DOWNLOAD PDF ASSESSMENTS FOR INFRASTRUCTURE PROTECTION

Chapter 1 : Critical Infrastructure Protection Unit

Critical infrastructure vulnerability assessments are the foundation of the National Infrastructure Protection Plan's risk-based implementation of protective programs designed to prevent, deter, and mitigate the risk of a terrorist attack while enabling timely, efficient response and restoration in an all-hazards post-event situation.

CIP[edit] The U. CIP is a national program to ensure the security of vulnerable and interconnected infrastructures of the United States. Take, for example, a computer virus that disrupts the distribution of natural gas across a region. This could lead to a consequential reduction in electrical power generation , which in turn leads to the forced shutdown of computerized controls and communications. Road traffic, air traffic, and rail transportation might then become affected. Emergency services might also be hampered. An entire region can become debilitated because some critical elements in the infrastructure become disabled through natural disaster. The federal government has developed a standardized description of critical infrastructure, in order to facilitate monitoring and preparation for disabling events. The government requires private industry in each critical economic sector to: Assess its vulnerabilities to both physical or cyber attacks Plan to eliminate significant vulnerabilities Develop systems to identify and prevent attempted attacks Alert, contain and rebuff attacks and then, with the Federal Emergency Management Agency FEMA , to rebuild essential capabilities in the aftermath Infrastructure sectors[edit] CIP defines sectors and organizational responsibilities in a standard way: Note that CIP in this sector is different from energy security , which is the politics and economics of supply. Additionally, operating under the auspices of the Federal Energy Regulatory Commission is the North American Electric Reliability Corporation NERC , a non-profit organization that defines and enforces reliability standards for the bulk power system. Search and rescue teams formed from various emergency services coordinated by FEMA Federal and municipal services: They guarantee continuity of government at the federal, state, and local levels to meet for provision of essential services. This includes safe water systems and drainage. In the remit was expanded to include: Agriculture and food, with the Department of Agriculture overseeing the safe supply of meat, poultry, and egg products. National monuments and icons, under the Department of the Interior With much of the critical infrastructure privately owned, the Department of Defense DoD depends on commercial infrastructure to support its normal operations. The Department of State and the Central Intelligence Agency are also involved in intelligence analysis with friendly countries. It is going to be against commercial infrastructure". Later this fear was qualified by President Clinton after reports of actual cyber terrorist attacks in We lost our Pacific fleet at Pearl Harbor. In the past, the systems and networks of the infrastructure elements were physically and logically independent and separate. They had little interaction or connection with each other or other sectors of the infrastructure. With advances in technology, the systems within each sector became automated, and interlinked through computers and communications facilities. As a result, the flow of electricity, oil, gas, and telecommunications throughout the country are linkedâ€”albeit sometimes indirectlyâ€”but the resulting linkages blur traditional security borders. While this increased reliance on interlinked capabilities helps make the economy and nation more efficient and perhaps stronger, it also makes the country more vulnerable to disruption and attack. This interdependent and interrelated infrastructure is more vulnerable to physical and cyber disruptions because it has become a complex system with single points of failure. In the past an incident that would have been an isolated failure can now cause widespread disruption because of cascading effects. One catastrophic failure in this sector now has the potential to bring down multiple systems including air traffic control, emergency services, banking, trains, electrical power, and dam control. The elements of the infrastructure themselves are also considered possible targets of terrorism. Traditionally, critical infrastructure elements have been lucrative targets for anyone wanting to attack another country. Now, because the infrastructure has become a national lifeline, terrorists can achieve high economic and political value by attacking elements of it. Disrupting or even disabling the infrastructure may reduce the ability to defend the nation, erode public confidence in critical services, and reduce economic strength. Additionally, well chosen terrorist attacks can become easier and less costly than traditional warfare because of the interdependence of infrastructure elements. These infrastructure elements can become easier targets where there is a low probability of detection. The elements of the infrastructure are also increasingly vulnerable to a dangerous mix of traditional and nontraditional types of threats. Traditional and non-traditional threats include equipment failures, human error, weather and natural causes, physical attacks, and cyber attacks. For each of these threats, the cascading effect caused by single points of failure has the potential to pose dire and far-reaching consequences. Challenges[edit] There are fears that the frequency and severity of critical infrastructure incidents will increase in the future. One reason for this is that a good understanding of the inter-relationships does not exist. There is also no consensus on how the elements of the infrastructure mesh together, or how each element functions and affects the others. Securing national infrastructure depends on understanding the relationships among its elements. Thus when one sector scheduled a three-week drill to mimic the effects of a pandemic flu , even though two-thirds of the participants claimed to have business continuity plans in place, barely half reported that their plan was moderately effective. CIP is important because it is the link between risk management and infrastructure assurance. It provides the capability needed to eliminate potential vulnerabilities in the critical infrastructure. CIP practitioners determine vulnerabilities and analyze alternatives in order to prepare for incidents. They focus on improving the capability to detect and warn of impending attacks on, and system failures within, the critical elements of the national infrastructure. Organization and structure[edit] PDD mandated the formation of a national structure for critical infrastructure protection. The different entities of the national CIP structure work together as a partnership between the government and the public sectors. In addition, there are grants made available through the Department of Homeland Security for municipal and private entities to use for CIP and security purposes. These include grants for emergency management, water security training, rail, transit and port security, metropolitan medical response, LEA terrorism prevention programs and the Urban Areas Security Initiative. These are national defense, foreign affairs, intelligence, and law enforcement. Each lead agency for these special functions appoints a senior official to serve as a functional coordinator for the federal government. A private sector counterpart, a Sector Coordinator, was also identified. Together, the two sector representatives, one federal government and one corporate, were responsible for developing a sector NIAP. Additionally the national structure must ensure there is a national CIP program. This program includes responsibilities such as education and awareness, threat assessment and investigation, and research. The process includes assessments of: Protection - Can be defined as the state of being defended, safeguarded, or shielded from injury, loss, or destruction from natural or unnatural forces. Vulnerability â€” The quality of being susceptible to attack or injury, warranted or unwarranted, by accident or by design. Risk â€” The possibility or likelihood of being attacked or injured. Mitigation â€” The ability to alleviate, reduce, or moderate a vulnerability, thus reducing or eliminating risk. Controversy[edit] There have been public criticisms of the mechanisms and implementation of some security initiatives and grants, with claims they are being led by the same companies who can benefit, [12] and that they are encouraging an unnecessary culture of fear. Commentators note that these initiatives started directly after the collapse of the Cold War , raising the concern that this was simply a diversion of the military-industrial complex away from a funding area which was shrinking and into a richer previously civilian arena. Grants have been distributed across the different states even though the perceived risk is not evenly spread, leading to accusations of pork barrel politics that directs money and jobs towards marginal voting areas. The Urban Areas Security Initiative grant program has been particularly controversial, with the infrastructure list covering 77, assets, including a popcorn factory and a hot dog stand. An absence of comparative risk analysis and benefits tracking it has made it difficult to counter such allegations with authority. In order to better understand this, and ultimately direct effort more productively, a Risk Management and Analysis Office was recently created in the National Protection and Programs directorate at the Department of Homeland Security. But as part of the CIP program, DoD has responsibilities that traverse both the national and department-wide critical infrastructure. PDD identified the responsibilities DoD had for critical infrastructure protection. First, DoD had to identify its own critical assets and infrastructures and provide assurance through analysis, assessment, and remediation. DoD was also responsible for identifying and monitoring the national and international infrastructure requirements of industry and other government agencies, all of which needed to be included in the protection planning. DoD also addressed the assurance and protection of commercial assets and infrastructure services in DoD acquisitions. Other DoD responsibilities for CIP included assessing the potential impact on military operations that would result from the loss or compromise of infrastructure service. There were also requirements for monitoring DoD operations, detecting and responding to infrastructure incidents, and providing department indications and warnings as part of the national process. Ultimately, DoD was responsible for supporting national critical infrastructure protection. In response to the requirements identified in PDD, DoD categorized its own critical assets by sector, in a manner similar to the national CIP organization. The DoD identified a slightly different list of infrastructure sectors for those areas that specifically required protection by DoD. DoD sectors[edit] There are ten defense critical infrastructure sectors that are protected by the DoD. Financial Services - Defense financial services support activities related to officially appropriated funds. These activities include the disbursement of cash, receipt of funds, and acceptance of deposits for credit to officially designated Treasury general accounts. This sector also provides financial services to individuals and on-base organizations, including deposits, account maintenance, and safekeeping. These include surface, sea, and lift assets; supporting infrastructure; personnel; and related systems. Public Works - Public works includes four distinct physical infrastructure sectors: This defense infrastructure sector is composed of networks and systems, principally for the distribution of the associated commodities. The Corps of Engineers is responsible for coordinating the assurance activities of the public works infrastructure sector. The GIG is the globally interconnected set of personnel, information, and communication capabilities necessary to achieve information superiority. C2 includes assets, facilities, networks, and systems that support mission accomplishment. Intelligence Surveillance, and Reconnaissance, or ISR - The Defense Intelligence, Surveillance and Reconnaissance infrastructure sector is composed of facilities, networks, and systems that support ISR activities such as intelligence production and fusion centers. The Defense Intelligence Agency , or DIA, is responsible for coordinating the assurance activities of this infrastructure sector. Health Affairs - The health care infrastructure consists of facilities and sites worldwide. Some are located at DoD installations; however, DoD also manages a larger system of non-DoD care facilities within its health care network. These health care facilities are linked by information systems. Personnel - The defense personnel infrastructure sector includes a large number of assets hosted on component sites, a network of facilities, and information systems linking those sites and facilities. In addition to being responsible for its own assets, the personnel infrastructure sector also coordinates commercial services that support the personnel function. These services include recruitment, record keeping, and training. The Defense Human Resources Activity is the designated lead component for the Defense Personnel infrastructure sector. Space - The defense space infrastructure sector is composed of both space- and ground-based assets including launch, specialized logistics, and control systems.

Chapter 2 : Critical infrastructure protection - Wikipedia

for the Office of Infrastructure Protection and the Office of Cyber Infrastructure and Analysis to develop andsubmit a three-year strategic plan to guide vulnerability assessments, analytic assessments, and the Regional Resiliency.

Chapter 3 : Law Enforcement Critical Infrastructure Protection

Critical Infrastructure Protection Assessments. Cabezon's assessment team consists of nationally recognized substantive experts on Critical Infrastructure-Key Resource (CIKR) Protection for the majority of the DHS Critical Sectors.

Chapter 4 : Critical Infrastructure Protection Assessments | Cabezon Group Inc.

These assessments help critical infrastructure owners and operators take actions to improve security and mitigate risks. Six private sector representatives told GAO that threat information is the most useful type of risk information because it allows owners and operators to react immediately to improve their security posture.

Chapter 5 : House Committee on Homeland Security

and Infrastructure Protection (IA/IP) Directorate. In particular, the IA/IP Directorate is to integrate threat assessments with vulnerability assessments in an effort to.