Minutes for Delaware Continuity Coordinator Council
05/26/22

Attendees: Sandra Alexander, Andrea Bayline, Gwen Bray, Dan Cahall, Karen Carson, Cathleen Carter, Timothy Collins, Kara Colpo, Sam Cucinotta, Cherie Dodge Biron, Robert Dreibelbis, Ebony Edwards, Kevin Eickman, Denise Elliott, Elizabeth Emerson, Marcella England, Alfred Finch, Sheeron Fuller, Lori Gorman, Christopher Hall, Robin Hartnett-Sterner, Kristin Harvey, Samantha Hemphill, Mark Hogan, Christopher Horton, Robert Hudson, Katherine Hughes, Blair Hyde, Jamie Johnstone, Cheryl Jones, Samara Kaminski, Griffin Kanich, Andy Kloepfer, Peter Korolyk, Michael Krumrine, Stacey Lassiter-Watson, Tim Li, Theora Lowe-Staton, John Mancus, Nuno Martins, Susan Mitchell, Lori Murray, Meghan Niddrie, Gregory Nolt, Stephanie Parker, Jerome Passon, Coleen Ponden, Danka Prilepkova, Janet Roberson, John Rudd, Antoinette Russum-Hane, Judi Schock, Robert Sisk, Elizabeth Sloven, Danielle Stevenson, Andrew Sumner, Rachel Surratte, Syd Swann, Karin Sweeney, Terri Thomas, Victor Ting, Mickie Troubetaris, Alfred Tunnell, Heather Volkomer, James Wagner, Lorri Wall, Jennifer Walls, Ryan Ward, Arielle Winston, Dana Wise, Brian Wishnow, Sonja Wood, Jessica Wurzel, Claudette Wus, Denise Zielinski, Margaret Zimmerman

Agenda:

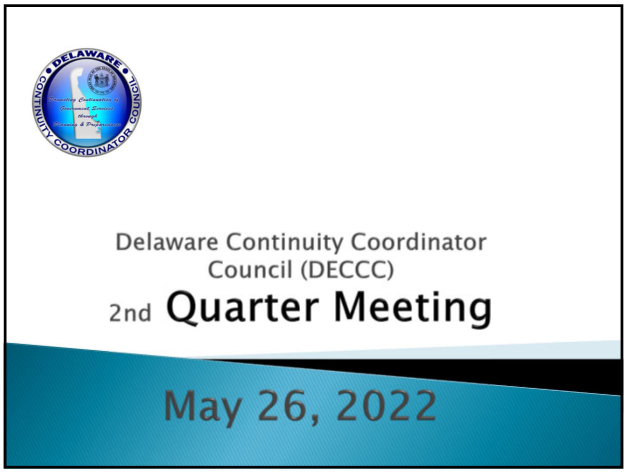
- **Welcome/Introductions**
- **DECCC Updates- see ppt**
  - New Plan Builders & Kudos
  - Upcoming Opportunities
  - COOP News
    - Risk and DR Recommendations report
    - DECCC Extranet Updates
    - Exercises Modules
- **Cyber Security Planning- see ppt**

  There is no doubt that the number of cyber-attacks is growing and the need for a cyber response plan is critical for agencies. But what do you put in your cyber plan? How does it intersect with your COOP plan? Who should be in it? How do you exercise it?
- **Continuity Considerations during a Cyber-Attack- see ppt**

  Listen as we are joined by FEMA Region 3's Continuity Program Manager, Blair Hyde. She will share their top action items and considerations for continuity planning during a Cyber-Attack. This high-level material shares with you the top areas of concern for FEMA in light of the current cyber threat environment.

DECCC Steering Committee members:

Tony Lee: Co-Chair Lori Gorman: Co-Chair Cherie Dodge-Biron**: Vice-Chair**
Dawn Hollinger: Education & Training John Mancus: Disaster Preparedness Officer
Dan Cahall: IT Systems Officer Tim Li***:*** Vital Records Officer
Vanessa Briddell: Member



Delaware Continuity Coordinator Council (DECCC)

