Not “If”, But "When": The Value of COOP Planning

Presented by:
Kyle Benser, Judicial Programs Administrator, AOPC
Rick Pierce, Judicial Programs Administrator, AOPC

What are we going to learn today?

- Planning is more critical and valuable than the plan
- Differentiate between emergency action planning and continuity of operations planning.
- Define and understand what is a COOP and what is in it and why
- Explain Incident Command Structure (ICS)
- Amending your COOP for cyber attack response
- Testing your response

What is EAP? What does COOP mean?

- Emergency Action Plan (EAP)- A written document providing guidance to and expectations of employees responding to various emergency situations. Pa. R.J.A. 1950

- Continuity of Operations-The process during and following an emergency, by which a court maintains at least minimum levels of service. Pa. R.J.A. 1950

Emergency Rules of Judicial Administration

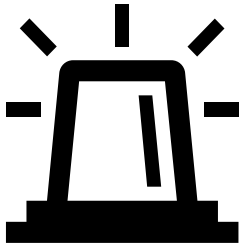
- Responsibilities of court officials in an emergency:
  - Role of the PJ-Pa. R.J.A. 1952 (B)
  - Role of the DCA-Pa. R.J.A. 1952 (D)

- County officials play a key role as well
  - Local Court Security Committee- Pa. R.J.A. 1954

When Does an Emergency Affect Operational Continuity?

- What is an emergency?
  - Any event that presents conditions of threat or danger to personal safety that requires immediate action.

- What was your first test of an emergency response?
  - A fire drill at school or preschool



Let's test your comprehension of EAP and COOP

- There is an active attacker incident in your courthouse.
  - Do you activate your COOP **or** your EAP?
  - Under what conditions, and when?

- The National Weather Service has issued a tornado warning for your MDJ office location. Do you activate your COOP **or** EAP?

- A pipe burst in your DRS office over the weekend. There is some standing water. Do you activate your COOP **or** your EAP?
  - What if after several days mold is discovered?

- Your court experiences a cyber-attack. Do you activate your EAP?

The Three Phases of COOP

Activation

How?

Alert and Notification

To Whom?

Transition to Alternate Facility, if Necessary

What Is In Your COOP and Why

- Essential functions and staff details
  - Answers "What" and "Who"
- Alternate Facility
  - Answers "Where"
- Specific disruptions call for specific responses
- Data recovery and restoration

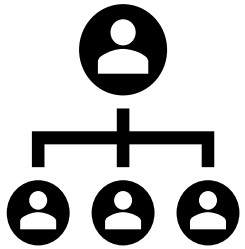
Who.What.When.Where.How…Why?

- Communication Plan

  -Includes modes of communication

  and their interoperability

- Reconstitution
- Pandemic Preparedness



Incident Command Structure

- Who decided what issues to address and the priority of questions to answer?
- Who has the authority to make critical decisions?
- Who has the responsibility to carry out these critical decisions?
- COOP and COG? What is a COG?

What Constitutes an "Event" to Activate COOP?

- Any disruption to court operations that will require your court to significantly modify its operation for longer than ***72 hours.***

- What about a cyber attack? Does the time frame change? YES!!
  - Activation must be immediate-AOPC must remove threat to all other counties if possibility of compromise of CPCMS or MDJS, for example.

- County IT will need immediate notification to mobilize resources and follow steps included in your COOP for data restoration and recovery.

We Have Activated our COOP, How and When Do We Notify the AOPC?

AS SOON AS POSSIBLE!

Contact us at:

COOPActivation@pacourts.us

Please Include:

- **Your Name**
- **Title**
- **County**
- **Phone Number**
- **And a brief explanation of the situation**

Don't forget to copy your DCA!

Who does your email notify at AOPC?

- **Andrea Tuominen** – State Court Administrator
- **Wendy Hosch** – Assistant Director of AOPC IT
- **Geri St. Joseph** – Director of JDOP
- **Christy Beane** – Assistant Director of JDOP
- **Stacey Witalec** – Director of Communication
- **Rick Pierce** – JDOP Program Administrator
- **Kyle Benser** – JDOP Program Administrator
- **AOPC Help Desk** – the NOC

Cyber Attack Response

- We discussed who you are alerting at the AOPC, who and how are you alerting locally?
- You more than likely already have a court security committee. You may need to add some additional partners but use the court security committee as the foundation.
  - RJA 1954 recommends: an individual responsible for county and court records, an individual responsible for courthouse security, a courthouse facility or risk manager, representatives of the other county offices housed in the court facility, a representative from the county information technology office, and a member of county or local law enforcement.

Cyber Attack Priorities

- Does your County IT department know what priority the court needs local systems restored?
  - Civil case management system for Prothonotary's Office
  - Phones if using VOIP
  - Transcript processing system
  - Criminal case imaging system
  - Payroll system

Technology Priorities					
IT Application/ Vital Record	Priority in Cyber Event	IT Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Unit Responsible/Point of Contact	Notes

- AOPC's priorities: MDJS, CPCMS, epay higher priorities than case management system for appellate courts. Why?

- Please identify critical IT applications and vital records. Once those are determined, prioritize the for restor ation during a cyber incident.

Cyber Incident Response Team

Identify members of the County's Crisis Management Team (CMT) and IT Cyber Incident Response Team (CIRT)

Crisis Management Team (CMT)	
Title	**Name**

IT Cyber Incident Response Team (CIRT)	
Title	**Name**

Let's Share Our Experiences

- Lessons learned?
- Have you added anything to your COOP?

Why Test My Coop?

- Testing is an essential element to the planning process.
  - Critical to determine strengths and deficiencies.
- Two types of test:
  - Tabletop
  - Drill
- Following exercise, what's next?
  - "Hot wash"
  - After-Action Report

How can we help you?

Please Contact Us

Rick Pierce
717-231-3300 ext. 4011
Rick.Pierce@pacourts.us

Kyle Benser
717-873-9162
Kyle.Benser@pacourts.us