BrainDumps Collection

Free Questions for ISSEP by braindumpscollection

Shared by Perry on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which of the following organizations incorporates building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions?

Options:

A- DTIC

B- NSA IAD

C- DIAP

D- DARPA

Answer:

B

Explanation:

Answer option A is incorrect. The Defense Technical Information Center (DTIC) is a repository of scientific and technical documents for the United States Department of Defense. DTIC serves the DoD community as the largest central resource for DoD and government-funded scientific, technical, engineering, and business related information available today. DTIC's documents are available to DoD personnel and defense contractors, with unclassified documents also available to the public. DTIC's aim is to serve a vital link in the transfer of information among DoD personnel, DoD contractors, and potential contractors and other U.S. Government agency personnel and their contractors. Answer option D is incorrect. The Defense Advanced Research Projects Agency (DARPA) is an agency of the United States Department of Defense responsible for the development of new technology for use by the military. DARPA has been responsible for funding the development of many technologies which have had a major effect on the world, including computer networking, as well as NLS, which was both the first hypertext system, and an important precursor to the contemporary ubiquitous graphical user interface. DARPA supplies technological options for the entire Department, and is designed to be the 'technological engine' for transforming DoD. Answer option C is incorrect. The Defense-wide Information Assurance Program (DIAP) protects and supports DoD information, information systems, and information networks, which is important to the Department and the armed forces throughout the day-to-day operations, and in the time of crisis.The DIAP uses the OSD method to plan, observe, organize, and incorporate IA activities. The role of DIAP is to act as a facilitator for program execution by the combatant commanders, Military Services, and Defense Agencies. The DIAP staff combines functional and programmatic skills for a comprehensive Defense-wide approach to IA. The DIAP's main objective is to ensure that the DoD's vital information resources are secured and protected by incorporating IA activities to get a secure net-centric GIG operation enablement and information supremacy by applying a Defense-in-Depth methodology that integrates the capabilities of people, operations, and technology to establish a multi-layer, multidimensional protection.

Question 2

Question Type: MultipleChoice

Which of the following terms describes the measures that protect and support information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation?

Options:

A- Information Systems Security Engineering (ISSE)

B- Information Protection Policy (IPP)

C- Information systems security (InfoSec)

D- Information Assurance (IA)

Answer:

D

Explanation:

Information Assurance (IA) describes the measures that protect and support information and

information systems by ensuring their

availability, integrity, authentication, confidentiality, and non-repudiation. These measures include

providing for restoration of information

systems by incorporating protection, detection, and reaction capabilities.

Answer option C is incorrect. The Information systems security (InfoSec) is described as the security of an information system against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to the authorized users or the provision of service to the unauthorized users, together with those measures necessary to detect, document and counter such threats.

Answer option A is incorrect. The Information Systems Security Engineering (ISSE) process is a combination of information assurance with SE. It provides incorporated processes and solutions throughout all phases of a system's life cycle in order to gather the requirements of system's information assurance. The main emphasis of ISSE is to identify the information protection needs first and then to use a process-oriented approach to identify the security risks and subsequently to minimize or contain those risks.

Answer option B is incorrect. The Information Protection Policy (IPP) is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality. The IPP document consists of the threats to the

information management and the security

services and controls needed to respond to those threats.

Question 3

Question Type: MultipleChoice

Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States?

Options:

A- Lanham Act

B- FISMA

C- Computer Fraud and Abuse Act

D- Computer Misuse Act

Answer:

B

Explanation:

The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a 'risk-based policy for cost-effective security'. FISMA requires agency program officials, chief information officers, and Inspectors

Generals (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act.

Answer option A is incorrect. The Lanham Act is a piece of legislation that contains the federal statutes of trademark law in the United States.

The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. It is also called Lanham Trademark Act.

Answer option D is incorrect. The Computer Misuse Act 1990 is an act of the UK Parliament which states the following statement:

Unauthorized access to the computer material is punishable by 6 months imprisonment or a fine 'not exceeding level 5 on the standard scale' (currently 5000).

Unauthorized access with the intent to commit or facilitate commission of further offences is punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment.

Unauthorized modification of computer material is subject to the same sentences as section 2 offences.

Answer option C is incorrect. The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1984 intended to reduce cracking of computer systems and to address federal computer-related offenses. The Computer Fraud and Abuse Act (codified as 18 U.S.C. 1030) governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or computers used in interstate and foreign commerce. It was amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. Section (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Computer Fraud and

Abuse Act but also those who conspire to do so.

Question 4

Question Type: **MultipleChoice**

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies?

Each correct answer represents a complete solution. Choose all that apply.

