United States Fire Administration

THE CRITICAL INFRASTRUCTURE PROTECTION PROCESS

Job Aid

(Developed by NATEK Incorporated for USFA)

Critical Infrastructure Protection Information Center
16825 South Seton Avenue
Emmitsburg, MD 21727
301-447-1325
usfacipc@fema.gov
www.usfa.fema.gov/cipc

Edition 1: May 2002

TABLE OF CONTENTS

I. INTRODUCTION

A. Background

1. Presidential Decision Directive 63 (PDD 63) was issued May 1998 in response to concerns about potential attacks against critical infrastructures.

2. PDD 63 defined critical infrastructures as the physical and cyber systems so vital to the operations of the United States that their incapacity or destruction would seriously weaken national defense, economic security, or public safety.

3. The directive designated the Federal Emergency Management Agency (FEMA) lead agency for the fire and emergency medical services (EMS) community.

4. FEMA directed the U.S. Fire Administration (USFA) to increase critical infrastructure protection (CIP) awareness throughout the fire and EMS community.

B. Fire and Emergency Medical Services Community

1. PDD 63 identified the Emergency Services Sector as one of eight critical infrastructures.

2. The fire and EMS community as well as the law enforcement community comprise the Emergency Services Sector.

3. USFA is the lead critical infrastructure protection (CIP) agency for the fire and EMS community.

C. Job Aid Purpose

1. This Job Aid is a guide to assist leaders of the fire and EMS community with the process of critical infrastructure protection.

2. The document intends only to provide a model process or template for the systematic protection of critical infrastructures.

3. It is not a CIP training manual or a complete roadmap of procedures to be strictly followed.

4. The CIP process described in this document can be easily adapted to assist the infrastructure protection objectives of any community, service, agency, or organization.

II. CIP OVERVIEW

A. Premise

1. Attacks on the physical and cyber systems of fire and emergency services departments will weaken performance or prevent operations.

2. There are three different types of possible attacks:

a. ***Deliberate*** attacks are caused by people (e.g., terrorists, other criminals, hackers, delinquents, employees, etc.).

b. ***Natural*** attacks are caused by nature (e.g., hurricanes, tornadoes, earthquakes, floods, wildfires, etc.).

c. ***Accidental*** attacks are caused by HazMat accidents involving nuclear, biological, or chemical substances.

3. These attacks are serious "threats" against critical infrastructures.

B. Objectives

1. To protect the people, physical entities, and cyber systems that are indispensably necessary for survivability, continuity of operations, and mission success.

2. To deter or mitigate attacks on critical infrastructures by people (e.g., terrorists, hackers, etc.), by nature (e.g., hurricanes, tornadoes, etc.), and by HazMat accidents.

C. Philosophy

1. Among all the important procedures or things involved in emergency preparedness, CIP is possibly the most essential component.

2. There will probably never be enough resources (i.e., dollars, personnel, time, and materials) to achieve total emergency preparedness.

3. Senior fire and EMS leaders must make tough decisions about what department assets really need protection by the application of scarce resources.

4. There should be no tolerance for waste and misguided spending in the business of emergency preparedness and infrastructure protection.

5. From a municipal perspective, the CIP philosophy is to first protect those infrastructures absolutely required for citizen survivability and continuity of crucial community operations.

6. For the community emergency services, the corresponding CIP philosophy is to first protect those infrastructures absolutely required for the survivability of emergency first responders and the success of their missions.

7. It is impossible to prevent all attacks (e.g., terrorism, natural disasters) against critical infrastructures.

8. CIP can reduce the chances of some future attacks, make it more difficult for the attacks to succeed or degrade infrastructures, and mitigate the outcomes when they do occur.

9. Activities to protect assets essential for the accomplishment of missions affecting life and property are proactive, preemptive, and deterrent in nature, which is exactly what critical infrastructure protection is meant to be.

D. Psychology

1. CIP can be a tool to produce an American "mindset" of protection awareness and confidence in our nation's security and prosperity. Given these new thoughts, it may evoke behaviors that are fully supportive and cooperative with necessary protective measures.

2. CIP may also be a means to change the behavior of terrorists. The proper protection of American critical infrastructures has the potential to develop a new "mindset" among terrorists that their actions will be futile and not yield the results they seek.

3. Community leaders and department chiefs should make occasional public announcements that their critical infrastructures are being protected. This must be done without divulging any details that would be useful to adversaries. Such announcements are not intended to be a ruse or disinformation campaign, but an honest declaration for the "psychological" benefit of both friends and foes.

E. CIP Process Preface

1. CIP involves the application of a systematic analytical process fully integrated into all fire and EMS department plans and operations.

2. It is a security related, time efficient, and resource-restrained practice intended to be repeatedly used by department leaders.

3. The CIP process can make a difference only if applied by department leaders, and periodically reapplied when there have been changes in physical entities, cyber systems, or the general environment.

4. It consists of the following five steps:

a. ***Identifying critical infrastructures*** essential for the accomplishment of sector missions (e.g., fire suppression, EMS, HazMat, search and rescue, and extrication).

b. ***Determining the threat*** against those infrastructures.

c. ***Analyzing the vulnerabilities*** of threatened infrastructures.

d. ***Assessing risk*** of the degradation or loss of a critical infrastructure.

e. ***Applying countermeasures*** where risk is unacceptable.

III. CIP Process Methodology

A. Identifying Critical Infrastructures

1. Identifying critical infrastructures is the first step of the CIP process.

2. The remaining steps of the CIP process cannot be initiated without the accurate identification of a department's critical assets.

3. Critical infrastructures are those physical and cyber assets essential for the accomplishment of missions affecting life and property.

4. They are the people, things, or systems that will seriously degrade or prevent survivability and mission success if not intact and operational.

5. The following are some examples of critical infrastructures:

a. Firefighters and EMS personnel.

b. Fire and EMS stations, apparatus, and communications.

c. Public Safety Answering Points (or 9-1-1 Centers).

d. Computer-aided dispatch and computer networks.

e. Pumping stations and water reservoirs for major urban areas.

f. Major roads and highways serving large population areas.

g. Bridges and tunnels serving large population areas.

h. Regional or local medical facilities.

6. Despite many similarities, the differences in physical and cyber systems among individual departments necessitate that senior leaders identify their own critical infrastructures.

7. Remember that protection measures cannot be implemented if what needs protection is unknown!

8. The Fire Department of New York continued to serve the citizens of New York City following the collapse of the World Trade Center towers. However, their ability to do so was tremendously degraded for a period of time given the unprecedented losses of personnel and equipment—the foremost among critical infrastructures.

B. Determining the Threat

1. Determining the threat against identified critical infrastructures is the second step of the CIP process.

2. A threat is the potential for an attack from people, nature, HazMat accident, or a combination of these.

3. The remaining steps of the CIP process depend upon whether or not a department's critical infrastructures are threatened.

4. A determination of credible threat must be made for each critical infrastructure identified in step one.

5. If there is no threat of an attack against one of a department's critical infrastructures, then the CIP process can stop here for that particular asset.

6. If there is only a low threat against one of a department's critical infrastructures (e.g., an earthquake), then leaders can choose to continue the CIP process or stop it here for that particular infrastructure.

7. When there is a credible threat of an attack against a department's critical infrastructures, then it is necessary to determine the following prior to proceeding to the next step of the CIP process:

   a. Exactly which critical infrastructures are threatened?

   b. By whom or what is each of these infrastructures threatened?

8. Two examples of credible threats against critical infrastructures:

   a. "National intelligence assets warn that suspected terrorists may attempt to steal fire trucks or ambulances."

   b. "Police cite increasing incidents of juvenile delinquents breaking into water pumping stations and tampering with equipment."

9. Leaders should concentrate only on those threats that will dangerously degrade or prevent survivability and mission accomplishment.

10. Resources should be applied to protect only those infrastructures for which a credible threat exists!

C. Analyzing the Vulnerabilities

1. Analyzing the vulnerabilities of credibly threatened infrastructures is the third step of the CIP process.

2. This step requires an examination of the security vulnerabilities (or weaknesses) in each of the threatened infrastructures.

3. A vulnerability is a weakness in a critical infrastructure that renders the infrastructure susceptible to degradation or destruction.

4. There are two types of vulnerabilities to consider in the CIP process:

a. A weakness in a critical infrastructure that renders the infrastructure susceptible to disruption or loss from a deliberate attack by human adversaries.

b. A weakness in a critical infrastructure that will further weaken or completely deteriorate as a result of a natural or accidental attack (i.e., natural disaster or HazMat accident).

5. An efficient vulnerability analysis will examine each credibly threatened infrastructure from the "threat point of view."

6. The analysis will seek to understand the ways by which threats from adversaries, nature, or HazMat accidents might disrupt or destroy the examined infrastructure.

7. If a threatened infrastructure has no vulnerabilities, then the CIP process can stop here for that particular infrastructure.

8. The CIP process should proceed to the fourth step only for those threatened infrastructures having vulnerabilities.

9. The following are two examples of vulnerabilities:

a. Public Safety Answering Points (PSAPs or 9-1-1 Communication Centers) because of their physical locations, power sources, line routing, Internet-based controls of switching, etc.

b. Computer Aided Dispatch (CAD) because of its network connections with Internet connectivity.

10. The protection of threatened and vulnerable infrastructures cannot be accomplished without knowing what or where the vulnerabilities are!

D. Assessing Risk

1. Assessing risk of the degradation or loss of a critical infrastructure is the fourth step of the CIP process.

2. The following priority guidance applies for this assessment:

a. Threatened and vulnerable infrastructures are a high priority for the application of countermeasures.

b. Infrastructures that are either threatened or vulnerable, but not both, are a low priority for protective measures.

3. Focusing on each high priority infrastructure, decision makers must evaluate the cost of countermeasures in terms of available resources (e.g., personnel, time, money, materials).

4. The determined costs of protective measures (doing something) for each high priority infrastructure are now weighed against the impact of the degradation or loss of that infrastructure (doing nothing).

5. Risk is unacceptable if the impact of the degradation or loss of an infrastructure (doing nothing) is considered catastrophic. The CIP process, therefore, must proceed to the final step for the immediate application of countermeasures.

6. If the impact of the degradation or loss of an infrastructure is not considered great, then decision makers can temporarily decide to accept risk until resources become available.

7. For the infrastructures that are risk adverse and require protection, community leaders should decide the order in which they will receive the allocation of resources and application of countermeasures.

8. For example, research reveals that water pumping stations in rural America are notoriously unprotected. If department leaders follow the CIP process and determine the community pumping station to be a high priority infrastructure, then they should not accept risk and seek local government assistance to apply countermeasures as soon as possible.

9. Failure to assess risk can result in the inefficient application of resources and a subsequent reduction in operational effectiveness!

E. Applying Countermeasures

1. Applying countermeasures where risk is unacceptable is the fifth step of the CIP process.

2. Countermeasures are any protective actions that reduce or prevent the degradation or loss of a critical infrastructure to an identified threat.

3. Countermeasures protect infrastructures and preserve the ability of emergency first responders to efficiently perform their services.

4. They are measures of protection applied to high priority infrastructures that necessitate the allocation of resources.

5. Possible countermeasures differ in terms of feasibility, expense, and effectiveness.

6. Countermeasures can be simple or complex actions limited only by imagination and creativity.

7. In few instances, there may be no effective means to protect a critical infrastructure. Sometimes, prohibitive costs or other factors make the application of countermeasures impossible.

8. Decisions requiring the application of countermeasures will influence personnel, time, and material resources as well as drive the security budget.

9. The following are two examples of countermeasures:

a. To protect their personnel infrastructure, all FDNY digital radios will be inexpensively reprogrammed so that one channel will override all others and emit a long tone to warn each firefighter to immediately evacuate a building.

b. To protect both their personnel and equipment, a growing number of departments are keeping their apparatus bay doors closed at all times.

10. High priority infrastructures should be considered a loss to plans and operations if not protected by countermeasures!

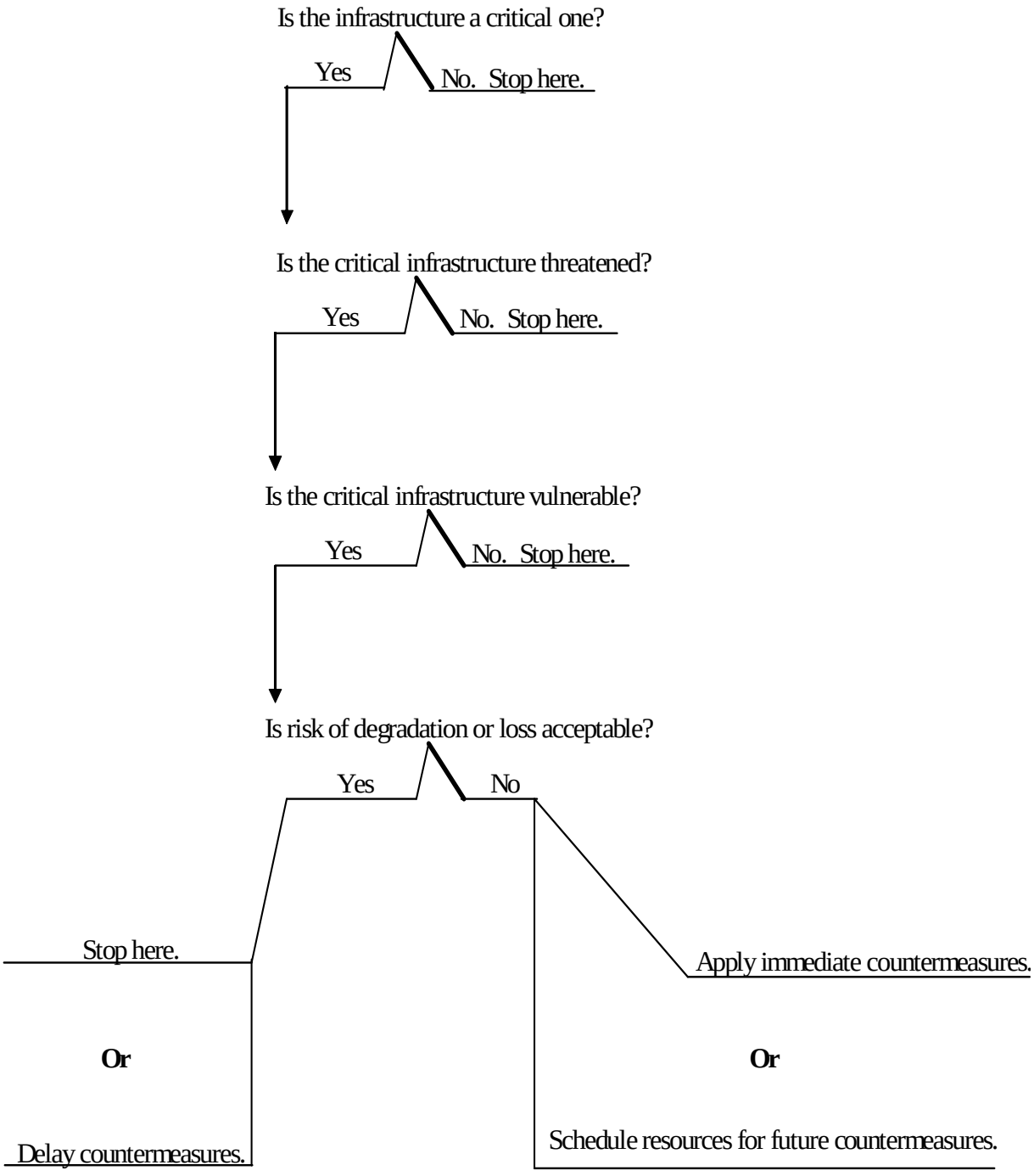
IV. CIP Process Question Navigator

DIRECTIONS: Answer questions for each infrastructure.

