Defense Logistics Agency

INSTRUCTION

DLAI 8550.01
Effective May 14, 2013

DP

SUBJECT: Social Media

References: Refer to Enclosure 1.

1. PURPOSE. This Instruction:

a. Establishes policy, assigns responsibilities and provides procedures concerning DLA-sanctioned internal and external social media applications and accounts in accordance with the authority in Reference (a).

b. Supersedes Chief Information Office, DLA Memorandum, “Social Networking Web Sites and Web 2.0 Technologies in DLA,” September 11, 2009 (Reference (b).

c. Identifies DLA social media as a component of Web 2.0 at DLA, and addresses internal social media and external social media.

d. Ensures the usage of internal and external applications comply with existing Department of Defense (DOD) and DLA policies and procedures, to include Operations Security (OPSEC) and Information Assurance (IA) cited in Enclosure 1.

e. Provides DLA an innovative and economical mode of public communication that grows Agency visibility and transparency while fostering greater public trust.

f. Promotes customer and stakeholder awareness of, and participation in, two-way communication processes (e.g. discussion, questions and answers, issue resolution), thereby increasing the knowledge and advocacy of defense logistics.

g. Escalates Web traffic to DLA.mil and other stakeholder and customer sites, enabling DLA to engage the public, reach new demographics through mainstream applications, and promote DLA.

h. Positions DLA to better integrate future internal and external social media applications and technologies.

i. Inspires greater interagency, public, customer, and stakeholder relations while educating participating audiences and putting a dynamic and engaging face on DLA and Defense logistics.

j. This Instruction shall be communicated to the DLA Enterprise and enforced at all DLA sites to standardize and streamline policies governing social media usage at DLA.

2. APPLICABILITY. This Instruction:

a. Applies to all of DLA for official social media use regardless of activity location, platform, time, place or device.

b. It does not apply to unofficial personal social media accounts used during non-duty hours or social media use on personal devices.

3. DEFINTIONS.

a. Social media is Web applications that facilitate interactive information sharing, interoperability, user-centered design, and collaboration on the World Wide Web.

b. Internal social media consists of thin (server-based) or thick (client-based installed on user devices) applications that are Agency-owned and not accessible to the general public (e.g. PeoplePages, Defense Technology Information Center, Techpedia, or Wikis).

c. External social media consists of thin or thick applications that are not Agency-owned, and are accessible by the general public (e.g. Facebook, Twitter, YouTube).

4. POLICY. It is DLA policy that:

a. The DLA Public Affairs Directorate (DP) maintains and enforces the DLA Social Media Program for the development, coordination, approval, operation and periodic review of DLA social media platforms and sites in accordance with this instruction. This work is performed in coordination with the DLA Social Media Working Group (SMWG), but in times of emergent circumstances the DLA Social Media Program Manager (PM) shall have the authority to change, edit, moderate, remove or close any posts, comments, photos, videos, or other materials on DLA-operated social media sites, regardless of owner. The PM shall also, in emergent situations, have authority to close DLA social media sites, irrespective of owner.

b. DLA social media platforms and sites shall consist of those internal and external internet based capabilities as defined by DODI 8550.01, DoD Internet Services and Internet-Based Capabilities (Reference (a)).

c. Civilian, military, and contractor personnel who work in support of DLA shall adhere to the general, internal, and external social media tenets as described in this Instruction when using social media in their official capacity, from DLA provided equipment or on a DLA official platform or site.

d. All DLA social media site managers, administrators and moderators shall comply with this Instruction, its requirements and principles as defined in Enclosure 2.

e. Operations and information security (OPSEC and INFOSEC), privacy and personally identifiable information (PII) requirements shall be exactingly enforced. Failure to meet these requirements is cause for platform closure in accordance with Enclosures 3 and 4.

f. Each site manager, administrator and moderator shall complete the required training for operation of a DLA social media site and certify completion using DLA Form 1940-1, Social Media Certification. Information Assurance and PII training requirements shall be recertified yearly.

5. RESPONSIBILITIES. Refer to Enclosure 2.

6. PROCEDURES. Refer to Enclosure 3.

7. INFORMATION REQUIREMENTS.

a. Below are the information requirements for requesting and operating an official DLA social media platform.

(1) DLA Form 1940, Social Media Application.

(2) DLA Form 1940-1 and the training it represents, is required for each site manager, administrator and moderator.

Note: An electronic verion of DLA Form 1940 and DLA Form 1940-1 are available on the DLA Forms Management Program Web Site at http://www.dla.mil//dss/forms.

(3) Communications plan detailing proposed site, communication and business objectives, posting calendar(s), site manager, administrator, and moderator(s). This plan shall be completed and provided to the DLA Social Media Working Group for each individual site requested. Group communication plans and applications shall not be approved. Refer to Enclosures 3 and 4.

b. The DLA Public Affairs Collaboration Room (eWorkplace) shall serve as the knowledge and information gathering platform for the DLA Social Media Program. The eWorkplace room will:

(1) Display examples of communications plans, training modules, and "how to" aides for social media operations.

(2) Maintain a list of current sites and platforms in operation, along with platform administrators and moderators.

(3) Training information shall NOT be kept as part of this site. No personal contact information or other PII shall be kept as part of the collaboration room.

8. INTERNAL CONTROLS.

a. DLA Form 1940-1 shall be digitally signed by both applicants and their supervisors, indicating the training is complete. Waivers, substitutions, variations and denials determined by the PM and SMWG shall be annotated on the form and maintained for recordkeeping and review purposes.

b. DLA Form 1940 shall be digitally signed by the applicant, the appropriate DLA Public Affairs Officer and the activity authorizing official, indicating knowledge and concurrence with the application. Denials, reviews, and closures by the PM and SMWG shall be annotated on the form and maintained for recordkeeping purposes.

c. All social media platform and site communication plans shall be maintained in the DLA Public Affairs Collaboration Room (eWorkplace) for use in review and retention procedures.

