**QUESTION 956**
A systems administrator wants to replace the process of using a CRL to verify certificate validity. Frequent downloads are becoming problematic. Which of the following would BEST suit the administrator's needs?

A. OCSP
B. CSR
C. Key escrow
D. CA

**Answer:** A

**QUESTION 957**
A contracting company recently completed it's period of performance on a government contract and would like to destroy all information associated with contract performance Which of the following is the best NEXT step for the company to take?

A. Consult data disposition policies in the contract.
B. Use a pulper or pulverizer for data destruction
C. Retain the data for a period of no more than one year.
D. Burn hard copies containing PII or PHI.

**Answer:** A

**QUESTION 958**
Which of the following implements two-factor authentication on a VPN?

A. Username, password. and source IP
B. Public and private key
C. HOTP token and logon credentials
D. Source and destination IP addresses

**Answer:** A

**QUESTION 959**
A technician has installed a new AAA server, which will be used by the network team to control access to a company's routers and switches. The technician completes the configuration by adding the network team members to the NETWORK_TEAM group, and then adding the NETWORK_TEAM group to the appropriate ALLOW_ACCESS access list. Only members of the team should hace access to the company's routers and switches.
NETWORK_TEAM

Lee
Andrea
Pete
ALLOW_ACCESS
DOMAIN_USERS
AUTHENTICATED_USERS
NETWORK_TEAM
Members of the network team successfully test their ability to log n to various network devices configured to use the AAA server. Weeks late, an auditor asks to review the following access log sample.
5/26/2017 10:20 PERMITS: Lee
5/27/2017 13:45 PERMITS: Andrea
5/27/2017 09:12 PERMITS: Lee
5/28/2017 16:37 PERMITS: John
5/29/2017 08:53 PERMITS: Lee
Which of the following should the auditor recommend based on the above information?

A. Configure the ALLOW_ACCESS group logic to use AND rather than OR.
B. Move the NETWORK_TEAM group to the top of the ALLOW_ACCESS access list.
C. Disable groups nesting for the ALLOW_ACCESS group in the AAA server.
D. Remove the DOMAIN_USERS group from the ALLOW_ACCESSgroup

**Answer:** D

**QUESTION 960**
A Chief Information Security Officer (CISO) is performing a BIA for the organization in case of a natural disaster. Which of the following should be at the top of the CISO's list?

A. identify redundant and high-availability systems
B. identify mission-critical applications and systems
C. identify the single point of failure in the systems
D. identify the impact on safety of the property

**Answer:** B

**QUESTION 961**
A company wants to provide centralized authentication for its wireless system. The wireless authentication system must integrate with the directory back end. Which of the following is a AAA solution that will provide the required wireless authentication?

A. TACACS+
B. MSCHAPv2
C. RADIUS
D. LDAP

**Answer:** C

**QUESTION 962**
Which of the following is unique to a stream cipher?

A. It encrypts 128 bytes at a time
B. It uses AES encryption
C. It performs bit-level encryption
D. It is used in HTTPS

**Answer:** C

**QUESTION 963**
A system uses an application server and database server. Employing the principle of at least privilege, only database administrators are given administrative privileges on the database server, and only application team members are given administrative privileges on the application server. Audit and log file reviews are performed by the business unit (a separate group from the database and application teams).
The organization wants to optimize operational efficiency when application or database changes are needed, but it also wants to enforce least privilege, prevent modification of log files, and facilitate the audit and log review performed by the business unit.
Which of the following approaches would BEST meet the organization's goal?

A. Restrict privileges on the log file directory to "read only" and use a service account to send a copy of these files to the business unit.
B. Switch administrative privileges for the database and application servers. Give the application team administrative privileges on the database servers and the database team administrative privileges on the application servers.
C. Remove administrative privileges from the both the database and application servers, and give the business unit "read only" privileges on the directories where the log files are kept.
D. Give the business unit administrative privileges on both the database and application servers so they can independently monitor server activity.

**Answer:** A

**QUESTION 964**
A corporation is concerned that, if a mobile device is lost, any sensitive information on the device could be accessed by third parties. Which of the following would BEST prevent this from happening? (Select TWO). Initiate remote wiping on lost mobile devices. Use FDE and require PINs on all mobile devices. Use geolocation to track lost devices Require biometric logins on all mobile devices. Install antivirus on mobile endpoints. Patch critical vulnerabilities at least daily. A corporation is concerned that, if a mobile device is lost, any sensitive information on the device could be accessed by third parties. Which of the following would BEST prevent this from happening? (Select TWO).

A. Initiate remote wiping on lost mobile devices.
B. Use FDE and require PINs on all mobile devices.
C. Use geolocation to track lost devices
D. Require biometric logins on all mobile devices.
E. Install antivirus on mobile endpoints.
F. Patch critical vulnerabilities at least daily.

**Answer:** AB

**QUESTION 965**
A security technician must prevent unauthorized external access from stolen passwords. Which of the following authentication methods would allow users to use their current passwords while enhancing security?

A. Biometrics
B. Cognitive passwords
C. Trusted platform module
D. One-time password

**Answer:** D

**QUESTION 966**
An organization is drafting an IRP and needs to determine which employees have the authority to take systems offline during an emergency situation. Which of the following is being outlined?

A. Reporting and escalation procedures

B. Permission auditing
C. Roles and responsibilities
D. Communication methodologies

**Answer:** B

**QUESTION 967**
A network technician needs to monitor and view the websites that are visited by an employee. The employee is connected to a network switch. Which of the following would allow the technician to monitor the employee's web traffic?

A. Implement promiscuous mode on the NIC of the employee's computer.
B. Install and configure a transparent proxy server.
C. Run a vulnerability scanner to capture DNS packets on the router.
D. Configure a VPN to forward packets to the technician's computer.

**Answer:** A