions are compliant • Local regulations are followed (state/local/tribal/territorial) • Federal regulations are followed • Required disclosures are made <u>Preserve chain-of-custody:</u> • Documents & physical evidence (logs, backups, current/previous system images) • Determine insurance policies' coverage of incident expenses (including obligations to notify insurance prior to incurring costs)

Legal Team Roles (continued)

ROLES

Role / Description	Responsibilities / Authorities

General Counsel / Legal Team (continued)	• Issues legal holds for relevant records
	• Retains external expertise
	(in consultation with business office and CIRT & Steering Teams)
	• Prepares legal agreements with 3rd parties assisting with incident:
	  • Non-disclosure agreements (NDA)
	  • Information sharing agreements
	
	<u>Assist Communications Team:</u>
	• Help develop communication plan (internal and external)
	• Help choose appropriate spokesperson
	(usually facility staff member)
	• Help business office develop government relations/notifications plan
	
	Note: Legal counsel normally reviews and approves <u>all</u> communications

Communications Team Roles (continued)

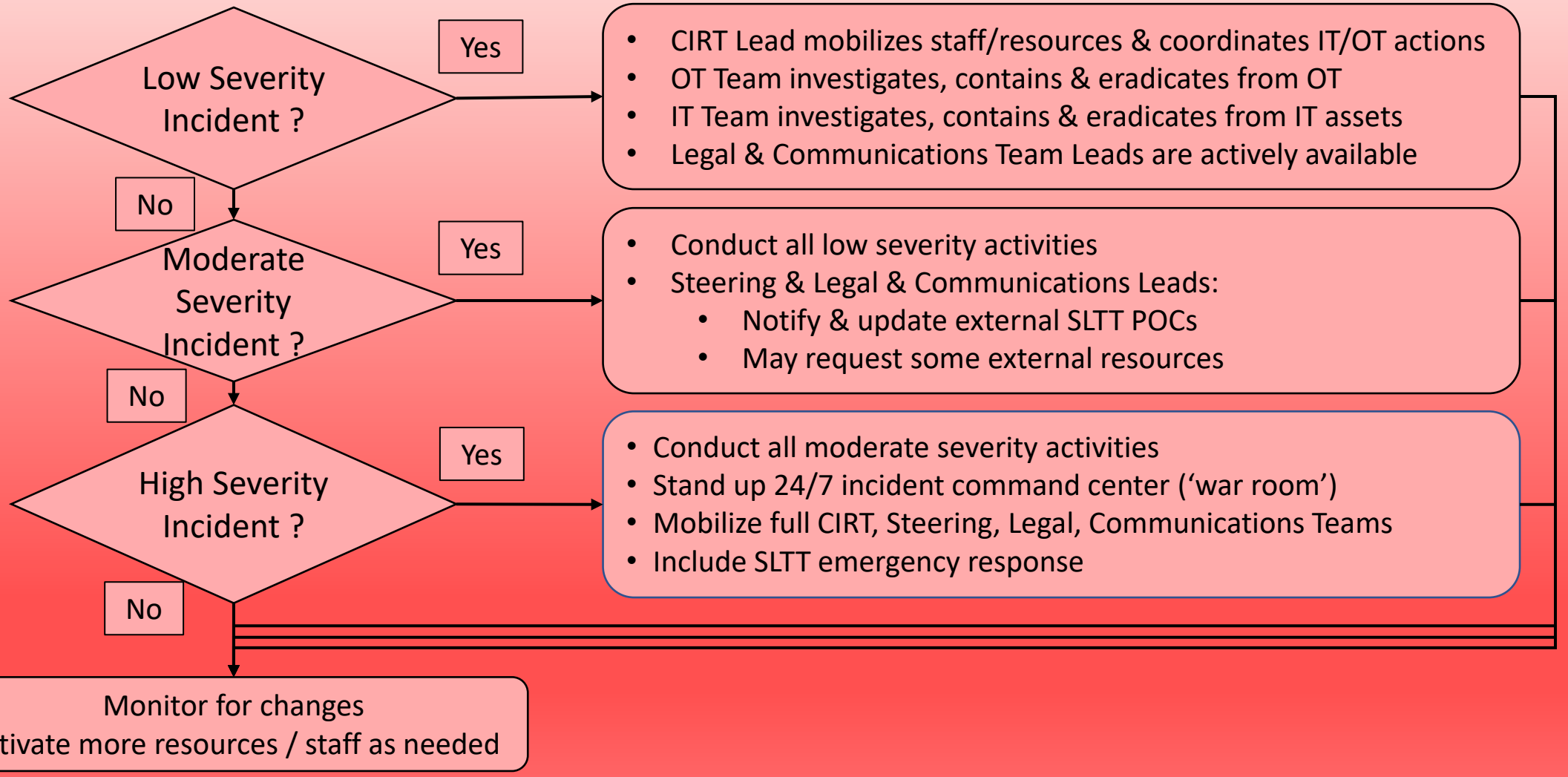
ROLES

Role / Description	Responsibilities / Authorities
Communications Team	<u>Determine stakeholders:</u> • Response stakeholders (external agencies/partners with whom coordinating) (law enforcement, government, utilities, partners, 3rd parties) • Non-response stakeholders (internal non-CIRT staff, customers, media, & SLTT leaders) <u>Prepare messaging:</u> • For internal CIRT to give to response stakeholders • Situational awareness for non-response stakeholders (for both external stakeholders & internal facility staff) <u>Determine:</u> • Types of information different stakeholders need • POC for each need • Media methods/outlets for each stakeholder/need • Key messages • Triggers for alerts/notifications

Escalate

Facility Actions by Incident Severity

PROCESS



- CIRT Lead mobilizes staff/resources & coordinates IT/OT actions
- OT Team investigates, contains & eradicates from OT
- IT Team investigates, contains & eradicates from IT assets
- Legal & Communications Team Leads are actively available

- Conduct all low severity activities
- Steering & Legal & Communications Leads:
  - Notify & update external SLTT POCs
  - May request some external resources

- Conduct all moderate severity activities
- Stand up 24/7 incident command center (‘war room’)
- Mobilize full CIRT, Steering, Legal, Communications Teams
- Include SLTT emergency response

Escalate

Investigate & Document Evidence

PROCESS

Prepare to Document & Preserve:

