Student Guide

Course: Information Security Emergency Planning

Introduction

In the years following the 9/11 attacks there has been a dramatic effort across the security community to re-prioritize our national preparedness. Historically, emergency plans were only deployed when a disaster occurred. Based on recent natural disasters and world events, organizations must now adopt a proactive mindset continually reassessing, refining and adjusting their emergency plans.

Emergency planning is a fundamental principle that must be recognized if installations are to accomplish their mission. No longer can we afford to be complacent and wait to react to an emergency, the cost of non-compliance is too high.

In this course we will examine emergency planning and the need to be ready to respond in the event of a disaster as it relates to information security and classified information. We will look at each step of the process from anticipating threats, prioritizing, and planning considerations for our classified information to ultimately being ready to meet a need when the time comes.

Course Objectives

By the end of this course you will be able to:

- Demonstrate an understanding of DoD policies and how they relate to safeguarding classified information
- Recognize how military operations affect provisions of DoD Manual 5200.01, Volume1, Enclosure 3
- Identify types of threats and their impact on information security
- List factors to be considered when planning for emergency handling of classified information
- Apply the planning process in the development of emergency plans.

DoD Manual

The DoD Information Security Program Manual (DoDM 5200.01) Volumes 1 and 3 defines the basic requirements for safeguarding classified information and includes guidance for protecting classified information during military operations and other emergencies to minimize the risk of its compromise.

The provisions for classified information within DoDM 5200.01, Volume 1, Enclosure 3 pertaining to accountability, dissemination, transmission and storage of classified information and material may be modified by military commanders as necessary to meet local conditions encountered during military operations.
Military operations include:

- Combat
- Peacekeeping Operations
- NOT routine Military deployments or exercises

Emergency Planning Steps

There are four steps to developing an information security emergency plan:
Step 1 is to identify the threats.
Step 2 is to assess the risks.
Step 3 is to determine possible protection strategies.
Step 4 is to develop the emergency plan.

Step 1 – Identify Threats

The first step in developing the emergency plan is to conduct an evaluation and assessment of the potential threats. To minimize the risk of compromise, plans must be developed for the protection, removal or destruction of classified material in case of physical, environmental or human threats to national security information. These threats include fire, natural disasters, civil disturbances, terrorist activities and enemy actions.

Fire

Fire is one of the most common physical threats that your installation may encounter and must be addressed during emergency planning. First, you must identify what kind of fire prevention and protection program your command or installation currently has in place.

The following questions can help in the evaluation process:

- Should Continental United States (CONUS) plans differ from Outside the Continental United States (OCONUS)?
- Are there procedures in place for emergency entrance into the spaces that store classified material?
- Are there procedures in place for after the emergency?
- Should you take time to secure classified information before evacuating?
- What should you do about emergency response personnel who may have come into contact with classified information?
    - Do you require emergency response personnel to complete a non-disclosure agreement?

Answers to all these questions will depend on whether the fire is imminent, the type of classified information that must be secured and several other factors that would require planning on a case by case basis.

Natural Disasters

Natural disasters, such as earthquakes, hurricanes, floods, tornados, tsunamis and volcanoes are environmental threats that must be taken into consideration when developing emergency plans. Even though the behavior of weather-related emergencies may be somewhat predictable, they can still be terribly devastating to National Security.

DoD has been impacted by several natural disasters that have affected not only the facility itself, but have caused operations to cease altogether.
Some notable examples are:

- The 1991 eruption of Mt. Pinatubo in the Philippines, which forced the U.S. to evacuate Clark Air Force Base (AFB).
- Hurricane Andrew (1992), which caused tremendous damage to Florida's Homestead AFB. Entire buildings were blown apart, scattering their contents throughout the area, including sensitive and classified documentation.

Preparedness is the key to effectively dealing with natural disasters. Advance planning and practicing the implementation of your emergency plan will allow for a smooth transition during an emergency.

Civil Disturbances

Civil disturbances must also be perceived as a possible human threat when developing emergency plans. Civil disturbances most often arise from political grievances, urban economic conflicts, community unrest, terrorist acts, or foreign influences.

Commonly targeted locations are nuclear weapons facilities, power plants, and U.S. government facilities such as recruiting offices, federally-leased buildings, ROTC buildings, and federal courthouses.

Civil disturbances can range from peaceful picketing to full-blown riot situations. Some of the most notable civil disturbances in recent U. S. history are:

- The 1968 Democratic National Convention which was held in Chicago during a year of violence, political turbulence, and civil unrest, with riots in more than 100 cities following the assassination of Martin Luther King, Jr. and Senator Robert F. Kennedy.
- The Kent State shootings in Ohio in May of 1970, protesting the American involvement in Cambodia.
- In 2005, during the aftermath of Hurricane Katrina; looting, violence and other criminal activity became serious problems.

Whatever forms a civil disturbance takes; it can impact your operations.

Maintaining current, valid information is vital in the development of the emergency plan. The following questions can help you in collecting the necessary data:

- Who are the demonstrators?
- When and where will they demonstrate?
- What are their capabilities and possible courses of action?

Again, preparedness is the key to continuing the mission of your organization.

Terrorist Activities

Since 9/11 terrorist activities has become a main focus of emergency planning considerations. DoD has been impacted by terrorist activities not only overseas but also stateside. Some of the most significant examples of terrorist attacks against the U.S. include:

- The terrorist bombing of a military barracks in Beirut, Lebanon resulting in the deaths of 241 U.S. Marines on October 23, 1983.
- In October 1993 terrorist attacks on U.S. forces in Mogadishu, Somalia resulted in the wounding of 73 service members and 18 fatalities.
- The terrorist bombing at Khobar Towers, Saudi Arabia which resulted in the wounding of hundreds of service members and 19 U.S fatalities in June of 1996.
- The terrorist suicide bombing of the USS Cole, at Aden, Yemen, which resulted in the deaths of 17 U.S. sailors and another 39 wounded in October 2000, and
- The attack on the Pentagon, which resulted in the deaths of 184 U.S. military, government and civilian workers on September 11, 2001.

A well-defined emergency plan can help to mitigate the possible impacts of future terrorist attacks.

Enemy Actions

Enemy action is the last type of human threat we will examine. Hostile actions can come in many forms.

One interesting example involves the Iran Hostage Crisis on November 4, 1979. On this date, the U.S. Embassy in Tehran, Iran was overtaken by a mob of Iranian students resulting in 66 individuals being taken captive. Although the Iranian Government denied any involvement, they applauded the event. During the crisis, the revolutionaries produced secret documents that were taken from the embassy; some of them were painstakingly reconstructed after shredding.

Now that you are aware of the types of threats that warrant emergency planning, let’s try a practice activity.

Knowledge Check

Can you identify the possible threat as indicated in the photos?

Step 2 – Assess Risks

Once you have identified the potential threats, the next step is to evaluate their respective levels of risk.

The results of the risk assessment for each of the identified threats will determine the appropriate level of detail that is necessary in the emergency plan and the amount of testing and rehearsal required to minimize the possibility of compromise to the classified information.

The DoD Information Security Program Manual (DoDM 5200.01), Volumes 1 and 3 provides guidance with respect to accountability, dissemination, transmission and storage of classified information.

For detailed information on the DoD Risk Management process, CDSE offers 2 courses, Introduction to Risk Management and Risk Management for DoD Security Programs. Access the STEPP website to register for these courses.

DoDM 5200.01

Per DoDM 5200.01, Volume1, Enclosure 3, "Classified information should only be introduced into combat areas, zones, or areas of potential hostile activity when it is necessary to accomplish the military's missions".

Some military planning and operations documents may be classified, but are essential to battlefield operations. Before introducing any classified information into combat areas, a risk evaluation must be completed.

COMSEC

Planning for emergency protection (including emergency destruction under no-notice conditions) of classified Communications Security (COMSEC) material shall be developed in accordance with requirements of the Committee on National Security Systems/NSA Instruction 4004.1 *Destruction and Emergency Protection*

Procedures for COMSEC and Classified Materials with amended ANNEX B, Dated January 9, 2008; (August 2006).

Planning should emphasize maintaining security control over the material without endangering life until order is restored. Hold only the minimum amount of COMSEC material at any time; conduct routine destruction frequently and dispose of excess COMSEC material according to regulations.

Because of the importance of our codes, the COMSEC program mandates that emergency procedures must be documented and tested on a regular basis.

Knowledge Check

Choose the best answer.

1. Your installation is located in a remote forested area. Temperatures have been 15 degrees above normal and the area has suffered severely from a lack of rainfall. What is the most likely threat?

    a. Terrorist Attack
    b. Natural Disaster
    c. Fire
    d. Civil Disturbance
    e. Enemy Action

2. You are located in a federally-leased building in a large metropolitan area. People Protesters have been gathering daily in increasingly large numbers nearby in recent weeks to voice their displeasure about the government's latest domestic economic policies. Some of these protesters have attempted to physically block employees from entering the building. What is the most likely threat?

    a. Terrorist Attack
    b. Natural Disaster
    c. Fire
    d. Civil Disturbance
    e. Enemy Action

3. You are located at an Air Force test and evaluation facility in an isolated area of California where a major fault line runs underneath your facility. What would be the most likely threat?

    a. Terrorist Attack
    b. **Natural Disaster**
    c. Fire
    d. Civil Disturbance
    e. Enemy Action

Step 3 – Determine Protection Strategies

After you have evaluated the potential risk to your classified holdings you must then address possible protection strategies. These strategies may include:

- Protection of the classified information in place

- Removal or evacuation of the classified information, or
- Emergency destruction of the classified information.

Each of these options requires careful consideration and coordination throughout your activity.

Protection from flooding may warrant a different emergency response than protection from civil disturbance. Considerations include:

- Capability of security countermeasures in order to secure in place
- Fire and water protection for safeguarding in place
- Transportation requirements for removal and evacuation
- Alternate safeguarding site for evacuation and removal, and
- Adequate high speed destruction equipment capable of destroying the volume of classified information within a short period of time.

Most Emergency Plans will incorporate at least two if not all three protection strategies based upon the specific threat being addressed.

Knowledge Check

Choose the correct answer.

1. What would be the best protection strategy for classified information if your facility is located near an urban area that is routinely subjected to flooding in the spring?
   a. Removal
   b. Destruction
   c. Protection in Place

2. Your facility is located near a federal courthouse that frequently hands down controversial decisions, leading to large scale protests by citizens and arrests by local law enforcement. What is the best protection strategy for the classified information at your facility?
   a. Removal
   b. Destruction
   c. Protection in Place

3. Your facility is located deep in the heart of a foreign city where car-bombings and suicide bombings occur weekly. The majority of your classified holdings consist of COMSEC material. What is the best protection strategy for the classified information at your facility?
   a. Removal
   b. Destruction
   c. Protection in Place

Step 4 – Developing the Emergency Plan

When preparing emergency plans, consideration should be given to:

- Reducing the amount of classified material on hand.
  This can be achieved through the permanent transfer of the classified information, movement of eligible classified material to archive systems, or destruction of obsolete, surplus, extraneous or unnecessary classified information, at the discretion of the installation's commander.

- Storing less-frequently-used classified material at a more secure location by utilizing an off-site secure storage facility.
  Frequently, organizations can store classified material at other locations, or enter into an agreement with another DoD entity to provide off-site storage. Be sure to create regular back-up copies of information in electronic formats for off-site storage.
- Transferring classified information; these include high density formats; to microforms or to removable automated information systems (AIS) media to reduce the bulk. AIS include magnetic or digital media such as tapes, databases, and DVD's.

The level of risk is in direct proportion to the level of detail that must be included in your emergency plan. If you possess extremely sensitive classified materials, you are located close to hostile or potentially hostile countries, you have a limited ability to defend, you conduct sensitive operations or the potential for hostile action is great – then you need to ensure that your emergency plan is well thought-out, detailed, and rehearsed regularly.

As you develop your emergency plan, you must keep in mind two important factors:

- First, we cannot place our people in jeopardy. Remember, there is a mandate that states the Commander or Supervisor must maintain a safe working environment.
- Second, the primary objective of any plan is to prevent unauthorized disclosure of classified information in an emergency situation.

Emergency Plan Recommendations

The following recommendations will assist in the development of the plan.

- Make your plan as simple as possible, but ensure that you have accounted for all possible threats and the associated risks. Be sure to coordinate the plan throughout your activity to ensure accuracy of all concerned facilities, services and personnel.
- Develop a checklist of actions to be taken. Ensure that all personnel involved understand their role. You may want to create index cards with each person's roles and responsibilities in the event of an emergency.
- Identify emergency destruction priorities if it is a requirement of your activity. The current DoDM 5200.01, Volume 3 prohibits the external marking of classified storage containers revealing the level of classified information or the evacuation destruction priority. This does not include applying decals or stickers the DNI requires for containers and equipment used to store or process intelligence information. Be sure to detail the destruction priorities in your plan.
- Schedule periodic practices to ensure that the emergency plan is working and to reinforce roles and responsibilities. During the "staged" emergencies, be sure to make any modifications and adjustments to your emergency plan as situations warrant.

Remember, emergency plan rehearsal must stop at a certain point….!

Summary

Now that you have completed this course, you should be able to:

- Demonstrate an understanding of DoD policies and how they relate to safeguarding classified information
- Recognize how military operations affect provisions of DoD Manual 5200.01, Volume1, Enclosure 3
- Identify types of threats and their impact on information security
- List factors to be considered when planning for emergency handling of classified information
- Apply the planning process in the development of emergency plans.

What is your next step?

Currently DoD does not provide a lot of guidance on emergency planning. The guidance we do have makes it clear that we must develop emergency plans for a variety of threats. The level of detail of the plan is dependent upon your local threats, the level of assessed risks and other circumstances. Keep your plan as simple as possible and thoroughly coordinate your plan throughout your organization. As with any plan you must continually test it and be sure to utilize the results of the testing to identify problems and make the necessary adjustments to improve your plan.

Following the guidance provided by this course will help your activity develop a comprehensive and practical emergency plan that adequately protects classified information and ultimately our national security.

In the attachments tab on the top right of the screen is a copy of the FEMA Comprehensive Preparedness Guide (CPG101), which provides general guidelines on developing emergency operations plans and can be used as a reference. Please take careful note however, that your emergency plan MUST be developed according to your agency's needs and MUST provide the necessary level of detail for your installation.

For questions pertaining to this course, please contact DSS Information Security via email at dss.informationsecuritytraining@mail.mil.