



DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, U.S. ARMY GARRISON FORT MEADE
4551 LLEWELLYN AVENUE
FORT GEORGE G. MEADE, MARYLAND 20755-5000

NETC-SYC-DG

JAN 03 2023

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Fort George G. Meade (FGGM) Policy #13, Authorization to Conduct Required Wireless Assessment Scans

1. References:

- a. DISA STIG, Network Policy – Version 8, Release 6, dated 29 April 2011
- b. Army Best Business Practice (BBP), Wireless Security Standards (09-EC-M-0010) Version 4, dated 26 June 2013
- c. Army Regulation 25-2, Army Cyber Security, 4 April 2019
- d. 7th Signal Command (Theater) (7th SC T) OPORD 190822-395, Wireless Network Discovery Scans Using Flying Squirrel Assessment Tool Suite, dated 28 August 2019

2. Background. The Fort George G. Meade Network Enterprise Center (NEC) is required to conduct at a minimum, monthly wireless assessment scans per references cited above. The purpose of the scans is to detect possible unauthorized “rogue” Wireless Local Area Networks (WLANs) and devices. These scans are authorized, by 7th SC (T), for sites that do not have the required Wireless Intrusion Detection Systems (WIDS) deployed.

3. Requirements:

- a. All personnel conducting scans using the Flying Squirrel application must be authorized and certified by completing the Flying Squirrel training course on the U.S. Army Information Assurance Virtual Training website. The IA training is located at <https://cs.signal.army.mil/>.
- b. A copy of this authorization letter will be provided to the security office prior to conducting wireless network discovery scans.
- c. A brief description of the government vehicle(s) to be used and license plate numbers will be provided to the security office.

NETC-SYC-DG

SUBJECT: Fort George G. Meade (FGGM) Policy #13, Authorization to Conduct Required Wireless Assessment Scans

d. Personnel will only conduct scans while on FGGM. At no time will an active scan be conducted or directed off the installation.

e. Personnel conducting wireless scans will adhere to the Flying Squirrel Scanning User Agreement, DOD, and Army Security requirements.

f. Personnel are authorized to determine only the location of the wireless devices. At no time are personnel authorized to actually monitor traffic or attempt penetration of the network.

g. Capture results must be kept on an external hard drive or CD/DVD and retained for one year.

4. The proponent for this policy is the Network Enterprise Center (NEC) point of contact, Mr. Wallace Ruffin, wallace.r.ruffing.civ@army.mil, (301) 677-1275.



MICHAEL A. SAPP
COL, MI
Commanding

DISTRIBUTION:

A
B