- The type of the incident
- The date and time of the incident
- If the incident is ongoing
- How the incident was discovered and the personnel who discovered it
- Affected devices, applications, or systems
- Current or anticipated impacts of the incident, both inside and outside the organization
- The type and sensitivity of data stored in affected systems
- Any mitigation measures planned or already taken
- Logs or other records of the incident
- List of stakeholders already contacted or other resources engaged
- Organization and incident response team points-of-contact (POC) details

from: NIST 800-82r2

Consider Pre-Staging Equipment for Forensic Analysis:

- A designated forensic workstation and blank, removable hard drives to create disk images, preserve log files, and save other relevant incident data.
- Spare or virtual workstations, servers, and networking equipment to restore backups, test malware, etc.
- Dedicated laptops installed with digital forensic software to analyze disk images and packet sniffers/protocol analyzers to capture and analyze network traffic.
- Evidence gathering accessories, such as incident handling forms, chain of custody forms, evidence storage bags/tags, and locked evidence storage boxes.

from: NIST 800-82r2

Escalate

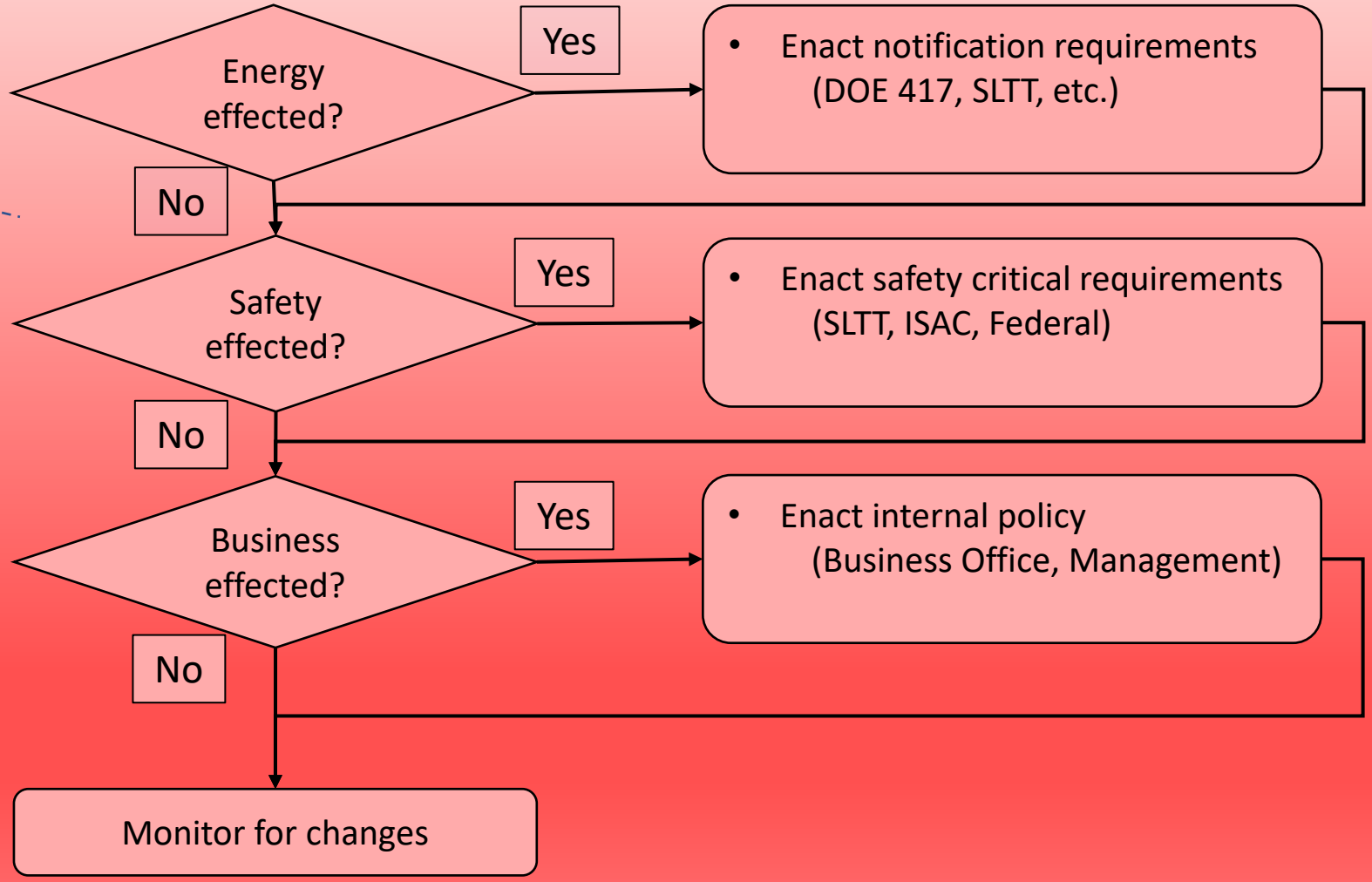
Notify / Report

PROCESS

Escalation actions can become complex, making and including a fully-functional flowchart on a single page isn't feasible.

Instead, general steps are given here with links to a more complete process on the next pages (Resources).

The assumption is a team of level-headed technical staff with practical-minded leaders can understand and act.



Escalate

RESOURCES

ES-C2MS – *Electricity Subsector Cybersecurity Capability Maturity Model* (Version 1.1)
https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf
- [page 39-42] *Event and Incident Response, Continuity of Operations* (**activities for MIL0 MIL1 MIL2**)

ES-C2MS

DHS CISA C2M2 - *Dams Sector Cybersecurity Capability Maturity Model*
https://www.cisa.gov/sites/default/files/publications/dams-c2m2-508.pdf
- [page 40] *Event and Incident Response, Continuity of Operations* (**activities for MIL0 MIL1 MIL2**)
- [page 41-44] *TABLE 13.—Objectives and Practices for the Event and Incident Response, Continuity of Operations, and Service Restoration Domain.* (**activities for MIL0 MIL1 MIL2**)

