



# Welcome

## NASCIO's Disaster Recovery Webinar Series

**Moderator: Drew Leatherby, NASCIO  
Issues Coordinator**



## Asking Questions

- Please use the Question & Answer feature to ask questions at any time
- All questions will be addressed at the end of the presentation
- Responses to any questions not answered on the call will be distributed to all participants via email after the event



## Technical Support

**If you need technical assistance at any time:**

- **Dial \*0 (if you have joined by phone)**
- **Call Raindance Tech Support at 1-888-966-8686 (if you have selected the Webcasting option)**

# Today's Speakers



**AJ Briding**  
Certified Emergency Mgr.  
CIBER, Inc.

**AJ Briding** is CIBER's advisor on emergency operations for the City of New Orleans. He assists the City with Strategic Planning, Organizational Alignment, Emergency Communication, Evacuation Processing, and implementation of the National Incident Management System (NIMS).

Formerly, he was a homeland security analyst for the US Northern Command, and a winner of the 1998 President's Award for Quality Improvement.



**Col. Terry J. Ebbert,**  
**USMC (Ret.)**  
Director of Homeland Security  
City of New Orleans

**Col. Ebbert** possesses operational and planning responsibility for the City's Police Dept., Fire Dept., and Office of Emergency Preparedness and Emergency Medical Services (EMS).

Col. Ebbert is a distinguished twice-wounded combat veteran who was awarded the Navy Cross, the United States' second highest award for valor.



**ciber**<sup>®</sup>

Are You Ready?  
An Emergency Management Perspective  
for Governmental CIOs

# Are You Ready?

## An EM Perspective for Governmental CIOs

- What is Emergency Management (EM)?
- Why Is It Important to Governmental CIOs?
- The IT Challenge and Opportunities
- Are You Ready?



# What is Emergency Management?

- Preparation for, prevention and mitigation of, response to and recovery from natural and man-made disasters of any size and complexity
- For governments at risk from disasters, it's the crucial but often neglected companion piece to continuity of operations and government

# Full-Spectrum Emergency Management

## Pre-Disaster

- Prevention
- Preparation
- Mitigation



## Post-Disaster

- Response
- Recovery

Crisis Management & Emergency Operations



- Continuity of Operations (COOP)
- Continuity of Government (COG)



# Emergency Management PDCA Cycle

- Risk assessment
  - Impact analysis
  - National standards
  - COOP/COG planning
  - Lessons Learned
- PLAN**



- DO**
- Implement
  - Mitigate
  - Train
  - Exercise



- Situational Awareness
- COP
- Decision Support

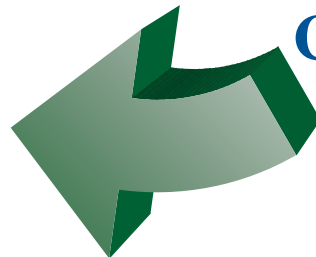
**ACT**

**CHECK**

- Evaluations
- Hot washes
- Assessments
- BPM
- Metrics



**Prevent  
Respond  
Recover**



# Why Is Emergency Management Important?

## The #1 role of government

- Public safety and security?



## The dilemma:

- Daily governmental services can be much more compelling than preparing for disasters that may never happen



## The true catastrophe

- Governments failing to properly protect their public from disasters



# The Challenge to Government

- **Serve**
  - Provide services to its citizens (police and fire services, licenses and permits, health services, etc)
  - Keep essential services running during an emergency, and restore full services afterward
  
- **and Protect**
  - Protect citizens and property from disasters
  - Provide emergency response and recovery when necessary

# Growing Public Awareness

- The American public is acutely aware of catastrophic risk facing them today
- Consider the daily headlines:
  - The lingering devastation of Katrina
  - Coastal vulnerability to surge and tsunami
  - Earthquake predictions
  - Nuclear and chemical plant and transportation accidents
  - Bird flu pandemic
  - Increasing threat of terrorism



# Growing Requirements and Expectations

- Katrina failures have highlighted the American citizen's bottom line
- **Government readiness, from local to federal**
  - Integrating large, complex response and recovery operations
  - Mitigating risk to acceptable levels
  - Terrorism prevention
  - Hurricane warning and protection
  - Effective evacuation and sheltering
  - Effective hazardous materials response



# The Challenge to Governmental CIOs

- IT is the essential enabler behind COOP/COG and emergency services
- IT roles and responsibilities are at best poorly understood in the EM domain
- Emergency operations leave no room for failure



# EM: The Rest of the Iceberg



# The Consequences of Failure

- The results of poor emergency readiness:
  - New Orleans lost essential services, IT resources, and data
  - Government services are still struggling to recover
  - City CIO testified to Congress why New Orleans lost all communications

New Orleans City Hall  
after Katrina



# IT Challenges in Emergency Mgmt.

- Institutional understanding of roles and responsibilities
  - Enterprise approach
  - Collaboration
  - Resources
  - Knowledge retention
  - Training and exercises
  - Complacency
- ➡ IT needs to be part of the EM solution

