Executive Certificate in Defense Technology Innovation

Cybersecurity and Information Assurance

Cybersecurity
Cybersecurity refers to the practice of protecting computer systems, networks, and data from digital attacks. These attacks can come in various forms, such as malware, ransomware, phishing, and denial-of-service attacks. Cybersecurity measures aim to prevent unauthorized access, data breaches, and other cyber threats.

Information Assurance
Information Assurance encompasses the protection, availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems. It involves implementing policies, procedures, and technologies to ensure that data is secure and trustworthy.

Access Control
Access control is the process of restricting access to resources or information to authorized users. This can include using passwords, biometrics, smart cards, or other authentication methods to verify a user's identity before granting access.

Advanced Persistent Threat (APT)
An Advanced Persistent Threat (APT) is a sophisticated, long-term cyber attack in which an unauthorized user gains access to a network and remains undetected for an extended period. APTs are often carried out by nation-states or organized crime groups.

Authentication
Authentication is the process of verifying the identity of a user or system. This can involve using passwords, biometrics, security tokens, or other methods to ensure that only authorized individuals have access to a system or network.

Botnet
A botnet is a network of infected computers or devices that are controlled by a malicious actor. Botnets are often used to carry out distributed denial-of-service (DDoS) attacks, spam campaigns, or other malicious activities.

Cryptography
Cryptography is the practice of securing communication by encoding messages to make them unreadable to unauthorized users. It involves using algorithms and keys to encrypt and decrypt data, ensuring confidentiality and integrity.

Data Breach
A data breach occurs when sensitive or confidential information is accessed, stolen, or leaked without

authorization. Data breaches can result in financial losses, reputational damage, and legal consequences for organizations.

Defense in Depth
Defense in Depth is a cybersecurity strategy that involves implementing multiple layers of security controls to protect against various threats. This approach aims to make it more difficult for attackers to compromise a system by adding redundancy and diversity in defenses.

Denial-of-Service (DoS) Attack
A Denial-of-Service (DoS) attack is a cyber attack that disrupts the normal operation of a network, system, or service by overwhelming it with a flood of traffic or requests. This can result in downtime, slow performance, or complete unavailability of the targeted resource.

Encryption
Encryption is the process of converting plaintext data into ciphertext to protect it from unauthorized access. This is done using cryptographic algorithms and keys to ensure that only authorized parties can decrypt and read the information.

Firewall
A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls can help prevent unauthorized access, malware infections, and other cyber threats.

Hacker
A hacker is an individual who uses technical skills to gain unauthorized access to computer systems, networks, or data. Hackers can be classified as white hat (ethical), black hat (malicious), or gray hat (in between) based on their intentions and actions.

Incident Response
Incident Response is the process of detecting, analyzing, and responding to cybersecurity incidents. This involves identifying security breaches, containing the damage, eradicating threats, and recovering affected systems to minimize the impact of an attack.

Information Security
Information Security focuses on protecting the confidentiality, integrity, and availability of information assets. This includes implementing security policies, procedures, and controls to safeguard data from unauthorized access, disclosure, alteration, or destruction.

Malware
Malware is malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or networks. Common types of malware include viruses, worms, Trojans, ransomware, spyware, and adware.

Penetration Testing
Penetration Testing, also known as ethical hacking, is a security assessment technique that involves simulating real-world cyber attacks to identify vulnerabilities in systems, networks, or applications. Penetration testers use authorized methods to exploit weaknesses and provide recommendations for remediation.

Phishing
Phishing is a cyber attack technique in which attackers impersonate legitimate entities to trick individuals into revealing sensitive information, such as passwords, personal details, or financial data. Phishing attacks are typically carried out via email, text messages, or fake websites.

Ransomware
Ransomware is a type of malware that encrypts a victim's files or locks them out of their system until a ransom is paid. Ransomware attacks can cause data loss, financial damage, and operational disruptions for individuals and organizations.

Risk Management
Risk Management is the process of identifying, assessing, and mitigating risks to an organization's information assets. This involves analyzing threats, vulnerabilities, and potential impacts to develop strategies for minimizing the likelihood and impact of security incidents.

Social Engineering
Social Engineering is a technique used by cyber attackers to manipulate individuals into divulging confidential information or performing actions that compromise security. This can involve psychological manipulation, deception, or impersonation to exploit human vulnerabilities.

Two-Factor Authentication (2FA)
Two-Factor Authentication (2FA) is a security mechanism that requires users to provide two different forms of identification to access a system or account. This typically involves something the user knows (password) and something the user has (security token, biometric data).

Vulnerability
A Vulnerability is a weakness or flaw in a system, network, or application that can be exploited by attackers to compromise security. Vulnerabilities can result from software bugs, misconfigurations, design flaws, or inadequate security controls.

Zero-Day Exploit
A Zero-Day Exploit is a cyber attack that targets a previously unknown vulnerability in software or hardware. Zero-day exploits are dangerous because they are typically used before a patch or fix is available, leaving systems vulnerable to exploitation.