|  |  |  |
| --- | --- | --- |
| Questions | Comments | Adequate Level of Understanding? |
| Yes/No |
| 1. What is Operations Security (OPSEC)? What is the purpose of OPSEC? |  |  |
| 1. Do you know who your department’s OPSEC Working Group representative is? Do you know who the Command OPSEC Officer is? |  |  |
| 1. In your job, what kind of information would an adversary find useful? |  |  |
| 1. Describe some weaknesses or vulnerabilities an adversary can exploit at this command. |  |  |
| 1. Are you familiar with what a Foreign Intelligence Entity (FIE) is and how they collect information? |  |  |
| 1. Are you familiar with the terms “Critical Information” and “indicators”? Have you seen the command’s Critical Information List? |  |  |
| 1. Are you familiar with ways to prevent an adversary from collecting information from you? |  |  |
| 1. Have you received an OPSEC awareness brief in the past year? Did this brief help you better understand the purpose of OPSEC? |  |  |
| 1. Have you ever found sensitive information in the trash, or received an e-mail containing sensitive information that was unencrypted? |  |  |
| 1. Is there a Portable Electronic Device (PED) policy in place at this command? Is it enforced? Please explain. |  |  |
| 1. Do all command personnel badge in properly or show proper identification? Do you feel an unauthorized person could gain access to the command? |  |  |
| 1. Describe the term “social engineering”. Have you ever experienced social engineering or elicitation for information? |  |  |
| 1. Do you have a social media page? (Facebook, WhatsApp, Instagram, etc.) If yes, do you ever post any information about your work? |  |  |
| 1. Do you feel that personnel assigned to this command take the protection of sensitive information seriously? |  |  |
| 1. Have you noticed any practices in your workspace, department, or at the command in general that could compromise critical information or indicate operational activity? |  |  |