# Making It Work: Force Multipliers

- Common Operating Picture (COP)
- Situational Awareness
- Decision Support



- Web-centric architectures
- GIS
- BPM
- Virtual servers
- Self-healing broadband nets

# Clash of Cultures

- Classic operator – techie dichotomy is alive and well
  - Techies love bells and whistles—operators hate them
  - “IT Nazis”
- Murphy’s Law of IT:
  - For every IT department action, there is an equal and opposite operator reaction
- Information security and HIPAA: “Yeah right”
- Operator’s Creed: KISS

# Bridging the Gap: The IT / EM Partnership

- Ultimate criteria for success: building bridges that work
  - “Bridges” that deliver IT performance under field conditions
  - Partnership bridge between the IT department and EM



Span of Success

- OR -



Valley of Failure

What the IT experts picture . . .  
(And it may take this, on their end!)

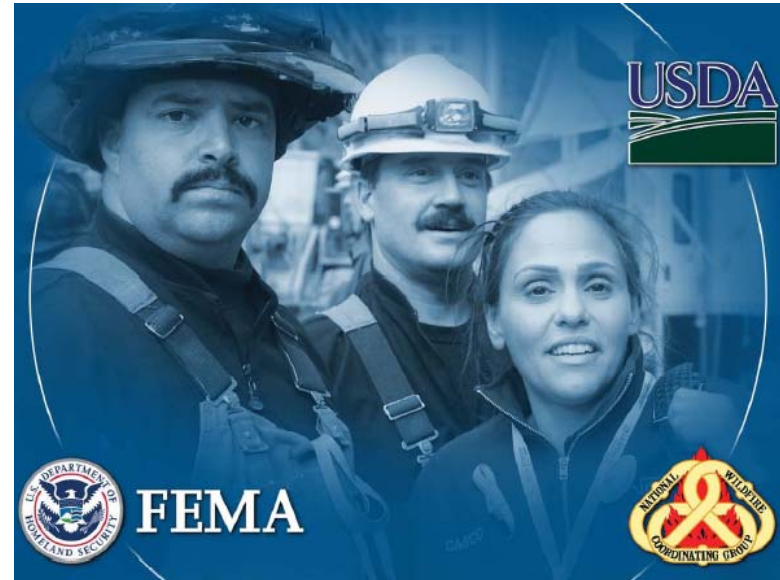
What the operator wants . . .  
Simple, durable, dependable,  
effective

# What Do CIOs Need to Know?

- What is ICS?
- What is NIMS?

# Incident Command System (ICS)

- Standardized, on-scene emergency management
- Integrated organizational structure equal to the complexity and demands of single or multiple incidents
  - Command and control
  - Resource management
  - Situational awareness
  - Decision support



# National Incident Management System (NIMS)

- Mandatory framework for incident management at all levels of government
  - Includes the Incident Command System (ICS)
- Applicable to all hazards
- Key components:
  - Command and management
  - Preparedness
  - Resource management
  - Communication and information management
  - ***NIMS compliance necessary for federal preparedness (DHS) funding***

# Follow the Money: Grant Funding

## HSGP Funding Distribution — FY 2006 and FY 2007

Homeland Security Grant Program	FY 2006	FY 2007
Urban Areas Security Initiative	\$ 710,622,000	\$ 746,900,000
State Homeland Security Program	\$ 528,165,000	\$ 509,250,000
Law Enforcement Terrorism Prevention Program	\$ 384,120,000	\$ 363,750,000
Metropolitan Medical Response System Program	\$ 28,808,920	\$ 32,010,000
Citizen Corps Program	\$ 19,206,000	\$ 14,550,000
<b>Total</b>	<b>\$ 1,670,921,920</b>	<b>\$ 1,666,460,000</b>

- DHS awarded \$11.3 billion to state and local governments for prevention, preparation, response and recovery from acts of terrorism
- HHS is providing \$897 million to states for Public Health emergencies in 2007

# DHS Grant Programs

- Homeland Security Grant Program (HSGP)
  - State Homeland Security Grant Program (SHSGP)
  - Urban Area Security Initiative (UASI)
  - Law Enforcement Terrorism Prevention Program (LATPP)
  - Metropolitan Medical Response System (MMRS)
  - Citizen Corps Program (CCP)
- Emergency Management Performance Grant (EMPG)
- Buffer Zone Protection Program (BZPP)
- Transit Security Grant Program (TSGP)

# DHS Grant Programs (cont.)

- Port Security Grant Program (PSGP)
- Assistance to Firefighters Grant Program (AFGP)
- National Bioterrorism Hospital Preparedness Program (NHBPP)
- Public Health Emergency Preparedness Cooperative Agreement
- FEMA Mitigation Grants
  - Pre-disaster, flood, hazard
- Hazardous Materials Emergency Preparedness Grant Program (HMEP)

