



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

DISA INSTRUCTION 630-225-18*

MAY 28 2014

INFORMATION SERVICES

Internet-based Capabilities

1. **Purpose.** This Instruction prescribes policy and assigns responsibilities for Internet-based capabilities.

2. **Applicability.** This Instruction applies to DISA military and civilian employees and to DISA contractors when using government-furnished information technology (IT) equipment. It also applies to all DISANet users and those connected to the Nonsecure Internet Protocol Router Network (NIPRNet) to carry out work paid for by DISA.

3. **Scope.** This Instruction applies to all Internet-based capabilities, which are all publicly accessible information capabilities and applications available across the Internet in locations not owned, operated, or controlled by DoD or the Federal Government. Internet-based capabilities include collaborative tools; such as, social networking service, social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g., You Tube, Facebook, MySpace, Twitter, and Google Apps).

4. References.

4.1 DoDI 8550.01, DoD Internet Services and Internet-Based Capabilities, 11 September 2012.

4.2 DISAI 630-225-15, Authorized Unofficial Use of Government-Provided Information Technology (IT), 14 August 2008.

4.3 DoDI 5230.29, Security and Policy Review of DoD Information for Public Release, 8 January 2009.

4.4 DISAI 240-110-37, Operations Security (OPSEC), 14 August 2012.

5. **Policy.** DISA encourages the use of Internet-based capabilities to enhance communication, collaboration, and information exchange in support of the Agency's mission. In accordance with DoD Instruction (DoDI) 8550.01 (reference 4.1), requirements for participation will be contingent upon an individual's role and the intended outcome of an individual's activities.

5.1 Access, Use, and Conduct.

5.1.1 In accordance with reference 4.1, external official presences on Internet-based capability sites are considered official public affairs activities. Permission to establish such presence shall be obtained from the Director for Strategic Planning and Information (SPI).

5.1.1.1 Internet-based capability sites owned and operated by SPI will serve as the primary channels to communicate with external audiences.

5.1.1.2 The authority to decommission Internet-based capability sites that do not comply with this Instruction or the references has been granted to SPI.

5.1.2 The workforce is permitted to use Internet-based capabilities for official, mission-related activities unrelated to public affairs activities (including activities to support cross-Agency collaboration, mission awareness, and general research). Regular or routine access or participation will be coordinated with and approved by the individual's supervisor. A disclaimer will be included by an individual when personal opinions about mission-related activities are expressed (e.g., "This statement is my own and does not necessarily represent the views of DISA or DoD.") (See reference 4.1)

5.1.3 Limited personal use of Internet-based capabilities is permitted if the use does not interfere with official business and involves minimal additional expense to the government. This limited personal use of government-provided IT equipment should take place during the employee's nonwork time. In addition, Agency personnel do not have a right, nor should they have an expectation, of privacy while using any government-provided IT equipment. (See DISA Instruction (DISAI) 630-225-15 [reference 4.2].)

5.1.4 Use of Internet-based capabilities will comply with laws and regulations, including, but not limited to, copyright, records retention, information security, Freedom of Information Act, First Amendment, and privacy laws. (See enclosure 3 of reference 4.1.)

5.2 Content.

5.2.1 Official Agency content not previously approved for release and destined for an Internet-based capability site must be reviewed and approved by SPI and by the Manpower, Personnel, and Security Directorate (MPS). (See DoDI 5230.29 [reference 4.3] and DISAI 240-110-37 [reference 4.4].)

5.2.2 Sensitive content may only be published on sites that are restricted to users with DoD public key infrastructure (PKI) certificates and approved external PKI certificates, as appropriate, to support authentication procedures.

5.2.3 The Agency's Web site (DISA.MIL) will remain DISA's primary Internet presence. Wherever possible, content posted to Internet-based capability sites will also be available on DISA.MIL and should link back to DISA.MIL to provide in-depth information and resources.

5.2.4 Employees will immediately comply with any direction to restrict or remove any content that was released in violation of this Instruction or any law.

5.3 **Security.** The workforce will adhere to operations security principles and remain vigilant to prevent any possible harm to warfighters or to the mission when releasing information on Internet-based capability sites.

6. Responsibilities.

6.1 **Director for Strategic Planning and Information Directorate (SPI).** The Director, SPI, shall:

6.1.1 Serve as the lead for the operations and management of the Agency's Internet-based capability program.

6.1.2 Provide guidance to the Agency regarding the use of Internet-based capabilities and promote understanding of guidelines and compliance with requirements. (Guidance is provided in the Agency Social Media Handbook [see paragraph 7].)

6.1.3 Approve requests to establish official, external Internet-based capability sites.

6.1.4 Decommission unapproved, noncompliant external official Internet-based capability sites.

6.1.5 Provide a public affairs review of content to be published on Internet-based capability sites, in coordination with MPS.

6.1.6 Implement records management, in accordance with subparagraph 7.b.(5) of enclosure 2 of reference 4.1.

6.2 **Director for Manpower, Personnel, and Security Directorate (MPS).** The Director, MPS, shall:

6.2.1 Participate in the review and evaluation of requests to establish official, external Internet-based capability sites.

6.2.2 Provide the workforce with training to promote understanding and compliance with operations security (OPSEC) principles as they relate to the usage of Internet-based capabilities.

6.2.3 Provide OPSEC-focused reviews of content to be published on Internet-based capability sites, in coordination with SPI.

6.3 **Chief Information Officer (CIO).** The CIO shall:

6.3.1 Ensure Agency compliance with the Privacy Act for DISA implementation of requirements, as specified in reference 4.1.

6.3.2 Ensure information is available for access under the Freedom of Information Act for DISA actions, as specified in reference 4.1.

6.3.3 Ensure effective implementation of computer network defense mechanisms for DISA actions implementing reference 4.1.

6.3.4 Maintain records of Agency Internet services and official uses of Internet-based capability, in accordance with DoDD 5015.2, DoD Records Management Program.

6.4 Principal Directors, Directors, Chiefs, and Commanders of Major Organizational Elements. These individuals will ensure organizational personnel adhere to the policies outlined in this Instruction.

7. Agency Social Media Handbook. The Agency Social Media Handbook published by SPI and located at <https://east.esps.disa.mil/disa/org/S15/Shared%20Documents/DISA-Social-Media-Handbook.pdf> provides tactical guidance and best practices regarding the use of Internet-based capabilities. The workforce can reference the handbook when questions arise regarding conduct, participation, and/or procedural requirements of Internet-based capabilities.



FREDERICK A. HENRY
Brigadier General, USA
Chief of Staff

*This Instruction cancels Director's Policy Letter 2011-4, 12 May 2011. This Instruction must be reissued, canceled, or certified current within 5 years of its publication. If not, it will expire 10 years from its publication date and be removed from the DISA issuances postings.

OPR: SPI - disa.meade.spi.mbx.web-team@mail.mil

DISTRIBUTION: P