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

DIRECTIVE

Social Media

DeCAD 100-04
May 15, 2012

Corporate Communication Directorate
OPR: DeCA/BEC

References: See Enclosure 1

1. PURPOSE. This Directive:

a. Recognizes that Internet-based Capabilities (IbC) are integral to operations across the Agency, providing its employees with the latest technologies that enable them to connect and communicate with each other, customers, and Industry partners in the performance of their official duties. This Directive establishes policy and assigns responsibilities for the responsible and effective use of IbC, including social networking service (SNS) for all employees at all levels of the Agency. This Directive also explains how current and future Defense Commissary Agency (DeCA) SNS are to be used and managed to effectively reach DeCA's strategic communication goals as described in DeCA Directive (DeCAD) 100-1, "Defense Commissary Agency Public Affairs Program," February 26, 1993, (Reference (a)), implementing Department of Defense (DoD) Directive-Type Memorandum (DTM) 09-026, "Responsible and Effective Use of Internet-based Capabilities," Change 4, May 9, 2012, (Reference (b)). This Directive serves as policy and guidance for all DeCA employees who use IbC.

b. Establishes DeCA's Social Media Manual (DeCAM) 100-04.1, May 7, 2012, **(**Reference (c)) as a tool to implement its policy on the use of IbC and SNS by its employees.

c. Is established in compliance with all references listed in Enclosure 1.

2. APPLICABILITY. This Directive applies to all 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.

3. POLICY. It is DeCA policy that:

a. In accordance with (IAW) Reference (b), DeCA's Non-classified Internet Protocol Router Network (NIPRNet) will be configured to provide all employees at all levels of the Agency access to IbC, as necessary for the performance of their official duties.

b. DeCA's official SNS, such as: Facebook, Twitter, YouTube, and Flickr will be developed, monitored, and maintained by the Corporate Communication Directorate (BEC). It will be used to enhance DeCA's strategic communication goals IAW the provisions of Reference (a), and "The Freedom of Information Act, as amended, Section 552 of Title 5, United States Code," (Reference (d)).

c. Only the Director and CEO can authorize the creation of an official SNS for the Agency.

d. DeCA employees may create personal social media pages, using personal resources, and may use government resources to access social media pages for limited personal use, as set forth in DeCA Handbook 50-6, "Civilian Employee Handbook," March 25, 2011, (Reference (e)).

e. Whether DeCA employees are using their personal resources, or government resources, they will not present themselves as an official representative of the Agency, create the appearance of being an official representative of the Agency, or use information obtained in their official capacity on any social media pages.

f. Employees must comply with Reference (b) and paragraph 2-301 of chapter 2 of DoD 5500.7-R, "Joint Ethics Regulation (JER)," November 17, 2011, (Reference (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.

g. When accessing IbC, individuals shall employ sound OPSEC measures IAW DoD Manual 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008, (Reference (g)); and shall not represent the policies or official position of DoD or DeCA.

h. No information shall be released on any SNS by a DeCA employee when disclosure would adversely affect national security; violate the safety or privacy of U.S. Government installations, facilities, personnel or their families; violate the privacy of citizens of the United States; or post personally identifiable information (PII), confidential financial information, or proprietary information. Information posted on SNS, by employees, will comply with DoD policy for dissemination of information and Reference (f).

i. PII will not be collected without the users' explicit knowledge and consent, and no PII will be stored or retrieved without first complying with DeCAD 80-21, "Privacy Act Program," April 15, 2010, (Reference (h)).

j. Comments and responses on DeCA's official SNS will be managed, stored, and disposed of IAW DeCAD 5-2, "Records Management Program," August 2007, (Reference (i)), and IAW any additional guidance from DeCA's Chief Information Officer (CIO).

k. The CIO has final say on how DeCA's information technology (IT) will be operated.

l. Management, at all levels, will monitor the use of IbC from government communication devices by their subordinates, to ensure employees are complying with guidelines set forth in Reference (c) and take appropriate action when guidelines are violated, IAW Reference (e).

m. Management, at all levels, will ensure use of IbC from government equipment complies with References (f) and (h); and take appropriate action if such guidelines are violated, IAW Reference (e).

n. Agency employees using IbC from government communication devices must complete the latest DoD social networking training at: http://iase.disa.mil/eta/sns_v1/sn/launchPage.htm, "Social Networking V1.0," prior to gaining access, keeping the original certificate of completion at his or her workstation. Employees who already have access to IbC, and have not completed this training, must do so.

4. RESPONSIBILITIES. The following DeCA directorates are responsible for establishing and maintaining policies, procedures, guidelines, training, etc., as directed in Reference (b) and IAW all other references noted in Enclosure 1.

a. Director, Corporate Communication Directorate. BEC shall:

(1) Develop, monitor, and maintain DeCA's current and future official SNS.

(2) Maintain a registry of DeCA's official external presences.

(3) Publish guidance for responsible and effective use of DeCA's official SNS.

(4) 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 (b), DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1, 1982, (Reference (j)); and DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008, (Reference (k)); and in conjunction with guidance from the CIO and Store Operations Directorate. Suspected fraudulent or criminal activity will be reported to DeCA's Office of Inspector General/Security (CCI).

(5) Provide advice, guidance, and assistance to ensure DeCA's current and future SNS are used responsibly, effectively, and IAW the DoD Social Media User Agreement (http://www.defense.gov/socialmedia/user-agreement.aspx) and Reference (a).