# Pre-Authorized DHS Grant Areas

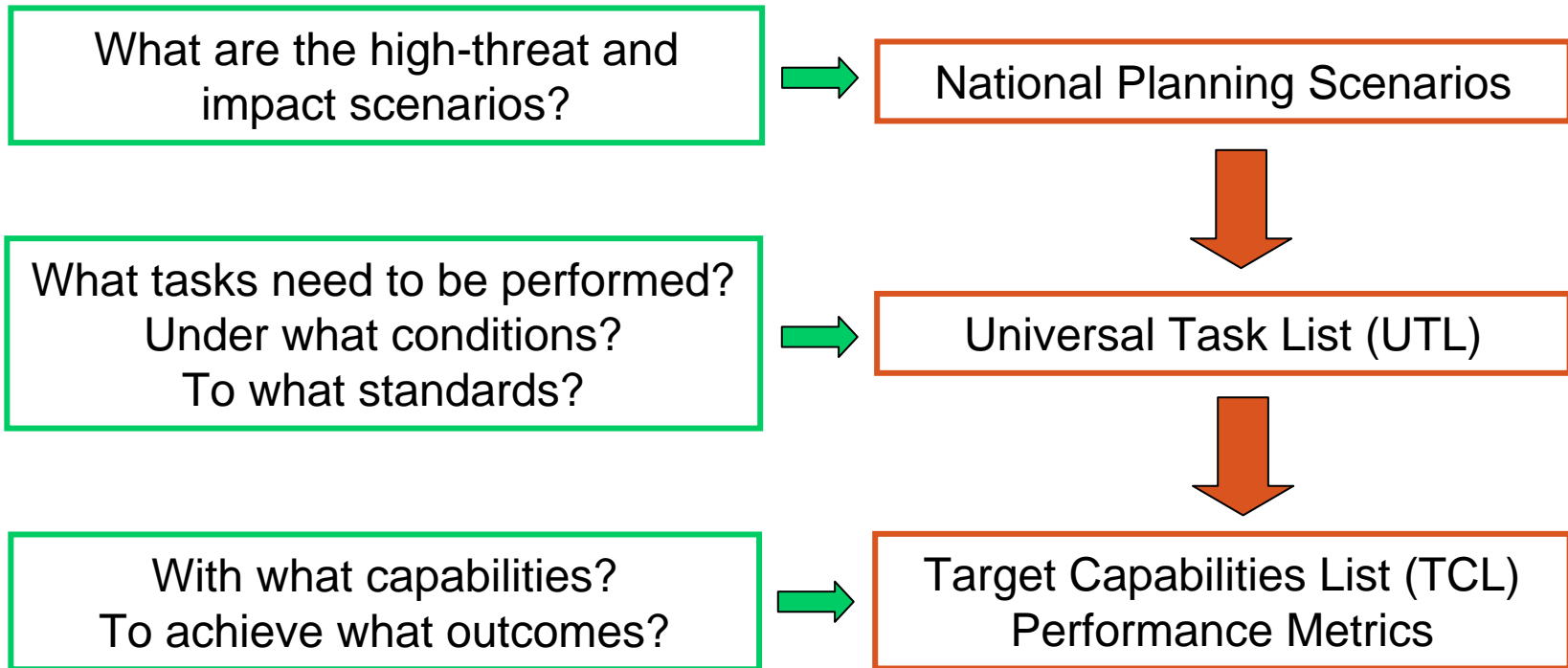
- Emergency notification systems
- Public warning systems
- Crisis information management systems
- Common Operating Picture technology
- Network and server equipment
- Information security equipment & applications
- Badging and access control systems
- Satellite and other communications

# Capabilities-Based Planning and Solutions

- Methodology used by DHS and DoD
- Define required capabilities
- Identify gaps
- Determine best solution sets
- Excellent analysis methodology for building solutions based on assessment results



# Capabilities-Based Planning



# Target Capabilities List (TCL)

## **Common**

- Planning
- Communications
- Risk Management
- Community preparedness and participation

## **Prevent Mission Area**

- Information gathering & recognition of indicators and warnings
- Intelligence analysis and production
- Intelligence / information sharing and dissemination
- Law enforcement investigation and operations
- CBRNE detection

## **Protect Mission Area**

- Critical infrastructure protection
- Food & agriculture safety and defense
- Epidemiological surveillance & investigation
- Public health laboratory testing

## **Recover Mission Area**

- Structural damage & mitigation assessment
- Restoration of lifelines
- Economic & community recovery

## **Respond Mission Area**

- Onsite incident management
- Emergency operations center management
- Critical resource logistics and distribution
- Volunteer management and donations
- Responder safety and health
- Public safety and security response
- Animal health emergency support
- Environmental health
- Explosive device response operations
- Firefighting operations / support
- WMD / HazMat response & decontamination
- Citizen protection: Evacuation and/or in-place protection
- Isolation and quarantine
- Urban search & rescue
- Emergency public information & warning
- Triage & pre-hospital treatment
- Medical surge
- Medical supplies management & distribution
- Mass prophylaxis
- Mass care (sheltering, feeding and related services)
- Fatality management

# Education Grants

- Dept of Education Emergency Response and Crisis Management Grant Program
  - Fiscal Year 2006 \$23 million
  - Average New Award: \$229,515
  - Range of New Awards: \$100,000–\$500,000
  - “to strengthen and improve their emergency response and crisis plans, at the district and school-building level. Grantees are required to address all four (*sic*) phases of crisis planning: prevention and mitigation, preparedness, response, and recovery.”

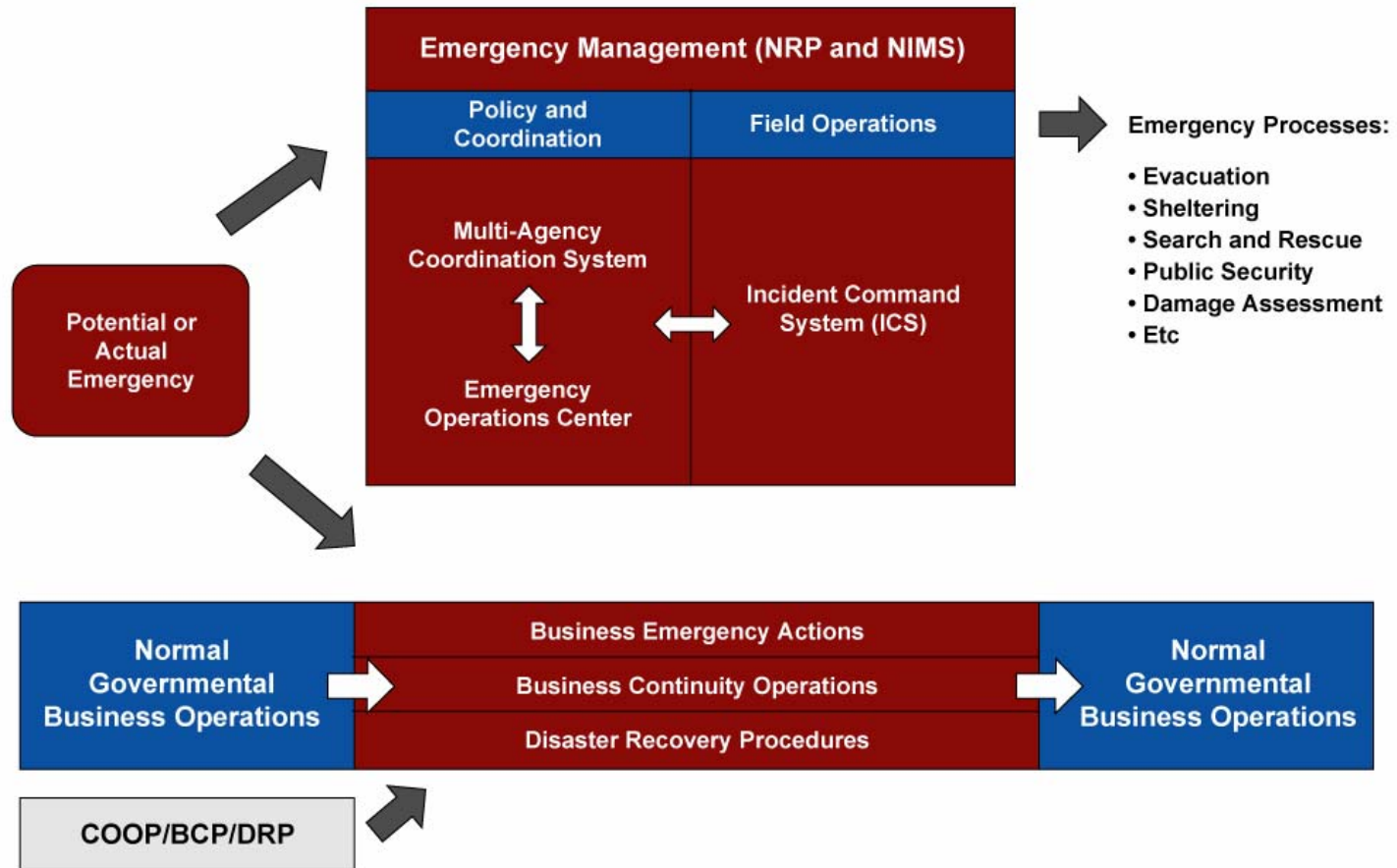
# Measures of Success

- The government's bottom line:
  - How effective and efficient are our business processes?
  - How well do we protect our citizens and property?

