Copy ___ of ___ copies
US Army Cyber Command and Second Army
Fort Belvoir, VA
171450Z February 2016

(U) US Army Cyber Command and Second Army (ARCYBER & 2A) Operation Order (OPORD) 2016-033 Implementation of Updated Policy for the Documentation of Privileged Users (U//FOUO)

(U) References:

(a) (U) Army Regulation (AR) 25-2, Information Assurance (IA), 23 March 2009.

(b) (U) AR 25-1, Army Information Technology (IT), 25 June 2013.

(c) (U) AR 380-67, Personnel Security Program, 24 January 2014.

(d) (U) Department of Defense (DoD) 8570.01-M, IA Workforce Improvement Program, 24 January 2012.

(e) (U) CNSSI No. 4009, Committee on National Security Systems Glossary, April 6, 2015.

(f) (U) HQDA EXORD 055-16 ISO DoD Cybersecurity Scorecard Reporting.

(g) (U) HQDA CIO/G-6 Memorandum "Privileged/Elevated Access to Army Information Systems, Networks and Data." 26 January 2016.

(U) Time Zone Used Throughout the OPORD: ZULU

1. (U//FOUO) Situation. Recent leaks of classified information and Personally Identifiable Information (PII) highlight the failures of technical and administrative measures to prevent exploitation by both internal and external threats. To address core vulnerabilities exploited in recent cyber incidents and updated policy requirements, ARCYBER & 2A is directing actions associated with privileged access to Army information systems (IS) and data.

a. (U) Per CNSSI 4009, privileged users (PU) are individuals who are authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

b. (U) System Administrators, Data Transfer Agents, and those with special access to use portable drives, CD/DVDs, thumb drives, etc. are inherently PU.

(U) US Army Cyber Command and Second Army (ARCYBER & 2A) Operation Order (OPORD) 2016-033 Implementation of Updated Policy for the Documentation of Privileged Users (U//FOUO)

c. (U) This order implements policy contained in reference (g), which is a policy update from August 2014. New requirements from this updated policy include additional information required in appointment letters and the requirement to validate Army Training and Certification Tracking System (ATCTS) documentation of PUs quarterly.

2. (U) Mission. All Army organizations will manage privileged users IAW this order NLT 31 March 2016 in order to protect the Army's portion of the DoD Information Network (DODIN) against adversary exploitation.

3. (U//FOUO) Execution.

a. (U) Commander's Intent.

(1) (U) Purpose. Enable mission command by improving the defense-in-depth of Army networks and the integrity, availability, and confidentiality of data.

(2) (U) Key Tasks.

(a) (U) Properly document and monitor PUs in Army Training and Certification Tracking System (ATCTS).

(b) (U) Quarterly review and update PU access.

(3) (U) End State. Commanders have visibility on PUs' access to networks and data, PU policies and standards are strictly enforced, and adversaries face a more effective DODIN defense.

b. (U) Concept of Operation. All Army organizations will implement procedures to properly request and document PU access, and conduct routine reviews of PUs' continued need for elevated levels of access.

c. (U) Tasks to Units. ACOMs, ASCCs, DRUs, Field Operating Agencies, NGB and ARNG.

(1) (U) Units will comply with tasks in paragraph 3e NLT 31 March 2016.

(2) (U) Coordinate reporting through NETCOM as directed.

d. (U) Tasks to Subordinate units.

(1) (U) Regional Cyber Centers (RCCs). Comply with tasks in paragraph 3e NLT 31 March 2016.

(U) US Army Cyber Command and Second Army (ARCYBER & 2A) Operation Order (OPORD) 2016-033 Implementation of Updated Policy for the Documentation of Privileged Users (U//FOUO)

(2) (U) NETCOM.

(a) (U//FOUO) Consolidate all unit reports (ACOMs, ASCCs, DRUs, Field Operating, NGB, ARNG, and RCCs) from paragraph 3e(9) and randomly verify, using ATCTS global visibility, that units are properly updating PU appointment letters, non-disclosure agreement (NDA) and privileged access agreement (PAAs) and properly updating ATCTS.

(b) (U//FOUO) Provide consolidated weekly report on Fridays using Annex R starting on 262000Z February 2016 to the POC in paragraph 5c(5) until units report 100% compliance.

e. (U) Coordinating Instructions.

(1) (U//FOUO) Organizations will maintain the ability to nominate Soldiers, Civilians, contractors and other individuals as candidates for privileged/elevated access via signed appointment letters. However, official manning documents (TDA, Position Description, or Contract Modification) must be updated. Each candidate for privileged/elevated access must complete and sign a PAA and a NDA and upload them in their ATCTS accounts at (https://atc.us.army.mil) once the Information System Security Manager (ISSM) or Information System Security Officer (ISSO) signs off IAW reference (g).

(2) (U) All packets for privileged/elevated access will be referred to their security manager for clearance verification. If required, the security manager will initiate a new clearance to meet requirements of the designated IT level.

(3) (U//FOUO) Organization ISSM or ISSO will coordinate with their security manager to conduct a quarterly review of all PUs security clearances to ensure PU has the appropriate clearance for the IT Level that he/she has been designated.

(4) (U//FOUO) All units will notify and coordinate with their respective NEC, service providers and ISSM/ISSO to revoke privileged/elevated access from any user whose functions no longer require such access.

(5) (U//FOUO) Commands and other Army activities will coordinate with their NECs and service providers to oversee this policy and its associated processes via quarterly reviews of documentation (e.g., appointment letter, PAAs, NDAs, decisions) for the request, authorization, and denial of privileged/elevated access.

(6) (U//FOUO) All units report weekly on Fridays IAW Annex R starting on 261800Z February 2016 to the POC in paragraph 5c(3) until units report 100% compliance.

(U) US Army Cyber Command and Second Army (ARCYBER & 2A) Operation Order (OPORD) 2016-033 Implementation of Updated Policy for the Documentation of Privileged Users (U//FOUO)

(7) (U//FOUO) All units are required to update PU appointment letters and include the specific functions performed as part of their job. All appropriate documentation must be uploaded to ATCTS IAW reference (g).

(8) (U) Command Inspection Programs will include PU Identification and Management in their inspection checklists within 90 days of this order.

(9) (U) Validation of ATCTS includes validation of user profile data (Personnel Type, Personnel Security Classification Level IT-I/IT-II/IT-III, Information Assurance Profile Assignment Level, training, certifications and appointment orders) in ATCTS and Active Directory.

4. (U) Sustainment. There is no separate funding for the requirements of this order or the associated policy.

5. (U) Command and Signal.

a. (U) Command.

(1) (U) ARCYBER is the supported command. All others are supporting.

(2) (U) Command. Commander, U.S. Army Cyber Command is located at the Nolan building on Fort Belvoir, VA.

b. (U) Control. Use existing telephonic and NIPR/SIPR network communications and reporting procedures. SIPRNET is the designated C2 Network for ARCYBER & 2A.

c. (U) Signal. Points of Contact.

(1) (U//FOUO) ARCYBER & 2A G35 DODIN POC is MAJ Clifford W. Elder, Comm: (703) 706-2162; NIPR: clifford.w.elder.mil@mail.mil, SIPR: clifford.w.elder.mil@mail.smil.mil.

(2) (U//FOUO) CIO/G-6, Cybersecurity Directorate POC is Ms. Phyllis Bailey, COMM: (703) 545-1698; NIPR: Phyllis.e.bailey2.civ@mail.mil.

(3) (U//FOUO) NETCOM Fusion Center SIPR: usarmy.huachuca.netcom.mbx.g3-operations-center@mail.smil.mil; DSN: 520-538-2179.

(4) (U//FOUO) ARCYBER & 2A after duty hours POC: ACOIC Command Duty Officer, DSN 235-1384, Comm: (703) 706-1384; SIPR: usarmy.belvoir.arcyber.mbx.acoic-cdo@mail.smil.mil.

(U) US Army Cyber Command and Second Army (ARCYBER & 2A) Operation Order (OPORD) 2016-033 Implementation of Updated Policy for the Documentation of Privileged Users (U//FOUO)

(5) (U//FOUO) ARCYBER & 2A ACOIC G33 DODIN, 703-706-1780/1636, SIPR usarmy.belvoir.arcyber.mbx.acoic-toc@mail.smil.mil.

ACKNOWLEDGE: All addressees will acknowledge receipt of this message within 24 hours via email to the ACOIC Current Operations at usarmy.belvoir.arcyber.mbx.acoic-current-ops@mail.smil.mil.

CARDON
LTG

OFFICIAL:
//ORIGINAL SIGNED//
ZERUTO

ANNEXES:
Annex R (Reporting)

DISTRIBUTION:
HQ, Department of the Army
Assistant Secretary of the Army, Acquisition, Logistics, & Technology [ASA (ALT)]
US Army Forces Command (FORSCOM)
US Army Training and Doctrine Command (TRADOC)
US Army Materiel Command (AMC)
US Army Pacific (USARPAC)
US Army Central (USARCENT)
US Army Europe (USAREUR)
US Army Africa (USARAF)
US Army North (USARNORTH)
US Army South (USARSOUTH)
US Army Special Operations Command (USASOC)
Military Surface Deployment and Distribution Command (SDDC)
US Army Space and Missile Defense Command/Army Strategic Command (USASMDC/ARSTRAT)
Eighth US Army (EUSA)
US Army Medical Command (MEDCOM)
US Army Intelligence and Security Command (INSCOM)
US Army Criminal Investigation Command (USACIDC)
US Army Corps of Engineers (USACE)

(U) US Army Cyber Command and Second Army (ARCYBER & 2A) Operation Order (OPORD) 2016-033 Implementation of Updated Policy for the Documentation of Privileged Users (U//FOUO)

US Army Military District of Washington (MDW)
US Army Test and Evaluation Command (ATEC)
US Army Reserve Command (USARC)
US Army Installation Management Command (IMCOM)
Superintendent, US Military Academy (USMA)
US Army Acquisition Support Center (USAASC)
Command and Control Support Activity (CCSA)
Information Technology Agency (ITA)
Human Resources Command (HRC)
Chief, National Guard Bureau (NGB)
US Army National Guard (ARNG)
US Army Network Enterprise Technology Command (NETCOM)
Regional Cyber Center-Western Hemisphere (RCC-WH)
Regional Cyber Center-Pacific (RCC-P)
Regional Cyber Center-Europe (RCC-E)
Southwest Asia Cyber Center (RCC-SWA)
Regional Cyber Center-Korea (RCC-K)

CF:
5th Signal Command (Theater)
7th Signal Command (Theater)
311th Signal Command (Theater)
335th Signal Command (Theater)