(6) Follow Reference (a) 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.

(7) Ensure DeCA's current and future SNS comply with references in this Directive and:

(a) Use DeCA's official seal IAW Reference (a).

(b) Include DeCA's mission statement, as directed in Reference (a).

(c) Create a link to DeCA's official Web Site on DeCA's current and future SNS, where appropriate.

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

(e) Ensure information posted does not contain PII and information discussed in Reference (h).

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

(g) Provide links to official DoD content, hosted on DoD Web Sites, where applicable.

(h) Ensure posts are free of advertisement and endorsements, as mandated by Reference (a).

b. DeCA's Chief Information Officer. The CIO shall:

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

(2) 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 operations security (OPSEC) or to address bandwidth constraints.

(3) Ensure implementation, validation, and maintenance of applicable Information Assurance (IA) controls, and information security procedures, are in place IAW DeCAD 35-39, "Computer Network Defense," December 14, 2009, (Reference (l)); DoD Directive 8500.01E, "Information Assurance," certified current as of April 23, 2007, (Reference (m)); and DeCA Directive 35-31, "Information Assurance," December 14, 2009, (Reference (n)).

(4) Make reference to Reference (c), in IA education, training, and awareness activities.

(5) 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 and the Federal Records Act.

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

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

c. Office of Inspector General/Security. CCI shall:

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

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

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

d. General Counsel (CCG). The CCG shall:

(1) Provide guidance and direction to Agency officers, BEC, and employees concerning:

(a) The application of paragraph 2-301 of Chapter 2 of the Joint Ethics Regulations.

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

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

(2) In conjunction with BEC, monitor the use of DeCA's current and future SNS to ensure use complies with Reference (d) paragraph 2-301 of Chapter 2 of Reference (f) and with Reference (i).

(3) Provide guidance and advice to managers and first-line supervisors concerning the appropriate action to take for violations of this Directive.

(4) Review BEC's comments and responses IAW DeCAD 80-4, "Litigation Involving DeCA," January 1, 1992, **(**Reference (o)).

e. Heads of all directorates/special staff offices shall:

(1) Ensure employees assigned to their directorates:

(a) Read and understand this Directive and Reference (c).

(b) Complete the latest DoD social networking training at: http://iase.disa.mil/eta/sns_v1/sn/launchPage.htm, "Social Networking V1.0," prior to gaining access, keeping the original certificate of completion at his or her workstation. Employees who already have access to IbC, and have not completed this training, must do so.

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

(2) Monitor their employee's use of IbC.

(3) Advise against accessing sites with prohibited content, as described above.

f. DeCA employees at all levels of the Agency shall:

(1) Read and understand the policies and procedures set forth in this Directive and Reference (c).

(2) Complete the latest DoD social networking training at: http://iase.disa.mil/eta/sns_v1/sn/launchPage.htm, "Social Networking V1.0," prior to gaining access, keeping the original certificate of completion at his or her workstation. Employees who already have access to IbC, and have not completed this training, must do so.

(3) Comply with the policies, procedures, and guidelines in all references cited in this Directive.

(4) 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.

(5) Not access or engage in prohibited activity via IbC as annotated in this Directive and its references, as well as Reference (c) and its references.

(6) Immediately report suspicious activity on any IbC to the CIO and suspicious activity on any of DeCA's current and future SNS to BEC and DeCA's Security Officer.

(7) Report suspected fraud, waste, and abuse, or criminal activity on any of DeCA's current and future SNS to the CCI.

5. RELEASABILITY – UNLIMITED. This Directive is approved for public release and is located on DeCA's Internet Web Site at www.commissaries.com and on OneNet.

6. EFFECTIVE DATE. By order of the Director of DeCA, this Directive is effective immediately.

Teena P. Standard
Chief, Executive Services Division

Enclosure
References
Glossary – Definitions
– Acronyms

ENCLOSURE 1

REFERENCES

(a) DeCA Directive 100-1, "Defense Commissary Agency Public Affairs Program," February 26, 1993
(b) Directive-Type Memorandum (DTM) 09-026, "Responsible and Effective Use of Internet-based Capabilities," (Change 4), May 9, 2012[1]
(c) DeCA Manual 100-04.1, "Social Media Manual," May 9, 2012
(d) The Freedom of Information Act, as amended, Section 552 of Title 5, United States Code[2]
(e) DeCA Handbook 50-6, "Civilian Employee Handbook," March 25, 2011
(f) DoD 5500.7-R, "Joint Ethics Regulation," November 11, 2011[3]
(g) DoD Manual 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008
(h) DeCA Directive 80-21, "Privacy Act Program," April 15, 2010
(i) DeCA Directive 5-2, "Records Management Program," August 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 35-39, "Computer Network Defense," December 14, 2009
(m) DoD Directive 8500.01E, "Information Assurance," certified current as of April 23, 2007
(n) DeCA Directive 35-31, "Information Assurance," December 14, 2009
(o) 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/

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). As defined by the Department of Defense (DoD): All publicly accessible information capabilities and applications available across the Internet in locations not owned, operated, or controlled by the DoD 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	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
CCI	Inspector General
IA	Information Assurance
IAW	in accordance with
IbC	Internet-based Capabilities
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