**or both?**



# Putting It All Together



# Are You Ready?

- 2006 DHS Nationwide Plan Review:
  - “The majority of the Nation’s [urban and state] current emergency operations plans . . . cannot be characterized as fully adequate, feasible, or acceptable to manage catastrophic events”
    - Highlights significant shortcomings in:
      - Continuity of operations and government
      - Communications
      - Public warning and emergency notification
      - Public information
      - Resource management: “Achilles heel”

# Ready or NOT?

- Trust for America's Health (TFAH) 2006 Report on Public Health readiness in:
  - Pandemic planning
  - All-hazards emergency operations planning
  - Bioterrorism response and recovery
  - Interoperable communications



# TFAH Public Health Services Scores

(10 is best; 1 is worst)

SCORES BY STATE						
10 (1 state)	9 (1 state)	8 (12 states)	7 (11 states)	6 (13 states)	5 (8 states & D.C.)	4 (4 states)
Oklahoma	Kansas	Alabama Kentucky Michigan Missouri Montana Nebraska South Dakota Texas Virginia Washington West Virginia Wyoming	Delaware Florida Georgia Hawaii Idaho Illinois Minnesota New Hampshire New York North Dakota Tennessee	Colorado Indiana Louisiana Massachusetts Mississippi Nevada New Mexico North Carolina Oregon Rhode Island Utah Vermont Wisconsin	Alaska Arizona Arkansas Connecticut D.C. Maine Ohio Pennsylvania South Carolina	California Iowa Maryland New Jersey

# New Orleans Lessons Learned

## Planning Factors for Response

- Must be capabilities-based
- Must consider people as well as IT equipment
  - Must be redundant for both
  - Single point of failure in IT infrastructure deadly
- Offsite backup is essential
- Continuity of Government requires IT infrastructure
- Communications

# Planning Guides for Response

- Mission vs. Compliance
- Risk Management vs. Risk Avoidance
- Logistics System
- Command and Control
- People endurance factors
- Written plans!!

# Recommendations

- Plan, Train, Exercise / Plan, Train, Exercise
- Strong Emergency Management / IT working partnership
- Security balance with mission

# Questions & Answers

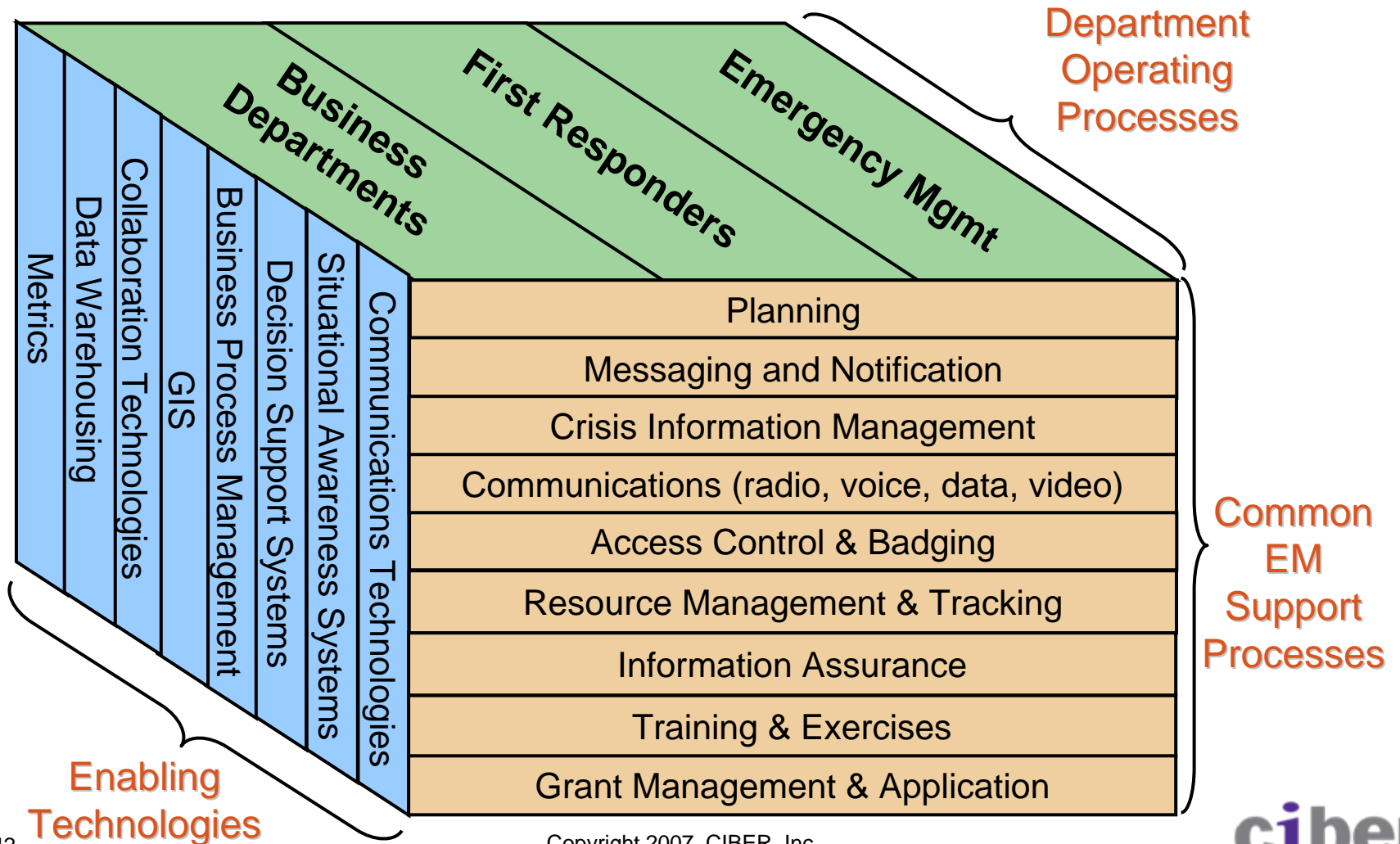
## Thank you for attending!

For more information about this presentation or CIBER's emergency management services, please contact Robin Caputo at [rcaputo@ciber.com](mailto:rcaputo@ciber.com) or at 303-267-3876

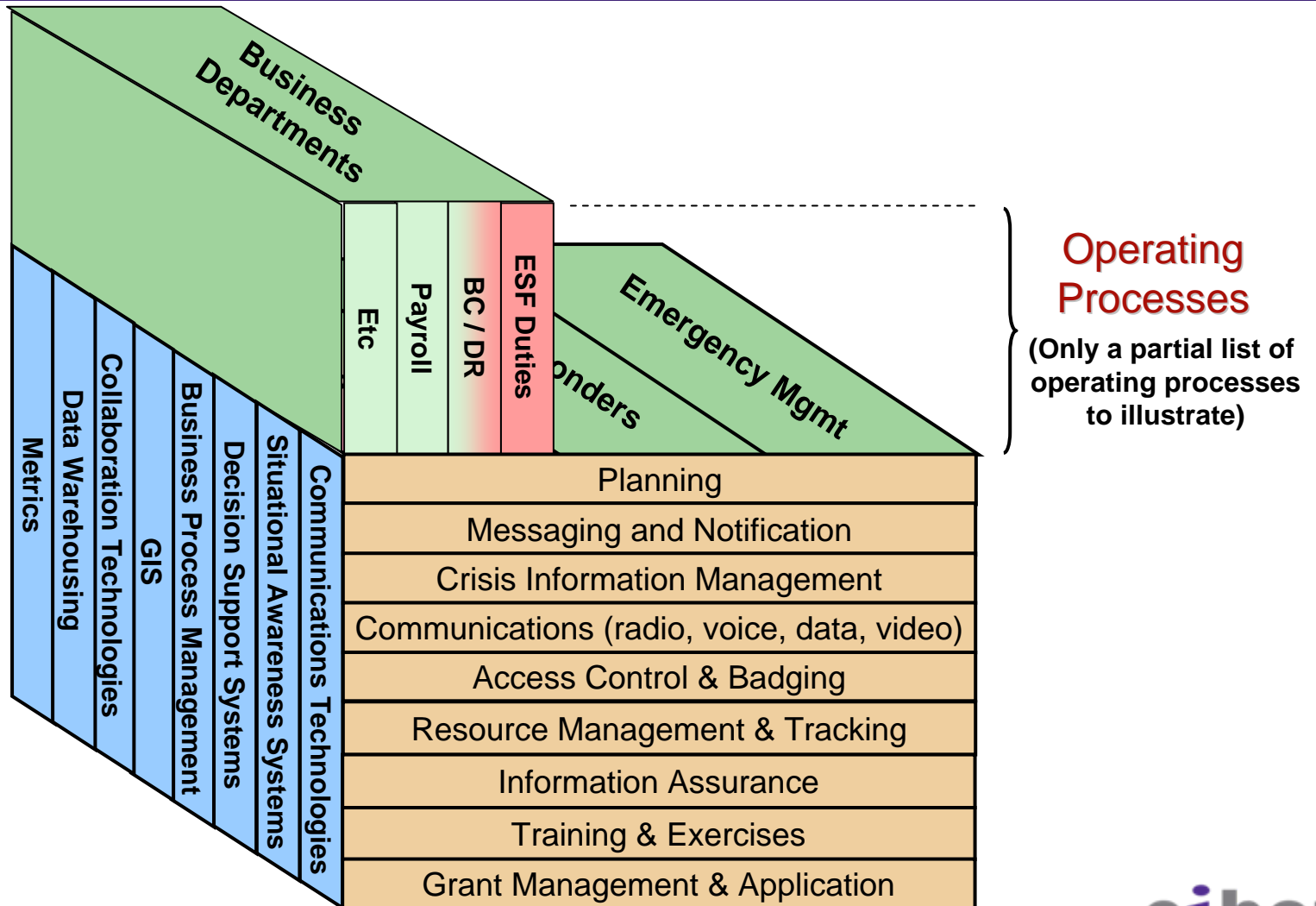


# BACKUP SLIDES

# CIBER Cube Model ©

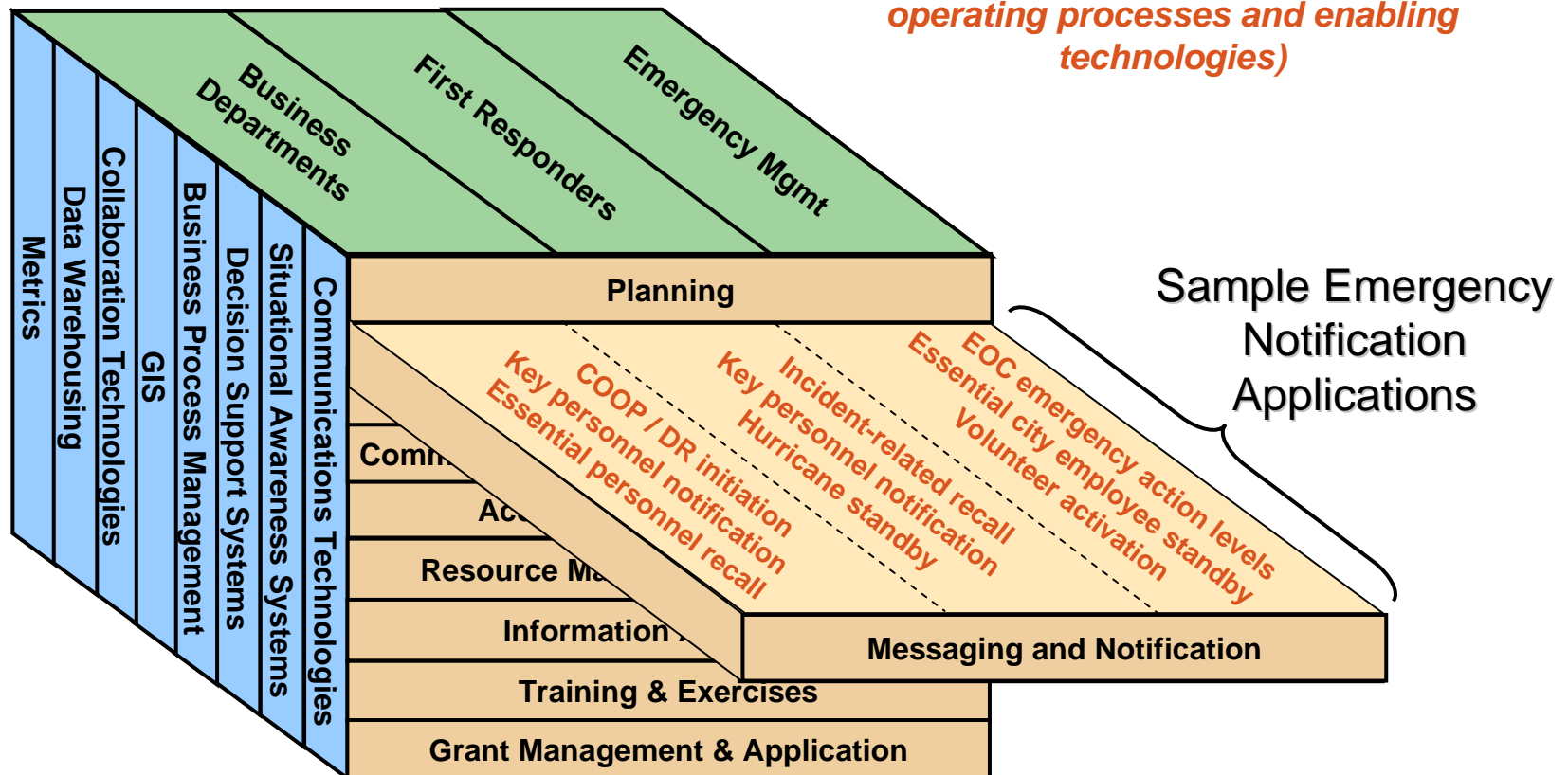


# Operating Process Slice: Business Departments

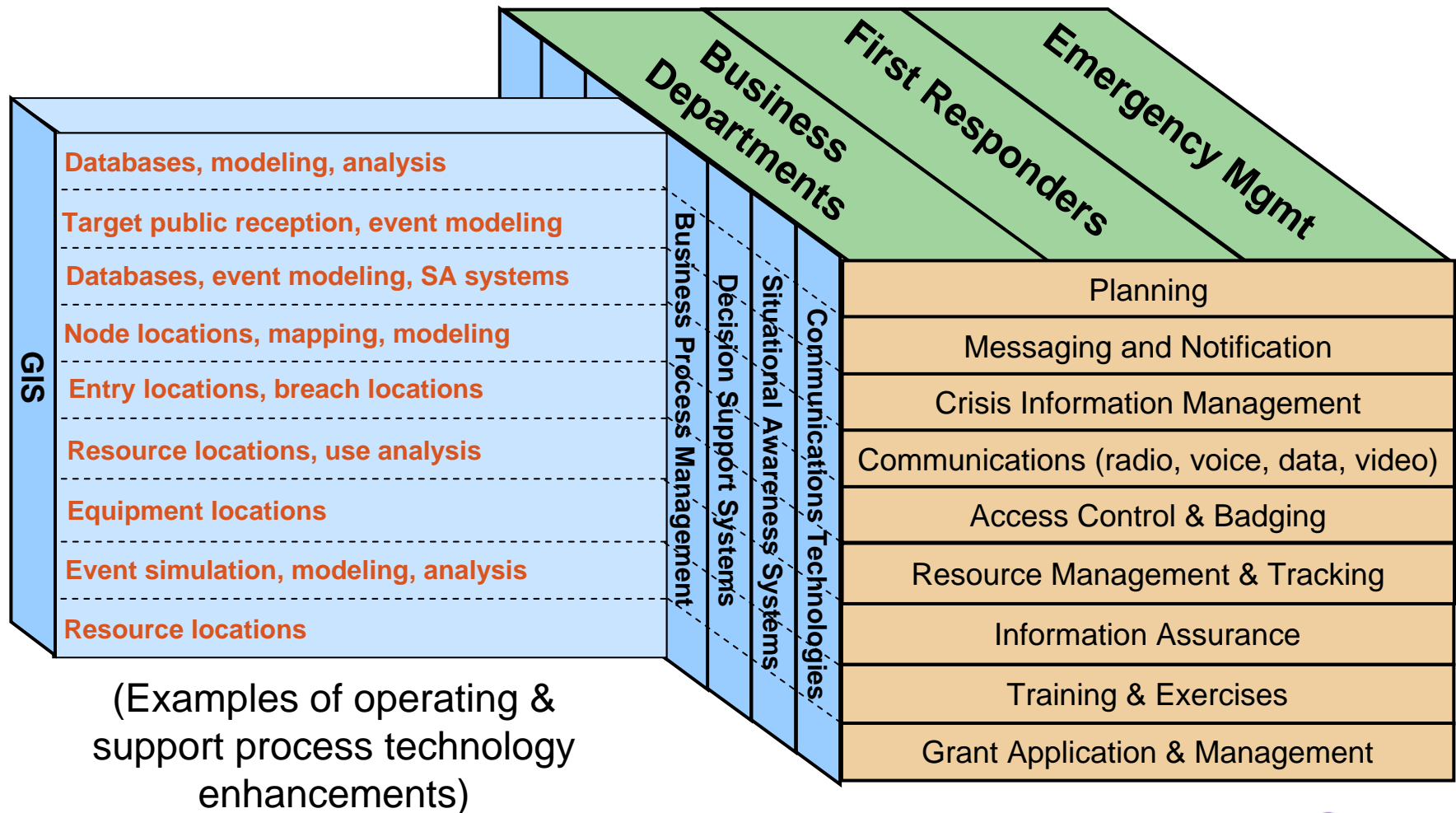


# Support Process Slice: Messaging & Notification

*(Note that each support process intersects, and can be analyzed with reference to, both operating processes and enabling technologies)*



# Enabling Technologies Slice: Geographic Information Systems



# Authorized Equipment List (AEL): Information Technology

- Application Systems and Software
