

Best Practices Collection Proposal
Emergency Services Sector Coordinating Council
February 13, 2008

Background: On September 20, 2007 the Emergency Services Sector Coordinating Council (SCC)¹ met with representatives from the Department of Homeland Security (DHS) in order to begin substantive collaboration between the SCC and the Government Coordinating Council (GCC) to establish a Best Practices Project (“the Project”) in order define the our sector’s Best Practices for infrastructure protection and resilience.

The objective of the Project is for the SCC to develop a conceptual framework with which to categorize and subsequently identify Emergency Services Sector (ESS) best practices, the results of which will be attached as an appendix to the Sector Specific Plan (SSP)² in order to provide “a sector-approved discussion of best practices...that will allow owners and operators throughout the sector to understand what has been identified as best practices, and to potentially adopt them for their own assets, systems, networks or functions.”³

On November 13, 2007 the SCC began a series of meeting to establish a draft framework approach to identifying and determining the Sector’s best practices. From these meetings, the SCC and its identified Subject Matter Experts (SMEs) created a graphic representation of the framework, which is demonstrated in Appendix A, and outlined the strategy behind the framework in the below section entitled “Framework Summary.”

Definitions: Throughout the process of the Project, the SCC has operated with the following definitions in mind:

Infrastructure Protection—“Infrastructure protection” for the Emergency Services Sector comprises the totality of personnel, systems, networks, activities and programs that maintain and/or improve the ability of the Sector to protect and preserve its own integrity in an imminent or on-going emergency. Infrastructure protection may include physical protection, but it does not focus exclusively upon this aspect. See Infrastructure Resilience.

¹ The Emergency Services SCC is the industry-component of a public-private partnership council set up to coordinate critical infrastructure protection (CIP) in the systems and activities that promote and protect the capability of the Emergency Services Sector (ESS) to provide services to the public, other sectors and the nation. The SCC is comprised of representatives from: National Sheriffs’ Association; International Association of Fire Chiefs; International Association of Chiefs of Police; National Emergency Management Association; International Association of Emergency Managers; and the National Association of State EMS Officials.

² The Sector Specific Plan establishes a coordinated approach to national priorities, goals, and requirements for critical infrastructure and key resources protection. The SSP provides the means by which the National Infrastructure Protection Plan is implemented across the Emergency Services Sector, as well as a national framework to address its unique characteristics and risk landscape. This coordinated approach allows federal funding and resources to be applied in the most effective manner to manage risk.

³ Letter from Assistant Secretary for Infrastructure Protection, Robert Stephan, sent to Sector Specific Agencies on November 1, 2006.

Best Practices—When speaking of “best practices” (also known as “model practices” or “promising practices”) we are referring to those systems, networks, activities and programs related to infrastructure protection that have, through industry experience, proven most efficient and effective in achieving the desired result.

All-Hazards—The term “all-hazards” is taken to address a full range of potential emergency events, from natural disasters and infectious disease outbreak, to man-made incidents, both intentional and unintentional.

Infrastructure Resilience—Infrastructure resilience addresses and resolves the “protection gaps” in critical infrastructures and facilitates an earlier return to normal operations. Infrastructure resilience provides redundancy for Sector infrastructures and enhances the ability of an organization to expeditiously recover from a disaster and reconstitute essential services with minimum disruption to personnel, processes, procedures, information, and facilities.

Framework Summary: First, the SCC approached the framework by clarifying DHS’ expectations for this project, essentially answering the question: “What is DHS looking for with the Project” OR, “What does DHS want and/or need from the ES SCC in relation to the Project?”

As the Project is intended to become an appendix to the SSP and given that the SSP is a risk management framework document itself that is intended to be read by individuals at all levels of understanding, the SCC determined that the final product of the Best Practices project should be a high-level, easily understood and concise summation of the systems, networks, activities and programs that highlight the successes of the Sector.

Additionally, the SCC determined that the framework should be constructed using a conceptual lens that is familiar to DHS and its federal partners. To accomplish this, all of the best practices considered should be National Incident Management System (NIMS)⁴ compliant and have the capability to apply to All-Hazards events.

Furthermore, as the Project is intended to be an appendix to the SSP, it seemed logical to categorize the best practices in the same criteria that the SSP uses to delineate critical assets. That is, we will evaluate each best practice by whether it is a Cyber related best-practice (Information Technology & Communications), a Physical related best-practice (Facilities & Logistics) or a Human related best-practice.⁵

Finally, to address the totality of systems, networks, activities and programs that may represent the Sector’s best practices, the SCC decided to consider both interoperable and operable best practices.

