Exam Name : USDA-ISA-FY2013-POST Exam Sequence Id : 2184
Date : 9/18/2012
User ID : _____ User Name : _____

Question #1

All of the following are common ways of spreading malicious code **except**:

- a. Peer-to-peer software
- b. E-mail attachments
- c. Backup important files
- d. Downloading files from the web

Question #2

Darren wants to make sure that he protects his identity. He should do all of the following **except**:

- a. Ask how information will be used before giving it out.
- b. Carry his social security card in his wallet.
- c. Pay attention to his credit and bank statements.
- d. Shred unwanted documents that contain his identifying information.

Question #3

Which of the following vulnerabilities is most likely to be exploited by an **external** threat to the infrastructure?

- a. Software flaws
- b. Floods
- c. Insufficient cooling
- d. Disgruntled employees

Question #4

Which of the following are an example of a security incident?

- a. Attempts to send electronic junk mail in the form of commercial announcements.
- b. Attempts by unidentified or unauthorized people to obtain sensitive personal or business information.
- c. Loss of a government laptop containing personnel information.
- d. All of these are security incidents.

Question #5

One easy way to protect your Government computer from internet threats is to:

- a. Visit only web sites that use ActiveX or JavaScript code.
- b. Install software to prevent Denial of Service Attacks.
- c. Install spyware software.
- d. Avoid casual or unnecessary internet browsing.

Question #6

What is not PII?

- a. Gender
- b. Employment History
- c. Place of birth
- d. Information about or associated with an individual

Question #7

Edna wants to create a strong password. She should avoid all of the following **except**:

- a. Sports teams
- b. Birthdays
- c. Special characters
- d. Family or pet names

Question #8

The only acceptable use in this list for any USDA computer asset is:

- a. Gambling on the Internet.
- b. Viewing or downloading pornography.

c. Conducting private commercial business.

d. Conducting research for a work project.

Question #9

What should you do to ensure the physical security of USDA information, you should do all of the following **except**:

a. Challenge people who dont follow physical security policies.

b. Allow people to enter the facility by following others.

c. Know your organizations security policy.

d. Secure your office at night and during emergency procedures.

Question #10

Which term refers to a secure systems ability to protect against the unauthorized modification or destruction of information?

a. Confidentiality

b. Integrity

c. Availability

d. Nonrepudiation

Question #11

Lauren gets an E-mail with an attachment from the director of her agency. It has a file attachment with an unfamiliar file extension. Lauren should do all of the following **except**:

- a. Open the attachment.
- b. Be suspicious of this E-mail and attachment.
- c. Call the help-desk for advice on handling this.
- d. Verify that the sender sent the E-mail and attachment.

Question #12

The Federal Information Security Management Act (FISMA):

- a. Defines national security systems.
- b. Mandates a computer security program at all federal agencies.
- c. Requires a greater level of protection for Government information systems that contain Privacy Act information.
- d. All of the above