The following correction applies to page 427 of the *CISA® Review Questions, Answers & Explanations Manual 11th Edition*. Justification B has been bolded to indicate that B is the correct answer.

A5-153 In transport mode, the use of the Encapsulating Security Payload (ESP) protocol is advantageous over the Authentication Header (AH) protocol because it provides:

A. connectionless integrity.
B. data origin authentication.
C. antireplay service.
D. confidentiality.

D is the correct answer.

Justification:
A. Both forms of Internet Protocol Security (IPSec), Authentication Header (AH) and Encapsulating Security Payload (ESP), provide connectionless integrity.
B. Both AH and ESP authenticate data origin.
C. The time stamps used in IPSec will prevent replay attacks.
D. Only the ESP protocol provides confidentiality via encryption.

A5-154 IS management recently replaced its existing wired local area network (LAN) with a wireless infrastructure to accommodate the increased use of mobile devices within the organization. This will increase the risk of which of the following attacks?

A. Port scanning
B. Back door
C. Man-in-the-middle
D. War driving

D is the correct answer.

Justification:
A. Port scanning will often target the external firewall of the organization. Use of wireless will not affect this.
B. A back door is an opening implanted into or left in software that enables an unauthorized entry into a system.
C. Man-in-the-middle attacks intercept a message and can read, replace or modify it.
D. A war driving attack uses a wireless Ethernet card, set in promiscuous mode, and a powerful antenna to penetrate wireless systems from outside.

A5-155 Which of the following is the **GREATEST** concern associated with the use of peer-to-peer computing?

A. Virus infection
B. Data leakage
C. Network performance issues
D. Unauthorized software usage

B is the correct answer.

Justification:
A. While peer-to-peer computing does increase the risk of virus infection, the risk of data leakage is more severe, especially if it contains proprietary data or intellectual property.
B. Peer-to-peer computing can share the contents of a user hard drive over the Internet. The risk that sensitive data could be shared with others is the greatest concern.
C. Peer-to-peer computing may utilize more network bandwidth and therefore may create performance issues. However, data leakage is a more severe risk.
D. Peer-to-peer computing may be used to download or share unauthorized software, which users could install on their PCs unless other controls prevent it. However, data leakage is a more severe risk.