9. RELEASEABILITY. UNLIMITED. This instruction is approved for public release and is available on the Internet from the DLA Issuances Internet Website.

10. EFFECTIVE DATE. This Instruction:

a. Is effective on May 14, 2013.

b. Notionally, the Instruction shall be reviewed and updated bi-yearly to ensure all appropriate social media developments and emergent platforms are accounted for by the Instruction. At minimum, the Instruction shall be reissued, cancelled, or certified current within five years of its publication in accordance with this DLAI 5025.01, DLA Issuance Program. If not, it will expire effective May 14, 2023 and be removed from the DLA Issuances Website.

GOLDENBERG.PHYLLISA.S.1229115878

Digitally signed by GOLDENBERG.PHYLLISA.S.1229115878
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DLA, cn=GOLDENBERG.PHYLLISA.S.1229115878
Date: 2013.05.14 14:27:36 -04'00'

PHYLLISA S. GOLDENBERG
Director, DLA Strategic Plans and Policy

Enclosure(s)
Enclosure 1 – References
Enclosure 2 – Responsibilities
Enclosure 3 – Procedures
Enclosure 4 – Platform Approval and Retirement Processes

ENCLOSURE 1

REFERENCES

(a) DODI 8550.01, DOD Internet Services and Internet-Based Capabilities, Sep 11, 2012
(b) Chief Information Office, DLA Memorandum, Social Networking Web Sites and Web 2.0 Technologies in DLA, September 11, 2009. (Superseded)
(c) DODD 5500.07, Standards of Conduct, November 29, 2007
(d) DODD 5230.9, Clearance of DOD Information for Public Release, August 22, 2008
(e) Message, SECDEF dated 090426Z August 2006, Information Security/Web site Alert
(f) DLA Headquarters, OPSEC: A Guide to Releasing Information to the Public through Websites and other Media, May 21, 2008
(g) DOD Internet Services and Internet-Based Capabilities (IbC), September 11, 2012
(h) DLAI 6406, Web site Development and Administration, October 30, 2009
(i) DLAI 5202, Display of DLA Emblem, September 11, 2009
(j) Information Assurance (IA) Rules of Behavior, March 2, 2010
(k) DLA Style Guide, October 16, 2010
(l) DODI 5400.16, DOD Privacy Impact Assessment (PIA) Guidance, February 12, 2009
(m) Office of Management and Budget, M-10-22 Guidance for Online Use of Web Measurement and Customization Technologies, June 25, 2010
(n) Office of Management and Budget, M-10-23 Guidance for Agency Use of Third Party Web sites and Applications, June 24, 2010
(o) Office of Management and Budget, Social Media, Web-based Interactive Technologies, and the Paperwork Reduction Act, April 7, 2010
(p) DODD 5400.11, DOD Privacy Program, September 1, 2011
(q) DOD (DD) Form 2930A, Adapted PRIVACY IMPACT ASSESSMENT (AD-PIA), August 2011
(r) DOD (DD) Form 2930, Privacy Impact Assessment (PIA), November 2008

ENCLOSURE 2

RESPONSIBILITIES

1. GENERAL. The following responsibilities apply to all DLA for the use of both internal and external social media:

a. Acceptable Usage and Conduct. All employees and contractor staff using DLA internal and external social media applications are expected to use them in a professional and ethical manner.

b. Users shall comply with the following:

(1) Use internal and external social media applications for their deemed purposes. (i.e. Wikis as a knowledge gathering and dissemination platform, Facebook to educate, entertain and promote DLA.)

(2) Policies and guidelines outlined in the DLA Information Assurance (IA) Rules of Behavior (ROB) apply to the use of social media.

(3) DLA employees and contractors shall ensure that all user content associated with internal and external social media applications is consistent with employee work, DLA values, and professional standards.

(4) Social media administrators and moderators shall make every effort to publish user-generated content in its entirety and without editing in order to maintain the meaning, tenor, and nuance. However, they must carefully consider DLA's integrity and standing and shall discard user generated content that:

(a) Contains profanity, vulgarity, "hate speech," allegation, insinuation, or any measure of libelous, defamatory, or offensive language.

(b) Advertises services or products, solicits contributions or private information, or violates the Federal and DOD Web Site Privacy Policy.

(c) Contains or advocates material(s) deemed defamatory, disruptive, false, abusive, libelous, obscene, indecent, lewd, pornographic, harassing, threatening, or violent.

(d) Content containing phone numbers, mailing addresses, email addresses, or other PII shall NOT be posted.

(e) Formal discussions/inquiries with media outlets shall not occur on social media applications.

(f) Official business inquires or issues are not appropriate for social media applications and shall immediately be referred to the proper DLA activity.

2. CONTENT ADMINISTRATORS AND MODERATORS.

a. The DLA Social Media Program is administered through a four level series of managers. The highest of these is the DLA Social Media Program Manager (PM) located in the DLA Office of Public Affairs. The DLA PM oversees the program at the Enterprise level, ensuring compliance with DOD and Federal policies, testing and certifying new platforms and other oversight functions. The PM also operates the Enterprise external and internal platforms and applications.

b. The DLA Social Media Working Group (SMWG) is made up of the PM, the PLFA Social Media Site Managers or their appointed representatives, as well as specific J and D staff (J1, J6 and DG). The SMWG operates at the Enterprise level and represents the concerns of each PLFA and J-code office involved in the program.

c. DLA Social Media Administrators work at the PLFA or J-code level. They are responsible for the oversight of specific social media platforms at those organizations. Administrators may hold responsibility for more than one social media platform. An administrator may hold oversight authority over several platforms and applications operated by social media moderators, yet not actively post to those platforms

d. DLA Social Media Moderators work at the PLFA or J-code level. They are responsible for all aspects of a specific social media platform. Moderators do not hold responsibility for multiple platforms.

