



DEPARTMENT OF THE ARMY
HEADQUARTERS, 25TH INFANTRY DIVISION
580 KOLEKOLE AVENUE
SCHOFIELD BARRACKS, HAWAII 96857-6000

APVG-CG

04 AUG 2016

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: 25th Infantry Division Policy Letter #8 - Commander's Program to Manage Cyberspace Risk

1. REFERENCES:

- a. Memorandum, Secretary of the Army, 1 February 2013, subject: Mandatory Information Assurance/Cybersecurity Awareness.
- b. Memorandum, Secretary of the Army, 11 August 2014, subject: Privileged Access to Army Information Systems and Networks.
- c. DoD Directive 8570.01-M, Information Assurance Workforce Improvement Program, 10 November 2015.
- d. Army Regulation 25-1, Army Information Technology, 25 June 2013.
- e. Army Regulation 25-2, Information Assurance, 23 March 2009.
- f. Army Regulation 380-5, Department of the Army information Security Program, 29 September 2000.
- g. Army Regulation 15-6, Procedures for Administrative Investigations and Boards of Officers, 1 April 2016.
- h. Army Regulation 380-67, Personnel Security Program, 24 January 2014.
- i. FRAGO 2, February 2013, to U.S. Army Cyber Command EXORD 2012-276, Unauthorized Disclosure of Classified Information via Electronic Communication Reporting Procedures, 7 June 2012.
- j. 4th Regional Cyber Center – Pacific (4RCC-PAC) CS Incident Response Plan version 4.5, 12 April 2016.
- k. U.S. Army Pacific (USARPAC) Network Security Violation (NSV) Policy – Policy Memorandum 06-09, 10 July 2009.

APVG-CG

SUBJECT: 25th Infantry Division Policy Letter #8 - Commander's Program to Manage Cyberspace Risk

I. Chief Information Officer/G-6, Cyber Directorate, Best Business Practices 05-PR-M0002, IA Training and Certification Version 5.0, March 2012.

2. PURPOSE. To establish a commander's program that manages cyberspace risk through increased training, information assurance, greater situational awareness, and creating secure and resilient network environments.

3. APPLICABILITY. This policy applies to all personnel assigned, attached, or under the operational control of 25th Infantry Division (25th ID), including Department of Defense (DoD) civilian employees, invited contractors, technical representatives, and all family members.

4. DEFINITION.

a. A cybersecurity incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

b. Examples of cybersecurity incidents include, but are not limited to:

(1) Unauthorized disclosure of classified information (UDCI) or the synonymous common term "negligent discharge of classified information" (NDCI). UDCIs include, but are not limited to:

(2) Spillages: The introduction of classified information on a lower classified information system or a system with incompatible releasability restrictions. Spillages must be contained and sanitized from every component of the Department of Defense (DoD) enterprise that may be infected.

(3) Loss of any information system equipment or media containing sensitive or classified information.

(4) Cross Domain Violations (CDVs): The connection of a device and transfer of information on an information system that differs from its approved classification. CDVs typically occur when discipline is not properly enforced while moving a device connected to a DoD information system.

(5) Attempts to use or attach equipment and removable media (e.g., thumb drives, discs, etc.) not authorized for connection to DoD information systems. Such violations potentially introduce malware on a system.

APVG-CG

SUBJECT: 25th Infantry Division Policy Letter #8 - Commander's Program to Manage Cyberspace Risk

(6) Attempts to access or collect data for which an individual has not been cleared.

(7) Attempts to circumvent information system access controls designed to protect sensitive or classified information.

5. BACKGROUND. Commanders must have the freedom and confidence to operate securely in the cyber domain. Across 25th ID, cyberspace enables every aspect of our mission command, training, force generation, logistics, and administration. Yet our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity – the security of the technologies and information that we use each day. Cybersecurity incidents may be intentional or unintentional. The unintentional compromises caused by human error, lack of supervision, and inadequate training are significantly more prevalent and can have severe consequences. Protecting against these unintentional compromises also protects us from intentional compromise and external threats. How commanders leverage the opportunities of cyberspace, while managing inherent uncertainties and reducing vulnerabilities, will significantly impact our readiness.