Options:

A- Regulatory

B- Advisory

C- Systematic

D- Informative

Answer:

A, B, D

Explanation:

Following are the different types of policies:

Regulatory: This type of policy ensures that the organization is following standards set by specific

industry regulations. This policy type

is very detailed and specific to a type of industry. This is used in financial institutions, health care

facilities, public utilities, and other

government-regulated industries, e.g., TRAI.

Advisory: This type of policy strongly advises employees regarding which types of behaviors and

activities should and should not take

place within the organization. It also outlines possible ramifications if employees do not comply with

the established behaviors and

activities. This policy type can be used, for example, to describe how to handle medical information,

handle financial transactions, or

process confidential information.

Informative: This type of policy informs employees of certain topics. It is not an enforceable policy,

but rather one to teach individuals

about specific issues relevant to the company. It could explain how the company interacts with

partners, the company's goals and

mission, and a general reporting structure in different situations.

Answer option C is incorrect. No such type of policy exists.

Question 5

Question Type: **MultipleChoice**

Which of the following agencies provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations?

Options:

A- DARPA

B- DTIC

C- DISA

D- DIAP

U- S. Government agency personnel and their contractors.
Answer option A is incorrect. The Defense Advanced Research Projects Agency (DARPA) is an agency of the United States Department of Defense responsible for the development of new technology for use by the military. DARPA has been responsible for funding the development of many technologies which have had a major effect on the world, including computer networking, as well as NLS, which was both the first hypertext system, and an important precursor to the contemporary ubiquitous graphical user interface.
DARPA supplies technological options for the entire Department, and is designed to be the 'technological engine' for transforming DoD.

Answer:

C

Explanation:

The Defense Information Systems Agency is a United States Department of Defense combat support agency with the goal of providing real-time information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military Services, and the Combatant Commands.

DISA, a Combat Support Agency, engineers and provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations.

Answer option D is incorrect. The Defense-wide Information Assurance Program (DIAP) protects and supports DoD information, information systems, and information networks, which is important to the Department and the armed forces throughout the day-to-day operations, and in the time of crisis.

The DIAP uses the OSD method to plan, observe, organize, and incorporate IA activities. The role of DIAP is to act as a facilitator for program execution by the combatant commanders, Military Services, and Defense Agencies. The DIAP staff combines functional and programmatic skills for a comprehensive Defense-wide approach to IA.

The DIAP's main objective is to ensure that the DoD's vital information resources are secured and protected by incorporating IA activities to get a secure net-centric GIG operation enablement and information supremacy by applying a Defense-in-Depth methodology that integrates the capabilities of people, operations, and technology to establish a multi-layer, multidimensional protection.

Answer option B is incorrect. The Defense Technical Information Center (DTIC) is a repository of scientific and technical documents for the United States Department of Defense. DTIC serves the DoD community as the largest central resource for DoD and government-funded scientific, technical, engineering, and business related information available today. DTIC's documents are available to DoD personnel and defense contractors, with unclassified documents also available to the public.

DTIC's aim is to serve a vital link in the transfer of information among DoD personnel, DoD contractors, and potential contractors and other

Question 6

Question Type: MultipleChoice

You work as a systems engineer for BlueWell Inc. You want to communicate the quantitative and qualitative system characteristics to all stakeholders. Which of the following documents will you use to achieve the above task?

Options:

A- IMM

B- CONOPS

C- IPP

D- System Security Context

Answer:

B

Explanation:

The Concept of Operations (CONOPS) is a document describing the characteristics of a proposed

system from the viewpoint of an individual

who will use that system. It is used to communicate the quantitative and qualitative system

characteristics to all stakeholders. CONOPS are

widely used in the military or in government services, as well as other fields.

A CONOPS generally evolves from a concept and is a description of how a set of capabilities may be

employed to achieve desired objectives or

a particular end state for a specific scenario.

Answer option A is incorrect. The IMM is the source document describing the customer's needs based on identifying users, processes, and

information.

Answer option C is incorrect. The IPP is the source document, which is most useful for the ISSE when

defining the needed security

functionality. The IPP document contains the threats to the information management and the

security services and controls required to

counter those threats.

Answer option D is incorrect. The System Security Context is the output of SE and ISSEP. It is the

translation of the requirements into system

parameters and possible measurement concepts that meet the defined requirements.

Question 7

Question Type: MultipleChoice

There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event?

Options:

A- Acceptance

B- Enhance

C- Share

D- Exploit

Answer:

A

Explanation:

Acceptance response is a part of Risk Response planning process. Acceptance response delineates

that the project plan will not be changed

to deal with the risk. Management may develop a contingency plan if the risk does occur.

Acceptance response to a risk event is a strategy

that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types:

Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk.

Active acceptance: Such responses include developing contingency reserves to deal with risks, in

case they occur.

Acceptance is the only response for both threats and opportunities.

Answer options D, B, and C are incorrect. These are risk response for positive risks.