**COOP Drill Facilitation Questions**

**To correspond with Q1: *What level of response is needed to properly respond to this incident?***

Incident Response Team

1. With the listed incident, who would be the first person contacted? How would that person be contacted?
2. Are procedures in place to develop an Incident Management Team (IMT)?
3. Who comprises the Incident Management Team that will evaluate the incident? What positions does each individual serve, i.e. Incident Management Manager, Command Staff, etc.
4. How is the IMT advised of the incident? Are notification procedures in place including current contact information? Does each IMT individual provide multiple devices for communication?
5. Are the IMT’s roles, responsibilities, and tasks documented?
6. Are alternate Incident Management Team members designated in the event the primary individual is not available? Is the designation documented? Where is that documentation located? Does the plan contain Succession Planning and Delegation of Authority Documents to convey this information?
7. Is the IMT prepared to operate over a 24-hour period? Is there enough staff to cover the IMT over an extended period of time allowing for IMT staff alternate shifts?
8. Are IMT individuals trained in their primary and alternate positions?
9. Have alternates served in the primary roles during exercises? When was the last time this was practiced?
10. When was the last time the Incident Management Plan been updated? How often is the plan updated? What triggers a change in the plan?

Other Staff

1. Does this incident require operational staff to be notified? What process is used to notify staff?
2. Is current contact information included in COOP plan?
3. Are periodic notification drills conducted? Are notification drills conducted after hours?

**To correspond with Q2: *What documentation needs to be referenced based on the event and related variables?***

1. Are Vital Documents attached to the COOP Plan, i.e. Delegation of Authority, Succession Planning, Emergency Procedures, Vital agency manuals, etc.
2. How often are these documents updated and distributed?
3. Does each Section Head have access to these documents available outside of the work location?

**To correspond with Q3: *What critical business processes in your plan are impacted by this event?***

1. Are the critical business processes listed in the COOP plan?

Alternate Facilities

1. Does the incident require relocation to an alternate facility to recover or sustain critical business processes?
2. Have multiple alternate facilities been pre-established and documented with Memorandum of Understandings (MOU)? Where are the MOUs documented?
3. What process has been established to activate alternate facilities? Are these procedures documented? Where is the documentation located?
4. Do the alternate facilities have designated areas to set up a Command Center, Communications room, Staging area, area to conduct operations, and cafeteria/food preparation area?
5. What type of back-up utilities do the alternate facilities have?
6. What procedures are in place during system/software inaccessibility to institute manual ways of conducting the critical business processes?
7. Have exercises been conducted in activating, relocating, and working from each of the alternate facilities?
8. What security is needed at the alternate facility? How is security established at the alternate facility? Who is responsible for security at the alternate facility?
9. Is essential staff aware of the alternate facility locations?
10. What procedures are in place to deactivate, inventory and restock work resources, and reconstitute work activities back to the primary work location?
11. Are procedures in place for communicating status of recovery events to appropriate positions, i.e. Incident Response Manager?

System Recovery

1. Which systems support the critical business processes identified? Are the systems listed in the COOP plan?
2. Is the IT unit considered essential staff to recover/monitor critical systems?
3. Is there an IT recovery strategy in place? Does it include system interdependencies? Does it include a priority listing of system recovery?
4. Are critical systems backed up and stored off-site?
5. Are emergency tape/media recall procedures documented?
6. Do the recovery plans include recovery procedures? How often are they updated? How often are they tested? Are the procedures stored off-site?
7. Are end users aware of the time that each system will take to recover? Does this impede the recovery of the critical business processes?
8. Is the Recovery Point Objective (RPO) documented? Where is the documentation located? Do any of the systems risk data loss?

**To correspond with Q4: *What resources (supplies, equipment, software, and assets) do you need and are they documented in your plan?***

1. Are the alternate facilities pre-positioned with necessary work resources such as network accessibility, computers/laptops, phones, fax machines, printers, and basic office supplies?
2. Does each alternate facility have television and battery or crank radios available to monitor activities outside of the facility?
3. Where in the alternate facilities are the work and emergency equipment located? Who is responsible for distributing equipment?
4. If resources need to be purchased or leased, is financial staff designated as being essential in the COOP plan?
5. Are procedures documented on how to record personnel time during this type of event?
6. How will the agency speed the process of procuring needed resources during this type of event?

**To correspond with Q5: *Do you need to contact Vendors who supply goods or services to your organization? Do you have vendor contact information documented in your plan?***

1. Which vendors would you need to contact during this type of event?
2. What services or products do these vendors provide? What type of impact would occur if you could not get the vendors to deliver?
3. Are each of the vendors documented in the COOP plan? Are the vendor representative contact information included in the plan?

**To correspond with Q6: *Are there any emergency medical needs resulting from the event?***

1. Do any staff members have CPR/First Aid certification? How would you determine which employees to call to render such care? Are those staff members identified in the COOP plan?
2. If applicable, does the situation require a need to contact employees’ Emergency Contact source? Where is this information stored? Based on the scenario, is the Emergency Contact information accessible? If not, what backup plans would you use to get the information to the Emergency Contact source?

**To correspond with Q7: *Do you need to send emergency responders from your group to assist?***

1. Based on the incident, are any emergency responders needed to assist with the emergency at hand?
2. Who is considered an emergency responder? Are they considered COOP Essential in the COOP plan?
3. Does the plan contain a manual call list?

**To correspond with Q8: *Does the event require an offsite system restore?***

1. Where are critical systems identified? Do any processes in the COOP plan identify these critical systems?
2. Is staff designated to recover critical systems? How are they activated?
3. Are recovery activation procedures documented? Where is the documentation located?
4. Are there other agencies and/or vendors that you depend on to restore data?

**To correspond with Q9: *Who from your team, if anyone, should be delegated to support the offsite system restore efforts?***

1. Who is part of the recovery team?
2. Who is the lead IT recovery person?
3. What other teams does the IT unit collaborate with to recover systems?

**To correspond with Q10: *Do you have sufficient personnel remaining to support your operations?***

1. What remaining staff will be left to conduct normal operations?
2. Are there any areas that lack coverage? What are they? Are there any plans to cover the gap?
3. Are any units able to cover for lacking units?
4. Does your section rely on other sections? What would be the impact if those other sections have a shortage of personnel?