CISA C2M2

DHS CISA 508 – *Dams Sector Crisis Management Handbook: A Guide for Owners and Operators*:
https://www.cisa.gov/sites/default/files/publications/dams-crisis-management-handbook-2015-508.pdf
"Target Audience: This handbook has been prepared for Dams Sector owners and operators, regardless of the size or type of the facility."
- [page 34] *Notification Flowchart* (**call sequence**) reproduced in References section
- [page 37-38] *Step 2: Notification and Communication* (**3 paragraph description**)
- [page 3] *Response agencies and stakeholders for your community and geographic region* (**POCs list**)

CISA 508

FEMA 64 – *Federal Guidelines for Dam Safety: Emergency Action Planning for Dams*
https://www.fema.gov/ EAP_Federal_Guidelines_FEMA_P-64.pdf
- [Appendix F] Table F-1: Examples of Notification Information by Emergency Level

FEMA

Crisis

Crisis

ACTIONS

Depart: any other state
Enter: crisis

Inputs:

- Incident artifacts
- Status of facility devices & systems

Actions:

- Activate Incident Command System (NIMS ICS)
- Transition to external command
- Support external command

Outputs:

- Support Incident Commander & Teams

Simultaneously: respond & recover

Depart: crisis
Enter: post-incident activities

Facility Staff / Teams

ROLES

Role / Description	Responsibilities / Authorities
Steering Committee	• Activate NIMS Incident Command System • Activate Mutual Aid/Compacts • Transition to support role (e.g. MAC Group)
Cyber Incident Response Team	• Transfer incident artifacts to Incident Commander/Team • Transition to support role (e.g. ICS, EOC, JIS)
System Owner(s)	• Continue securing systems & networks as much as possible • May continue working to identify source of attack
Engineering Manager	• Dispatch engineers/crews as necessary • Dispatch liaison to SLTT (County EOC)
Dam Operator	• Operate facility equipment in emergency mode/manually

Hydroplant staff may be asked to join incoming teams

FBI, CERT, DOE, DHS, EA organizations, state EA team, National Guard

NIMS Incident Command System Leads

ROLES

Role / Description	Responsibilities / Authorities
Incident Commander	• Has overall management responsibility for the incident
Public Information Officer & Staff	• Disseminates community information to the public
Safety Officer & Staff	• Assesses safety hazards and works to ensure personnel safety during incident operations
Liaison Officer & Staff	• Provides the single point of contact for those that are not part of the command staff
Intelligence Investigation Officer & Staff (optional)	• Coordinates intelligence and investigation efforts

ROLES

Role / Description	Responsibilities / Authorities
Operations Section Chief & Staff	• Manages all aspects of the Operations Section • Provides the tactical assignments documented in the Incident Action Plan (IAP) and directs its execution • Makes expedient changes to current operations based on the complexity or magnitude of the incident and reports those changes to the Incident Commander (IC) • Manages all operations and progress related to the incident • Ensures the safety and welfare of Operations Section personnel 6. Coordinates operations at the local level • Establishes or transitions into the Operations Section • Supervises and configures section with branches, divisions, groups, and units to support operations

ROLES

Role / Description	Responsibilities / Authorities
Planning **Section Chief & Staff**	• Manages all aspects of the Planning Section • Coordinates planning efforts across multiple jurisdictions • Develops & implements transition plan based on escalating incident complexity • Manages the preparation of strategies and plans for the incident and submits incident status reports • Prepares, collects, evaluates, disseminates, and uses incident information to develop the Incident Action Plan (IAP) • Facilitates incident information to maintain situational awareness (current and future) • Provides periodic predictions on incident potential and incident course of actions • Coordinates planning efforts at the local level • Establishes or transitions into the Planning Section • Supervises and configures section with units and single resources as necessary

ROLES

Role / Description	Responsibilities / Authorities
Logistics **Section Chief & Staff**	• Manages logistical needs across the five mission areas for incidents (protection, prevention, mitigation, response, and recovery) • Provides facilities, services, people, and materials in support of the incident • Advises the Incident Commander (IC) on all matters relating to logistics planning, facilities, communications, ordering, receipt, storage, transport, and onward movement of goods, services, and personnel • Coordinates logistics at the local level • Establishes or transitions into the Logistics Section • Supervises and configures section to support operations with branches, divisions, groups, and units as necessary • Supports or participates in the Incident Action Plan (IAP) process as necessary