(1) The following responsibilities apply to DLA Social Media Administrators for the platforms and applications under their oversight:

(a) Administer social media sites and associated usernames, passwords, and permissions in conjunction with J6 and the site manager.

(b) Monitor social media operations and update internal and external social media applications, content, and contributor databases for their platforms, as needed.

(c) Ensure internal and external social media applications are used to provide accurate and timely information without jeopardizing operational integrity or individuals' right to privacy.

(d) For platforms on which content does not "age out," ensure removal of content according to the expiration date unless otherwise requested by the content owner.

(e) In compliance with DLA recordkeeping policies, ensure content is scheduled for disposition and archive using social media management modules or by means of electronic storage.

(f) Maintain open lines of communication and coordination with J6 and other social media stakeholders regarding system operations and maintenance, recordkeeping, IA, OPSEC/INFOSEC, Freedom of Information (FOIA) and privacy issues, system administration and access privileges, database inclusions/exclusions, public inquiries/complaints and other issues or topics.

(g) Elevate issues concerning internal and external social media applications through the site manager to the SMWG and PM.

(h) Analyze social media capabilities to ensure they are continually viable and conducive to DLA's mission and responsibility to disseminate information for the education and consideration of the public.

(i) In conjunction with J6, review system operating and maintenance plans to ensure ongoing operations and validity.

(j) Notify J6 of errors or technical problems resulting from J6-operated equipment, software, or network security measures.

(k) As requested, attend meetings, training sessions, design/system enhancement sessions, and assist in the updating and developing of system plans and proposals.

(l) As requested, participate in and operate internal and external social media applications during training exercises that test and demonstrate information dissemination capabilities and develop familiarity with the platforms' capabilities amongst content providers, heads of J-codes, and DLA activities.

(m) Ensure all moderators receive training as required in this Instruction to include specialized OPSEC training and DLA annual IA and PII training prior to granting permission operate and to the sites.

(n) Prepare all paperwork and planning documents required by this Instruction and submit paperwork through site managers to the SMWG for consideration.

(2) The following responsibilities apply to DLA Social Media Moderators:

(a) Generate and solicit content (i.e., video, photos, audio and text).

(b) Manage and administer (i.e., accept/deny, standardize, post, deactivate and/or delete) external content submissions.

(c) Ensure that social media content conveys an appropriate message and tone to all audiences.

(d) Ensure that timely and accurate communications are posted to DLA internal and external social media applications.

(e) Ensure that social media content does not compromise DLA or stakeholder operations, or cause undue alarm or speculation within the media and community.

(f) In conjunction with J6, manage DLA Real Simple Syndication feeds as needed.

(g) In conjunction with J6 and social media administrator, supervise all aspects of platform operations.

(h) Ensure platform does not associate advertisements with user home pages except as approved by the DLA General Counsel (i.e. Armed Forces recruiting ads).

(i) In conjunction with J6 and administrator, review system operating and maintenance plans to ensure ongoing operations and validity.

(j) Notify J6 of errors or technical problems resulting from J6-operated equipment, software, or network security measures.

(k) As requested, attend meetings, training sessions, design/system enhancement sessions, and assist in the updating and developing of system plans and proposals.

(l) As requested, participate in and operate internal and external social media applications during training exercises that test and demonstrate information dissemination capabilities and develop familiarity with the platforms' capabilities amongst content providers, heads of J-codes, and DLA Field Activities.

(m) Complete all training required by this Instruction to include specialized OPSEC training and DLA annual IA and PII training prior to granting permission to operate the sites.

(n) Prepare or assist in preparation of applications and planning documents required by this Instruction and submit paperwork through administrator to the SMWG for consideration.

(o) Monitor content of DLA social media accounts operating on external and internal platforms and applications, ensure that content falling under records management requirements is directed away from externally-owned platforms and applications to appropriate offices and/or archive capable systems.

(p) Review all information for OPSEC/INFOSEC concerns prior to posting and ensure DLA's critical information is not posted in a public forum.

(3) The following responsibilities apply to DLA Social Media Site Managers and to accounts under their oversight:

(a) Function as a social media advocate and as an intermediary to authorized agencies/agents who are either practicing or prospective content contributors.

(b) Perform outreach to advance social media capabilities, solicit content submissions, and outline its benefits to the public, governments and commercial logistics organizations.

(c) Develop and steward a directory of authorized agencies/agents permitted to request and/or submit content.

(d) Monitor content of DLA social media accounts operating on external and internal social media platforms and ensure that content falling under records management requirements is directed away from externally owned platforms to appropriate offices and/or archive capable systems.

(e) Perform periodic review of information across site platforms for OPSEC/INFOSEC, privacy and PII to ensure compliance with DOD and DLA policies.

(f) Oversee social media sites and associated usernames, passwords, and permissions in conjunction with administrators and J6.

(g) Oversee social media operations and ensure internal and external social media platforms, content, and contributor databases for platforms are updated.

(h) Ensure internal and external social media applications are used to provide accurate and timely information without jeopardizing operational integrity or individuals' right to privacy.

(i) Maintain open lines of communication and coordination with J6 and other social media stakeholders regarding system operations/maintenance, records keeping, security, FOIA and privacy issues, system administration and access privileges, database inclusions/exclusions, public inquiries/complaints, and other topics and issues.

(j) Elevate issues concerning internal and external social media applications to the SMWG and PM.

