DEPARTMENT OF DEFENSE
Defense Commissary Agency
Fort Lee, VA 23801-1800

MANUAL

Social Media

DeCAM 100-04.1
May 15, 2012

Corporate Communication Directorate
OPR: DeCA/BEC

1. POLICY. This Manual implements polices as defined in Defense Commissary Agency Directive (DeCAD) 100-04, "Social Media," **TBD**, (Reference (a)), and is in compliance with references listed within this document.

2. PURPOSE. This Manual provides detailed procedures for carrying out DeCA's Social Media policy, and guidance for the responsible and effective use of Internet-based Capabilities (IbC) and assigns responsibilities for its current use on social network service (SNS) sites such as Facebook, YouTube, Twitter, Flickr, and any future SNS.

3. APPLICABILITY. This Manual applies to all Defense Commissary Agency (DeCA) employees at all levels and all activities whose access to IbC is necessary for the performance of their official duties. Employees who are not authorized users are those whose access has been taken away for noncompliance with the Social Media Directive, Manual, or any of the references associated with these documents.

4. MANAGEMENT CONTROL SYSTEM. This Manual contains internal management control provisions that are subject to evaluation and testing as required by DeCAD 70-2, "Internal Control Program," December 17, 2007, (Reference (b)).

5. RELEASABILITY – UNLIMITED. This Manual is approved for public release and is located on www.commissaries.com and DeCA's intranet website, OneNet.

6. EFFECTIVE DATE. This Manual is effective immediately.

Gary Frankovich
Acting Director,
Corporate Communication Directorate

TABLE OF CONTENTS

REFERENCES

(a) DeCA Directive xx-xx, "Social Media," xxx xx, 2010
(b) DeCA Directive 70-2, "Internal Control Program," December 17, 2007
(c) Directive-Type Memorandum (DTM) 09-026, "Responsible and Effective Use of Internet-based Capabilities," Change 4, May 9, 2012[1]
(d) DeCA Directive 35-33, "Internet and Electronic Mail Usage Policy, May 2, 2006
(e) DeCA Handbook 50-6, "Civilian Employee Handbook," March 25, 2011
(f) DoD 5500.7-R, "Joint Ethics Regulation," November 17, 2011
(g) DoD Manual 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008
(h) DeCA Directive 35-39, "Computer Network Defense," December 14, 2009
(i) DoD Directive 8500.01E, "Information Assurance," certified current as of April 23, 2007
(j) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1, 1982
(k) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(l) DeCA Directive 100-1, "Defense Commissary Agency Public Affairs Program," February 26, 1993
(m) DeCA Directive 80-21, "Privacy Act Program," April 15, 2010
(n) DeCA Directive 35-31, "Information Assurance," December 14, 2009
(o) The Freedom of Information Act, as amended, Section 552 of Title 5, United States Code[2]
(p) DeCA Directive 5-2, "Records Management Program," August 28, 2007
(q) DeCA Directive 80-4, "Litigation Involving DeCA," January 1, 1992

[1]Copies of DoD directives, manuals, regulations or DTMs may be obtained from the Internet at http://www.dtic.mil/whs/directives/corres/pub1.html
[2]The Freedom of Information Act can be found at http://www.archives.gov/foia/

CHAPTER 1

RESPONSIBILITIES

1-1. PURPOSE. Reference (a) establishes policy and assigns responsibility for the responsible and effective use of IbC, including current and future SNS used at DeCA. This Manual explains how IbC are to be used at all levels of the Agency and how its current and future SNS are to be used and managed to effectively reach DeCA's strategic communication goals, according to Directive-Type Memorandum (DTM) 09-026, "Responsible and Effective Use of Internet-based Capabilities," May 9, 2012, (Reference (c)). This Manual also provides procedures for carrying out DeCA's social media policy, assigns responsibilities for its management, and provides guidance for its use.

1-2. BACKGROUND. DeCA recognizes that IbC provide its employees with the latest technologies that enable them to connect and communicate with each other, customers, and industry partners. Therefore, DeCA has granted employees access to IbC, using government-provided communication devices since all employees are considered authorized users when access to IbC is necessary for the performance of their official duties. However, it is mandatory that the procedures, policies, and guidelines in this manual be strictly adhered to at all times.