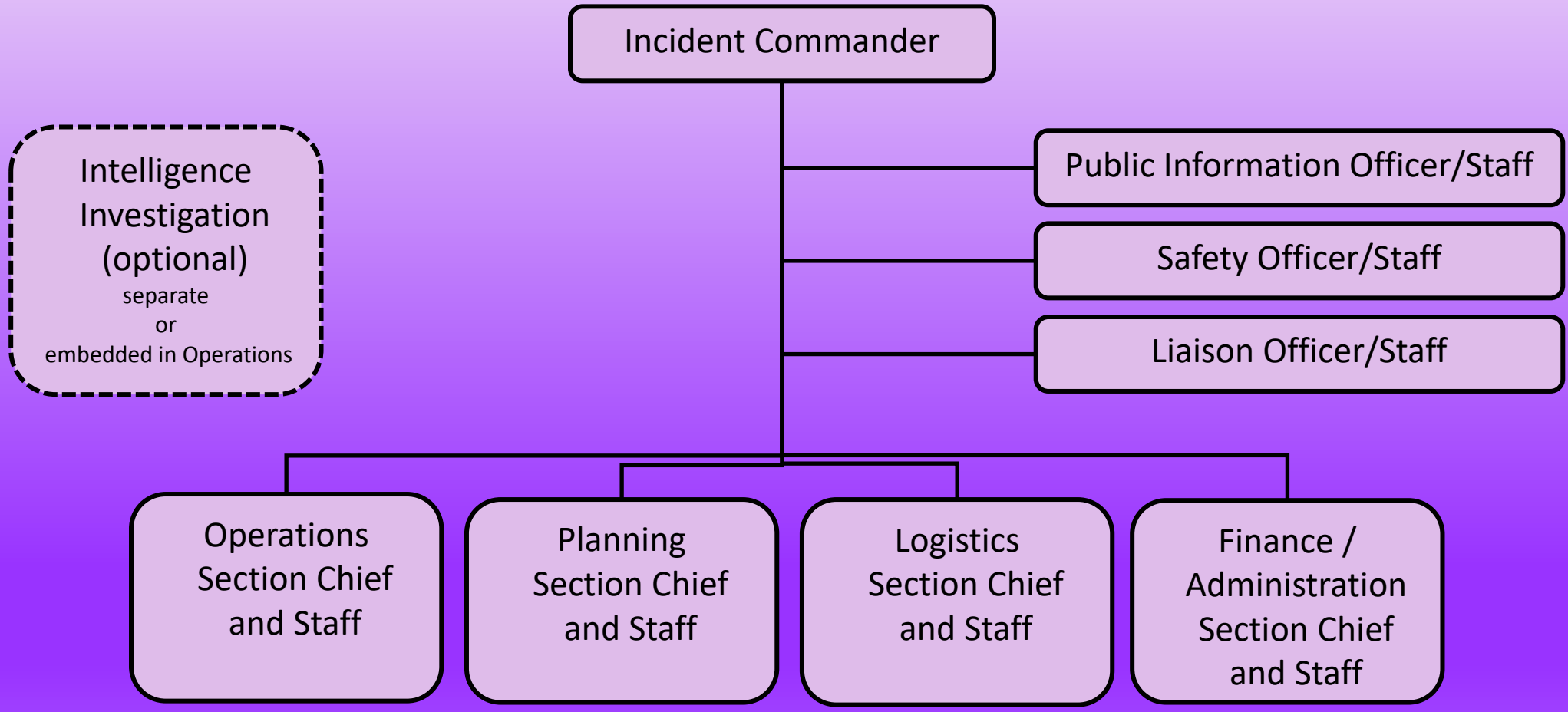
ROLES

Role / Description	Responsibilities / Authorities
Finance / Administration Section Chief & Staff	• Is responsible for all financial, administrative, and cost analysis aspects of an incident • Maintains daily contact with agency administrative headquarters on finance and administration matters • Meets with assisting and cooperating agency representatives • Advises the Incident Commander on financial and administrative matters • Develops the operating plan for the Finance/Administration Section • Coordinates finances at the local level • Establishes or transitions into an existing Finance/Administration Section • Supervises and configures section with units to support as necessary

Crisis

NIMS Incident Command System Structure

ROLES



Crisis

NIMS Incident Response Team (main actions)

PROCESS

Actions:

NIMS ICS*-qualified personnel will:

- Stand-up Incident Command System Structure — for tactical coordination
- Engage Emergency Operations Center (EOC) — for coordinated operational support
  (EOC may operate at partial or full activation)
- Deploy Joint Information System (JIS) — for coordinated information flow
- Assemble Multi Agency Coordination (MAC) Group — for policy level coordination

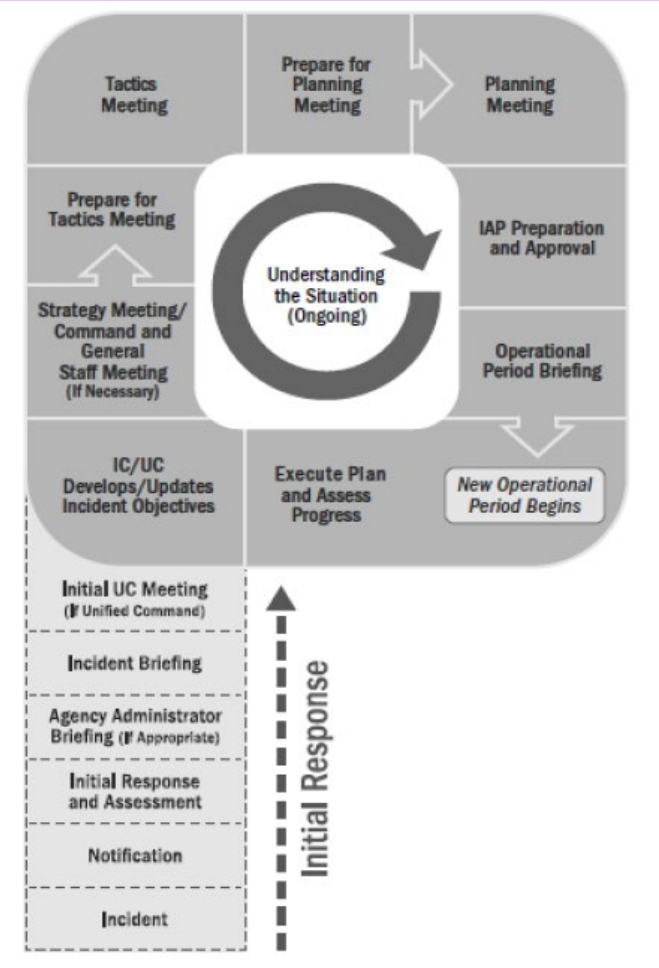
- Utilize hydroplant facility staff's expertise

*ICS stands for Incident Command System in the context of Crisis Response and Recovery (not Industrial Control System)
The ICS, EOC, JIS, and MAC Group structure are outside hydro facilities' purview and beyond the scope of this guide.

Crisis

NIMS Support Team (main actions)

P R O C E S S



NIMS (FEMA-ICS)

←

Operational Period Planning Cycle:

1. Identify Requirements
2. Acquire Resources
3. Mobilize Resources

Resource Management Process: →

(Leverage Mutual Aid Agreements & Compacts)

1. Identify Requirements
2. Acquire Resources
3. Mobilize Resources
4. Track Resources – Keep Records
5. Demobilize
6. Reimburse & Restock

from FEMA NIMS 2017 Learning Materials document

RESOURCES

NIMS – ICS (FEMA's National Incident Management System – Incident Command System)
(2017 NIMS)

NIMS website:
https://www.fema.gov/emergency-managers/nims

National Incident Management System:
https://www.fema.gov/media-library-data/1508151197225-ced8c60378c3936adb92c1a3ee6f6564/FINAL_NIMS_2017.pdf

NIMS Overview: (excellent detailed overview of NIMS structure, roles, and functioning)
https://training.fema.gov/nims/docs/nims.2017.instructor%20student%20learning%20materials.pdf

NIMS Site

NIMS Document

NIMS Overview

Crisis

RESOURCES

Other External Assistance:

- US-CERT, ICS-CERT, ESCC Cyber Mutual Assistance Program
- DOE CESER Energy cybersecurity Assistance
- Department of Homeland Security (DHS)
  - Presidential Policy Directive (PPD)-41 Cyber Incident Coordination
  - National Cybersecurity and Communications Integration Center (NCCIC)
  - NCCIC Hunt and Incident Response Team (HIRT)
  - NCCIC's Incident Response Team
- ODNI Cyber Threat Intelligence Integration Center
- DOD Defense Support of Civil Authorities
- DOE 417
- E-ISAC
- MS-ISAC
- US-CERT
- ICS-CERT
- ESCC
- SANS
- ISC2

Facility Resources:

(Don't forget about resources not commonly used.)