(k) Analyze social media capabilities to ensure they are continually viable and conducive to DLA's mission and responsibility to disseminate information for the education and consideration of the public.

(l) In conjunction with administrators, moderators and J6, review system operating and maintenance plans to ensure ongoing operations and validity.

(m) Ensure J6 receives notification of errors or technical problems resulting from J6-operated equipment, software, or network security measures.

(n) Receive all training on topics including, but not limited to, account creation, maintenance, and management of all internal and external social media applications as established by the DLA Social Media Instruction.

(o) As required, attend meetings, training sessions, design/system enhancement sessions, and assist in the updating and developing of system plans and proposals.

(p) As required, participate in and operate internal and external social media applications during training exercises that test and demonstrate information dissemination capabilities and develop familiarity with the platforms' capabilities amongst content providers, heads of J-codes, and DLA Field Activities.

(q) Complete mandatory training as outlined in this Instruction to include specialized OPSEC training and DLA annual IA and PII training. Ensure all social media administrators and moderators also complete mandatory training prior to granting permission to operate the sites.

(r) Review all paperwork and planning documents submitted for consideration by the SMWG (Enclosures 3 and 4).

(4) The following responsibilities apply to the DLA SMWG who shall:

(a) Develop and enforce all policies, operating procedures, requirements and other necessary administrative documents and measures for the operation of the DLA Social Media Program.

(b) Be chaired by the PM.

(c) Review, discuss and approve or reject all applications for social media platforms, internal and external in operation at DLA.

(d) Evaluate use of new or additional internal and external social media applications semiannually or more frequently as needed. This process is defined in the Application and Approval of Social Media Topics and Media Process Flow (Enclosures 3 and 4).

(e) Maintain a repository which includes accurate metacontent, creation date, audit dates, and points of contact for all internal and external social media planning documents and applications.

(f) Conduct an audit of existing media and planning documents semiannually or more frequently as needed, and retire platforms it finds unnecessary or inactive. This process is defined in the Retirement of Social Media Topics and Media Process Flow (Enclosures 3 and 4).

(g) Other roles and responsibilities of the SMWG and its members shall be further defined in the group charter.

(5) The following responsibilities apply to the DLA Social Media Program Manager:

(a) Oversee development and enforcement of all policy, operating procedures, requirements and other necessary administrative documents and measures for the operation of the DLA Social Media Program.

(b) Chair the SMWG.

(c) Provide final review and approval/rejection of all applications for social media platforms, internal and external in operation at DLA.

(d) Propose new or additional internal and external social media applications for evaluation as needed. This process is defined in the Application and Approval of Social Media Topics and Media Process Flow (Enclosures 3 and 4).

(e) Ensure the SMWG maintains a repository which includes accurate metacontent, creation date, audit dates, and points of contact for all internal and external social media planning documents and applications.

(f) Ensure and certify audits of existing media and planning documents are preformed semiannually or as needed, and that platforms found unnecessary or inactive are retired. This process is defined in the Retirement of Social Media Topics and Media Process Flow (Enclosure 3 and 4).

(g) Serve as the primary source of research and development of new platforms. Ensure all platforms adopted are viable and conducive to DLA's mission and responsibility to disseminate information for the education and consideration of the public.

(h) Analyze social media content and capabilities to ensure they are viable and conducive to DLA's mission and responsibility to disseminate information for the education and consideration of the public.

(i) Function as a social media advocate and as an intermediary to authorized agencies/agents who are either practicing or prospective content contributors.

(j) Perform outreach to advance social media capabilities, solicit content submissions, and outline its benefits to the public, governments and commercial logistics organizations.

(k) Develop and steward an Enterprise directory of authorized agencies/agents permitted to request and/or submit content.

(l) Monitor content of all DLA social media accounts operating on external and internal platforms and applications, ensure that content falling under records management requirements is directed away from externally owned platforms to appropriate offices and/or archive capable systems.

(m) Perform periodic review of information across Enterprise social media platforms for OPSEC/INFOSEC, privacy and PII to ensure compliance with DOD and DLA policies.

(n) Oversee maintenance of a database of all social media sites and associated usernames, passwords, and permissions in conjunction with J6, site managers and administrators.

(o) Oversee social media operations and ensure internal and external applications, content, and contributor databases for all platforms are updated. Operate official Enterprise platforms and applications as laid out in this Instruction.

(p) Ensure internal and external social media applications are used to provide accurate and timely information without jeopardizing operational integrity or individuals' right to privacy.

(q) Maintain open lines of communication and coordination with J6 and other stakeholders regarding system operations/maintenance, records keeping, security, FOIA and privacy issues, system administration and access privileges, database inclusions/exclusions, public inquiries/complaints and other issues and topics.

(r) Ensure resolution of issues concerning internal and external platforms and applications brought to the SMWG.

(s) Develop and certify all training on social media including, but not limited to, account creation, maintenance, and management of all internal and external social media applications as established by this Instruction.

(t) Sponsor meetings, training sessions, design/system enhancement sessions, and assist in the updating and developing of system plans and proposals.

(u) Sponsor and participate in and operate internal and external social media applications during training exercises that test and demonstrate information dissemination capabilities and develop familiarity with the platforms' capabilities amongst content providers, heads of J-codes, and DLA activities.

(v) Ensure all social media site managers, administrators and moderators receive training as required by this Instruction to include specialized OPSEC training and DLA annual IA and PII training prior to granting permission to operate the sites.

ENCLOSURE 3

PROCEDURES

1. ADMINISTRATION:

a. General. Procedures apply to both external and internal social media platforms and applications.

