Glossary

Course: Cybersecurity for Security Personnel

Accidental Threats: Accidental threats are unintentional threats made by a single user or privileged user or administrator when performing their everyday responsibilities.

Adversarial Threats: Adversarial threats are from individual, group, organization, or nation-state seeking to exploit the organization's dependence on cyber resources.

Authentication: The cybersecurity attribute that authorizes or allows access to computer systems and networks and the data that resides there. Loss of or incorrect authentication services could allow unauthorized access to classified data.

Availability: The cybersecurity attribute that ensures timely and reliable access to and use of information.

Confidentiality: The cybersecurity attribute that preserves authorized restrictions on information disclosure and includes the ability to protect personal privacy and proprietary information.

Cyber Attack: Attempts by hackers to damage or destroy a computer network or system.

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Cybersecurity Workforce: The DoD cybersecurity policy stating that cybersecurity workforce functions must be identified and managed.

Cyberspace Defense: The DoD cybersecurity policy indicating they are employed to protect, detect, characterize, counter, and mitigate unauthorized activity and vulnerabilities.

Department of Defense Information: The document that outlines the overarching risk management process.

Environmental Threats: Environmental threats are natural or man-made disasters, unusual natural events, or an infrastructure failure or outage.

Identity Assurance: The DoD cybersecurity policy stating that identity assurance must be used to ensure strong identification, authentication, and eliminate anonymity.

Information Technology: Any system or device that receives, processes, stores, displays, or transmits DoD information.

Insider Threats: Insider threats are malicious threats to an organization that comes from people within the organization who have legitimate access to information concerning the organization's security practices, data and computer systems.

Integration and Interoperability: Cybersecurity must be fully integrated into system life cycles and will be a visible element of DoD Component IT portfolios.

Integrity: The cybersecurity attribute that guards against improper modification to or destruction of information.

Mission Partners: The DoD cybersecurity policy indicating that capabilities that are shared with mission partners will be consistent.

Mobile Computing Threats: Mobile computing is technology that allows transmission of data, voice, and video via a computer or any other wireless enabled device without having to be connected to a physical link.

Non-repudiation: The cybersecurity attribute that ensures that a party in an electronic exchange cannot deny their participation or the authenticity of the message.

Operational Resilience: The DoD cybersecurity policy that indicates information and services are available to authorized users whenever and wherever required according to mission needs and priorities.

Performance: The DoD cybersecurity policy indicating implementation of cybersecurity will be overseen and governed through the integrated decision structures and processes. Performance will be measures, assessed for effectiveness, and managed.

Personnel Security: Personnel Security limits access to the IS to cleared personnel with a need-to-know and/or ensuring that IS users are aware of the policies associated with it and their responsibilities to protect the information it contains.

Physical Security: Procedures developed to limit unauthorized access to facilities, information systems, and the information contained within those systems.

Procedural Security: Procedural security puts organization-wide countermeasures into place.

Risk Management: The DoD cybersecurity policy that indicates the DoD will implement a multi-tiered cybersecurity risk management process. DoD must consider all cybersecurity risks. Risk management will be addressed as early as possible.

Risk Management Framework: The framework used to execute the risk management system. The seven steps are Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor.

Risk Management System: The risk management system provides an overarching methodology to follow when managing risks. The three components are assessment, mitigation, and evaluation.

Social Media Threats: Social media includes websites and applications that enable users to create and share content or to participate in social networking.

Structural Threats: Structural threats are failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances.