Section 107 Terms List

1. **General Order 1:** o take charge of this post and all government property in view.
2. **General Order 2:** To walk my post in a military manner, keeping always on alert and observing everything that takes place within sight or hearing.
3. **General Order 3:** To report all violations of orders I am instructed to enforce.
4. **General Order 4:** To repeat all calls from post more distant from the guardhouse than my own.
5. **General Order 5:** To quit my post only when properly relieved.
6. **General Order 6:** To receive, obey, and pass on to the sentry who relieves me all orders from the commanding officer, officer of the day, and officers and noncommissioned officers of the guard only.
7. **General Order 7:** To talk to no one except in the line of duty.
8. **General Order 8:** To give the alarm in case of fire or disorder.
9. **General Order 9:** To call the corporal of the guard in any case not covered by instructions.
10. **General Order 10:** To salute all officers and all colors and standards not cased.
11. **General Order 11:** To be especially watchful at night and during the time for challenging, to challenge all persons
12. **Anti-Terrorism (AT) program:** Security-related program that falls under the overarching Combating Terrorism and Force Protection programs
13. **Interior Guard:** detailed by a Commander to preserve order, protect property and enforce regulations within the jurisdiction of his/her command
14. **Field Officer of the Day:** Supervises the entire Interior Guard. Receives orders from the CO only, and serves as the CO's direct personal representative.
15. **Officer of the Day (OOD):** supervises the main guard Charged with the execution of all orders of the CO which concern the security of the area within the assigned jurisdiction. In case of alarm, acts immediately to protect life, government property and to preserve order.
16. **Commander of the Guard**: Ensures proper instructions, discipline and performance of the duty of the main guard. Ensures that all members of the guard are correctly instructed in their orders and duties, and they are understood and properly executed.
17. **Sergeant of the Guard (SOG):** Assists the Commander of the Guard in ensuring proper instructions, discipline, and performance of the duties of the main guard.
18. **Corporal of the Guard (COG):** Supervises the members of the guard assigned to that relief. Assigns sentries on that relief to posts.
19. **Main Guard Sentries:** All members of the guard will memorize, understand, and comply with the General Orders for sentries.
20. **Access**: The ability and opportunity to obtain knowledge or possession of classified information.
21. **Classification**: The determination by an authorized official that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure.
22. **Compromise**: An unauthorized disclosure of classified information to one or more persons who do not possess a current valid security clearance. Compromise can be intentional or inadvertent.
23. **Spillage**: Occurs when data is placed on an information technology system possessing insufficient information security controls to protect the data at the required classification, i.e. secret information on an unclassified machine.

24. **Classified Information:** Information that has been determined under Executive Order (EO) 12958, or any successor order, EO 12951, or any successor order, or the Atomic Energy Act of 1954 (42 USC. 2011) to require protection against unauthorized disclosure.
25. **Top Secret:** Classification level applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.
26. **Secret**: Classification level applied to information whose unauthorized disclosure could reasonably be expected to cause serious damage to the national security.
27. **Secret**: Classification level applied to information whose unauthorized disclosure could reasonably be expected to cause serious damage to the national security.
28. **Confidential**: Classification level applied to information whose unauthorized disclosure could reasonably be expected to cause damage to the national security.
29. **Operational Security (OPSEC):** a systematic method used to identify, control, and protect critical information using the following:
30. **Human Intelligence (HUMINT):** The collection of information from human sources.
31. **Signals Intelligence (SIGINT):** Refers to electronic transmissions that can be collected by ships, planes, ground sites, or satellites.
32. **Open-Source Intelligence (OSINT):** Refers to a broad array of information and sources that are generally available, including information obtained from the media (newspapers, radio, television, etc.), professional and academic records (papers, conferences, professional associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.).
33. **Imagery Intelligence (IMINT):** Intelligence derived from the exploitation of imagery collected by visual photography, infrared, lasers, multi-spectral sensors, and radar.
34. **Measurement and Signatures Intelligence (MASINT)**: Relatively little-known collection discipline that concerns weapons capabilities and industrial activities.
35. **insider threat:** a person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities
36. **Terrorism**: Unlawful use or threatened use of violence to force or to intimidate governments or societies to achieve political, religious, or ideological objectives.
37. **FPCON**: a standardized DoD identification system for recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities.
38. **FPCON NORMAL:** Applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.
39. **FPCON ALPHA**: Applies when there is an increased general threat of possible terrorist activity against personnel or facilities, and the nature and extent of the threat are unpredictable.
40. **FPCON BRAVO:** Applies when an increased or more predictable threat of terrorist activity exists.
41. **FPCON CHARLIE**: Applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely.
42. **FPCON DELTA:** Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent.