USFA Home → Fire Service → CIP (EMR-ISAC) → About CIP → What is CIP and why is it important?

What is CIP and why is it important?

Numerous officials within the public and private sectors of the United States have been actively promoting and applying critical infrastructure protection (CIP). Yet it was not too long ago that most citizens never heard of such words. So why is there now so much attention being given to CIP?

The urgent call for the protection of critical infrastructures began on 11 September 2001, when leaders of government and industry as well as millions of private citizens were awakened from their slumber of national safety and security. Since that unforgettable day, the American people have been confronted with the possibility of living and working without one or more of the many basic necessities we have come to expect and depend on. For example, can you imagine surviving without water, electricity, home heating oil, natural gas, automobile gasoline, telephones, Internet access, emergency services, etc.?

Homeland Security Presidential Directive – 7 (HSPD-7) issued in December 2003 established the policy of the United States to enhance the protection of national critical infrastructures against terrorist acts that would significantly diminish the responsibility of federal, state, and local governments to perform essential security missions and to ensure the general public health and safety. The USA PARTRIOT Act of 2001 defines critical infrastructures as "those physical and cyber-based systems so vital to the operations of the United States that their incapacity or destruction would have a debilitating impact on national defense, economic security, or public safety." More specifically, critical infrastructures are those people, things, or systems that must be intact and operational in order to make daily living and working possible.

The term "critical infrastructure protection" (CIP) pertains to the proactive activities for protecting critical infrastructures: the people, physical assets, and communication/cyber systems that are indispensably necessary for national security, economic stability, and public safety. CIP methods and resources deter or mitigate attacks against critical infrastructures caused by people (e.g., terrorists, other criminals, hackers, etc.), by nature (e.g., hurricanes, tornadoes, earthquakes, floods, etc.), and by HazMat accidents involving nuclear, radiological, biological, or chemical substances (i.e., all hazards). Plainly stated, CIP is about protecting those invaluable assets that make life, liberty, and the pursuit of happiness a national reality.

To promote CIP by police, fire, emergency medical, and emergency management agencies, i.e., the Emergency Services Sector (ESS), the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) developed the CIP program to support this ESS initiative. Primarily, the EMR-ISAC disseminates information to bolster the infrastructure protection efforts of emergency first responders nationwide. Located at the National Emergency Training Center in Emmitsburg, MD, the EMR-ISAC imparts that critical infrastructures of the emergency services are essential for the accomplishment of missions affecting life and property. For further clarification, they are the people, physical assets, and communication/cyber systems that must be intact and operational 24x7 to ensure survivability, continuity of operations, and mission success.

Community leaders, including those of emergency first responders, have the responsibility to decide which infrastructures must be protected from all hazards. Scarce resources (i.e., time, money, personnel, and material) make these decisions somewhat complicated. How then, does one determine the fewest indispensable infrastructures to receive the application of these scarce resources? The EMR-ISAC recommends the implementation of the CIP process.

The CIP process is an analytical model or template to guide the systematic protection of critical infrastructures. More basically, it is a reliable decision sequence that assists leaders in ultimately determining exactly what really needs protection as well as when the protection should be activated. As a time-efficient and resource-restrained practice, the process ensures the protection of only those infrastructures upon which survivability, continuity of operations, and mission success depend. The process, that can make a favorable difference if periodically reapplied by ESS leaders, consists of the following steps:

- **Identifying critical infrastructures** essential for mission accomplishment.
- **Determining the threats** against those infrastructures.
- **Analyzing the vulnerabilities** of threatened infrastructures.
- **Assessing the risks** of the degradation or loss of a critical infrastructure.
- **Applying countermeasures** where risk is unacceptable.

To assist leaders and managers of emergency first responders, the EMR-ISAC developed a CIP Process Job Aid as a user-friendly guide for the implementation of the CIP process. The Job Aid is an easy reading document accessible at the following website: http://www.usfa.dhs.gov/downloads/doc/cipc-jobaid.doc. Questions about CIP or the Job Aid can be directed to the EMR-ISAC at (301) 447-1325 or emr-isac@dhs.gov.

When applied by the emergency services, CIP is not a product; it is a process to secure the effective protection of mission critical people and systems. While it may be impossible to prevent all attacks against critical infrastructures, CIP can reduce the chances of future attacks, make it more difficult for attacks to succeed, and mitigate the outcomes in the event they do occur. Thus, among all the important procedures or things involved in emergency preparedness, CIP is possibly the most essential component. Without question, it is a practice that the ESS leadership cannot afford to disregard.

Last Reviewed: December 28, 2006