2nd Quarter Meeting

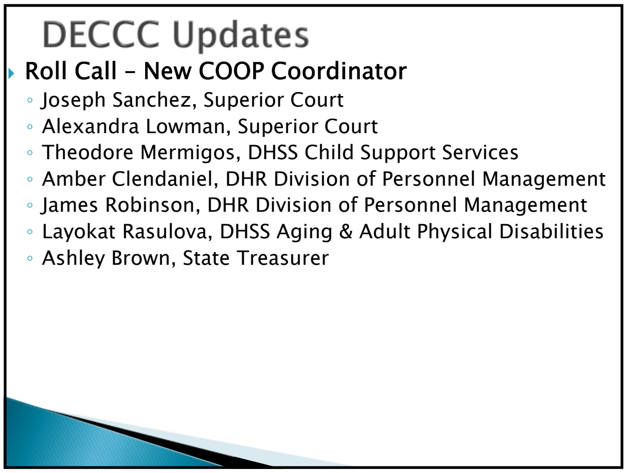
May 26, 2022

1

Agenda

- Welcome/Introductions
- DECC Updates
  - New plan builders
  - Upcoming Opportunities
  - COOP News
- Cyber Incident Planning
  - Sandra Alexander, Director of Risk Management and Governance, DTI
- Continuity Considerations During a Cyber-Attack
  - Blair Hyde, FEMA Region 3

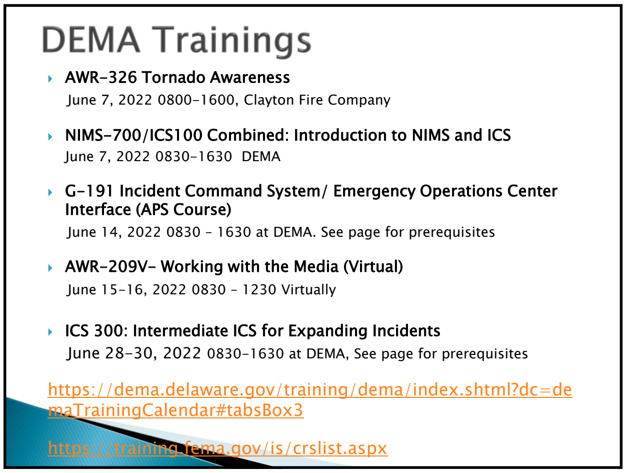
2



DECCC Updates

- Roll Call – New COOP Coordinator
  - Joseph Sanchez, Superior Court
  - Alexandra Lowman, Superior Court
  - Theodore Mermigos, DHSS Child Support Services
  - Amber Clendaniel, DHR Division of Personnel Management
  - James Robinson, DHR Division of Personnel Management
  - Layokat Rasulova, DHSS Aging & Adult Physical Disabilities
  - Ashley Brown, State Treasurer

3



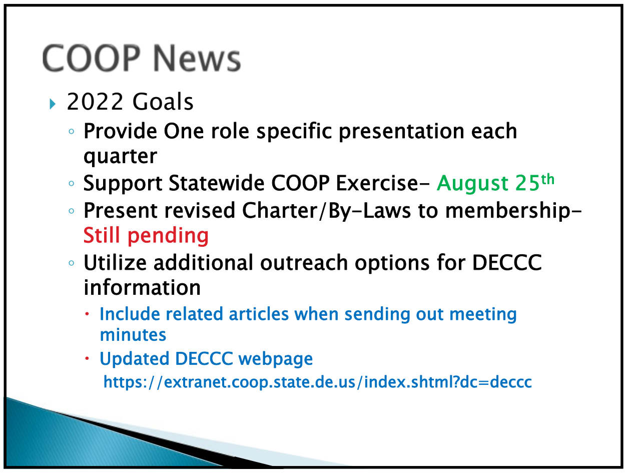
DEMA Trainings

- **AWR-326 Tornado Awareness**
  June 7, 2022 0800-1600, Clayton Fire Company
- **NIMS-700/ICS100 Combined: Introduction to NIMS and ICS**
  June 7, 2022 0830-1630 DEMA
- **G-191 Incident Command System/ Emergency Operations Center Interface (APS Course)**
  June 14, 2022 0830 - 1630 at DEMA. See page for prerequisites
- **AWR-209V- Working with the Media (Virtual)**
  June 15-16, 2022 0830 - 1230 Virtually
- **ICS 300: Intermediate ICS for Expanding Incidents**
  June 28-30, 2022 0830-1630 at DEMA, See page for prerequisites

https://dema.delaware.gov/training/dema/index.shtml?dc=demaTrainingCalendar#tabsBox3