1-3. APPLICABILITY. The procedures, policies, and guidance in this Manual apply to the use of all IbC by all DeCA employees at all levels and activities when access to IbC is necessary for the performance of their official duties

1-4. AUTHORIZATION AND USE OF INTERNET-BASED CAPABILITIES (IbC)

a. Who May Establish an Official SNS Behalf of DeCA? Only the Director and CEO can authorize the establishment of an official SNS or an official external presence for the Agency; and only the Director, Corporate Communication Directorate (BEC) can develop and maintain official IbC on the behalf of the Agency. In accordance with (IAW) Reference (c), the Agency is not authorized more than one official presence on any one IbC; e.g.: Facebook, Twitter, YouTube, and Flickr. Therefore, separate sites for DeCA area offices or stores are not authorized.

b. Are DeCA's Current Sites Official Government Sites? Yes, they are authorized by the DeCA Director, monitored and maintained by BEC, and are registered with the Department of Defense (DoD) IAW Reference (c).

c. Who, at DeCA, Has Access to IbC and When? All DeCA employees, at all levels and activities, whose access to IbC is necessary for the performance of their official duties, have permission to access IbC from government equipment on government time, but must follow all set procedures, policies, and guidelines annotated within this Manual and its references. Prior to gaining access, every employee must complete the latest DoD social networking training at: http://iase.disa.mil/eta/sns_v1/sn/launchPage.htm, "Social Networking V1.0," and keep the original certificate of completion at his or her workstation.

d. Who Can Comment or Respond to a Question on DeCA's Social Media Sites? DeCA employees, who are appointed as "administrators," are the only employees authorized to upload comments, responses,

photographs, videos, or any other media to DeCA's current and future SNS. All uploads will be made IAW all references cited in this Manual. Employees not designated as administrators may neither initiate a comment nor respond to a question or upload photographs, videos, or any other media onto DeCA's current and future SNS on behalf of the Agency or represent they have the authority to do so. Any employee who uploads comments, responses, photographs, videos, or any other media to any IbC will identify themselves as a DeCA employee when discussing the Agency or their job at DeCA.

CHAPTER 2

RULES FOR USING INTERNET-BASED CAPABILITIES (IbC)

2-1. PURPOSE. This chapter includes procedures, policies guidelines, and reminders to follow when accessing IbC as a DeCA employee using government equipment; when using government equipment for limited personal use; or when discussing the Agency in a personal capacity using personal resources. These are offered as recommendations and are not meant to infringe upon anyone's personal interaction.

2-2. PROCEDURES, POLICIES, AND GUIDELINES. The procedures, policies, and guidelines in this Manual are designed to help employees at all levels and activities make appropriate decisions about their use of IbC. These augment DeCA's email and Internet policy, DeCA Directive (DeCAD) 35-33, "Internet and Electronic Mail Usage Policy," May 2, 2006, (Reference (d)).

a. Confidential and Proprietary Information on IbC. Employees will not share information on any IbC that is confidential and proprietary. This includes any nonpublic information like personally identifiable information (PII); source selection or procurement information; or such information as trademarks, upcoming product releases, sales and finances, number of products sold, company strategy, or any other information that has not been approved for public release by the Agency. These are given as examples only and do not cover the broad range of what the Agency, its employees, contractors, or its business partners consider confidential and proprietary. Employees with questions or concerns about what information may be released or have doubts about what can and cannot be released, should contact their first-line supervisor, who will staff their question through BEC and the General Counsel (CCG). This must be done prior to releasing information that could potentially harm the Agency or current and potential products, employees, partners, and customers. Protection of this information is referenced in the nondisclosure agreement (DoD Information System User Agreement) employees are required to sign before they are granted access to DeCA's information systems.

b. Official Seal, Shopping Cart Logo, and Cornucopia. DeCA's official seal, its shopping cart logo, and the cornucopia may not be used by employees on any IbC, other than by DeCA's SNS administrators when responding in an official capacity. This will prevent the appearance that an employee is speaking on behalf of or representing the Agency in an official capacity.

c. Right to Privacy, Respect, and Copyrighted Materials. DeCA encourages its employees to write knowledgeably, accurately, and use appropriate professionalism whenever interacting on SNS, using government and non-government devices in either a professional or personal capacity when commenting on or referring to the Agency. Despite disclaimers, Internet interactions can result in members of the public forming opinions about DeCA, its employees, business partners, and products.

(1) Honor the privacy of DeCA's employees by seeking their permission before writing about or displaying internal company events that might be considered to be a breach of their privacy and confidentiality.

(2) Speak respectfully about DeCA and current and potential employees, customers, and business partners. Do not engage in name calling or behavior that would reflect negatively on anyone's reputation.

(3) Note that the use of copyrighted materials, unfounded or derogatory statements, and misrepresentations is not authorized. Using these materials and statements can result in disciplinary

action, as annotated in DeCA Handbook 50-6, "Civilian Employee Handbook," March 25, 2011, (Reference (e))

d. Restrictions to Using IbC on Government Equipment. No DeCA employee will access IbC on government equipment to promote, sell, or endorse products and services.

e. Legal Liability. DeCA employees are legally liable for anything they post or otherwise upload to IbC and can be disciplined by the Agency for commentary, content, or image(s) that is or are defamatory, pornographic, proprietary, harassing, libelous, discriminatory, or create a hostile work environment. DeCA employees can also be sued by other DeCA employees, business partners, or an individual or company that views the commentary, content, image(s) as defamatory, pornographic, proprietary, harassing, libelous, discriminatory, or that creates a hostile work environment.

f. Media Contact. All media queries about DeCA and its current and potential products, employees, business partners, customers, and competitors must be referred to BEC for coordination and guidance.

g. Government-Provided Communication Equipment. As discussed in Reference (e), DeCA owns any communication sent and stored on its equipment. Therefore, first-line supervisors or any authorized staff members have the right to access any employee's government-provided communication equipment to monitor content. Based on the guidelines in this reference, employees should not consider their government-provided electronic communication devices as storage areas or to be private.

h. The Internet is Permanent. DeCA employees must understand that once they put information on the Internet, it is essentially part of a permanent record – even if it is removed or deleted.

i. Discriminatory Comments, Responses, Photographs and Videos. Comments; responses, photographs; or videos that contain offensive, obscene, or threatening language that is based on race, color, religion, sex, gender, national origin, disability, age, or other protected classification or which may be construed to advocate discrimination, harassment, or retaliation against protected groups, based on those protected classifications, are prohibited and may result in disciplinary action that may lead to employment termination.

2-3. LIMITED AUTHORIZED PERSONAL USE.

a. Paragraph 2-301 of Department of Defense (DoD) 5500.7-R, "Joint Ethics Regulation," August 1, 1993, (Reference (f)), permits limited personal use of federal government resources when authorized by the Agency designee, so long as such use does not adversely affect official business.

b. All DeCA employees who use IbC in their personal capacity, on government-furnished communication devices, must comply with References (a) and (f). In addition, when using government-furnished communication devices, employees who mention or comment on DeCA or current and potential products, employees, business partners, customers, and competitors in his or her personal comment or response, or publish, comment on or respond to nonpublic information, should provide a disclaimer when his or her personal opinion is expressed and state that views expressed are his or hers alone and do not represent DeCA's views. Additionally, employees must limit the use of government-furnished communication devices to access and manage personal IbC sites during official duty hours.

c. When using their personal communication devices to connect to IbC in their personal capacity, employees who mention DeCA or current and potential products, employees, business partners, customers, and competitors in his or her personal comment or response, should identify himself or herself as a DeCA employee and state that views expressed are his or hers alone and do not represent DeCA's views. In no event may a DeCA employee reveal nonpublic information concerning DeCA, it employees, or its business partners that he or she has gained in the performance of his or her official duties when using personal communication devices to access IbC in their personal capacity.

CHAPTER 3

ROLES AND RESPONSIBILITIES

3-1. DECA DIRECTOR AND CHIEF EXECUTIVE OFFICER (CEO): DeCA Director/CEO shall:

a. Approve the establishment of DeCA's external and internal "official presence."

b. Ensure the implementation, validation, and maintenance of applicable IA controls, information security procedures, and OPSEC measures.

c. Ensure computer network defense mechanisms that provide adequate security for access to IbC from DeCA's network are in place, effective, and compliant with DeCAD 35-39, "Computer Network Defense," December 14, 2009, (Reference (h)) and DoD Directive 8500.01E, "Information Assurance," certified current as of April 23, 2007, (Reference (i)).

d. Ensure employees are educated about, trained in, and are made aware of the responsible and effective use of IbC.

e. Ensure IbC are established, monitored, and maintained to ensure compliance with Reference (a).

f. Coordinate with USD(I) regarding the use of IbC that collect user or other information to ensure compliance with Reference (i).

