



FEMA

What's In It for Us? 2011 Leadership Conference and Workshop

How to Motivate Senior Management to Collaborate with Government

One key to effective motivation begins with communicating the value. The mutual sharing of experience, best practices and challenges, build meaningful and accurate perception. Topics should include, but not limited to, examples of effective operational structure, program elements and specific in-action outcomes. They should include in-sector, cross-sector and cross government jurisdiction. When partners share their stories, and those stories are shared with senior management - awareness and confidence is fostered. Misperception of "risk", "competitive advantage", and "us versus them" mentalities diminish. Emphasis should be placed on the "Organizational Community", bound together by our interdependencies. Our partnership defines how we are inter-related to each other and helps to identify common needs resources and objectives. As we work in enterprise together to meet our common objectives, our pooled effort will meet and/or exceed the needs of our social communities that form the underpinning our success. These relationships should provide for sustainable growth. They should continue beyond the initial parties, and transcend the individuals, the organizations, and the network and ultimately contribute to – "The network of networks". They should weave through the fabric of our organizational cultures. The initial investment of time, talent and treasure grows organically, exponentially, and provides unparalleled return.

Key value proposition:

- Improve employee safety, satisfaction and inclusion.
- Results achieved for investments made.
- Residual risks remaining unaddressed.
- Key priorities that will have the biggest impact.
- Improved efficiency and improved ability to manage risk.

Program Elements:

- Validate and report readiness, response and recovery.
- Expand/ optimize recovery control environment.
- Influence the establishment of industry standards and best practices.
- Identify recoverability gaps between business expectations and technical capabilities.
- Enhance recovery preparedness measures.
- Memorandums of Understanding (MOU)
 1. Targeted partners w/critical interdependencies
 2. Partners susceptible to significant disasters
 3. Enhanced information sharing and access
 4. Collaborative opportunities to enhance public perception
 5. Strategic planning and coordination
- Dedicated Liaison(s) - Contact Database
 1. Central "repository" for contact information
 2. Actionable and geographically relevant and accessible.
 3. Continuous and sustainable liaison program.
 4. Restricted Access to "Sensitive" contacts.
 5. Regular Maintenance (Relationships and Database)
- Association Memberships
 1. California Resiliency Alliance
 2. Industry Specific
 3. Cross-Sector



FEMA

What's In It for Us?

2011 Leadership Conference and Workshop

In-Action Outcomes:

- Floods/Mudslides:
 1. Evacuation routes; pre-staging
 2. Shelters
 3. Disaster relief assistance
 4. Situational awareness/Daily Situation Reports
 5. Mobile Banking Center deployments
 6. Critical Infrastructure prioritization
 7. Disaster relief information sharing
 8. Relief funding requirements
 9. Real-time communications
 10. Essential resource requests
 11. Volunteer support need

- H1N1:
 1. Endurance of influenza virus on currency and common surfaces
 2. Common operational picture
 3. Public health guidance
 4. Banking and finance collaboration
 5. Best practices and interdependencies
 6. School closures

- Wildfires:
 1. Containment status
 2. Fire maps
 3. Buffer zones
 4. Public assembly areas
 5. Supplies needed (essential services)
 6. Resource requests

The Protected Critical Infrastructure Information (PCII)

The Protected Critical Infrastructure Information (PCII) Program is an information-protection program that enhances information sharing between the private sector and the government. The Department of Homeland Security and other federal, state and local analysts use PCII to:

- Analyze and secure critical infrastructure and protected systems,
- Identify vulnerabilities and develop risk assessments, and

If the information submitted satisfies the requirements of the [Critical Infrastructure Information Act of 2002](#), it is protected from:

- The Freedom of Information Act (FOIA),
- State and local disclosure laws, and
- Use in civil litigation.

PCII cannot be used for regulatory purposes and can only be accessed in accordance with strict safeguarding and handling requirements.

Submissions that do not meet the requirements are destroyed or returned to the submitter.