- Is the person, thing, or system part of the organization's infrastructure?
- If the answer is **NO**, stop here; but if it is **YES**, then:
- Is this infrastructure essential for survivability and mission success?
- If the answer is **NO**, stop here; but if it is **YES**, then:
- Is there potential for a deliberate, natural, or accidental attack against this critical infrastructure?
- If the answer is **NO**, stop here; but if it is **YES**, then:
- Is the threat of an attack against this critical infrastructure a truly credible one?
- If the answer is **NO**, stop here; but if it is **YES**, then:
- Is there a security vulnerability (or weakness) in the threatened critical infrastructure?
- If the answer is **NO**, stop here; but if it is **YES**, then:
- Does this vulnerability (or weakness) render the critical infrastructure susceptible to disruption or loss?
- If the answer is **NO**, stop here; but if it is **YES**, then:
- Is it acceptable to assume risk and delay the allocation of resources and the application of countermeasures?
- If the answer is **YES**, stop here; but if it is ***NO***, then:
- Apply countermeasures to protect this critical infrastructure as soon as available resources permit.

V. Infrastructure Protection Decision Matrix

DIRECTIONS: Complete the matrix for each infrastructure.



VI. Establishing a CIP Program

A. Justification

1. A quality CIP program supports the protection of the people, physical entities, and cyber systems upon which survivability, continuity of operations, and mission accomplishment depend.

2. The terrorist attacks of 11 September 2001 should provide all senior leaders with sufficient justification to immediately implement a critical infrastructure protection (CIP) program within their organizations.

3. If the threat of terrorism itself does not motivate action, then remember that the CIP process also mitigates or eliminates the devastation of critical assets caused by nature and HazMat accidents.

B. Program Manager

1. Critical infrastructure protection is primarily leader business. The department chief, commander, or director appoints a program manager from among the senior leadership of the organization.

2. The program manager administers the CIP program and maintains its value, relevance, and currency.

3. The program manager prepares, obtains approval for, and publishes the program's purpose, strategic goals, and immediate objectives.

4. The program manager proactively initiates actions that protect the organization's critical infrastructures from deliberate, natural, or accidental attacks.

C. Program Development and Management

1. The department chief, commander, or director institutes the organization's CIP program and delegates authority to a manager.

2. The following program development and management steps are recommended:

a. Select the program manager from among the senior decision-makers of the organization.

b. Firmly establish the relationship between the organization's mission and the purpose for critical infrastructure protection.

c. Win support of the department senior and junior leadership, and orient the CIP program to them.

d. Focus the program on the practice of the CIP process.

e. After determining which critical infrastructures must receive immediate protection, aggressively seek the resources required to apply countermeasures as soon as possible.

f. Revise and reissue the department security policy to include the CIP Program and the critical infrastructures that demand countermeasures.

g. Brief all department personnel regarding the revised policy and ensure awareness of actions they can take to bolster applied protective measures.

h. Practice operations security (protecting sensitive information) concurrently with CIP.

i. Remain vigilant for threat advisories and new CIP trends, methods, and conditions.

j. Maintain the program by reapplying the CIP process when there have been changes in the physical entities, cyber systems, or the general environment; however, attempt to do so at least semi-annually.

3. The USFA CIPIC will provide assistance (via telephone, electronic mail, or facsimile) to any organization establishing a CIP program. Contact the CIPIC by telephone at 301-447-1325, or by electronic mail at: usfacipc@fema.gov. If interested, visit the CIPIC website at: www.usfa.fema.gov/cipc.