- Policy Rules from facility processes (SOP's)
- Management
- Business Office
- Mutual Assistance Agreements
- Vendors
- Local Emergency Response POCs
- Regional Incident Response Center

Resources and Supplemental Information

Major Steps in Incident Response & Recovery

from NIST 800-61r2 [page 42]

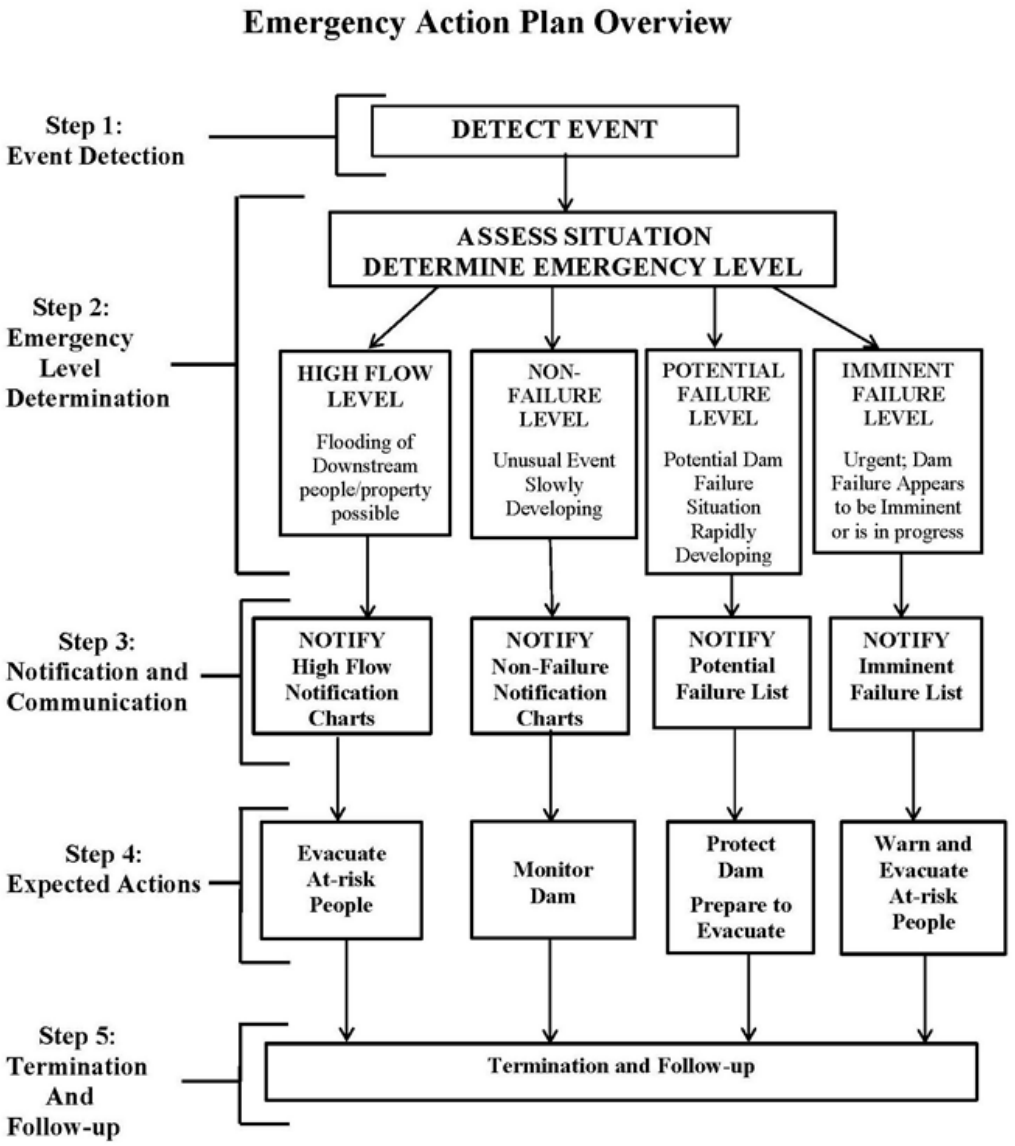
The checklist in Table 3-5 provides the major steps to be performed in the handling of an incident. Note that the actual steps performed may vary based on the type of incident and the nature of individual incidents. For example, if the handler knows exactly what has happened based on analysis of indicators (Step 1.1), there may be no need to perform Steps 1.2 or 1.3 to further research the activity. The checklist provides guidelines to handlers on the major steps that should be performed; it does not dictate the exact sequence of steps that should always be followed.

Table 3-5. Incident Handling Checklist

	Action	Completed
	Detection and 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)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and 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 (5) and eradicate (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	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

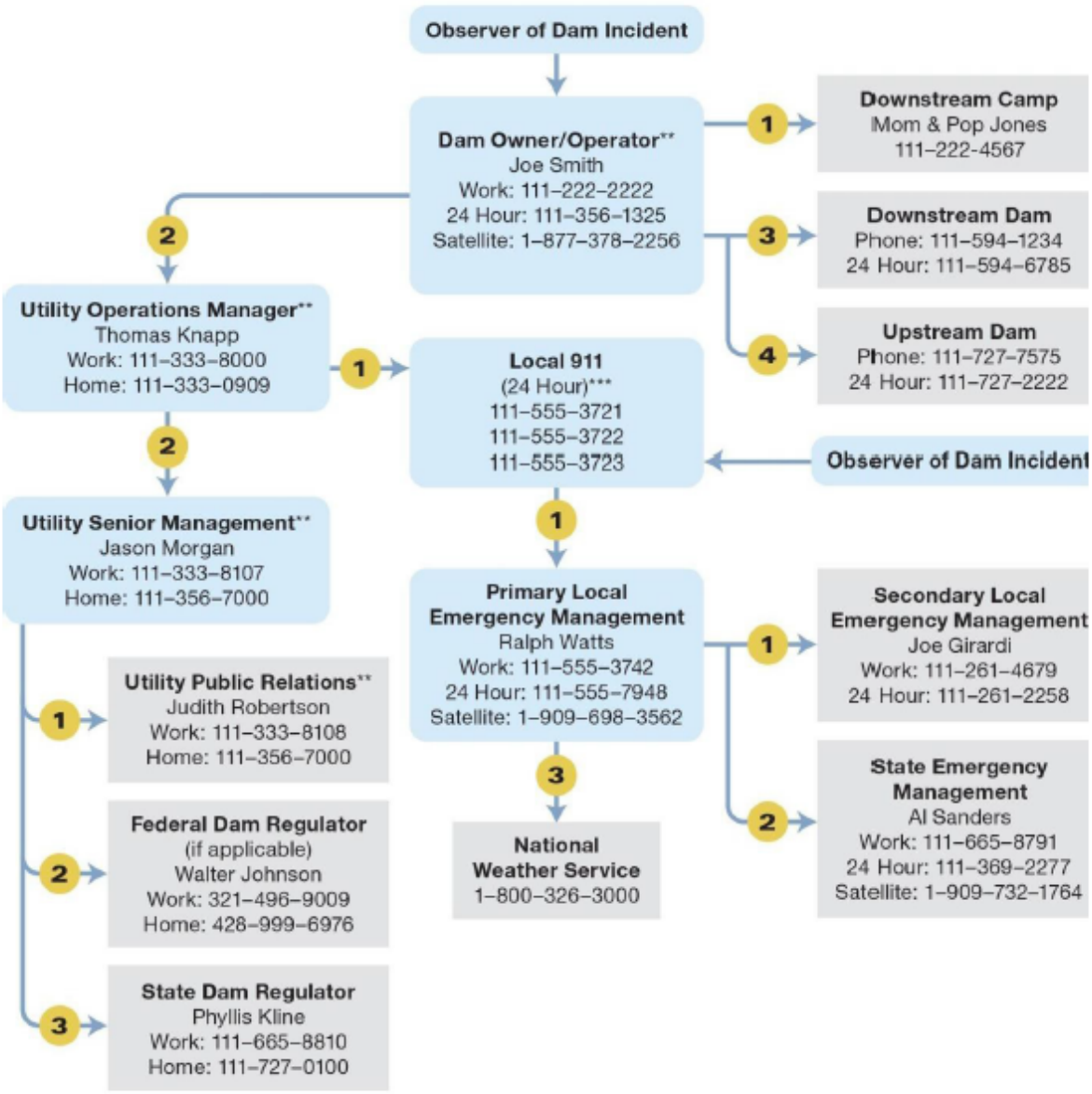
Major Steps in Incident Response & Recovery (graphic)

This graphic shows a typical 5-step EAP (Emergency Action Plan)



II. Notification Flowchart

Warning: Notification charts must be customized per local circumstances



= call sequence

* Use this chart in coordination with Notification Contact Table for additional contact information.

** Utility personnel should refer to EAP for sample warning messages.

*** Call Dam Operator if 911 is notified by non-utility observer.

Notification Flowchart from DHS CISA 508 [page 34]

Summary of Roles: IT & OT Leads and Teams

from the APPA CIR Playbook v11a

(Cyber) Incident Response Team Lead
- has working knowledge of facility IT systems
- has capable cybersecurity skills
- manages cyber incident beginning to end
- directs response procedures
- declares incident, categorizes severity including elevation
- notifies/liaises with senior management
- notifies/coordinates with Steering Committee

IT/OT Liaison / Operations Lead
- assesses possible impacts on facility control systems
  (has working knowledge of operations systems (e.g. SCADA, DMS))
- directs response actions that affect operations equipment/systems
- communicates impacts of decisions to CIRT Lead
- coordinate IT Technical Response and OT Operations Staff
  (has good relationships with IT/OT and good communication skills

Senior Management
- assesses business impact (with SME input)
- allocates resources
- determines point to (voluntarily) engage external support/mutual aid
- authorizes contracting with outside services
- communicates with outside agency officials

IT Technical Response Staff (generally)
(facility staff, municipal, contracted IT security dept)
- investigates/analyzes cyber incidents
- identifies & executes actions to contain/eradicate/respond/recover
  (under direction from Cyber Incident Response Manager)

IT Technical Response Staff – Network Manager
- analyzes, restricts, or blocks data flow to/from network
  (has technical understanding of whole utility's network)

IT Technical Response Staff – Workstation/Server Administrator
- analyzes compromised workstations/servers

IT Technical Response Staff – Application/Database Administrator
- detects abnormal behavior
  (has technical understanding of normal/baseline operation)

IT Technical Response Staff – Forensic Investigator
- determines root cause analysis
- gathers/analyzes evidence in legally admissible manner
  (under direction of legal counsel)

NOTE: Most bullets are phrased as actions – appropriate because recov[illegible]espon[illegible]re acti[illegible]s. But[illegible]e bull[illegible]e attrib[illegible]s whic[illegible] the p[illegible]n fulfil[illegible]he rol[illegible]st hav[illegible]

Summary of Roles: Communications Team

from the APPA CIR Playbook v11a

Note: *Communications is especially important during an incident's early stages, if the incident is 'high impact' (negatively affects region or external entities widely or severely) or is generating significant media interest.*
Note: *This team is a vital part of incident response, despite its support role. Pitfalls are avoided by well planned, coordinated, and executed messaging.*
Note: *The Legal Counsel/Team normally reviews and approves <u>all</u> communications prior to release.*
Note: *All communications should be on a need-to-know basis.*

Communications Team Lead
- Liaises between CIRT and Public Relations/Communications Team (embedded in CIRT, is considered a CIRT role)
- Liaises with Legal Counsel/Team

Communications Team
- Supports CIRT by crafting messaging to external stakeholders (coordinates with designated CIRT POC for this)
- Responds to inquiries from media, customers, and facility staff
- Coordinates messaging with sister utilities and external partners (for significant cyber events)

Communications Team (continued)
- Identify potential stakeholders/stakeholder groups (external and internal)
- Determine types of information different stakeholders need
- Determine POC for each need
  - response stakeholders (messaging prepared for internal CIRT to give to external agencies/partners with whom coordinating such as law enforcement, government, utilities, industry partners, and other such 3rd parties)
  - non-response stakeholders (primarily situational awareness messages for internal non-CIRT staff such as employees, customers, media, SLTT leaders)
- determine media methods/outlets for each stakeholder/need
- determine key messages
- determine triggers for alerts/notifications

Checklists
- communications timing
- trigger events w/prepared statement templates
  examples:
  - triggers: widespread/extended, effect customer-facing, widely reported/speculated, effect staff-facing, staff action required
  - templates: confirm incident, communicate R&R EAP

Summary of Roles: General Counsel / Legal Team

from the APPA CIR Playbook v11a

General Counsel / Legal Team

- works in parallel with Initial/Full CIRT
- preserves utility's legal posture
- assesses legal consequences stemming from incident and responses
- ensures:
  - compliance with regulations and contractual obligations
  - response actions comply
  - local regulations followed (municipal/county/tribal/state)
  - federal regulations followed
  - required disclosures made

<u>If event was initially reported to the facility by a service provider or business partner:</u>

- ensures appropriate internal/external notifications done
- confirms service provider/partner complies with utility's legal requirements
- seeks legal remedy/indemnification/reimbursement as appropriate

<u>If incident compromises PII:</u>

- assists investigation
- ensures properly documented
- oversees notifying affected individuals according to law
  (includes contracting credit monitoring, mail/email/call centers)
- oversees notifying 3rd parties (e.g. payment card, credit agencies)
- preserves chain-of-custody for:
  - documents
  - physical evidence (e.g. logs, backups, current/previous system images)
- issues legal holds for relevant records
- retains external expertise
  (in consultation with CIRT Team, Steering Committee, and Business Office)
- prepares legal agreements with 3rd parties assisting with incident:
  - non-disclosure agreements
  - information sharing agreements
- assists Communications POC/Team
  ****Legal counsel normally reviews and approves all communications*
  - helps develop communication plan (internal and external)
  - helps choose appropriate spokesperson (usually facility staff member)
  - helps business unit develop government relations/notifications plan
- determines insurance policies' coverage of incident expenses
  (including any obligations to notify insurance prior to incurring costs)

<u>In aftermath:</u>

- responds to inquiries from law enforcement and regulatory agencies
- leads proactive litigation if any (bringing action)
- leads reactive litigation if any (responding to lawsuit)

Resources: Assessing · Communicating

FEMA 64 – *Federal Guidelines for Dam Safety: Emergency Action Planning for Dams*

NOTE: *FEMA 64 is written for response & recovery from physical damage, but much is translatable to response & recovery from cyberattack damage*

https://www.fema.gov EAP_Federal_Guidelines_FEMA_P-64.pdf

FEMA

- [page II-6] *e. EAP Response Process* **(expands on 4 major steps, is for writing an EAP but helpful nonetheless)**
- [page II-6 – II-8] *Step 1: Incident Detection, Evaluation, and Emergency Level Determination* **(4 emergency categories)**
- [Appendix D] *Table D-1: Sample Guidance Table for Determining Emergency Level* **(for 'sabotage' substitute cyberattack)**
- [page II-9] *Step 2: Notification and Communication* **(overview of how & when described in 3rd & 4th paragraphs)**
- [Appendix C] *Example Notification Flowchart* (**call sequence**) reproduced in References section
- [Appendix F] *Table F-1: Examples of Notification Information by Emergency Level* **(what to include in messaging)**
- [page II-9] *Step 3: Emergency Actions* **(overviewed in 2 paragraphs)**
- [Appendix G] *Table G-1: Example Emergency Level* **(conditions, descriptions, actions; 'sabotage' substitute cyberattack)**

FERC – *Chapter 6 – Emergency Action Plans*

https://www.ferc.gov/sites/default/files/2020-04/chap6.pdf

FERC

- [page 102] *Appendix 6-H.1: Sample Guidance Table for Determining Emergency Level* **(similar to FEMA 64)**
- [page 110-112] *Table 6-K.1: Example Emergency Level – Potential Failure* **(especially 'sabotage and miscellaneous issues')**
- [page 99] *Appendix G: Example Notification Flowchart* **(meant as example, can serve as a guide)**
- [page 106] *Table 6-J.1: Emergency Notification Information and Messages* **(by severity level, key information to say)**
- [page 107-108] *Example Pre-Scripted Notification Messages* **(by severity level, actual scripts to say)**
- [page 114] *Appendix 6-L.1: Dam Emergency Incident Log* **(printable form)**

Resources: Escalating · Communicating

ES-C2MS – *Electricity Subsector Cybersecurity Capability Maturity Model* (Version 1.1)
https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf
- [page 39-42] *Event and Incident Response, Continuity of Operations* (**activities for MIL0 MIL1 MIL2**)

ES-C2MS

DHS CISA C2M2 - *Dams Sector Cybersecurity Capability Maturity Model*
https://www.cisa.gov/sites/default/files/publications/dams-c2m2-508.pdf
- [page 40] *Event and Incident Response, Continuity of Operations* (**activities for MIL0 MIL1 MIL2**)
- [page 41-44] *TABLE 13.—Objectives and Practices for the Event and Incident Response, Continuity of Operations, and Service Restoration Domain.* (**activities for MIL0 MIL1 MIL2**)

CISA C2M2

DHS CISA 508 – *Dams Sector Crisis Management Handbook: A Guide for Owners and Operators*:
https://www.cisa.gov/sites/default/files/publications/dams-crisis-management-handbook-2015-508.pdf
"Target Audience: This handbook has been prepared for Dams Sector owners and operators, regardless of the size or type of the facility."
- [page 34] *Notification Flowchart* (**call sequence**) reproduced in References section
- [page 37-38] *Step 2: Notification and Communication* (**3 paragraph description**)
- [page 3] *Response agencies and stakeholders for your community and geographic region* (**POCs list**)

CISA 508

FEMA 64 – *Federal Guidelines for Dam Safety: Emergency Action Planning for Dams*
https://www.fema.gov/ EAP_Federal_Guidelines_FEMA_P-64.pdf
- [Appendix F] Table F-1: Examples of Notification Information by Emergency Level

FEMA

Resources: Prioritizing · Containing · Responding · Communicating

NIST SP 800-61r2 - *Computer Security Incident Handling Guide*
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST 800

- [page 32] *3.2.6: Incident Prioritization* **(how to prioritize simultaneous incidents, 1st paragraph & 3 bullets)**
- [page 32] *3.2.6: Incident Prioritization* **(how to prioritize simultaneous incidents, 1st paragraph & 3 bullets)**
- [page 33] *Table 3-2. Functional Impact Categories* **(4 categories with definitions, helpful for prioritizing)**
- [page 33] *Table 3-3. Information Impact Categories* **(4 categories with definitions, helpful for prioritizing)**
- [page 33] *Table 3-4. Recoverability Effort Categories* **(4 categories with definitions, helpful for prioritizing)**
- [page 34] *Who should be notified (typically)* **(bulleted list)**
- [page 34] *Notification Methods* **(bulleted list)**
- [page 35] *Choosing a Containment Strategy* **(bulleted list of things to consider)**
- [page 36] *Evidence Gathering and Handling* **(bulleted list of chain-of-custody information to log, so is admissible in court)**

APPA - *American Public Power Cyber Incident Response Playbook*
https://www.publicpower.org/resource/public-power-cyber-incident-response-playbook **(requires registration)**

APPA

- [page 48-50] *Appendix A: Incident Response Plan Outline* **(EAP overview, most helpful for supporting incident response)**
- [page 51-55] *Appendix B: Incident Handling Forms* **(printable forms: contacts, asset inventory, start-to-end incident details)**
- [page 61-64] *Appendix D: Sample Cyber Mutual Assistance Program NDA* **(example NDA)**

Resources: Post-Incident Recovery

APPA - *American Public Power Cyber Incident Response Playbook*
https://www.publicpower.org/resource/public-power-cyber-incident-response-playbook **(requires registration)**

- [page 56] *Appendix C: DOE Electric Emergency Incident Disturbance Report* **(list of conditions triggering OE-417)**
- [page 57-60] *Appendix C: OE-417 Form* **(the form)**

APPA

DOE-OE-417 Event Reporting Form
https://www.oe.netl.doe.gov/oe417.aspx
https://www.oe.netl.doe.gov/docs/OE417_Form_05312021.pdf
OE417@hq.doe.gov Telephone: (202) 586-8100 Fax: (202) 586-8485

DOE OE

OE417

ES-C2MS – *Electricity Subsector Cybersecurity Capability Maturity Model* (Version 1.1)
https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

- [page 53-62] *Appendix A: References*
- [page 63-76] *Appendix B: Glossary*
- [page 77-78] *Appendix C: Acronyms*

ES-C2MS

Resources: IC3 · FBI · MS-ISAC

Internet Crime Complaint Center
www.ic3.gov

IC3

FBI Find your field office
www.fbi.gov/contact-us/field

FBI

MS-ISAC Security Operations Center
soc@msisac.org
866-787-4722
(can be contacted 24/7)

Resources: SANS Incident Forms and Logs

Contacts Lists

Contacts:	https://www.sans.org/score/incident-forms/IH-Contacts.pdf
Intellectual Property:	https://www.sans.org/score/incident-forms/IPIH-Contacts.pdf

Forms

Initial Incident Summary:	https://www.sans.org/score/incident-forms/IH-Identification.pdf
Effected System(s):	https://www.sans.org/score/incident-forms/IH-Survey.pdf
Intellectual Property:	https://www.sans.org/score/incident-forms/IPIH-FormChecklist.pdf
System Containment:	https://www.sans.org/score/incident-forms/IH-Containment.pdf
Eradication:	https://www.sans.org/score/incident-forms/IH-Eradication.pdf

SANS Incident Forms

Logs

Communications:	https://www.sans.org/score/incident-forms/IH-CommunicationLog.pdf

NIMS Crisis Management: Incident Command System Training

Recommended Sequence of ICS Training

All Emergency Management Practitioners

IS 0100: Introduction to the Incident Command System, ICS 100
IS 0700: National Incident Management System (NIMS), An Introduction

Emergency Management Supervisors add

IS 0200: Incident Command System for Single Resources and Initial Action Incidents
IS 0800: National Response Framework, An Introduction

Advanced NIMS Training for ICS Leaders/ Supervisors

G 0191: ICS/EOC Interface
E/L/G 0300: Intermediate ICS for Expanding Incidents
E/L/G 0400: Advanced ICS for Command and General Staff
NIMS ICS All Hazards Position Specific Courses (E/L/G 0949-0991)

NIMS Crisis Management: Emergency Operations Center Training

Recommended Sequence of EOC Training

All Emergency Management Practitioners

IS 0100: Introduction to the Incident Command System, ICS 100

IS 0700: National Incident Management System (NIMS), An Introduction

Emergency Management Supervisors add

IS 0775 or *IS 2200 (in development)* Basic EOC Management and Operations

IS 0800: National Response Framework, An Introduction

Advanced NIMS Training for EOC Leaders/ Supervisors

G 0191 ICS/EOC Interface Workshop

E/L/G 0775 or *E/L/G 2300 (in development)* Intermediate EOC Management and Operations

NIMS Crisis Management: Learn More About NIMS

FEMA National Incident Management System	https://www.fema.gov/national-incident-management-system
The Resource Typing Library Tool (RTLT)	https://www.fema.gov/resource-management-mutual-aid
The Intelligence and Investigations Guide	https://www.fema.gov/nims-doctrine-supporting-guides-tools
NIMS Reusable Learning Objects	https://training.fema.gov/rlo/
NIMS/ICS Resources and Section 508 Compliant NIMS Forms	https://training.fema.gov/emiweb/is/icsresource/
FEMA NIMS Training	https://training.fema.gov/nims/

FEMA NIMS site

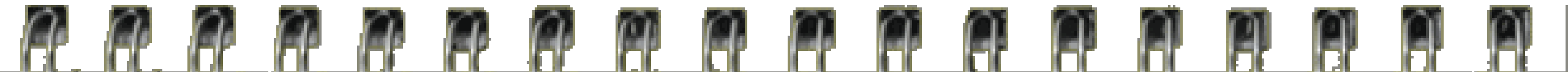
RLO Training

NIMS 508

NIMS Training

Questions? Send us e-mail: FEMA-NIMS@fema.dhs.gov

intentionally blank




DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA
Pacific Northwest
NATIONAL LABORATORY

Pacific Northwest National Laboratory

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

www.pnnl.gov