(1) Employee and Department Access. Access is granted to all social media applications using DLA approved Government-furnished mobile devices (mobile access must be in accordance with the DLA Mobile Device Policy). Internal sites shall be accessed using DLA Juniper or Citrix Virtual Private Networks (VPN).

(a) Common Access Card (CAC) authentication is required to access internal social media applications.

(b) Users shall access internal social media applications using their DLA domain account (e.g., john.doe@dla.mil).

(2) Account Management. For all social media account or access issues occurring when using DLA-provided equipment, users shall initially contact the DLA help desk. If the DLA help desk indicates the issues is with the platform or site, and platform or application access is required immediately the user should attempt to contact the platform or application business operations using alternate means. However, this is most often unsuccessful as these entities are largely Web-based.

(3) External Social Media Applications. The following applies to the use of external social media specifically.

(a) External Official Presences. External official presences shall follow the DOD policy established in DTM 09-026, Responsible and Effective Use of Internet-based Capabilities.

(b) Acceptable Usage and Conduct. Users shall adhere to the terms of use established by external social media applications and approved for Federal government use by the Government Services Administration.

b. Managers and Governing Bodies. The following applies to persons or groups responsible for posting, reviewing, and editing official content for both internal and external social media applications or governing the direction of those applications. The PM and SMWG:

(1) Govern and evaluate the use of internal and external social media applications.

(2) Approve the administrators, moderators and social media platforms/applications for internal and external use.

(3) May remove content administrators, moderators or close sites for violations to this Instruction.

(4) Additional information and procedures concerning the Social Media Working Group can be found in the Social Media Working Group Roles and Responsibilities (Enclosure 2) and Social Media/Topic Approval and Retirement Process Flows (Enclosure 4).

c. DLA Provided Equipment. Administrators and moderators manage internal and external social media applications using DLA-issued laptops and mobile devices in accordance with the DLA Mobile Device Policy.

(1) While not preferred, administrators and moderators may also manage external social media applications using personal laptops or mobile devices. This is permitted when administrators and moderators:

(a) Have completed training that instructs users on how to properly administer social media content, including precautions on personal laptop and mobile device use.

(b) Are posting while logged in using the official DLA account. The administrator/moderator shall, if possible, not post content from an alternate account on behalf of DLA.

(c) Does not remain logged in after posting activities (i.e., logs out when finished).

(2) It is recommended that personal devices used to manage external social media applications use password, PIN, or other security mechanisms in order to prevent access in the event of loss.

(3) Devices shall not store user names and passwords for either the official DLA account or those that are used to post on behalf of DLA.

d. Authorized Contributors. The follow apply to persons authorized to submit and edit content for internal and external social media applications. Contributions may include articles, visual or graphic information that further develops knowledge of the DLA Enterprise, stimulates discussion and debate on logistics or related topics, or adds to the dialogue surrounding the evolution and expansion of the military services, DOD or the logistics field.

(1) Organizations may request permission to provide site content by emailing the appropriate administrator or moderator. Such requests should explain the organization’s mission and roles in support of Defense or other Federal logistics, acquisition, or related fields. The administrator or moderator shall review and approve or deny the organization’s request, or request additional information as necessary.

(2) Organizations authorized to submit content to internal and external social media applications shall:

(a) Ensure submissions follow content and submission guidelines for the intended social media application as provided by this Instruction.

(b) Submit supporting documentation, including:

1. Point(s) of Contact (POC).

2. Content synopsis identifying information.

3. Organization permission to disseminate.

4. Date of deactivation (if applicable).

(c) Notify the social administrator or moderator if disseminated content changes, is incorrect, is conflicting, or becomes outdated or canceled.

(3) Content shall be adequately edited and/or cropped and formatted to allow for easy dissemination and viewing. Submitting organizations are responsible for obtaining approval to release video/still images of non-Governmental persons (e.g., volunteers and private citizens).

2. CONTENT MANAGEMENT:

a. Conducting Official Business. In accordance with DOD and DLA policy, all official information on Defense business activities must be archivable for a minimum of two years and compliant with FOIA. In order to ensure DLA social media platforms and sites comply with this requirement:

(1) Contract offerings, business opportunities, and job postings shall NOT use social media applications as the primary method of distribution and dissemination. Such material and information shall initially be posted on official websites and pages approved by DOD or other appropriate Federal agency. For example, position vacancies – USA Jobs; contract solicitations – FedBizOps.

(2) General solicitations and announcements may be provided through a link to an official DLA, DOD, General Services Administration (GSA) or other site.

(3) Contract, business, and job solicitations from the public submitted through social media sites shall be directed to route their request through official channels.

(4) Contract, business, and job solicitations from individuals who continue to attempt the solicitation or conduct of business with DLA through social media shall be contacted directly by the site administrator or moderator and provided the correct information to proceed appropriately. Individuals who ignore the direction provided may be blocked from the platform at the discretion of the administrator or moderator.

(5) Requests for official information received through social media sites: i.e. “how to do business with DLA” shall be directed to the appropriate directorate, office or DLA activity for response.

(6) Official business shall NOT be conducted over DLA social media sites solely or primarily.

b. Location-based Tagging. Broadcasting Global Positioning System (GPS) coordinates and/or locations on official social media platforms and sites is strictly prohibited. It is also strongly discouraged on personal sites for reasons of personal safety. All mobile device GPS settings must be disabled before accessing internal and external social media applications

(1) Social media application location settings shall be disabled before any content is posted. This includes but is not limited to text, photos, videos or “check in” applications.

(2) DLA employees and contractor staff are strongly discouraged from tagging or associating posted content with DOD or DLA facilities (i.e., John Doe creates a “check in” for DLA Headquarters on Facebook).

