**Security Systems Analysis Key Terms**

Access controls – allow the user and the system to communicate with each other; includes a controller, a card reader, door contacts, and a control locking device

Access credentials – used in conjunction with access controls, typically in the form of card readers and access cards

Application Protocol-based IDS – a system or person that actively monitors and surveys the application-based communication between a system and a group of servers

Authentication – identity confirmation

Authorization – access to a location and/or information that is granted to a proven individual

Biometrics – authorization and access based on an individual’s unique characteristics including handprints, fingerprints, or retinal scans

Centralized Access Control Administration – access control that is administered and controlled from one location

Console – a control unit that an individual uses to communicate with a computer system that also works together with sensors; includes a display and a keyboard

Contact chip – a small integrated circuit which must come in contact with a reader in order for the two to communicate with each other

Contactless chip – a small integrated circuit that functions through wireless technology (the circuit utilizes transceivers, antennas, and Radio Frequency Identification (RFID)

Cryptographic keys – cryptographic operations in which a string of bits are used by a cryptographic algorithm to change a piece of text into a cipher resulting in information that can only be read using private keys or digital signatures

Identification – a method used to verify a person’s identity

Intrusion Detection System (IDS) – a program that monitors a system for malicious activity and in turn reports the activity

Host-based IDS – a system on a host that detects intrusions by monitoring system calls, application logs, file-system modifications, and other host activities

Network IDS – a system that locates intrusions by investigating the network traffic and monitoring multiple hosts

Passive IDS – a system that sounds an alert when unusual (suspicious or malicious) activity is detected, and notifies the user when preventative action must be taken

Passphrase – a statement, phrase, or series of words that replaces a password and is used for access to a computer system

Preventative administrative controls – include policies, hiring practices, and security awareness

Preventative physical controls – include badges, swipe cards, guards, and fences Preventative technical controls – include passwords, encryption, and antivirus software

Profile-based anomaly detection – a program that monitors a system by analyzing previous system patterns and current system patterns that are highly deviated from an individual user’s activity

Protocol-based IDS – a system or person that actively monitors and surveys the communication between a system and the server

Reactive IDS – a system that sounds an alert when unusual activity (suspicious or malicious) is detected, and takes action immediately by blocking the system threat

Security awareness – an attitude held by security personnel and non-security client employees, that places a high value on detecting, deterring, and reporting security exposures such as crime, safety hazards, fire hazards, theft, intrusions, and vandalism

Security survey – used to identify potential security-related problem areas

Sensor – a device that detects some form of input or information (i.e. motion, light, heat) and sends the information to the console

Signature detection – a program that scans a system against already known computer viruses, malware, or attacks, and alerts the user if an attack in detected

Statistical anomaly detection – a program that monitors the normal activity of a system and then informs the user if unusual or anomalous activity is detected

Surveillance cameras – are capable of obtaining 24-hour steady video

Threshold detection – a program that records by counting the number of times an incident occurs within a system