

1. The value proposition for participating as a security partner within the NIPP framework refers to:
 - A. The funding provided by the Federal Government to local jurisdictions road improvements.
 - B. The expertise within the Government for protecting the country's infrastructure against terrorist attacks.
 - C. The research and development initiatives being conducted by the academic community to enhance infrastructure protection technology
 - D. The benefits gained by the public-private partnership.

2. The scope of the NIPP is designed to address which of the following types of events?
 - A. A virus that attacks Amtrak's computer system
 - B. A localized flood that causes dirt roads in a rural county to wash out
 - C. A military attack overseas on U.S. interests
 - D. A mass murder in London.

3. Which of the following statements about the NIPP is FALSE?
 - A. The NIPP framework is applicable for both terrorist attacks and natural disasters.
 - B. The NIPP replaces a business's continuity of operations and emergency operations plans.
 - C. The NIPP approach is to foster collaboration between the private sector and the public sector.
 - D. The NIPP is based on risk management and allows for differences based on unique sector characteristics.

4. Which of the following is NOT an example of critical infrastructure covered by the NIPP?
 - A. Nuclear powerplants
 - B. Agricultural distribution centers
 - C. Military installations
 - D. Highways and bridges

5. The NIPP advocates that the Government and private-sector security partners participate in multidirectional exchange of information. The NIPP refers to this as:
 - A. Hierarchal information sharing.
 - B. Cyber information sharing.
 - C. Networked information sharing.
 - D. Open-source information sharing.

6. What provides the basis for Department of Homeland Security (DHS) responsibilities in the protection of the Nation's CI/KR?
 - A. Homeland Security Presidential Directive 5 (HSPD-5)
 - B. The National Incident Management System (NIMS)
 - C. The National Response Plan (NRP)
 - D. The Homeland Security Act of 2002

7. Sector-Specific Agencies (SSAs) are responsible for:
 - A. Developing sector-specific plans to enable national cross-sector CI/KR protection program gap assessments.
 - B. Funding the implementation of optimal protection programs proposed by State, local, and tribal entities.
 - C. Evaluating the effectiveness of mandatory protection measures implemented by the private sector and industry.
 - D. Providing advice to the Secretary of Homeland Security on emergency management.

8. What is the name of the group (composed of private industry, academia, and State and local government representatives) that provides the President with advice on the security of the critical infrastructure sectors and their information systems?
 - A. Homeland Security Council (HSC)
 - B. National Infrastructure Advisory Council (NIAC)
 - C. Federal Leadership Advisory Council (FLAC)
 - D. CI/KR Protection Advisory Council (CI/KR-PAC)

9. Which of the following security partners are most likely to establish Centers of Excellence to provide independent analysis of CI/KR protection issues?
 - A. The academic community
 - B. Federal agencies
 - C. NIPP councils
 - D. State, local, and tribal governments

10. The Critical Infrastructure Partnership Advisory Council (CIPAC) facilitates effective coordination between Federal infrastructure protection programs and the infrastructure protection activities of the:
- A. Agencies and organizations within the Department of Homeland Security.
 - B. Private sector and State, local, territorial, and tribal governments.
 - C. Federal agencies and departments that are designated as Sector-Specific Agencies.
 - D. Nongovernmental organizations within designated high-risk regions.
11. Which of the following statements about Sector Coordinating Councils (SCCs) is FALSE?
- A. SCCs should be self-organized and self-governed.
 - B. SCCs represent the primary point of entry for Government into the sector with regard to CI/KR protection.
 - C. SCCs have approval authority for any mandatory regulations that the Government enacts within their sector.
 - D. SCC membership should be representative of a broad base of owners, operators, associations, and other entities within a sector.
12. In the context of the NIPP, risk is defined as:
- A. The elements within an asset, system, or network's design, location, or operation that render it susceptible to destruction.
 - B. The estimated magnitude of financial loss or damage that can be expected from a terrorist attack or natural disaster.
 - C. The likelihood that a particular asset, system, or network will suffer a terrorist attack or a natural disaster.
 - D. The expected magnitude of loss due to a terrorist attack or natural disaster, along with the likelihood of such an event occurring and causing that loss.
13. Read the following definition and select the component of risk being defined: A weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary, or disrupted by a natural hazard or technological failure.
- A. Consequences
 - B. Vulnerability
 - C. Threat

14. One step in the NIPP risk management framework is to:
- A. Identify assets, systems, networks, and functions.
 - B. Define roles and responsibilities.
 - C. Estimate budgetary needs.
 - D. Determine implementation timeframes.
15. The risk management framework is comprehensive and takes into account the assets, systems, and networks that include one or more of the following elements:
- Physical
 - Cyber
 - _____
- A. Resiliency
 - B. Financial
 - C. Human
 - D. Policies
16. Comparing the risk faced by different entities helps to accomplish all of the following outcomes, EXCEPT FOR:
- A. Selecting which CI/KR initiatives that State, local, and territorial governments can fund with DHS grant monies.
 - B. Directing decisions on how response and recovery resources are allocated during an incident to CI/KR restoration.
 - C. Evaluating security partners to determine regulatory compliance with the Federal infrastructure protection policies and procedures.
 - D. Identifying which security partners are most deficient in implementing cost-effective protective measures and actions.
17. In the NIPP Risk Management Framework, information about the current status of each sector is compared to the “baseline” of information collected and assessed during initial risk assessments to measure progress over time. During which step of the framework does this occur?
- A. Set security goals
 - B. Prioritize
 - C. Implement protective programs
 - D. Feedback loop

18. Protective actions or programs are designed to manage risks by:
- Deterring threats.
 - Minimizing consequences.
 - _____
- A. Eliminating consequences.
B. Mitigating vulnerabilities.
C. Counteracting consequences.
D. Neutralizing consequences.
19. According to the NIPP, the intention and capability of an adversary to undertake actions that would be detrimental to a particular asset, system, network or function is the:
- A. Risk.
B. Consequence.
C. Vulnerability.
D. Threat.
20. Sector-Specific Plans are:
- A. Developed by the Sector-Specific Agencies to address the unique characteristics of each sector.
B. Submitted by State, local, and tribal governments who receive Homeland Security grants.
C. Required as part of the Federal Government's regulatory oversight of vulnerable industries.
D. Designed to provide specific guidance for incorporation into local emergency operations plans.
21. The NIPP and the National Response Plan (NRP) work together to provide a comprehensive, integrated approach to the homeland security mission. The NRP provides:
- A. The detailed risk management model for CI/KR protection.
B. The approach for domestic incident management.
C. The system used to allocate resources for CI/KR protection.
D. The measures of CI/KR protection program effectiveness.
22. To ensure an effective, efficient CI/KR protection program over the long term, the NIPP relies on all of the following EXCEPT FOR:
- A. Enabling education, training, and exercise programs.
B. Creating mandatory programs regulated by DHS.
C. Conducting R&D and using technology.
D. Developing, safeguarding, and maintaining data systems and simulations.

23. Which program includes procedures that govern the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to the Department of Homeland Security?
- A. Protective Security Advisor Program
 - B. Control Systems Security Initiative
 - C. Protected Critical Infrastructure Information (PCII) Program
 - D. Protective Community Support Program
24. The NIPP:
- A. Recognizes that the disclosure of sensitive business or security information could cause serious damage to private firms, the economy, public safety, or security.
 - B. Mandates that State and local government disclose sensitive security information to all security partners within their jurisdictions.
 - C. Establishes reporting formats for the disclosure of sensitive CI/KR security information by government agencies to the public.
 - D. Prohibits the government from requesting sensitive business information from private-sector security partners.
25. According to the NIPP, effective protective actions and programs are:
- Comprehensive.
 - Coordinated.
 - Cost effective.
 - _____
- A. DHS approved.
 - B. Regionally centered.
 - C. Industry certified.
 - D. Risk based.