(3) DLA employees and contractor staff are strictly forbidden from tagging or associating posted content with secure government facilities. (i.e. special operator facilities or enclosures)

(4) DLA shall NOT create, maintain or sponsor any promotional or challenge-oriented competitions that encourage associations between employees, contractor staff, or the public and a DOD/DLA facility or activity through the use of location-based services (i.e., “checking in” on Foursquare or Facebook).

c. Style Requirements.

(1) Emblems, graphics, and colors shall adhere to DLA Instruction 5202, “Use of the Defense Logistics Agency (DLA) Emblem and Associated Visual and Graphic Products, February 2012 (Reference (i)) and the DLA Style Guide, February 2012 (Reference (k)), and shall be applied to social media pages in a manner and style reflective of DLA, its reputation and status. On internal platforms the style sheet shall be reflective of DLA Today.

(2) Any deviations from the standards established in the DLA Style Guide require prior submission of a draft rendering and consent or waiver from DLA Public Affairs. The request is submitted by email to Interact@dla.mil.

d. Archive and Recordkeeping Policy.

(1) Social media administrators and moderators, working in conjunction with DLA Recordkeeping, shall utilize schedules of record disposition for management of social media content (e.g., video, photos, audio and text).

(2) When required, administrators and moderators shall work with J6 for appropriate archiving and storage solutions to retain content, or retire content as determined necessary by DLA and DOD policies.

(3) Social media recordkeeping schedules are not stand alone items and shall be part of the recordkeeping schedules of the platform proponent office. Social media administrators and moderators are responsible for recordkeeping requirements.

(4) Copies of recordkeeping schedules shall be provided to the site manager upon approval by the DLA Records Manager and copies maintained as part of the DLA eWorkplace Public Affairs collaboration room.

e. Photo Tagging Policy.

(1) Photos posted to external social media sites, and not currently approved for public release by the originating organization, shall be approved for posting by the appropriate site manager. Photo tagging shall NOT be routinely used on DLA social media sites. Exception to this policy may be allowed when the individual pictured is a public figure, such as a DLA activity director or senior enlisted member.

(2) Individuals tagged in photos may request tag removal by providing a written or email request for such. No reason is required.

(3) All internally and externally operated DLA social media accounts shall disable any facial or structural recognition settings that automatically tag photos.

f. Photos, videos, graphics, posts, comments, and other materials deemed inappropriate by the site manager or PM shall be removed upon request. In emergent situations, if the platform moderator or administrator is unavailable the site or PM shall have the authority to remove the information.

g. Official Federal content engines (e.g., DLA.mil or Defense or Federal newsfeeds) or other suitable and approved information assets shall be leveraged to post content to external social media when available and appropriate.

3. <u>SECURITY</u>:

a. Only unclassified information shall be posted.

b. If a social media account is compromised the appropriate security personnel shall be notified in accordance with site computer security incident handling procedures. Immediate remediation must occur.

c. Monitoring of unauthorized external DLA social media accounts is a cooperative effort between the PM, SMWG, site managers, administrators, moderators, OPSEC/INFOSEC and J6. Discovery of unauthorized sites shall be reported to the appropriate site manager or in instances of possible fraud, espionage or illegal activities to the appropriate security or law enforcement office. All such instances shall be reported up the chain of command to the SMWG and PM.

d. Where possible, passwords for external social media application accounts shall meet the minimum DOD/DLA password requirements and change every 30 days.

4. PRIVACY: Personally Identifiable Information.

(a) DLA shall not solicit or collect specific PII as defined in DODD 5400.11, DOD Privacy Program, September 1, 2011 (Reference (p)), acknowledging that DLA has no control or guarantees regarding the security of external social media.

(b) External social media is considered a public commons where interactions among individuals, dependent upon "privacy settings," frequently occur in the open. Unsolicited PII posted to DLA external social media sites remains, primarily, the responsibility of the individual poster.

(c) Solicitation or collection of PII by third parties on third party-owned/operated external social media shall NOT be the responsibility of DLA. As documented in the DOD generic social media privacy impact statement, DD Form 2930A, Adapted PRIVACY IMPACT ASSESSMENT (AD-PIA), August 2011 (Reference (q)):

(1) Third party Web sites and applications may require individuals to register to access various accounts. However, DLA does not collect, maintain, use, or share such information collected by the third party Web sites and application providers. Any information that users provide to register for a third party Web site or application is voluntarily contributed and is not maintained by DLA.

(2) DLA shall NOT collect, maintain, use, or share PII that may become available. This (DOD) ADP-PIA provides transparency to the public regarding DLA's policy on the use of third party Web sites and applications.

(3) PII could become available from users' input. DLA shall NOT collect, maintain, use, or share PII that may become available. If PII inadvertently becomes available from user input, the PII will be removed to safeguard the individual's privacy per DOD policy.

(d) DLA social media site managers, administrators and moderators operating internal social media are strongly discouraged from operating sites that process PII. Those that do shall follow current DOD and DLA standards for the collection, storage, and disposal of that information to include:

(1) Privacy Impact Assessment (PIA).

(a) All internal and external social media sites and applications shall prepare a PIA prior to procuring or using a new internal or external system that collects PII. Creation of the PIA shall adhere to DOD PIA Guidance (Reference (l)) and use DD form 2930 (Reference (r)) .

(b) An ADP-PIA Form 2930A: DOD Use of Third Party Web sites and Applications was approved by DOD for use by all components in August 2011 to address privacy on third party social media sites. This blanket ADP-PIA shall be used by DLA for all third party social media sites, where applicable.

(c) A review and update of the PIA shall be prepared for internal or external social media cwithin three years of the PIA approval date or when any of the following occur:

1. Significant system management changes.

2. Significant merging of systems, capabilities, or data.

3. New public access.

4. Integration with commercial sources.

5. New interagency uses.

6. Alteration in character of data.

(2) Privacy Notice. A DLA Privacy Notice shall be posted on all internal and external social media applications which may collect PII, in compliance with (OMB) Guidance for Agency Use of Third Party Web sites and Applications (Reference (n)).