https://training.fema.gov/is/crslist.aspx

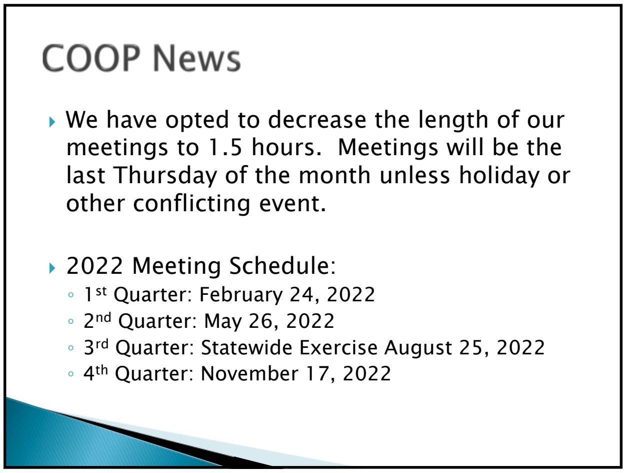
4



COOP News

- 2022 Goals
  - Provide One role specific presentation each quarter
  - Support Statewide COOP Exercise- August 25th
  - Present revised Charter/By-Laws to membership- Still pending
  - Utilize additional outreach options for DECCC information
    - Include related articles when sending out meeting minutes
    - Updated DECCC webpage
      https://extranet.coop.state.de.us/index.shtml?dc=deccc

5



COOP News

- We have opted to decrease the length of our meetings to 1.5 hours. Meetings will be the last Thursday of the month unless holiday or other conflicting event.
- 2022 Meeting Schedule:
  - 1st Quarter: February 24, 2022
  - 2nd Quarter: May 26, 2022
  - 3rd Quarter: Statewide Exercise August 25, 2022
  - 4th Quarter: November 17, 2022

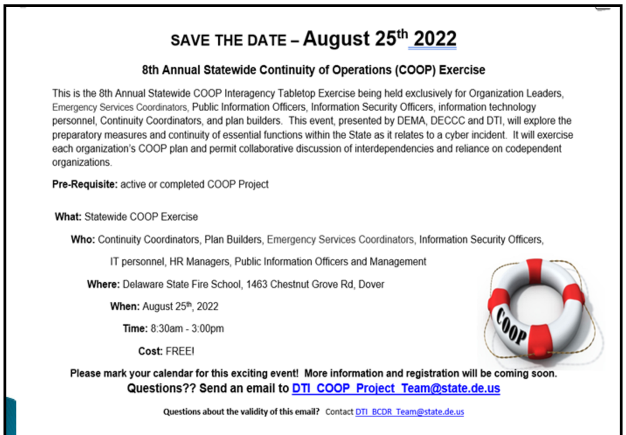
6

COOP News: Application Clean up

We are working to make ServiceNow the gold source for application data. Your liaison is working to compare ServiceNow with BCIC and will be scheduling meetings with each Division/Dept staff to review data.

- Applications in BCIC not in ServiceNow will be added;
- Applications in ServiceNow that are no longer valid will be deleted
- Applications in ServiceNow that are valid will be added to BCIC and need to be linked to the respective business processes.
- Please check the applications you have linked to your processes to ensure they are in fact valid (example: file services, or Internet web site).
- Determine the DR status for applications.

7



SAVE THE DATE – August 25th 2022

8th Annual Statewide Continuity of Operations (COOP) Exercise

This is the 8th Annual Statewide COOP Interagency Tabletop Exercise being held exclusively for Organization Leaders, Emergency Services Coordinators, Public Information Officers, Information Security Officers, information technology personnel, Continuity Coordinators, and plan builders. This event, presented by DEMA, DECCC and DTI, will explore the preparatory measures and continuity of essential functions within the State as it relates to a cyber incident. It will exercise each organization's COOP plan and permit collaborative discussion of interdependencies and reliance on codependent organizations.

Pre-Requisite: active or completed COOP Project

What: Statewide COOP Exercise

Who: Continuity Coordinators, Plan Builders, Emergency Services Coordinators, Information Security Officers, IT personnel, HR Managers, Public Information Officers and Management

Where: Delaware State Fire School, 1463 Chestnut Grove Rd, Dover

When: August 25th, 2022

Time: 8:30am - 3:00pm

Cost: FREE!

Please mark your calendar for this exciting event! More information and registration will be coming soon.

Questions?? Send an email to DTI_COOP_Project_Team@state.de.us

Questions about the validity of this email? Contact DTI_BCDR_Team@state.de.us

8

Questions/Comments

- **Q:** Will the meeting be recorded?
- **A:** No, we do not record the trainings to allow for a more open forum for communication.

- **Q:** Will the PPT be provided to the group?
- **A:** Yes, the ppt will be distributed with meeting minutes and placed on the extranet site.

- **Q:** What type of cascading effects can attendees think of that would be greatly impacted by any kind of extended loss of power or shutting down of certain payment systems?
- **A:** Dialysis, can't replenish fuel so food spoilage, medical equipment, wifi, even door locks.

9

Shared Thoughts

- Due to the many physical impacts that can result of a cyber incident– it is essential that employees take steps to be prepared. This includes at home and at the office. Some examples include:
  - Storing extra water and food (3 days worth per person)
  - Keeping vehicles fueled and batteries charged (including back-up batteries)
  - Consider back-up generators or and other sources for essential items (this includes wifi hubs).
  - Consider printing phone books to ensure you know critical numbers even if your cell loses power.

10

Shared Thoughts

- Does your primary/alternate facility have a generator and how long will it run?
- What work around procedures exist for critical processes if applications aren't available? Consider having some printed forms and other manual equipment available.
- Do you know where the keys are to door locks to your building if electronic locking systems go down? Consider how you will handle security for the building should this occur.
- **Ensure your COOP plans include a cyber incident response team with necessary tasks and personal pre-identified.**

11

Thank you and see you at the Next Meeting!

12

CYBER INCIDENT PLANNING

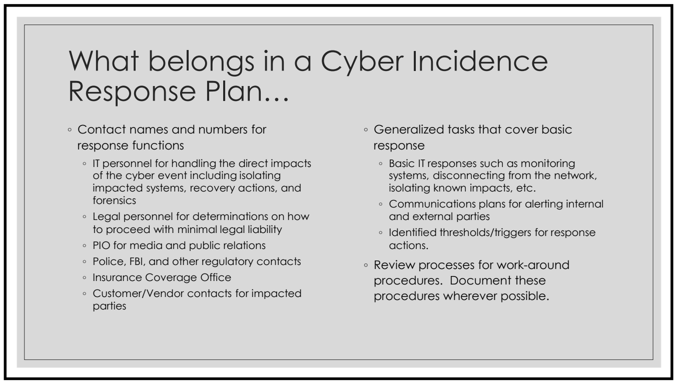
Sandra Alexander,
Dept of Technology and Information

1

Cyber Incident Planning

- WHAT IS NEEDED IN A CYBER RESPONSE PLAN
- HOW DO YOU INCORPORATE IT INTO YOUR EXISTING COOP PLAN
- ESTABLISHING THRESHOLDS FOR ACTION.

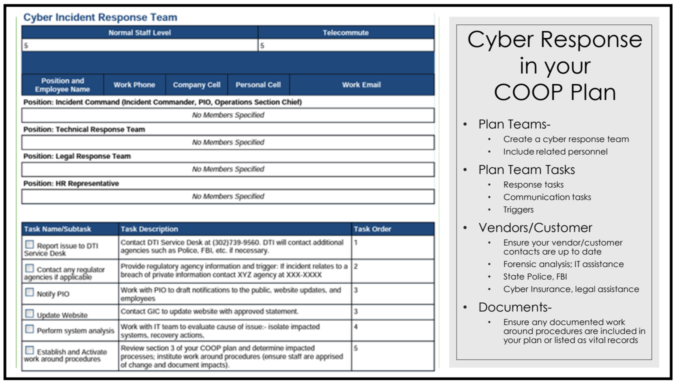
2



What belongs in a Cyber Incidence Response Plan…

- Contact names and numbers for response functions
  - IT personnel for handling the direct impacts of the cyber event including isolating impacted systems, recovery actions, and forensics
  - Legal personnel for determinations on how to proceed with minimal legal liability
  - PIO for media and public relations
  - Police, FBI, and other regulatory contacts
  - Insurance Coverage Office
  - Customer/Vendor contacts for impacted parties
- Generalized tasks that cover basic response
  - Basic IT responses such as monitoring systems, disconnecting from the network, isolating known impacts, etc.
  - Communications plans for alerting internal and external parties
  - Identified thresholds/triggers for response actions.
- Review processes for work-around procedures. Document these procedures wherever possible.

