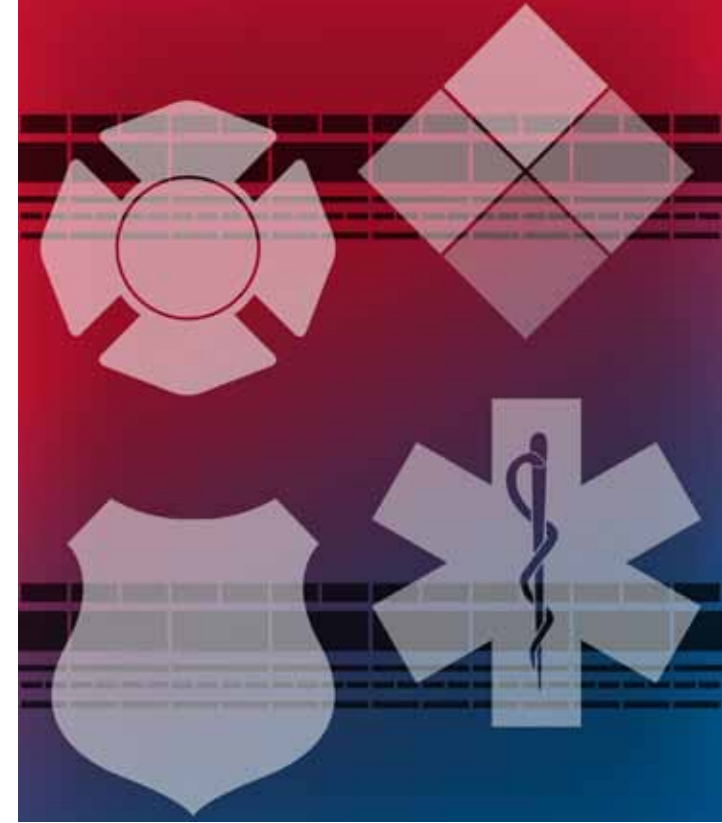


**PROTECTING AND ENSURING
THE RESILIENCY OF THE CRITICAL
INFRASTRUCTURE AND KEY
RESOURCES (CIKR) OF THE
UNITED STATES IS ESSENTIAL TO
THE NATION'S SECURITY, PUBLIC
HEALTH AND SAFETY, ECONOMIC
VITALITY, AND WAY OF LIFE.**

— 2009 National Infrastructure Protection Plan

**EMR-ISAC ONLINE AT
WWW.USFA.FEMA.GOV/EMR-ISAC**

**EMR-ISAC
National Emergency Training Center
16825 South Seton Avenue
Emmitsburg, MD 21727**



EMR-ISAC

**Emergency Management and
Response — Information
Sharing and Analysis Center**

Promoting critical infrastructure
protection and resilience by Emergency
Services Sector personnel nationwide



FEMA

BACKGROUND

Protecting and ensuring the continuity and resilience of the Critical Infrastructure and Key Resources (CIKR) of the United States are essential to the Nation's security, public health and safety, economic vitality, and way of life. To that end, Homeland Security Presidential Directive 7 has identified the Emergency Services Sector as one of the Nation's 18 CIKR Sectors.

The Emergency Services Sector (ESS) is a system of response and recovery elements that forms the Nation's first line of defense and prevention and reduction of consequences from any terrorist attack. It is a sector of trained and tested personnel, plans, redundant systems, agreements, and pacts that provide life safety and security services across the nation via the first responder community comprised of Federal, State, local, tribal, territorial, and private sector partners.

WHAT IS CRITICAL INFRASTRUCTURE PROTECTION?

Generally, critical infrastructure protection (CIP) consists of the proactive measures to protect essential personnel and resources from all hazards. More formally, it is an analytical process to guide the systematic protection of critical infrastructures by the application of a decision method that assists leaders to determine which critical resources need protection and when protective and resiliency measures must occur.

The process involves the following steps: identifying the organization's critical infrastructures, determining the threats against those infrastructures, analyzing the vulnerabilities of threatened infrastructures, assessing the risks of ruin or loss of a critical infrastructure, and applying preventative or resiliency measures where loss is unacceptable.

WHO IS RESPONSIBLE FOR CIP?

Community leaders, including those of emergency response organizations, have the responsibility to take an all-hazards approach to determine which infrastructures must be protected.

WHAT IS THE MISSION OF THE EMR-ISAC?

The mission of the Emergency Management & Response - Information Sharing & Analysis Center (EMR-ISAC) is the promotion of CIP, and to serve as a major information sharing mechanism for the collection, research, collaboration, and dissemination of CIP and emerging threat information to ESS departments and agencies nationwide.

CONTACT INFORMATION

For more information please contact the EMR-ISAC at emr-isac@fema.dhs.gov or 301-447-1325; or visit: www.usfa.fema.gov/emr-isac

WHAT ASSISTANCE DOES THE EMR-ISAC PROVIDE?

The EMR-ISAC disseminates critical infrastructure protection and threat information through Department of Homeland Security (DHS) information sharing mechanisms, and provides no-cost technical assistance CIP consultation services to ESS leaders.

THE EMR-ISAC ROUTINELY PUBLISHES:

The *InfoGram* – produced weekly, it typically includes four short articles about the protection of the critical infrastructures of communities and their emergency responders.

Bulletins – distributed as needed, contain timely, important homeland security information affecting the CIP of emergency response agencies.

The EMR-ISAC maintains Communities of Interest (COI) on the Homeland Security Information Network (HSIN) portal to share CIP and emergent threat information relevant to the ESS from Federal, State, local, tribal, territorial, and private sector partners.

ESS personnel currently in leadership positions in their respective departments and agencies, who subscribe for EMR-ISAC CIP information, may also be eligible to receive “For Official Use Only” (FOUO) information.