DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
4710 KNOX STREET
FORT BRAGG, NORTH CAROLINA 28310-5010

AFRC-CII 10 May 2019

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: United States Army Reserve Network (ARNET) Wireless Policy

1. References:

2. Fragmentary Order 001 to Operation Order 14-036.

a. MEMORANDUM FOR Facility Commander Reference: OPORD 14-036.

b. Army Regulation 25-2, Information Assurance, Rapid Action Revision, 23 March 2009.

c. Army CIO/G-6 Information Assurance Best Business Practice (IA BBP), Wireless Security Standards (09-EC-M- 0010), Version 4.0, 26 Jun 2013.

d. DoD Wireless Local Area Network Security Technical Implementation Guide Version 6, Release 15, 26 April 2019.

3. Purpose. This policy defines the requirements of the United States Army Reserve (USAR) Wireless Local Area Network (WLAN) infrastructure, security posture, intended users, primary mission, regulatory compliance, industry compliance, and key stakeholders. With the rapidly advancing wireless technology field, it is the intent of this policy to address the minimal security framework and the expected service delivery for a good user experience.

4. Applicability:

a. All ARNET eligible authenticated users, including but not limited to, USAR military personnel, Department of Army (DA) Civilians, contractors, consultants, temporary and other workers at the USAR, including all personnel affiliated with Department of Defense (DoD) that maintain an Army Reserve Account Maintenance and Provisioning (ARAMP) account or connects to the USAR Wireless Enterprise must adhere to this policy.

b. All wireless infrastructure devices that connect to an ARNET (enclave) or reside on a USAR site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of

wireless communication devices capable of transmitting packet data, .i.e., WiFi and Bluetooth.

c. This document supersedes all previous wireless policies.

5. Policy:

a. The requirements and priority of the WLAN deployment in reference 1a establish a secure and stable WLAN to meet the demands of the growing wireless community. This WLAN provides users with the same quality of service and performance level experienced on the wired LAN.

b. Scope of support for wireless access point (WAP):

(1) Covered via wireless:

(a) Team/conference rooms

(b) Classrooms

(c) Drill/assembly hall

(d) OMS/AMSA/TEMF bays

(e) Unit storage areas

(2) Not covered via wireless:

(a) Offices with wired connectivity.

(b) Spaces determined by United States Army Reserve Command (USARC) Chief Information Officer (CIO)/G-6 Network and Infrastructure (N&I) to be too costly

(c) Spaces determined by the Information Assurance Manager (IAM) to be a security hazard

(d) Spaces determined by Safety to be a health hazard

(3) Signal strength requirements:

(a) The optimal endpoint signal strength is -75 dBm or higher for a good user experience.

(b) When evaluating receive signal strength, the evaluator will consider the signal-to-noise ratio (SNR) for the best throughput and radio frequency (RF) quality.

(4) Capacity requirements:

(a) The facility manager will assist in determining the number of access points (AP) in a particular area. This number will be based on typical user density during peak training events, applications requirement, and desired performance.

(b) Placement of the APs to meet the demand of user coverage. Not more than one AP will be placed in a 40ft x 40ft area.

(c) Assessment of the coverage area is recommended upon completion of installation. Adds, moves, and changes may be challenged or required by the facility manager but must be approved and confirmed by N&I staff.

(5) Security requirements:

(a) Security is a crucial component of USAR Enterprise Wireless service. All current and future WLAN deployment must adhere to the requirement set forth in references 1b–e.

(b) The mode will be interoperable with the USAR Network Access Control Solution.

(c) All cryptography must be validated under Federal Information Processing Standards (FIPS) 140-2. The WiFi at the core foundation must make use of Advanced Encryption Standard (AES)–Counter Mode with Cipher Block Chaining (CBC) Message Authentication Code (MAC) Protocol (CCMP).

(d) The function of a Wireless Intrusion Detection System (WIDS) is only scanning. It does not facilitate endpoint access to the wireless network. At a minimum, each site requires one WIDS. The APs will participant in this duty when time permits.

(6) WIDS monitors the network for the presence of unauthorized APs and clients. It also logs and generates reports based on the logged information. The Wireless Intrusion Prevention System (WIPS) solution consists of a centralized server appliance with distributed sensors that are used for monitoring and interacts with the WLAN environment. WLAN network will monitor at a minimal the following:

(a) Hijacking

(b) RF jamming (DOS)

(c) Protocol attacks

(d) Eavesdropping

(e) Spoofing

(f) Man-in-the middle attacks

(g) Management interface exploits

(h) Encryption cracking

(i) Authentication attacks

(j) Peer-to-peer attacks

(k) KRACK (Key Reinstallation Attack)

6. Oversight: All phases of operations, life cycle, and funding will fall under the auspice of the N&I Branch Chief.

7. Responsibilities:

a. The IAM will determine the validation of all requirements set forth in this policy on an annual basis, with review by the N&I Branch Chief.

b. As the wireless technology advances, N&I is responsible for life cycle and determining the future requirements in order to meet the demands of the USAR mission.

c. Site Points of Contact (POC) will report ARNET wireless service degradation, outages, and other technical deviations to the USARC CIO/G-6 by opening an incident ticket on the USAR Enterprise Service Desk portal (https://esdhelp) or by calling the Service Desk at (855) 558-7272. Incident tickets will include the following:

(1) Incident Description: ARNET Wireless: Service Problem

(2) Physical Location of Device: FACID, Street Address, Building and Room Number

(3) Brief Description of the Problem

8. Effective Date: This policy is effective upon signature and will remain in effect until revised or superseded.

9. POC: Emilio G. Perez, USAR Facilities Infrastructure Manager, (910) 570-8442, emlio.g.perez3.civ@mail.mil.

REGISTER.KIMBERLY.MARIE.1037987553

Digitally signed by REGISTER.KIMBERLY.MARIE.1037987553
Date: 2019.05.10 15:43:29 -04'00'

KIMBERLY M. REGISTER
Chief, USARC CIO/G-6 Cybersecurity
Program Management (ISSM)

DISTRIBUTION:

GEOGRAPHIC COMMANDS:
1 MSC
7 MSC
9 MSC
63 DIV (R)
- USAG-FHL
81 DIV (R)
- USAG-Fort Buchanan
88 DIV (R)
- USAG-Fort McCoy
99 DIV (R)
- ASA-Dix

FUNCTIONAL COMMANDS:
3 MCDS
76 ORC
79 TSC
200 MP CMD
311 SC(T)
335 SC(T)
377 TSC
412 TEC
416 TEC
807 MCDS
ARCD
AR-MEDCOM
ARAC
LEGAL CMD
MIRC
USACAPOC(A)
75 TNG CMD (MC)
80 TNG CMD (TASS)
83 US ARRTC
84 TNG CMD (UR)
85 USAR SPT CMD
108 TNG CMD (IET)
USAR SPT CMD (1A)

AREC/ARET:
USARPAC
ARNORTH
ARSOUTH
(CONT)

DISTRIBUTION: (CONT)
ARCENT
AFRICOM
CENTCOM
USAREUR
USARAF
8TH ARMY
NORTHCOM
USARJ
I CORPS
PACOM
SOUTHCOM
III CORPS
XVIII ABC
USASOC
EUCOM
SOCOM

CF:
USARC XOs
USARC DIR/DEP/CH/ASST
OCAR Directors & Deputies