6. POLICY. Commanders will establish a program to manage cyberspace risk through increased training, information assurance, greater situational awareness, and creating secure and resilient network environments. All personnel are charged with adhering to the specific policy guidance below.

a. ASSESS. Commanders will assess their cybersecurity posture and program with regard to readiness, risk, resources, and reporting. The commander's assessment will include, but is not limited to, individual, leader, and unit training opportunities to improve cybersecurity awareness and practices; previous cybersecurity incidents; incident response plans; deterring and mitigating insider threats; and compliance with information assurance directives.

b. TRAIN. Commanders must focus on the fundamentals – compliance with basic network and information security tactics, techniques, and procedures. Cybersecurity incidents at the tactical level have more to do with training and discipline than technology.

(1) Adapt leader training to incorporate cybersecurity as both a protector and enabler of mission command. Information must be shared to enable mission command without compromising security.

(2) Implement a training program that addresses cybersecurity standards, preventative measures (cyber hygiene), threats, risks, mission impacts, incident

APVG-CG

SUBJECT: 25th Infantry Division Policy Letter #8 - Commander's Program to Manage Cyberspace Risk

responses, and costs associated with the various types of cybersecurity incidents. The goal is to ensure all information system users fully understand their individual and collective responsibilities for securing DoD networks and associated sensitive and classified information. These efforts must be continuous and should evolve to keep pace with emerging threats.

(3) Ensure all information system users register in the Army Training and Certification Tracking System (ATCTS). Registration in ATCTS is required to track training in accordance with (IAW) reference 1.b., paragraph 4-3. All users must register at <https://atc.us.army.mil/iastar/registration.php>. Unit S-6s will provide registration instructions to ensure users are tracked with the installation Network Enterprise Center (NEC). ATCTS tracks baseline DoD cybersecurity training requirements which complement but do not replace the commander's program requirements specified in the above paragraph.

(4) All general users will complete the DoD Cyber Awareness Challenge, Portable Electronic Devices and Removable Storage Media, Phishing Awareness, Safe Home Computing, Personally Identifiable Information (PII) courses as well as sign the Acceptable Use Policy (AUP) located at Fort Gordon Information Assurance Training Center website (ia.signal.army.mil).

(5) All privileged users will be trained and certified IAW DoDD 8570.01-M and Army Best Business Practices.

c. SECURE. Technological advances will forever present great risks to, and opportunities for, enabling mission command. More significant than technology, however, people present the greatest vulnerabilities and risks to cybersecurity. Leadership, training, and accountability are fundamental aspects of securing tactical-level and home-station networks.

(1) All network devices connected to the network or stand alone will comply with the Department of the Army published Information Assurance Vulnerability Management (IAVM) directives and network security policies.

(2) All information assurance incidents, whether suspected or in fact, will be reported through their respective Information Assurance Security Officer (IASO) to the 25th ID Information Systems Security (ISSM).

(3) All computers, laptops and media will be Data-At-Rest (DAR) compliant, will be labeled with the appropriate level of classification, and will be government furnished

APVG-CG

SUBJECT: 25th Infantry Division Policy Letter #8 - Commander's Program to Manage Cyberspace Risk

equipment. Virtual Private Network (VPN) accounts require a DAR compliance check of portable electronic devices before use outside of the ordinary office environment.

(4) No personally owned or government issued computer devices or portable electronic devices (PEDs) are allowed on the network regardless of situation. PEDs include cell phones, smart phones, iPhones, tablets, and mp3 players.

(5) All user accounts will be disabled upon Permanent Change of Station or Expiration of Term of Service.

(6) Personally Identifiable Information (PII) will be encrypted when contained within an e-mail or removed from a government facility. PII is any information about an individual that is private or intimate to the individual and as distinguished from information related solely to the individual's official functions or public life. This information includes, but is not limited to, any personal information which is linked or linkable to an individual, such as education, financial transactions, medical history, criminal or employment history, and information which can be used to distinguish or trace an individual's identity. Examples include social security numbers, date and place of birth, mother's maiden name, and electronic medical records.