  - Computer Aided Dispatch (CAD)
  - Position Locating Systems
  - Geographic Information Systems (GIS)
  - Risk Management Software
  - Incident Management
  - Analytical Tools
  - Inventory
  - Simulation
  - Notification & Warning Systems

# Authorized Equipment List (AEL): Information Technology (cont.)

- **Hardware**
  - Computers
  - Peripherals
- **Media Devices**
  - Cameras and surveillance equipment
  - Projectors
  - Displays
- **Sensor Devices**
  - Remote sensors
- **System and Networking Software**
  - Network Operating and Monitoring Systems (software)
  - Monitoring software (SCADA)

# Authorized Equipment List (AEL): Information Security Enhancement Equipment

- Authentication Devices
- Encryption
- Host Level Security
  - Forensic software
  - Malware protection software
  - Personal firewall
- Network Level Security
  - Network firewall
  - Intrusion detection system
  - Network vulnerability scanning tools
  - Security event incident management system
  - Patch/configuration management system

# Authorized Equipment List (AEL): Interoperable Communications Equipment

- Commercial
  - Cell – digital
  - Data & messaging
  - Satellite phone
  - Satellite data services
  - Priority services
- Private
  - Land-mobile radios and bases
  - Bridging / patching / gateway equipment
  - Wide-area networks
  - Wire-line communication
    - Audio teleconferencing bridge
    - Video teleconferencing bridge
    - Video teleconferencing