



DEPARTMENT OF THE ARMY  
US ARMY INSTALLATION MANAGEMENT COMMAND  
HEADQUARTERS, US ARMY GARRISON COMMAND AND FORT KNOX  
125 6TH AVENUE, SUITE 320  
FORT KNOX, KENTUCKY 40121-5719

REPLY TO  
ATTENTION OF:

Expires 28 November 2013

NECT-SFB-DK

28 November 2011

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters  
Commanders, Fort Knox Partners In Excellence  
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Fort Knox Policy Memo No. 33-11 – Network Access and Security Clearance  
Suspension/Denial/Revocation

1. References.

- a. AR 380-5, Department of the Army Information Security Program, 29 September 2000.
- b. AR 25-2, Information Assurance, 24 October 2007 (RAR 001, 23 March 2009).
- c. 7th SC (T), G-2 NIPRNET Access Waiver Procedures SOP, 25 August 2009.

2. Purpose. This policy explains the actions necessary and options available as a result of clearance suspension/denial/revocation relating to network accounts.

3. Applicability. This policy applies to all Soldiers, civilians, and contractors who connect to the Fort Knox Installation Campus Area Network (FKICAN).

4. Policy.

a. Investigation/Clearance Status. The Joint Personnel Adjudication System (JPAS) along with local records checks and screenings determine the investigation/clearance status for an individual. If the result is a letter of intent to deny/revoke, the clearance status is changed to suspended. Actions taken for a status of Suspended/Denied/Revoked will result in the following:

- (1) All existing accounts will be disabled.
- (2) All requests for new or additional accounts will be denied.
- (3) All access to classified information will be denied.

(4) The activity security manager will notify the organization Information Assurance Point of Contact (IA POC)/Information Management Officer (IMO) who will, in turn, notify the installation Information Assurance Manager (IAM).

NECT-SFB-DK

SUBJECT: Fort Knox Policy Memo No. 33-11 – Network Access and Security Clearance  
Suspension/Denial/Revocation

b. Appeals.

(1) Appeal options.

(a) The individual submits an appeal to the Department of the Army Appellate Board or a rebuttal or reconsideration letter to Central Clearance Facility (CCF). User accounts will remain disabled pending decision.

(b) The individual does not submit an appeal to the Department of the Army Appellate Board or a reconsideration letter to CCF. All user accounts will be removed from all information systems (IS).

(2) Appeal results.

(a) If the CCF adjudicates the individual's clearance favorably, the individual's account/request for account will be enabled/approved.

(b) If the CCF makes an unfavorable determination and revokes/denies the clearance and the Department of the Army Appellate Board revokes/denies the clearance, the individual's access to IS, computer accounts, and classified information will be removed permanently.

c. Waivers. If IS access is required during the appeal process, the activity commander may submit a request for an access waiver.

(1) Waivers will not be considered for the following:

(a) Any request for access to classified information.

(b) Personnel who caused the suspension due to information technology (IT) violations. Users designated in IT-1 positions will be removed from these positions.

(c) Personnel who have had a final adjudication revoked by CCF.

(d) Personnel who have not completed all requirements prior to CCF suspense and submitted a request to CCF for reconsideration.

(2) The waiver process is identified below:

(a) The organization director/commander reviews the data and *carefully and deliberately* makes a recommendation through the proper chain of command, the Fort Knox Network Enterprise Center, the 106th Brigade Commander, and the 7th SC (T) G2 to the FKICAN Designated Approving Authority (DAA). The waiver must show that the local security manager has completed local records checks and screenings, include the documentation on the steps that were taken by the employee and the command to regain their clearance, and resolve the issue that led to the suspension. The recommendations for waiver approval must outline assurances

NECT-SFB-DK

SUBJECT: Fort Knox Policy Memo No. 33-11 – Network Access and Security Clearance  
Suspension/Denial/Revocation

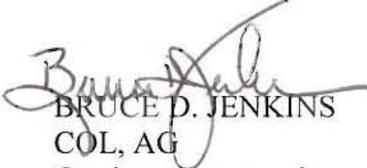
from the unit commander that procedures are in place to preclude access to classified data or systems, protective devices, and the individual will be highly supervised.

(b) Waivers processed for IT-II and IT-III personnel are only valid for a period of six months or less. If a second waiver extension is required, one may be granted as long as a new request for waiver is submitted.

(c) Newly reported derogatory information that has been verified will revoke any current waiver and result in immediate denial of access to the IS.

(d) No access will be granted until the waiver process has been completed and approval is received from the FKICAN DAA.

5. Point of contact is the Installation IAM at 502-624-5782.

  
BRUCE D. JENKINS  
COL, AG  
Garrison Commander

DISTRIBUTION:

A