(7) No malicious/unauthorized software (i.e. peer-to-peer downloads, instant messaging, or games) are allowed on government furnished information systems if not explicitly approved by the 25th ID ISSM.

(8) No unauthorized installation or removal of programs, disabling of security configurations or audit logs, altering system configurations, straining, testing, circumventing, or bypassing security mechanisms to include enabling the external storage devices unless explicitly permitted by the 25th ID ISSM.

(9) Failure to follow any of the above procedures, proper security and regulations will result in immediate suspension of network access and privileges.

(10) Commanders will consider the full range of corrective actions at their disposal when network or information security standards are violated. Individuals responsible for a cybersecurity incident may be subject to appropriate administrative, disciplinary, or criminal action. At a minimum, commanders will immediately suspend the account of the originating offender involved in a spillage while pending corrective action, and conduct a preliminary inquiry when a suspected cybersecurity violation is discovered. Commanders will determine if an additional investigation is required. For each violation, the offender will be required to take corrective training and recertification.

APVG-CG

SUBJECT: 25th Infantry Division Policy Letter #8 - Commander's Program to Manage Cyberspace Risk

Offender network access will not be restored until the above mentioned actions have been completed. Subsequent violations may require progressive corrective actions.

(a) First Offense – Memorandum signed by the Brigade Commander. The account may be reactivated after the memo has been accepted by the 25th ID Chief of Staff and following an automatic 15-day account suspension.

(b) Second Offense – Memorandum signed the Brigade Commander. The account may be reactivated after the memo has been accepted by the 25th ID Commanding General and following an automatic 30-day account suspension

(c) Any exception to paragraphs 10 (a) and 10 (b) will be based upon urgent mission needs and requires the approval of the 25th ID Chief of Staff.

(d) Any personally owned or government issued computer devices or PEDs connected to any classified network will be confiscated and turned in for processing by the Regional Cyber Center. Any incident involving this nature will undergo an AR 15-6 investigation. After the conclusion of the investigation, despite the results, the personal electronic device will not be returned to the owner and will be processed by the U.S. Army for proper disposal.

d. REPORT. Reporting is required in both technical and command channels. Cybersecurity incidents will be reported to the 25th ID ISSM in accordance with 25th ID Commander's Critical Information Requirements.

(1) Cybersecurity incidents will be reported to ensure all credible derogatory information is annotated in the Joint Personnel Adjudication System. Reporting is required regardless of whether the individual has a clearance or does not have a clearance. Commanders will report investigation outcomes and corrective actions in the closure report.

(2) The 25th ID G-2 and G-6 will assist the 25th ID G-3 in developing and managing the reporting requirements directed by this policy.

e. REIMBURSE. Incident cleanup costs are considerable and often involve the sanitization or destruction of hard drives, computers, servers, other network components, and related labor costs. The costs increase rapidly as classified information is passed through the network if UDCIs are not immediately reported and contained. To offset the damage and cleanup costs associated with UDCIs, the 25th ID unit that originated the incident will pay the associated costs. Typical costs for units that originate a UDCI is at least \$5,000 per incident that does not require server cleanup and

APVG-CG

SUBJECT: 25th Infantry Division Policy Letter #8 - Commander's Program to Manage Cyberspace Risk

at least \$10,000 per incident that requires server cleanup. UDCIs that require the impacted equipment be destroyed may cost significantly more. Commanders should consult with their servicing legal office regarding the financial liability (e.g., Financial Liability Investigation for Property or Loss) of individuals responsible for cybersecurity incidents.

7. This memorandum supersedes 25th Infantry Division Policy Letter #9, dated 5 November 2014 and remains in effect until superseded or rescinded in writing.

8. The point of contact for this memorandum is LTC Brian Jorgenson, 25th ID G6, at (808) 437-4317 (DSN 315), email: brian.m.jorgenson.mil@mail.mil.



CHRISTOPHER G. CAVOLI
Major General, USA
Commanding

DISTRIBUTION:

A