3-2. DIRECTOR, CORPORATE COMMUNICATION DIRECTORATE (BEC). BEC shall:

a. Develop, monitor, and maintain DeCA's current and future SNS.

b. Maintain a registry of DeCA's official external presences.

c. Publish guidance for responsible and effective use of DeCA's current and future SNS.

d. Monitor and evaluate DeCA's current and future SNS to ensure compliance with security requirements and to detect fraudulent or objectionable use as discussed in Reference (i); DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1, 1982, (Reference (j)); and DoDD 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008, (Reference (k)), in conjunction with DeCA's Chief Information Officer (CIO) and Operations and Policy Directorate. Suspected fraudulent or criminal activity will be reported to the DeCA's Inspector General (IG).

e. Provide advice, guidance, and assistance to ensure DeCA's current and future SNS are used responsively, effectively, and IAW the DoD Social Media User Agreement (http://www.defense.gov/socialmedia/user-agreement.aspx) and DeCAD 100-1 "Defense Commissary Agency Public Affairs Program," February 26, 1993, (Reference (l)).

f. Follow Reference (l) guidelines when uploading news, information, editorials, photographs, videos, and other media products and when responding to comments and questions on DeCA's current and future SNS

g. Ensure DeCA's current and future SNS comply with all references in this Manual and:

(1) Use DeCA's official seal IAW Reference (l).

(2) Include DeCA's mission statement as directed in Reference (l).

(3) Create a link to DeCA's official website on DeCA's current and future SNS, where appropriate.

(4) Ensure information posted on DeCA's current and future SNS is relevant and accurate.

(5) Ensure information does not contain PII and information discussed in DeCAD 80-21, "Privacy Act Program," April 15, 2010, (Reference (m)).

(6) Remove posts that contain PII or operationally sensitive information, are offensive, or are not in keeping with the DoD Social Media User Agreement.

(7) Provide links to official DoD content, hosted on DoD websites, where applicable.

(8) Ensure posts are free of advertisement and endorsements as mandated by Reference (l).

3-3. DECA'S CHIEF INFORMATION OFFICER (CIO). The CIO shall:

a. Configure DeCA's network to provide access to IbC IAW all references cited in this Manual, except where explicitly prohibited by DoD policy or law.

b. Defend DeCA's network against malicious activity: e.g., distributed denial of service attacks, intrusions; and take immediate and commensurate actions as required to safeguard the mission by temporarily limiting access to the Internet to preserve OPSEC or to address bandwidth constraints.

c. Ensure implementation, validation, and maintenance of applicable IA controls and information security procedures are in place IAW References (h), (i), and DeCAD 35-31, "Information Assurance," December 14, 2009, (Reference (n)).

d. Make reference to this manual in IA education, training, and awareness activities.

e. In consultation with BEC, establish processes and procedures to ensure use of IbC complies with applicable mandates, such as Section 508 of the Rehabilitation Act of 1973; Reference (f); and the Federal Records Act.

f. Act as the final authority for defining DeCA's Information Technology (IT) security requirements and policies to ensure compliance with DoD policy and law and on how DeCA's IT will be operated.

g. Monitor emerging IbC in order to identify opportunities for use and assess risks IAW Reference (n).

3-4. OFFICE OF THE INSPECTOR GENERAL/SECURITY. Security shall:

a. Ensure implementation, validation, and maintenance of applicable OPSEC measures are in place, IAW with Reference (g).

b. Develop procedures and guidelines for OPSEC reviews of information shared via IbC, based on those developed by the USD(I).

c. In conjunction with the CIO's Computer Network Defense Service Provider Program, develop and maintain threat estimates on current and emerging IbC.

3-5. GENERAL COUNSEL (CCG). The CCG shall:

a. Provide guidance and direction to Agency officers, BEC, and employees concerning:

(1) The application of paragraph 2-301 of Chapter 2 of the Joint Ethics Regulation.

(2) The use of IbC to promote the principles of The Freedom of Information Act.

(3) The protection of PII as prescribed by the Privacy Act.

b. In conjunction with BEC, monitor the use of DeCA's current and future SNS to ensure use complies with paragraph 2-301 of Chapter 2 of Reference (f), the "Freedom of Information Act," as amended, Section 552 of Title 5, United States Code (Reference (o)), and DeCAD 5-2, "Records Management Program," August 28, 2007, (Reference (p)).

c. Provide guidance and advice to managers and first-line supervisors concerning the appropriate action to take for violations of this Manual.

d. Review BEC's comments and responses prior to posting IAW DeCAD 80-4, "Litigation Involving DeCA," January 1, 1992, (Reference (q)).

