



DEPARTMENT OF THE ARMY
UNITED STATES ARMY EUROPE
UNIT 29351
APO AE 09014-9351

AEIM-I

24 October 2016

MEMORANDUM FOR All Army in Europe Leaders

SUBJECT: Army in Europe Cybersecurity and Operational Readiness (AE Cmd Memo 2016-046)

1. Protecting and defending our information and information systems (IS) to achieve and maintain information superiority is a team effort. Everyone must understand that operating in an unsecure environment presents an unacceptable risk to the Army in Europe. We must embrace a proactive cybersecurity culture that is driven by commanders who ensure that their units are resilient to emerging cyber threats.

2. Information security is crucial to mission assurance; compromising information can lead to dire consequences. To ensure information security and defend cyber threats, commanders must do the following:

a. Pay special attention to personally identifiable information (PII). PII is information that can be used to distinguish or trace an individual's identity. We must protect PII from compromise and exploitation. Phishing is an extremely effective means our adversaries use to compromise PII or gain unauthorized access to our IS. Commanders must train their units to avoid and report phishing. USAREUR's missions balanced with security requirements drive the appropriate level of availability, confidentiality, and integrity that we must apply to our information and IS.

b. Integrate cybersecurity into all mission and training objectives to ensure we are ready to fight tonight and maintain interoperability with our Allies and partner nations.

c. Know their cybersecurity responsibilities and posture by having their units participate in the Cyber Readiness Board and tracking their cyber focus areas.

d. Ensure all systems and networks are assessed and authorized. Timely completion of the assess-and-authorize process not only is in compliance with Federal law, it provides commanders the knowledge about their IS that they require to protect USAREUR's information.

e. Ensure cybersecurity violations are reported by completing and submitting [AE Form 25-2B](#), Cyberdefense Policy Violation Report, to their information systems security managers.

f. Meet and maintain cybersecurity baseline standards for program-managed and program-of-record systems in order for those systems to operate securely on the DOD information network.

AEIM-I

SUBJECT: Army in Europe Cybersecurity and Operational Readiness

3. Cybersecurity is everyone's responsibility. To meet this responsibility, we must minimize risk, protect our information, and prevent, detect, and report unauthorized activity while remaining vigilant and ensuring that Soldiers, Civilians, Contractors, and Family members are well-informed of their role as the first line of defense. We will also exercise the Information Technology Contingency Planning Process and determine its place within the overall Continuity of Operations Plan and Business Continuity Plan process. Army in Europe commanders, leaders, and cybersecurity professionals will engage in our persistent battle against cyber threats. Strong cyber ensures mission readiness.

A handwritten signature in black ink, appearing to read 'F. Hodges', with a long horizontal flourish extending to the right.

FREDERICK "BEN" HODGES
Lieutenant General, USA
Commanding