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

AFRC-CI 27 September 2019

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Quarantine Policy for United States Army Reserve Managed Networks

1. References:

a. Army Regulation (AR) 25-1, Army Information Technology, 19 July 2019.

b. AR 25-2, Army Cybersecurity, 4 April 2019.

c. National Institute of Standards and Technology (NIST) Special Publication 800-30, Guide for Conducting Risk Assessments, Revision 1, September 2012.

d. Memorandum, Secretary of the Army, 01 Feb 2013, subject: Mandatory Information Assurance/Cybersecurity Awareness.

e. Memorandum, Under Secretary of the Army, 10 May 2013, subject: Commander and Leader Responsibilities for Cybersecurity/Information Assurance (CS/IA) Incidents.

f. Army Cyber Command (ARCYBER) Situational Awareness Report (SAR) 2014-111, Clarification of CAT A Quarantine Process.

2. Purpose: This policy implements and enforces quarantine of assets with known vulnerabilities (also referred to as “noncompliant assets”) on United States Army Reserve (USAR) managed networks (unclassified and classified).

3. Background: The continued operation of assets with known vulnerabilities imposes an unacceptable level of risk to USAR managed networks. Noncompliant assets will not operate on USAR managed networks without an authorizing official (AO) approved risk acceptance, Plan of Action and Milestone (POA&M), and Mitigation Action Plan. If the risk of noncompliant assets is not accepted or mitigated, such assets will be quarantined from USAR managed networks.

4. Applicability: This policy applies to all USAR personnel that access or maintain USAR managed information systems and networks.

5. Responsibilities:

a. ISSM: Overall responsible for the health of USAR managed networks (unclassified and classified).

b. System Owners: Responsible for implementing policy on USAR managed networks and assets.

c. System Administrators: Responsible for the maintenance and compliance of individually assigned systems.

d. Cybersecurity Compliance: Responsible for scanning assets, identifying vulnerabilities, communicating findings to stakeholders, and verifying remediation.

e. Unit Information Management Officer (IMO): Responsible for responding to alerts that systems are subject to quarantine and take corrective actions.

f. Users: Communicate system warning banners to unit IMOs or submit request to the USAR Service Desk (https://esdhelp.ar.ds.army.mil/CAisd/DoDBanner.html) for assistance.

6. Policy: Systems with known vulnerabilities will not operate on USAR managed networks without proper adjudication within the USAR vulnerability management process (see paragraph 10 for exceptions).

7. Asset Quarantine Criteria:

a. Any information system with identified vulnerabilities, regardless of severity, will be quarantined if not remediated within 45 days of the release date.

b. Rogue/unauthorized systems are subject to immediate quarantine.

8. The quarantine process will involve rapid identification, diagnosis, and remediation of vulnerable assets.

a. Access to the quarantined device may be restricted to system administrators and Army approved cybersecurity tools.

b. Any information system not remediated within 60 calendar days will be removed from the network and must be reimaged.

9. USAR AO authorized quarantine may be executed with little or no prior notification to the field.

10. Exceptions:

a. In coordination with the United States Army Reserve Command (USARC) Chief Information Officer (CIO)/G-6, subordinate commands will use the Mission Critical System Template (encl) to properly categorize “mission critical” systems into a list, to include hostname, system use or purpose, and a detailed justification as to why systems have been identified as mission critical. The list will be provided to USARC CIO/G-6 via Secret Internet Protocol Router Network (SIPRNet) no later than 90 days from the date of this policy. The Mission Critical List will be updated quarterly thereafter. If a mission critical system is in danger of quarantine, the system owner must accomplish two tasks:

(1) Complete a MAP and submit to the POA&M Review Board.

(2) Send a memorandum requesting exemption from quarantine THRU the USARC CIO/G-6 to the AO.

b. Vulnerabilities that are already documented on the existing USAR POAM may, or may not, be quarantined.

c. False Positives: If a finding is determined to be a false positive, the system may be returned to the network upon verification that the vulnerability is a false positive. Validation of all false positive findings will be documented and tracked by the system owner and the Cybersecurity Operations Branch (COB).

11. System owners will ensure that they tailor their respective remediation procedures to avoid the quarantine of information systems. No later than 90 calendar days from the date of this policy, any departmental security plans will be updated to reflect quarantine authorization processes.

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

13. Point of Contact: Mrs. Kimberly Register, Chief, USARC CIO/G-6 Cybersecurity Program Management/ISSM, (910) 570-8653, kimberly.m.register.civ@mail.mil.

REGISTER.KIMBERLY.MARIE.1037987553
Digitally signed by REGISTER.KIMBERLY.MARIE.1037987553
Date: 2019.10.02 10:58:49 -04'00'

Encl

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

Enclosure: Mission Critical Systems Template