

What is CIP and why is it important?

In recent months, officials within the public and private sectors of the United States have spoken and written more frequently about 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?

To answer the question, this article will provide a brief history of CIP with pertinent definitions, review the United States Fire Administration's (USFA) CIP Program, highlight the CIP process, and encourage its implementation as a component of emergency preparedness plans and actions. When finished, the reader should have a better understanding of what CIP is and why it is important.

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 upon. For example, can you imagine surviving without water, electricity, home heating oil, natural gas, automobile gasoline, telephones, Internet access, emergency services, etc.?

Approximately four years ago, members of the United States Congress and the Executive Branch explored methods to prevent a denial of these fundamental services in addition to others affecting the minimum operations of the national economy and government. Presidential Decision Directive 63 (PDD 63) was issued in May 1998 to combat the threats against these services, which are crucial parts of the Nation's critical infrastructures. According to PDD 63, the national goal is to eliminate the "potential vulnerability" of critical infrastructures and protect the United States from intentional acts that would significantly diminish the Federal government's responsibility to perform essential security missions and to ensure the general public health and safety. PDD 63 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." In simpler terms, critical infrastructures are those people, things, or systems that must be intact and operational in order to make daily living and working possible.

It should be noted here that PDD 63 and the President's Commission on Critical Infrastructure Protection included emergency services as a critical infrastructure of the Nation. The commission's report explained that emergency services embody the firefighters, paramedics, police, and hospital personnel who respond to all incidents involving public health and safety. Assuming the reader appreciates the significance of this, then it will be helpful to examine what is meant by the protection of infrastructures.

Critical infrastructure protection (CIP) pertains to the proactive activities for protecting critical infrastructures: the people, physical entities, and 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, biological, or chemical substances. Plainly stated, CIP is about protecting those invaluable assets that make life, liberty, and the pursuit of happiness a national reality.

In October 2000, USFA initiated a CIP Program to support the provisions of PDD 63 and to address three major issues:

1. As components of the emergency services, fire and emergency medical services (EMS) departments are a critical infrastructure of their respective communities and should be protected. Fire service history substantiates that the failure to protect this infrastructure has resulted in major disruptions within several departments caused by the spread of hepatitis C, fires in fire stations, aerial ladder failures, inadequate training, etc. A brief synopsis of three case studies follows.

There were approximately twelve line-of-duty deaths among firefighters in a large Eastern city during the 1919 flu epidemic. It is estimated that at least twice that many were too ill to perform duties. Since the flu and infectious diseases are still prevalent, it begs the question regarding what procedures do modern departments practice to prevent the spread of incapacitating illnesses.

At a sizable mid-Western city, unknown persons disabled the power supply to a remotely located repeater station for the emergency services radio system. The back-up generator was activated, but soon ran out of fuel. A difficult period of sharply reduced communications occurred before trouble-shooting finally identified the cause of the problem. It quickly became obvious that a fence, locks, lights, or an alarm system would have averted this calamity.

An expansive Western metropolitan area introduced “rolling brownouts” as a means of electrical power management. Utility directors accepted that domestic water consumption would be interrupted. They were temporarily oblivious to the fact that their actions would deny necessary water for firefighting. Good coordination among members of the Local Emergency Planning Committees would ensure ample awareness of the ramifications of intended actions.

2. Firefighters and EMTs are constantly on the front lines of strife while protecting many other national, state, and local critical infrastructures. Electrical power systems, petroleum manufacturing plants and pipelines, transportation facilities, communications centers, etc., all rely upon the expedience and efficiency of emergency first responders.
3. The fire and EMS services must be included in the CIP portions of community emergency preparedness plans and actions. Communities that neglect periodic CIP planning risk the degradation or loss of critical infrastructures that their citizens require for safety and survival. No doubt, municipal leaders would prefer to avoid the potential chaos generated by a disruption or destruction of any critical infrastructure, most especially their emergency services.

To promote the CIP program and advance these issues, USFA opened its Critical Infrastructure Protection Information Center (CIPIC). The CIPIC also disseminates information to bolster the infrastructure protection efforts of emergency first responders throughout the United States. Located at the National Emergency Training Center in Emmitsburg, MD, the CIPIC imparts that critical infrastructures of the emergency services are those physical and cyber assets that are essential for the accomplishment of missions affecting life and property. For further clarification, they are the people, things, or systems that will seriously degrade or prevent survivability and mission success if not intact and operational. The following are some examples of critical infrastructures for the fire and emergency medical services:

- firefighters and paramedics,
- fire and EMS stations, apparatus, and communications,
- Public Safety Answering Points (or 9-1-1 Communications Centers),
- computer-aided dispatch and computer networks,
- pumping stations and water reservoirs for major urban areas,
- major roads and highways serving large population areas, and
- bridges and tunnels serving large population areas.

It is appropriate here to make special note of the intentional order of the above listing. Firefighters and emergency medical personnel are indeed among the frontline elements of homeland defense. Combined with law enforcers, they are the most critical of all infrastructures, and their safety and welfare should always take precedence.

Community leaders, including those of emergency first responders, have the responsibility to decide which infrastructures must be protected from attacks by people, nature, or HazMat accidents. 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 CIPIC 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. As a time-efficient and resource-restrained practice, the process ensures the protection of only those infrastructures upon which survivability and mission success depend. The process, which can make a favorable difference if repeatedly implemented by department leaders, consists of the following steps:

- **identifying critical infrastructures** essential for the accomplishment of department missions (e.g., fire suppression, EMS, HazMat, search and rescue, extrication, etc.),
- **determining the threat** against those infrastructures,
- **analyzing the vulnerabilities** of threatened infrastructures,
- **assessing risk** of the degradation or loss of a critical infrastructure, and
- **applying countermeasures** where risk is unacceptable.

To assist leaders and managers of emergency first responders, the CIPIC developed a CIP Process “Job Aid” as a user-friendly guide for the implementation of the CIP process. Currently under review, the Job Aid was prepared as an easy reading document that could be quickly comprehended by all readers. Once approved, the Job Aid will be accessible at the USFA website: www.usfa.fema.gov/cipc. Questions about CIP or the Job Aid can be directed to the CIPIC at (301) 447-1325.

When applied by the emergency services, CIP is not a product; it is a process to secure the effective protection of the people, physical entities, and cyber systems that are genuinely mission critical. 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 fire and EMS leaders cannot afford to disregard.