3-6. HEADS OF ALL DIRECTORATES. Heads of all directorates shall:

a. Ensure employees assigned to their directorates:

(1) Read and understand this Manual and Reference (a).

(2) Complete the latest DoD social networking training at: http://iase.disa.mil/eta/sns_v1/sn/launchPage.htm, "Social Networking V1.0," and keep the original certificate of completion at his or her workstation.

(3) Understand employees are not to access prohibited sites via the Internet: e.g., pornography, gambling, game sites, and hate-crime related IbC.

b. Monitor their employee's use of IbC.

c. Advise against accessing sites with prohibited content as described above.

3-7. DeCA Employees at All Levels of the Agency. All employees shall:

a. Read and understand the policies and procedures set forth in this Manual and Reference (a).

b. Complete the latest DoD social networking training at: http://iase.disa.mil/eta/sns_v1/sn/launchPage.htm, "Social Networking V1.0," and keep the original certificate of completion at his or her workstation.

c. Comply with the policies, procedures, and guidelines in all references cited in this Manual.

d. Ensure all use of IbC complies with paragraph 2-301 of Chapter 2 of Reference (f) and guidelines set forth in Chapters 1 to 4 of that reference.

e. Not access or engage in prohibited activity via IbC as annotated in this Manual and its references, as well as Reference (a) and its references.

f. Immediately report suspicious activity on any of DeCA's IbC to the CIO, BEC, and DeCA's Security Officer.

g. Report suspected fraud, waste, and abuse or criminal activity on any of DeCA's current and future SNS to the IG.

3-8. MANAGEMENT CONTROL SYSTEM. This Manual contains internal management control provisions that are subject to evaluation and testing as required by Reference (b).

3-9. RELEASABILITY – UNLIMITED. This Manual is approved for public release and is located on www.commissaries.com and DeCA's intranet website, OneNet.

GLOSSARY

DEFINITIONS

Agency designee. Defined in the Joint Ethics Regulation to mean the first-line supervisor, who is a commissioned military officer or a civilian above GS/GM 11 in the chain of command, or supervision of the DoD employee concerned. Except in remote locations, the Agency Designee may act only after consultation with his local Ethics Counselor.

authorized users. DeCA employees whose use of IbC is necessary for the performance of their official duties are considered authorized users; those who are not are those whose access has been taken away for noncompliance with the directive, manual, and references.

Facebook. A social networking site (SNS) where individuals and organizations can create and customize their own profiles; create their own pages, using photos, videos, and information about themselves and send e-mail or instant message with other members.

Flickr. An image and video hosting and sharing website, Web services suite, and online community platform.

Internet-based Capabilities (IbC). All publicly accessible information capabilities and applications available across the Internet in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. IbC include collaborative tools such as social network service (SNS), social media, user-generated content, social software, e-mail, instant messaging, and discussion forums: e.g., DeCA's YouTube, Facebook, Twitter, and Flickr pages.

social networking service (SNS). A social network service or social networking service, most often called SNS, is a medium for establishing social networks of people who share interests and/or activities. SNS allow users to share ideas, activities, events, and interests within their individual networks. Most social network services are Web based and allow users to build online profiles, share information, pictures, blog entries, music clips, etc.

social media. Media for social interaction, using highly accessible and scalable publishing techniques. Social media use Web-based technologies to transform and broadcast media monologues into social media dialogues.

Twitter. An online SNS where members can post short updates and keep up with other members through online profiles or cell phone text messages.

YouTube. A social networking site where members can post and share videos, comment on videos, and respond to videos. Organizations can create channels to post videos.

GLOSSARY

ACRONYMS

CEO	Chief Executive Officer
CIO	DeCA's Chief Information Officer
DeCA	Defense Commissary Agency
DeCAD	Defense Commissary Agency Directive
DeCAM	Defense Commissary Agency Manual
DoD	Department of Defense
DTM	directive-type memorandum
CCG	General Counsel
IA	Information Assurance
IAW	in accordance with
IbC	Internet-based Capabilities
IG	Inspector General
IT	information technology
BEC	Corporate Communication Directorate
OPSEC	Operations Security
PII	personally identifiable information
USD(I)	Under Secretary of Defense for Intelligence
SNS	social networking service