(3) Surveys. All information collections by DLA using external social media shall be compliant with the Paper Reduction Act (PRA) and OMB Guidance on Social Media, Web-based Interactive Technologies. As such, any survey that poses specific questions to ten or more members of the public and is posted on an internal or external social media site or application is subject to the public notice and comment requirements of the PRA and must have OMB approval prior to use, including an OMB control number.

5. <u>WEB MEASUREMENT AND CUSTOMIZATIONS TECHNOLOGIES:</u>

a. Use of Web measurement and customization technologies on internal and external social media must comply with policy established in OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (Reference (m)).

b. Under NO circumstances may DLA use Web measurement technologies to:

(1) Collect PII without the user’s explicit consent in any fashion.

(2) Track user individual-level activity outside of the Web site or application from which the technology originates.

(3) Share the data obtained through such technologies with other departments or agencies without the user’s explicit consent.

(4) Cross-reference any data gathered from Web measurement and customization technologies against PII to determine individual-level online activity without the user’s explicit consent.

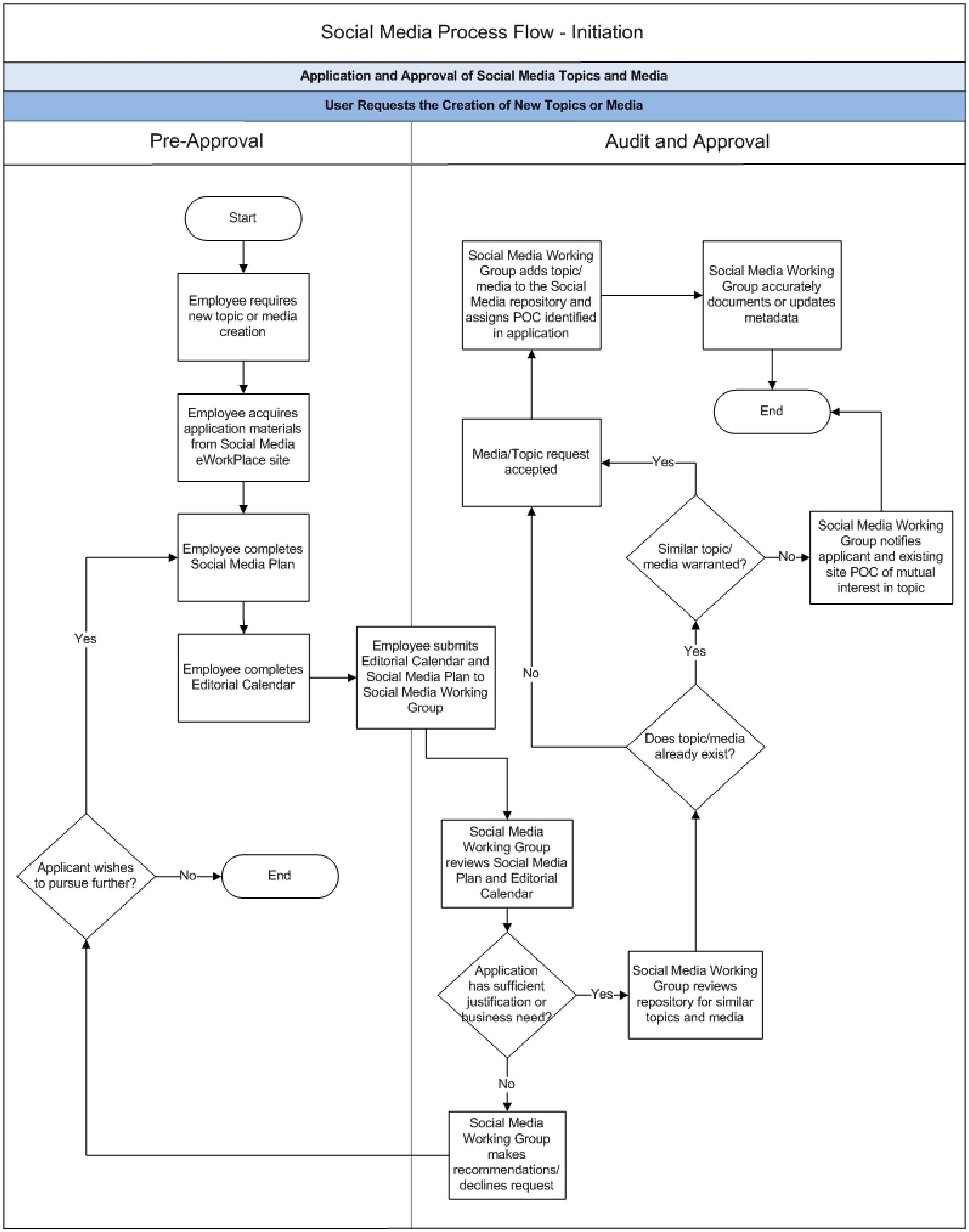
(c) DLA shall NOT use Web measurement and customization technologies that are difficult to for users to opt-out.

