

Instruction 36-4405

CYBERSECURITY AWARENESS AND TRAINING

Effective Date: 1 June 2024

Certified by: Col Angela K. Watkins, 502 CS/CC

1. PURPOSE

This instruction establishes local requirements for cybersecurity awareness training and compliance for all personnel assigned to or working at Joint Base San Antonio. It supplements AFI 17-130 and provides installation-level procedures.

2. TRAINING REQUIREMENTS

2.1. Annual Training. All personnel with network access must complete DoD Cyber Awareness Challenge training annually. Training must be completed within 30 days of account activation for new personnel.

2.2. Privileged Users. Personnel with elevated system privileges must complete additional role-based training as outlined in DoD 8570.01-M within 60 days of assignment to a privileged role.

2.3. Phishing Awareness. All users will participate in quarterly phishing awareness exercises conducted by the 502d Communications Squadron. Individuals who fail two consecutive exercises will have their network access suspended until remedial training is completed.

3. COMPLIANCE TRACKING

Unit Information Assurance Officers (IAOs) are responsible for tracking training compliance and reporting monthly to the 502 CS Information Assurance office. Units below 95% compliance will be reported to the 502 ABW/CC.

4. REMOVABLE MEDIA

Use of unauthorized removable media (USB drives, external hard drives) on government systems is prohibited. Authorized removable media must be registered with the unit IAO and scanned prior to each use.

ANGELA K. WATKINS, Col, USAF

Colonel, USAF

Commander, 502d Communications Squadron

Date: 1 June 2024