3



Cyber Incident Response Team

Normal Staff Level	Telecommute
5	5

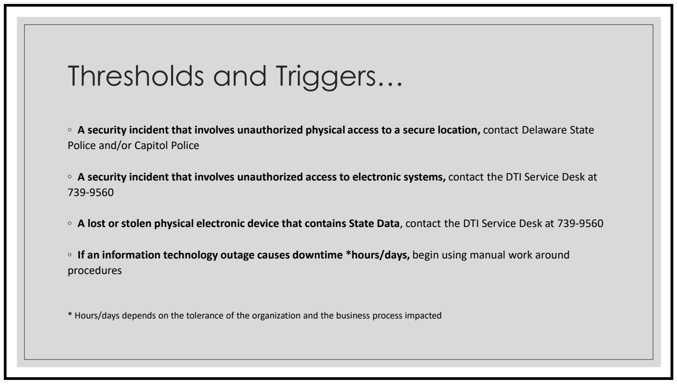
Position and Employee Name	Work Phone	Company Cell	Personal Cell	Work Email
Position: Incident Command (Incident Commander, PIO, Operations Section Chief)				
No Members Specified				
Position: Technical Response Team				
No Members Specified				
Position: Legal Response Team				
No Members Specified				
Position: HR Representative				
No Members Specified				

Task Name/Subtask	Task Description	Task Order
□ Report issue to DTI Service Desk	Contact DTI Service Desk at (302)739-9560. DTI will contact additional agencies such as Police, FBI, etc. if necessary.	1
□ Contact any regulator agencies if applicable	Provide regulatory agency information and trigger: If incident relates to a breach of private information contact XYZ agency at XXX-XXXX	2
□ Notify PIO	Work with PIO to draft notifications to the public, website updates, and employees	3
□ Update Website	Contact GIC to update website with approved statement.	3
□ Perform system analysis	Work with IT team to evaluate cause of issue:- isolate impacted systems, recovery actions.	4
□ Establish and Activate work around procedures	Review section 3 of your COOP plan and determine impacted processes; institute work around procedures (ensure staff are apprised of change and document impacts).	5

Cyber Response in your COOP Plan

- Plan Teams-
  - Create a cyber response team
  - Include related personnel
- Plan Team Tasks
  - Response tasks
  - Communication tasks
  - Triggers
- Vendors/Customer
  - Ensure your vendor/customer contacts are up to date
  - Forensic analysis; IT assistance
  - State Police, FBI
  - Cyber Insurance, legal assistance
- Documents-
  - Ensure any documented work around procedures are included in your plan or listed as vital records

4

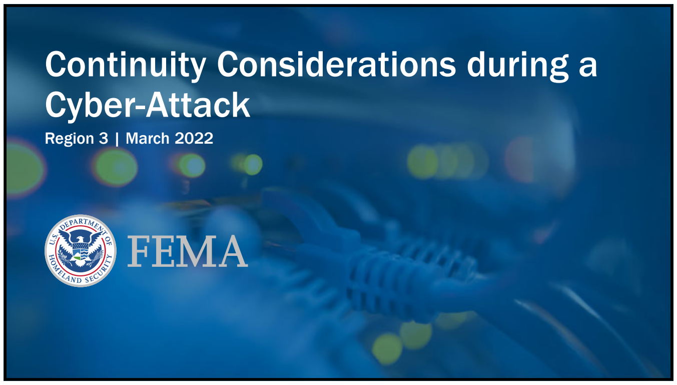


Thresholds and Triggers…

- **A security incident that involves unauthorized physical access to a secure location,** contact Delaware State Police and/or Capitol Police
- **A security incident that involves unauthorized access to electronic systems,** contact the DTI Service Desk at 739-9560
- **A lost or stolen physical electronic device that contains State Data,** contact the DTI Service Desk at 739-9560
- **If an information technology outage causes downtime *hours/days,** begin using manual work around procedures

* Hours/days depends on the tolerance of the organization and the business process impacted

