DEPARTMENT OF THE AIR FORCE

AFI 17-130

CYBERSECURITY PROGRAM MANAGEMENT

Effective Date: 15 November 2024

Certified by: Lt Gen Timothy D. Haugh, SAF/CN

1. PURPOSE

This instruction establishes policy and assigns responsibilities for the management of cybersecurity programs across all Department of the Air Force (DAF) information systems. It implements Department of Defense Instruction (DoDI) 8500.01, Cybersecurity, and DoDI 8510.01, Risk Management Framework for DoD Systems.

2. APPLICABILITY

This instruction applies to all DAF military, civilian, and contractor personnel who develop, implement, operate, maintain, or use DAF information systems, including systems operated by contractors on behalf of the DAF.

3. ROLES AND RESPONSIBILITIES

3.1. Chief Information Officer (SAF/CN):

a. Serves as the DAF Senior Information Security Officer (SISO) and oversees implementation of cybersecurity policy.

b. Ensures all DAF information systems comply with the Risk Management Framework (RMF) process.

c. Establishes cybersecurity metrics and reporting requirements for all DAF organizations.

3.2. Wing/Installation Commanders:

a. Appoint an Installation Cybersecurity Officer (ICO) to manage local cybersecurity programs.

b. Ensure all personnel complete annual cybersecurity awareness training within 30 days of assignment.

c. Report cybersecurity incidents within 1 hour of discovery through appropriate channels.

4. SYSTEM AUTHORIZATION

All DAF information systems must receive an Authorization to Operate (ATO) prior to processing, storing, or transmitting information. Systems operating without a valid ATO are subject to immediate disconnection from the network. Authorization decisions are based on the residual risk to DAF operations and assets.

4.1. ATO Duration. Standard ATOs are valid for three (3) years from the date of issuance. Interim ATOs may be granted for a period not to exceed 180 days when operational necessity requires system deployment prior to full assessment completion.

5. INCIDENT RESPONSE

All suspected or confirmed cybersecurity incidents shall be reported to the 16th Air Force (AFCYBER) through the appropriate Computer Emergency Response Team (CERT). Incident categories and response timelines are defined in accordance with CJCSM 6510.01B.

5.1. Category 1 incidents (root-level compromise) require notification within 1 hour. Category 2-7 incidents require notification within 24 hours of discovery.

6. TRAINING REQUIREMENTS

All DAF personnel with access to information systems must complete Cybersecurity Awareness Training annually. Personnel with privileged access must complete additional role-based training as outlined in DoD 8570.01-M. Failure to complete training within the specified timeframe will result in suspension of system access.

TIMOTHY D. HAUGH, Lt Gen, USAF
Lieutenant General, USAF

Chief Information Officer

Date: 15 November 2024