⁴ NIMS was developed so responders from different jurisdictions and disciplines can work together better to respond to natural disasters and emergencies, including acts of terrorism. NIMS seeks to promote a unified approach to incident management; standard command and management structures; and emphasis on preparedness, mutual aid and resource management.

⁵ See the Emergency Services Sector Specific Plan, pages 11-12.

The Request:

The resulting collection of Sector Specific best practices will assist local and regional entities in developing effective and comprehensive emergency plans that also include protection of their local critical infrastructures and key resources. Sharing of best practices will assist in local protection planning, information sharing, risk management, resource coordination, and program implementation efforts by providing examples of successful initiatives in other jurisdictions.

In order to gather best practices from the Sector and complete the framework established above, the SCC defined a set of criteria to assist sector members in selecting their own best practices. The criteria for selection are as follows:

- ✚ Scalability: Begins Locally, Expands Nationally
- ✚ Emphasizes Prevention, Protection and Resilience
- ✚ Cost-Effective & Replicable
- ✚ Enhances Sector Capability to Protect Itself, Quickly Restore Normal Operations after the Event and Improves Ability to Respond to Others
- ✚ National Incident Management System (NIMS) Compliant
- ✚ Preference for All-Hazards Application
- ✚ Usability for Credentialing, Training or Exercise

It is essential to note here that, while it is important to pay attention to the criteria, your best practices do not have to meet every standard. The above criteria are meant to guide you as you define and select what may be a best practice. Moreover, if you have a notable success that should be shared with the Sector but may not fit within the criteria, please feel free to include this on your list of best practices.

The deadline for submittal of your best practices to your association representative is March 3, 2008.

APPENDIX A
Conceptual Framework for Best Practices Identification
 For Internal Use Only — Not for Further Distribution

**Emergency Services Sector Strategic Overlay
 for Critical Infrastructure/Key Resources
 Protection and Support**

Best Practices selected from results of data-call by the Sector Coordinating Council's panel of experts.

InfoTech & Communications (Cyber)	Facilities & Logistics (Physical)	Human
<p>✚ Interoperability/Operability</p> <ul style="list-style-type: none"> - best practice - best practice - best practice - best practice - best practice - best practice 	<p>✚ Interoperability/Operability</p> <ul style="list-style-type: none"> - best practice - best practice - best practice - best practice - best practice - best practice 	<p>✚ Interoperability/Operability</p> <ul style="list-style-type: none"> - best practice - best practice - best practice - best practice - best practice - best practice

- Criteria and Standards for Best Practices Selection**
- Scalability (Begins Locally, Expands Nationally)
 - Emphasizes Prevention, Protection and Resilience
 - Cost-Effective and Replicable
 - Enhances Sector Capability to Protect Itself, Quickly Restore Normal Operations After the Event and Improves Ability to Respond to Others
 - National Incident Management System (NIMS) Compliant
 - Preference for All-Hazards Application
 - Usability for Credentialing, Training or Exercise

Best Practices Collection Proposal
Emergency Services Sector Coordinating Council
Submission Form

Program Name or Brief:

Point of Contact:

Name:

Department/Agency:

Address:

Phone:

Email:

The model practice being proposed addresses the security of which element of critical infrastructure? *(choose all that apply)*

- Information Technology and Communications (Cyber)
- Facilities and Logistics (Physical)
- Human

Which criteria does the proposed best practice meet? *(Choose all that apply)*

- Scalability: Begins Locally, Expands Nationally
- Emphasizes Prevention, Protection and Resilience
- Cost-Effective & Replicable
- Enhances Sector Capability to Protect Itself, Quickly Restore Normal Operations after the Event and Improves Ability to Respond to Others
- National Incident Management System (NIMS) Compliant
- All-Hazards Application
- Usability for Credentialing, Training or Exercise

Who was involved in the implementation of the proposed model practice? *(Choose all that apply)*

- Fire/rescue department
- Law enforcement
- Non-fire-based EMS
- Emergency management
- Public works
- Public health
- Other local government
- Other state government
- Private sector / industry

Provide a detailed description of proposed model practice. Please include any feedback you have received, or data that can support it being a model practice, etc.

Briefly discuss the financial aspects of the program; such as the cost a challenge, availability of grant funds, sharing costs regionally or across disciplines, purchasing or service issues, etc.

Briefly discuss the major challenges you encountered and how you address them.

Briefly discuss the highlights on how this program has enhanced security of the emergency services sector.

Aside from ensuring a response from emergency services, briefly discuss any secondary effects for your overall all-hazards security efforts. For example, it created a security model for the private sector; it enabled another long-standing need for routine duties; in strengthen interdisciplinary relationships, etc.

Please email completed proposals to adavison@iafc.org or fax to Ann Davison at (703) 273-9363