5

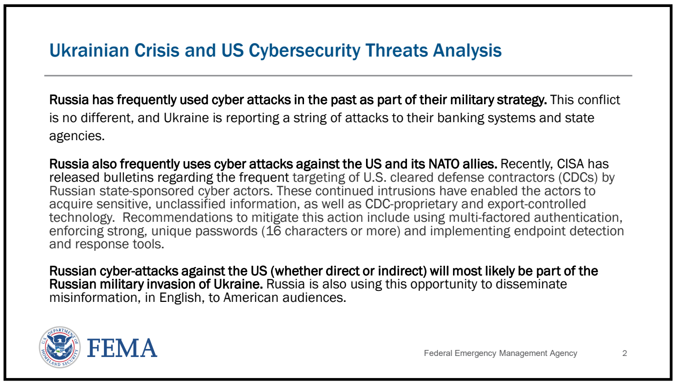


Continuity Considerations during a Cyber-Attack

Region 3 | March 2022

FEMA

1



Ukrainian Crisis and US Cybersecurity Threats Analysis

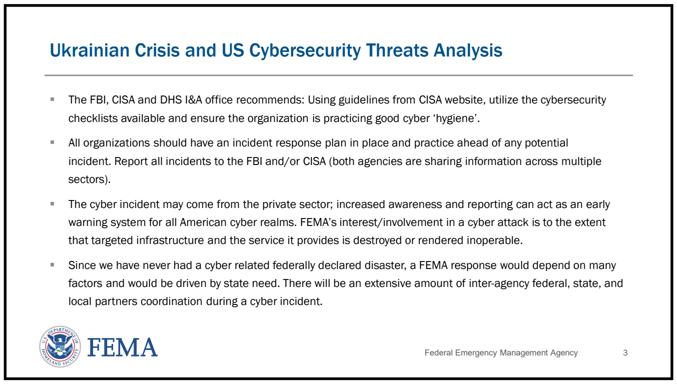
Russia has frequently used cyber attacks in the past as part of their military strategy. This conflict is no different, and Ukraine is reporting a string of attacks to their banking systems and state agencies.

Russia also frequently uses cyber attacks against the US and its NATO allies. Recently, CISA has released bulletins regarding the frequent targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber actors. These continued intrusions have enabled the actors to acquire sensitive, unclassified information, as well as CDC-proprietary and export-controlled technology. Recommendations to mitigate this action include using multi-factored authentication, enforcing strong, unique passwords (16 characters or more) and implementing endpoint detection and response tools.

Russian cyber-attacks against the US (whether direct or indirect) will most likely be part of the Russian military invasion of Ukraine. Russia is also using this opportunity to disseminate misinformation, in English, to American audiences.

FEMA

2

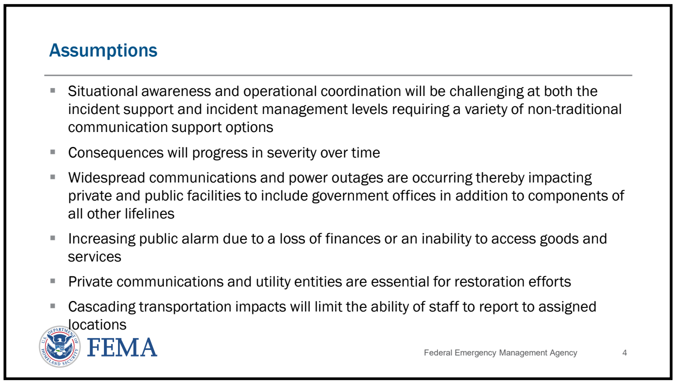


Ukrainian Crisis and US Cybersecurity Threats Analysis

- The FBI, CISA and DHS I&A office recommends: Using guidelines from CISA website, utilize the cybersecurity checklists available and ensure the organization is practicing good cyber 'hygiene'.
- All organizations should have an incident response plan in place and practice ahead of any potential incident. Report all incidents to the FBI and/or CISA (both agencies are sharing information across multiple sectors).
- The cyber incident may come from the private sector; increased awareness and reporting can act as an early warning system for all American cyber realms. FEMA's interest/involvement in a cyber attack is to the extent that targeted infrastructure and the service it provides is destroyed or rendered inoperable.
- Since we have never had a cyber related federally declared disaster, a FEMA response would depend on many factors and would be driven by state need. There will be an extensive amount of inter-agency federal, state, and local partners coordination during a cyber incident.

FEMA

3

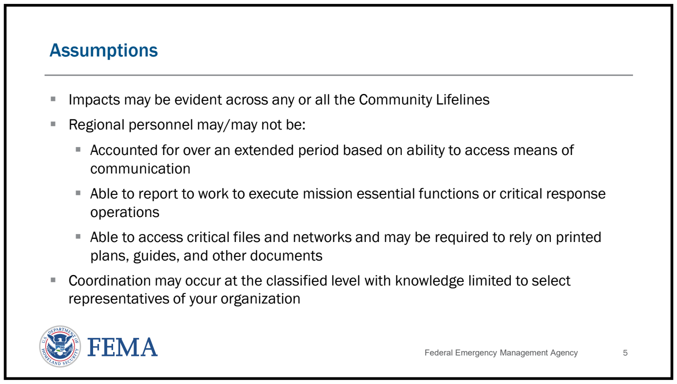


Assumptions

- Situational awareness and operational coordination will be challenging at both the incident support and incident management levels requiring a variety of non-traditional communication support options
- Consequences will progress in severity over time
- Widespread communications and power outages are occurring thereby impacting private and public facilities to include government offices in addition to components of all other lifelines
- Increasing public alarm due to a loss of finances or an inability to access goods and services
- Private communications and utility entities are essential for restoration efforts
- Cascading transportation impacts will limit the ability of staff to report to assigned locations

FEMA

4

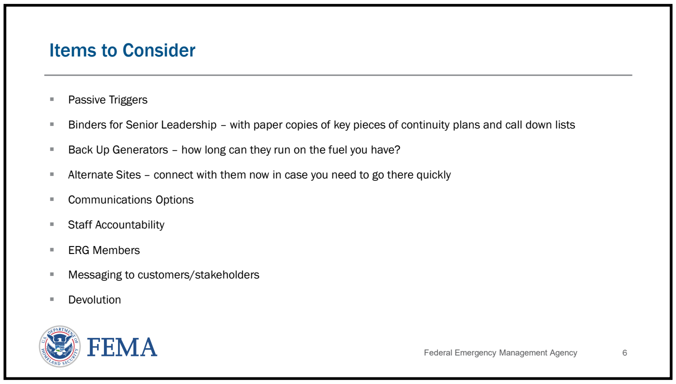


Assumptions

- Impacts may be evident across any or all the Community Lifelines
- Regional personnel may/may not be:
  - Accounted for over an extended period based on ability to access means of communication
  - Able to report to work to execute mission essential functions or critical response operations
  - Able to access critical files and networks and may be required to rely on printed plans, guides, and other documents
- Coordination may occur at the classified level with knowledge limited to select representatives of your organization

FEMA

5

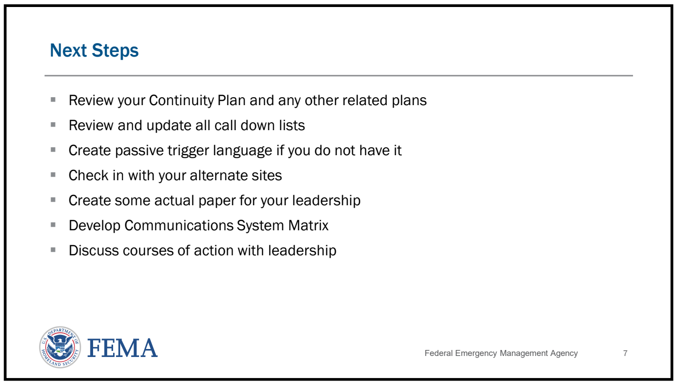


Items to Consider

- Passive Triggers
- Binders for Senior Leadership – with paper copies of key pieces of continuity plans and call down lists
- Back Up Generators – how long can they run on the fuel you have?
- Alternate Sites – connect with them now in case you need to go there quickly
- Communications Options
- Staff Accountability
- ERG Members
- Messaging to customers/stakeholders
- Devolution

FEMA

6



Next Steps

- Review your Continuity Plan and any other related plans
- Review and update all call down lists
- Create passive trigger language if you do not have it
- Check in with your alternate sites
- Create some actual paper for your leadership
- Develop Communications System Matrix
- Discuss courses of action with leadership

FEMA

Federal Emergency Management Agency 7

7

FEMA

8