DEPARTMENT OF THE ARMY
UNITED STATES MILITARY ACADEMY
West Point, New York 10996

REPLY TO
ATTENTION OF

MAIO (1oo) 31 March 2009

USMA POLICY MEMORANDUM NUMBER 25-IA-07-04

SUBJECT: USMA User/Computer Identity Disclosure Policy

1. **PURPOSE.** To establish policy, assign responsibility, and set procedures for the use of proxy servers, anonymizers, and other means to change, disguise, or hide a network user's identity.

2. **REFERENCES.** AR 25-1; AR 25-2; USMA Policy Memorandum 93-01, subj: Computer Network Use Policy, 1 Sep 2002; MEMORANDUM FOR United States Corps of Cadets, Accessing Unauthorized Web Sites, dated 23 May 2002; USCC SOP; Joint Ethics Regulations, DoD 5500.7-R; USMA Policy Memorandum 25-IA-5-02, subj: USMA Unauthorized Workstation Use Policy, 27 May 2003 .

3. **APPLICABILITY.** Applicability: This policy applies to all members of the West Point Community, the United States Military Academy (USMA), United States Military Academy Preparatory School (USMAPS) subordinate agencies and activities, cadets, cadet candidates, tenant units, and contractors who operate any computing device connected to the USMA network.

4. **BACKGROUND.**

a. Anonymizers and proxy server systems can be used hide or mask the various parts of the origin and/or destination information of Internet traffic. These types of hardware and software solutions have legitimate uses. We use a proxy server at West Point to translate the .mil part of our identity into an .edu identity and vice versa enabling authorized access to other .mil and .edu domains. They can also be used to optimize network traffic routing to improve performance or when authorized, bypass local port restrictions. Finally, they can be used to mask a user's identity in certain situations, though legitimate reasons for doing this are rare.

b. Anonymizers can also carry the privacy function too far by subverting the means to manage the USMA network. Use of anonymizers do not relieve individuals of the responsibility to use the Internet and USMA network resources IAW applicable policies, regulations and local, state and federal laws. Use of a proxy server to avoid detection while accessing porn, gambling or hacking sites, can be viewed as an aggravating circumstance to the act. Communicating with intent to hide one's identity is contrary to Army Values and may have regulatory, criminal and honor implications.

c. Finally, in any network, especially a government one, the user is assigned a specific identifier (userid) as a condition for using that network. The operators of the USMA network, as well as the larger DoD network, have a legitimate need to know who is using the network as part of regulatory information assurance measures.

5. **POLICY.**

a. This policy prohibits the use of all anonymizers and proxy servers services by users connected to the USMA network with the intent of masking or changing a user's identity, hiding source or destination address information or otherwise preventing accurate disclosure of standard network information for either malicious or non-malicious purposes. This policy is not intended to prohibit the ethical and proper use of handles in chat rooms, threaded discussions, bulletin boards, user groups, and other authorized collaboration software.

b. Approval to use an external proxy server for legitimate official reasons can be obtained by using the Information Technology Request (ITR) process.

c. Users are not authorized to change their machine's computer name once assigned by their IMO.

6. **RESPONSIBILITIES.**

a. All **users of the USMA network will:**

(1) Comply with this policy.

(2) Gain clarification by the appropriate technical experts prior to the use of any hardware or software that might have functions or features that could violate this policy.

(3) Contact the CIO office for additional clarification of this policy, as required.

b. All **supervisors will:**

(1) Ensure users are aware of and have read this policy.

(2) Ensure users are in compliance with this policy.

(3) When notified, provide assistance to Information Assurance personnel investigating potential violation of this policy.

(4) When validated, take appropriate steps to counsel, retrain or reprimand personnel in violation of this policy, as appropriate.

c. All **supervisors, to include the USCC Information Systems Officer (ISO) chain,** will ensure that their IT personnel thoroughly understand this policy, and are able to educate their personnel.

d. The **Information Assurance Manager (IAM)** is authorized to direct network scanning by Information Assurance personnel to ensure compliance with this policy.

e. All **IMOs, and DCOs will**:

(1) Ensure that users in their activity understand this policy.

(2) Approach the employee with an initial report from the DOIM

(3) Develop a computer naming convention for their activity, in coordination with the DOIM.

7. **PROCEDURES.**

a. The DOIM will periodically monitor network activity for use of proxy servers and anonymizers IAW authority granted in 6d, above. Initial reports of this kind of improper activity will be passed to the organization's IMO, Academic DCO, or cadet ISO for adjudication with the user. More serious action may be taken if the anonymizer/proxy server usage is determined to be related to violation of other USMA computer use policies. Reports of repeated activity will be elevated through the chain-of-command for appropriate action.

b. Only IMOs, DCOs and Goldcoats are authorized to assign a computer name.

8. **EXPIRATION.** This Policy Memorandum remains in effect until rescinded or superseded.

FOR THE SUPERINTENDENT:

MICHAEL S. YARMIE
COL, SC
Chief of Staff

DISTRIBUTION:
A-E Electronic