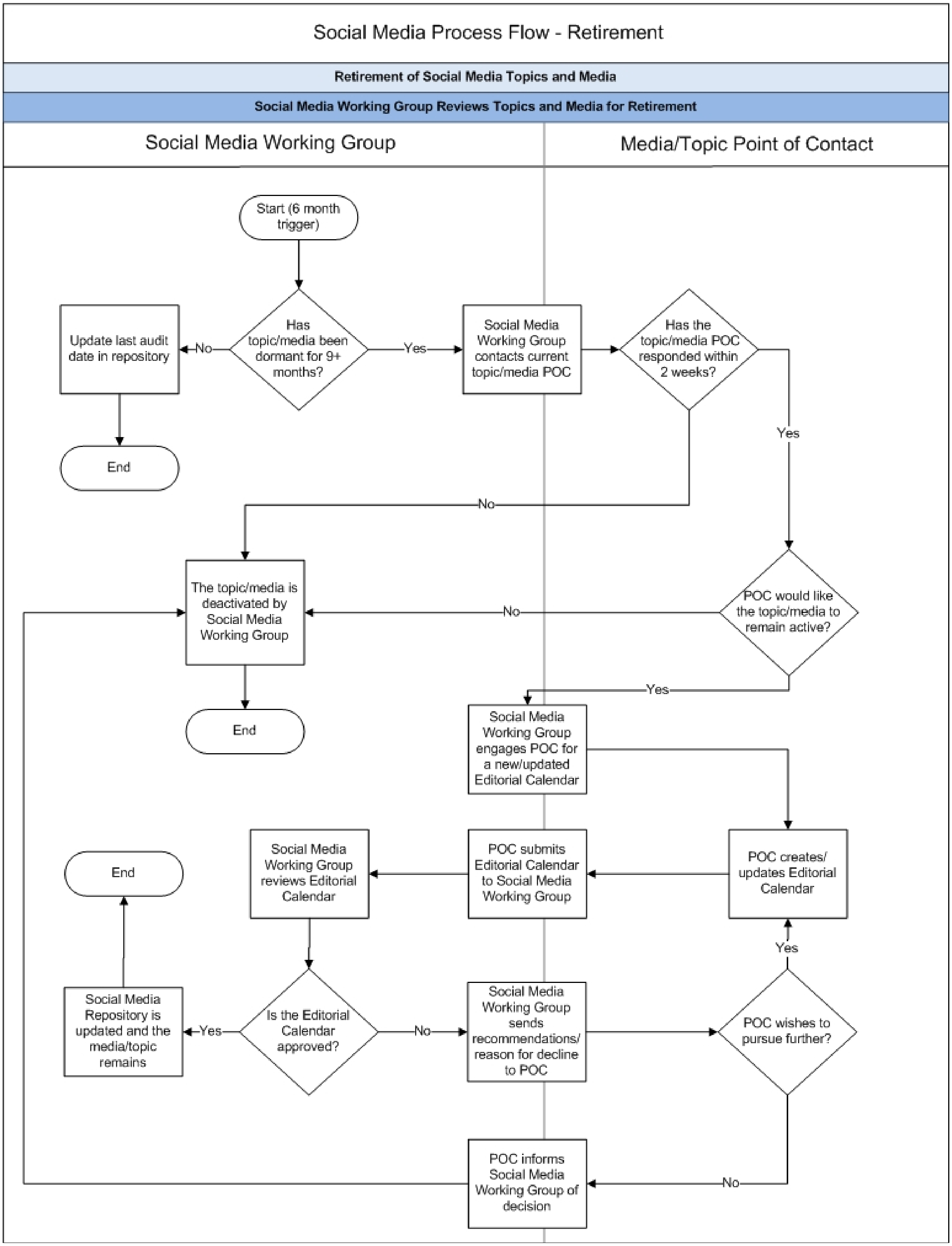
(d) DLA shall provide users who decline to opt-in or decide to opt-out with access to information that is comparable to the information available to users who opt-in or decline to opt-out.

(e) Use of Web measurement and customization by third parties on third party-owned/operated external Social Media shall NOT be the responsibility of DLA.

ENCLOSURE 4

Social Media / Topic Approval and Retirement Process Flows


Social Media Process Flow - Initiation
Application and Approval of Social Media Topics and Media
User Requests the Creation of New Topics or Media
Pre-Approval
Audit and Approval
Start
Employee requires new topic or media creation
Employee acquires application materials from Social Media eWorkPlace site
Employee completes Social Media Plan
Employee completes Editorial Calendar
Employee submits Editorial Calendar and Social Media Plan to Social Media Working Group
Social Media Working Group reviews Social Media Plan and Editorial Calendar
Application has sufficient justification or business need?
Yes
Social Media Working Group reviews repository for similar topics and media
No
Social Media Working Group makes recommendations/ declines request
Applicant wishes to pursue further?
Yes
No
End
Does topic/media already exist?
No
Yes
Similar topic/ media warranted?
Yes
No
Media/Topic request accepted
Social Media Working Group notifies applicant and existing site POC of mutual interest in topic
Social Media Working Group adds topic/ media to the Social Media repository and assigns POC identified in application
Social Media Working Group accurately documents or updates metadata
End


Social Media Process Flow - Retirement
Retirement of Social Media Topics and Media
Social Media Working Group Reviews Topics and Media for Retirement
Social Media Working Group
Media/Topic Point of Contact
Start (6 month trigger)
Has topic/media been dormant for 9+ months?
No
Update last audit date in repository
End
Yes
Social Media Working Group contacts current topic/media POC
Has the topic/media POC responded within 2 weeks?
Yes
No
The topic/media is deactivated by Social Media Working Group
End
POC would like the topic/media to remain active?
No
Yes
Social Media Working Group engages POC for a new/updated Editorial Calendar
POC creates/ updates Editorial Calendar
POC submits Editorial Calendar to Social Media Working Group
Social Media Working Group reviews Editorial Calendar
Is the Editorial Calendar approved?
Yes
Social Media Repository is updated and the media/topic remains
End
No
Social Media Working Group sends recommendations/ reason for decline to POC
POC wishes to pursue further?
Yes
No
POC informs Social Media Working Group of decision