Task 1:

IDS is a device or software application that monitors a network or systems for malicious activity or policy violations. IDS stands for **intrusion detection system.** An IDS works like a burglar alarm in that it detects a violation (some system activity analogous to an opened or broken window) and activates an alarm.

Task 2:

IPS stands for Intrusion Prevention System

SIEM stands for Security Information and Event Management

NIST stands for National Institute of Standards and Technology

Task 3:

Should install IDPS because:

1. According to the NIST documentation on industry best practices, there are several compelling reasons to acquire and use an IDPS:
   To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system
2. To detect attacks and other security violations that are not prevented by other security measures
3. To detect and deal with the preambles to attacks (commonly experienced as network probes and other “doorknob rattling” activities)
4. To document the existing threat to an organization
5. To act as quality control for security design and administration, especially in large and complex enterprises
6. To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors