Department of Defense
INSTRUCTION

NUMBER 8550.01
September 11, 2012

DoD CIO

SUBJECT: DoD Internet Services and Internet-Based Capabilities

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authority in DoD Directive (DoDD) 5144.1 (Reference (a)) and DoD Instruction (DoDI) 5025.01 (Reference (b)) and the requirements of the Office of Management and Budget (OMB) Memorandum M-05-04 (Reference (c)):

a. Incorporates and cancels Deputy Secretary of Defense (DepSecDef) Memorandum (Reference (d)), and Directive-Type Memorandum (DTM) 09-026 (Reference (e)).

b. Establishes policy, assigns responsibilities, and provides instructions for:

(1) Establishing, operating, and maintaining DoD Internet services on unclassified networks to collect, disseminate, store, and otherwise process unclassified DoD information.

(2) Use of Internet-based capabilities (IbC) to collect, disseminate, store, and otherwise process unclassified DoD information.

2. APPLICABILITY. This Instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

b. Applies to DoD Internet services and use of IbC provided by morale, welfare, and recreation (MWR), military exchanges, and lodging programs for use by authorized patrons.

c. Applies to contractors and other non-DoD entities that are supporting DoD mission-related activities or accessing DoD Internet services or IbC via DoD information systems, to the

extent provided in the contract or other instrument by which such authorized support or access is provided.

d. Does NOT:

(1) Prevent unit commanders or Heads of the DoD Components from providing alternate, stand-alone capabilities to allow access to IbC for mission or morale purposes.

(2) Prohibit DoD employees from using IbC from personal Internet-capable devices for personal purposes.

(3) Apply to using IbC specifically for penetration testing, communications security monitoring, network defense, personnel misconduct and law enforcement investigations, and intelligence-related operations.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. Decisions to collaborate, participate, or to disseminate or gather information via DoD Internet services or IbC shall balance benefits and vulnerabilities. Internet infrastructure, services, and technologies provide versatile communication assets that must be managed to mitigate risks to national security; to the safety, security, and privacy of personnel; and to Federal agencies.

b. DoD Internet services and IbC used to collect, disseminate, store, or otherwise process DoD information shall be configured and operated in a manner that maximizes the protection (e.g., confidentiality, integrity, and availability) of the information, commensurate with the risk and magnitude of harm that could result from the loss, compromise, or corruption of the information.

(1) For use of DoD Internet services, paragraph 4.b. applies to both public and non-public DoD information.

(2) For use of IbC, this applies to the integrity and availability of public DoD information. IbC shall not be used to collect, disseminate, store, or otherwise process non-public DoD information, as IbC are not subject to Federal or DoD information assurance (IA) standards, controls, or enforcement, and therefore may not consistently provide confidentiality.

c. DoD information systems (ISs) hosting DoD Internet services shall be operated and configured to meet the requirements in DoDD 8500.01E (Reference (f)) and DoDI 8500.2 (Reference (g)), and certified and accredited in compliance with DoDI 8510.01 (Reference (h)).

d. Effective information review procedures for clearance and release authorization for DoD information to the public are conducted in compliance with DoDD 5230.09 and DoDI 5230.29 (References (i) and (j)). DoD information intended for non-public audiences requires similar review and consideration prior to dissemination. DoD employees shall be educated and trained to conduct both organizational and individual communication effectively to deny adversaries the opportunity to take advantage of information that may be inappropriately disseminated.

e. Public DoD websites shall be operated in compliance with the laws and requirements cited in Reference (c). Detailed explanations, and implementation guidance are provided at the Web Manager's Advisory Council Website at http://www.howto.gov/web-content/.

f. DoD Internet services and the information disseminated via these services, where appropriate, shall be made available to Federal initiatives such as Data.gov, Recovery.gov, and USA.gov to reduce duplication and to foster greater participation, collaboration, and transparency with the public. Where feasible and appropriate, such DoD information shall be provided as datasets in raw (machine readable) format as defined in DepSecDef Memorandum (Reference (k)).

g. All unclassified DoD networks (e.g., Non-classified Internet Protocol Router Network (NIPRNET), the Defense Research and Engineering Network) shall be configured to provide access to IbC across all the DoD Components.

h. Authorized users of unclassified DoD networks shall comply with all laws, policies, regulations, and guidance concerning communication and the appropriate control of DoD information referenced throughout this Instruction regardless of the technology used. Furthermore, all personal use of IbC by means of Federal government resources shall comply with paragraph 2-301 of DoD 5500.7-R (Reference (l)).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives/.

8. EFFECTIVE DATE. This Instruction:

a. Is effective September 11, 2012

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with Reference (b). If not it will expire effective September 11, 2022 and be removed from the DoD Issuances Website.

Teresa M. Takai
DoD Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

TABLES

FIGURES

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
(b) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007, as amended
(c) Office of Management and Budget Memorandum M-05-04, "Policies for Federal Agency Public Websites," December 17, 2004
(d) Deputy Secretary of Defense Memorandum, "Web Site Administration," December 7, 1998 (hereby cancelled)
(e) Directive-Type Memorandum 09-026, "Responsible and Effective Use of Internet-based Capabilities," February 25, 2010 (hereby cancelled)
(f) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002, as amended
(g) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(h) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
(i) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(j) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," January 8, 2009
(k) Deputy Secretary of Defense Memorandum, "Support for the Open Government Initiative," April 14, 2010
(l) DoD 5500.7-R, "Joint Ethics Regulation (JER)," August 1, 1993
(m) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009
(n) Deputy Secretary of Defense Memorandum, "Reserve Component Joint Web Risk Assessment Cell," February 12, 1999
(o) DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007
(p) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1982
(q) DoD 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008
(r) DoD 8400.01-M, "Procedures for Ensuring the Accessibility of Electronic and Information Technology (E&IT) Procured by DoD Organizations," June 3, 2011
(s) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
(t) Unified Command Plan[1]
(u) DoD Instruction 8910.01, "Information Collection and Reporting," March 6, 2007
(v) DoD Instruction 7750.07, "DoD Forms Management Program," April 20, 2007, as amended
(w) DoD 7750.07-M, "DoD Forms Management Program Procedures Manual," May 14, 2008
(x) DoD Instruction 1100.13, "Surveys of DoD Personnel," November 21, 1996
(y) Chapter 91 of title 15, United States Code
(z) Office of Management and Budget Memorandum, "Information Collection under the Paperwork Reduction Act," April 7, 2010

[1] Requests for copies can be forwarded to the Director for Strategic Plans and Policy, J-5/Joint Staff, and will be provided in accordance with laws, regulations, and policies concerning the handling of classified information.

(aa) DoD 5200.1-R, "Information Security Program," January 14, 1997
(ab) Director, Administration and Management Memorandum, "Social Security Numbers (SSN) Exposed on Public Facing and Open Government Websites," November 23, 2010
(ac) DoD Instruction 5040.02, "Visual Information (VI)," October 27, 2011
(ad) Office of Management and Budget Memorandum, "Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act," April 7, 2010
(ae) Sections 552[2] and 552a[3] of title 5, United States Code
(af) Title 17, United States Code
(ag) DoD Directive 5535.4, "Copyrighted Sound and Video Recordings," August 31, 1984, as amended
(ah) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(ai) DoD Instruction 5030.59, "National Geospatial-Intelligence Agency (NGA) LIMITED DISTRIBUTION Geospatial Information," December 7, 2006
(aj) DoD Directive 5210.50, "Unauthorized Disclosure of Classified Information to the Public," July 22, 2005
(ak) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
(al) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984, as amended
(am) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," October 6, 1987
(an) DoD Directive 5405.2, "Release of Official Information in Litigation and Testimony by DoD Personnel as Witnesses," July 23, 1985, as amended
(ao) Office of Management and Budget Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007
(ap) Office of Management and Budget Memorandum M-06-16, "Protection of Sensitive Agency Information," June 23, 2006
(aq) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007, as amended
(ar) DoD Instruction 8552.01, "Use of Mobile Code Technologies in DoD Information Systems," October 23, 2006
(as) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009
(at) Office of Management and Budget Memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications," June 25, 2010
(au) DoD Instruction 8551.1, "Ports, Protocols, and Services Management (PPSM)," August 13, 2004
(av) DoD Instruction 8410.01, "Internet Domain Name Use and Approval," April 14, 2008
(aw) DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011
(ax) Defense Information Systems Agency, "Web Server Security Technical Implementation Guide, Version 7, Release 1," October 12, 2010[4]
(ay) DoD Chief Information Officer Memorandum, "DoD Enterprise Services Designation -- Collaboration, Content Discovery, and Content Delivery," February 2, 2009

[2] Section 552 is also known as "The Freedom of Information Act"
[3] Section 552a is also known as "The Privacy Act"
[4] http://iase.disa.mil/stigs/app_security/web_server/general.html

(az) Joint Committee on Printing U.S. Congress, Senate Publication 101-9, "Government Printing and Binding Regulations," February 1990[5]
(ba) DoD Directive 5500.07, "Standards of Conduct," November 29, 2007
(bb) Chapters 13 and 15 of title 31, United States Code
(bc) DoD Instruction 1015.10, "Military Morale, Welfare, and Recreation (MWR) Programs," July 6, 2009, as amended
(bd) DoD Instruction 5120.4, "Department of Defense Newspapers, Magazines and Civilian Enterprise Publications," June 16, 1997
(be) DoD Directive 5122.05, "Assistant Secretary of Defense for Public Affairs (ASD(PA))," September 5, 2008
(bf) Deputy Secretary of Defense Memorandum, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense," February 10, 2003
(bg) Office of Management and Budget Memorandum M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies," June 25, 2010
(bh) DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 2, 2008, as amended
(bi) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998, as amended
(bj) Public Law 107-198, "Small Business Paperwork Relief Act of 2002," June 28, 2002
(bk) Public Law 107-174, "Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002," May 15, 2002 (also known as "The No Fear Act")
(bl) Assistant Secretary of Defense for Networks and Information Integration Memorandum, "Use of Peer-to-Peer (P2P) File-sharing Applications Across DoD," November 23, 2004[6]
(bm) DoD Directive 5535.09, "DoD Branding and Trademark Licensing Program," December 19, 2007
(bn) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," February 15, 2012.
(bo) DoD Instruction 5400.13, "Public Affairs (PA) Operations," October 15, 2008
(bp) Subpart 2635.703 of title 5, Code of Federal Regulations[7]
(bq) Sections 3.104-4 and 3.104-5, Federal Acquisition Regulation (FAR)[8]

[5] http://www.house.gov/jcp/jcpregs.pdf
[6] https://powhatan.iiie.disa.mil//policy-guidance/novp2p-memo.pdf
[7] http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=%2Findex.tpl
[8] https://www.acquisition.gov/Far/

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CHIEF INFORMATION OFFICER (CIO). The DoD CIO, in addition to the responsibilities in section 7 of this enclosure, shall:

a. Develop and coordinate DoD issuances for the use, risk management, and policy compliance oversight of DoD Internet services and use of IbC, in accordance with authorities established in Reference (a) and DoDD 8000.01 (Reference (m)).

b. Integrate guidance regarding the responsible and effective use of DoD Internet services and IbC with operations security (OPSEC) and IA education, training, and awareness activities in conjunction with the Under Secretary of Defense for Intelligence (USD(I)).

c. Coordinate corrective action for DoD Internet services and use of IbC not operated in compliance with this Instruction.

d. Establish mechanisms to monitor emerging IbC in order to identify opportunities for use and assess risks.

e. Review, approve, and sign, in coordination with the General Counsel of the Department of Defense (GC, DoD), and the CDRUSSTRATCOM, and in consultation with the Assistant Secretary of Defense for Public Affairs (ASD(PA)), terms of service (ToS) agreements with IbC providers on behalf of DoD.

f. Provide technical guidance for the dissemination of DoD information (including datasets and metadata) via DoD Internet services and IbC.

g. Provide a consolidated list of education and training resources for the use of DoD Internet services and IbC.

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). The Director, DISA, under the authority, direction, and control of the DoD CIO, in addition to the responsibilities in section 7 of this enclosure, shall:

a. Provision and sustain the Global Information Grid (GIG) to host and serve Internet media via unclassified DoD Internet services.

b. Review DoD information disseminated via unclassified DoD Internet services and IbC for information and OPSEC vulnerabilities, through operational control of the Joint Web Risk Assessment Cell (JWRAC), as directed by DepSecDef Memorandum (Reference (n)).

c. Require JWRAC to conduct routine searches for unregistered DoD websites and official uses of IbC.

3. USD(I). The USD(I), in addition to the responsibilities in section 7 of this enclosure, shall:

a. Ensure information and OPSEC vulnerabilities found on DoD Internet services and IbC are identified to and resolved by the designated manager or the DoD or OSD Component Head.

b. Coordinate corrective action for DoD Internet services and use of IbC not operated in compliance with applicable information security and OPSEC policies with the responsible DoD and OSD Component Heads and the DoD CIO as necessary.

c. Integrate guidance, in coordination with the DoD CIO, regarding the responsible and effective use of DoD Internet services and IbC in OPSEC education, training, and awareness activities.

d. Provide policy, procedures, and oversight for DoD intelligence and intelligence-related activities that use DoD Internet services and IbC to collect information, making sure these activities are consistent with DoDD 5240.01 (Reference (o)) and DoD 5240.1-R (Reference (p)).

e. Provide guidance, consistent with DoD 5205.02-M (Reference (q)), for the OPSEC reviews of DoD information intended for distribution via DoD Internet services and IbC found at Appendix, Enclosure 3.

4. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 7 of this enclosure, shall develop, maintain, and distribute threat estimates on current and emerging Internet technologies, including IbC.

5. ASD(PA). The ASD(PA), in addition to the responsibilities in section 7 of this enclosure, shall:

a. Operate and maintain the Federal Agency Public Website for the DoD.

b. Host and operate a registration system(s) for the addresses of public DoD Internet services, EOPs, and other official uses of IbC, that is capable of producing individual DoD Component inventories.

c. Provide guidance for official identifiers for EOP.

d. Develop and make available education, guidance, and training for the responsible and effective use and management of EOP.

6. DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (WHS). The Director, WHS, under the authority, direction, and control of the Director of Administration and Management (DA&M), in addition to the responsibilities in section 7 of this enclosure, shall include release of DoD information via DoD Internet services and IbC in the responsibilities and procedures published in References (i) and (j).

7. DoD and OSD COMPONENT HEADS. The DoD and OSD Component Heads shall:

a. Be responsible for the operation of their Component's DoD Internet services and use of IbC, including:

(1) Defending against malicious activity affecting DoD networks (e.g., distributed denial of service attacks, intrusions) and taking immediate and commensurate actions, as required, to safeguard missions (e.g., temporarily limiting access to the Internet to preserve OPSEC, maintaining bandwidth to meet operational demand).

(2) Denying access to sites dedicated to prohibited content and prohibiting authorized users from engaging in prohibited activity via DoD Internet services and IbC while at work or when using government equipment.

(3) Establishing a reporting process for corrective action for users who discover access to prohibited content on DoD Internet services or IbC used by the Component.

(4) As appropriate, approving establishment and registration of EOP and official use of IbC.

(5) Ensuring that all DoD Internet services and IbC used by the Component to disseminate unclassified DoD information are registered in compliance with the procedure in paragraph 3.e. of Enclosure 3.

(6) Ensuring that the Components' web risk assessment cells search for unregistered sites on a routine basis and including findings in discrepancy reports.

(7) Ensuring the implementation, validation, and maintenance of applicable IA controls, information security procedures, and OPSEC measures.

(8) Ensuring the maintenance, operational integrity, and security of ISs supporting DoD Internet services used by the DoD Component.

(9) Assessing the need to isolate, disconnect, terminate, or otherwise shut down locally unclassified DoD Internet services and access to IbC within Component jurisdiction that are not brought into compliance with applicable policies within 90 calendar days of identification or notification of noncompliance and for which no plan of action and milestones for correction is in place.

b. Be responsible for disseminating DoD information via DoD Internet services and IbC, including:

(1) Establishing documented processes for reviewing information proposed for dissemination to ensure that adversaries do not gain advantages through access to inappropriately disseminated information, especially when that information is aggregated with the vast sources of public information.

(a) References (i) and (j) provide overarching policy and guidance for the public release of DoD information.

(b) The Appendix to Enclosure 3 and Reference (j) provide guidance for implementing information review that, at a minimum, addresses the intended audience for the information, security, levels of sensitivity, and other concerns.

(2) Applying these processes or equivalent evaluation to all information prior to dissemination to ensure that information is reviewed, cleared, and authorized for release to the public or to specific audiences.

(3) Ensuring that DoD Internet services and DoD information are accessible to disabled employees and disabled members of the public, and that access is comparable to that available to non-disabled individuals in compliance with DoD 8400.01-M (Reference (r)).

(4) Complying with Reference (k) to identify high-value datasets, that are of good quality and that do not pose any privacy, OPSEC, or other security threats, as possible candidates for publication on Data.gov.

(5) Implementing records management for DoD Internet services and official uses of IbC in compliance with DoDD 5015.2 (Reference (s)). The National Archives Records Administration provides emerging guidance at http://www.archives.gov.

(6) Ensuring compliance with References (o) and (p) in use of DoD Internet services or IbC to collect information for intelligence or intelligence-related activities.

c. Educate and train subordinate DoD employees in the responsible and effective use of DoD Internet services and IbC. Education and training shall include, but not be limited to, information security, OPSEC, IA, and information review for clearance and release authorization procedures.

d. Ensure that all DoD Internet services and IbC used by the Component to disseminate unclassified DoD information are assessed at least annually for compliance with this Instruction. Compliance assessment guidance is provided in the Appendix of Enclosure 2. Verify, at a minimum, that:

(1) The existing access controls appropriately protect the information.

(2) The information disseminated via public DoD Internet services and IbC has been reviewed, cleared, and authorized for public release.

(3) The DoD Component's information review for clearance and release authorization procedures are being followed, that the results correctly implement this policy, and that a copy(ies) of the documented review process(es) is maintained by the DoD Component's CIO.

(4) Corrective action is initiated and, as necessary, coordinated with the DoD CIO and U.S. Cyber Command (as delegated by USSTRATCOM), for any noncompliance discovered during the assessment.

8. DoD COMPONENT CIOs. The DoD Component CIOs shall:

a. Advise the DoD CIO and ensure that the policies and guidance for use of DoD Internet services and IbC issued by the DoD CIO are implemented within their Component.

b. In coordination with Component OPSEC and public affairs offices, provide advice, guidance, and other assistance to the respective Component Heads and other Component senior management to ensure that DoD Internet services and IbC are used responsibly and effectively.

c. Ensure effective implementation of computer network defense mechanisms as well as the proper use of DoD Internet services and IbC through the use of IA, OPSEC, and information security education, training, and awareness activities.

d. Establish risk assessment procedures to evaluate and monitor Component use of current and emerging Internet technologies in order to identify opportunities for use and to assess risks.

e. Maintain copy(ies) of the review processes documented in subparagraph 7.b.(1) established by the Component and subcomponents.

f. In coordination with Component website administrators, prepare and submit to the responsible Head of Component a plan of action and milestones for all websites and use of IbC within the Component jurisdiction that are not brought into compliance with applicable policies within 90 calendar days from identification of noncompliance. Noncompliance includes failure to implement the documented review processes tasked in subparagraph 7.b.(1) of this enclosure and to provide OPSEC training for website administrators.

g. In coordination with the Component public affairs office, assist in evaluating the intended use of IbC for EOP and other official purposes.

9. CDRUSSTRATCOM. The CDRUSSTRATCOM, in addition to the responsibilities in section 7 of this enclosure, shall:

a. Direct the defense and operation of the DoD information networks in accordance with the Unified Command Plan (Reference (t)).

b. Identify and assess operational risks associated with the use of DoD Internet services and IbC, and notify the DoD CIO of risk mitigations.

Appendix
Policy Compliance and Assessment

APPENDIX TO ENCLOSURE 2

POLICY COMPLIANCE AND ASSESSMENT

1. PURPOSE. This appendix establishes a sample process for gauging organizational compliance with this Instruction and information policies. It outlines the recommended procedures for creating a baseline of an organization's DoD Internet services and IbC portfolio, assigning roles and responsibilities associated with compliance assessment, scoring DoD Internet services and IbC for compliance, and analyzing and reporting results. This recommended process supports the DoD and OSD Components' obligatory annual assessment of policy compliance as required in paragraph 7.d. of Enclosure 2.

2. PRE-ASSESSMENT PROCEDURES

a. Baseline. Begin with a baseline of DoD Internet services and IbC under the organization's purview that require compliance assessment. Sources include, but are not limited to:

(1) A list of addresses registered in the DoD Internet Whitelist for Internet access, available via DoD Component network administrators.

(2) The ASD(PA)-hosted registration and inventory system(s) at http://www.defense.gov/.

(3) The DoD Component website registration systems.

b. Assigning Roles and Establishing a Timeline

(1) As the assessment begins, assign roles and responsibilities. Assigning roles and responsibilities helps ensure accountability and clear lines of authority during the assessment process. The following roles are recommended to ensure accurate validation, analysis, and reporting:

(a) Assessment Lead.

(b) Analyst.

(2) The size and scope of an organization's portfolio influences the length of time required to complete an assessment. Within the first 2 weeks of the assessment cycle, establish a timeline with milestones and due dates in accordance with the example provided in Table 1. Tailor the assessment timeline to the scope of the organization's DoD Internet services and IbC portfolio. The assessment lead should ensure adherence to the tailored timeline.

Table 1. Example of 3-Month Assessment Cycle Timeline

Days 1-7	Gather and establish baseline list of DoD Internet services or IbC to be assessed
Day 1	Assignment of Roles and Responsibilities
Day 7	Establishment of Timeline/ Creation of Checklist
Days 12-60	Assessment of Organization Websites
Days 60-70	Validation of Assessment
Days 70-80	Analysis of Information
Days 80-90	Non-Compliance and Corrective Action

3. VALIDATION PROCEDURES

a. Review each DoD Internet service or IbC used for compliance with the policies and directives listed within each area of the procedures section of this Instruction. Note whether or not the DoD Internet service or use of IbC is in compliance using a compliance checklist based on the example in Table 2. Expand this example to include a short description of the requirements, with applicable section and paragraph citations in the left column, to reflect the procedures listed in Enclosure 3 as needed.

Table 2. Compliance Checklist Example

1	PUBLIC AND PRIVATE DoD INTERNET SERVICES AND IbC	Y	N
1.a	The DoD Internet service or DoD information on IbC meets Electronic and Information Technology Accessibility Standards as defined in Reference (r).		
1.b	Information collection complies with DoD manuals, instructions, or PLs where appropriate, as listed in References (o) and (p) and in DoDI 8910.01, DoDI 7750.07, DoD 7750.07-M, DoDI 1100.13, chapter 91 of title 15, United States Code (U.S.C.), OMB Memorandum "Information Collection under the Paperwork Reduction Act," DoD 5200.1-R, and DA&M Memorandum, "SSN Exposed on Public Facing and Open Government Websites" (References (u) through (ab))		
1.c	The DoD Internet service or IbC includes a notice of copyright, if applicable, and the specific copyrighted work(s) and owner of the copyright(s) are identified.		
1.d	The DoD Internet service or IbC does not contain official DoD imagery altered in any way, except as allowed by DoDI 5040.02 (Reference (ac)).		
1.e	The DoD Internet service or IbC only contains unclassified information that is of value to the intended audience.		
1.e	The DoD Internet service or IbC only contains unclassified information and information has been removed that could put missions or personnel at risk, or constitute in aggregate classified or sensitive information.		

b. In Table 2, the compliance of Public and Private DoD Internet Services and IbC – part 1 is being evaluated. In the example, letter "1.a." represents paragraph 1.a. of Enclosure 3. The text asks whether or not the DoD Internet service or DoD information on IbC meets the Electronic and Information Technology Accessibility Standards from Reference (r). A checklist may be one or more pages, depending on the number of elements in the section of the Procedures being

evaluated for compliance. All of the Procedures section items should be used in a Policy Compliance Checklist, unless they do not apply (e.g., the section on IbC would not apply in an assessment of a private DoD website).

4. NON-COMPLIANCE AND CORRECTIVE ACTION

a. Non-Compliance. Once a DoD Internet service or use of an IbC is assessed, areas of non-compliance should be tracked until all are remedied.

b. Corrective Action. Consistent with subparagraph 7.a.(9) of Enclosure 2, unclassified DoD Internet services and access to IbC shall be assessed to determine if there is a need to isolate, disconnect, terminate, or otherwise shut them down if they are not brought into compliance with applicable policies through other remediation. Websites and associated processes not brought into compliance with this Instruction within 90 calendar days from identification of noncompliance must have a plan of action and milestones in place for achieving compliance or are to be assessed for shutdown or disconnection by the DoD or OSD Component Heads, U.S. Cyber Command (as delegated by USSTRATCOM), or the DoD CIO, as applicable.

ENCLOSURE 3

PROCEDURES

1. PUBLIC AND PRIVATE DoD INTERNET SERVICES AND IbC

a. Accessibility. DoD Internet services and DoD information shall be accessible to disabled employees and disabled members of the public, and access shall be comparable to that available to non-disabled individuals in compliance with the requirements and alternatives in Reference (r). Current specific standards and methods are provided at http://www.section508.gov/.

b. Collecting Information

(1) Information collection via surveys, forms, DoD Internet services, IbC, or other means are subject to the same regulations and guidance as listed in subparagraphs 1.b.(1)(a) and 1.b.(1)(b) of this enclosure. Specific applications of these regulations are governed by distinct policies and guidelines.

(a) When collecting information from DoD personnel, their families, other Federal agency personnel, contractors, or members of the public, comply with Reference (p) and References (u) through (y), as applicable to the intent or target audience of the collection.

(b) OMB Memorandums (References (z) and (ad)) provide specific additional guidance to help determine when a collection is governed by or subject to References (p) and (u) through (y).

(2) Consistent with sections 552 and 552a of title 5, U.S.C. (Reference (ae)), no information shall be collected on how an individual exercises rights protected by the First Amendment to the Constitution of the United States, including the freedoms of speech, assembly, press, and religion, except when:

(a) Specifically authorized by statute.

(b) Expressly authorized by the individual about whom the record is maintained.

(c) The record is pertinent to, and within the scope of, an authorized law enforcement, intelligence collection, or counter intelligence activity.

c. Copyright. The application of title 17, U.S.C. (Reference (af)) to specific situations is a matter for interpretation by legal counsel. It is essential to keep in mind that:

(1) The rights of copyright owners shall be recognized consistent with DoDD 5535.4 (Reference (ag)).

(2) Works of the U.S. Government (USG), prepared by DoD employees (or any officer or employee of the USG) as part of their official duties, are not protected by copyright in the United States in accordance with Reference (af). This includes documents authored by DoD employees during official assignments to attend school.

(3) USG works may contain or incorporate privately created copyrighted work(s) (e.g., quote, photograph, chart, drawing, software, script, image) that are used with permission of the copyright owner or otherwise in accordance with law. Such incorporation in a USG work does not place the private work in the public domain.

(4) Contractors and grantees are not considered USG personnel; they may or may not hold copyright in works that they produce for the USG, in accordance with the terms of their contract or agreement with the agency, as well as the contractual relationship between the contractor and its employees. Consult legal counsel for assistance with copyright licenses or assignments. The USG may be granted legal rights in copyrighted works, including copyright ownership via an assignment of title, or copyright license rights via a nonexclusive, irrevocable, paid-up, royalty-free, worldwide license to use, modify, reproduce, release, perform, display, or disclose those works. The scope of the USG's rights determines allowable use and distribution.

(5) Copyrighted works created or owned by non-USG parties may be posted on DoD Internet services or IbC only with the permission of the copyright owner or otherwise in accordance with law.

(6) When placing copyrighted material on DoD Internet services or IbC, a clear disclaimer detailing the copyrights retained by USG or non-USG contributors and identifying the specific copyrighted work(s) (e.g., information, image, video, sound, design, code, template, service, technology) shall be included.

d. Image Alteration. Official DoD imagery cannot be altered beyond the allowances in Reference (ac).

e. Information Control, Dissemination, and Marking

(1) Policies and guidance governing dissemination and marking of specific categories of information shall be complied with when those specific categories of information are disseminated. (See References (f), (g), (i), and (j) as well as DoD 5200.1-R, DoD 5400.11-R, DoDI 5030.59, DoDD 5210.50, DoDD 5230.24, DoDD 5230.25, DoDI 5230.27, DoDD 5405.2, and OMB Memorandums M-06-15 and M-06-16 (References (aa) and (ah) through (ap)).

(2) Personally identifiable information (PII), as defined in DoDD 5400.11 (Reference (aq)), shall not be disclosed beyond the allowances described in Reference (ah). Personal and personnel security must be considered, and public disclosure of PII should be limited to pictures, names, biographies, and contact information of DoD personnel who, by the nature of their position and duties, frequently interact with the public, such as general or flag officers, public affairs officers, or personnel designated as official spokespersons. Public disclosure of family

information shall be generic and not include specific information such as names or ages. This includes PII in photographs, videos, captions, and other media.

(3) Social security numbers (SSNs) shall not be posted in whole or in part, and release of documentation containing them must follow Reference (ab).

(4) Potential privacy, OPSEC, and IA consequences of distributing information must be evaluated before dissemination. Only unclassified information of value (useful) to a given audience (less adversaries) should be disseminated via unclassified DoD Internet services or IbC.

(5) A process for information review shall be implemented as defined in the Appendix to Enclosure 3.

(6) DoD Internet service and IbC users who believe that DoD information available via an unclassified DoD Internet service or IbC is classified, sensitive, or would constitute classified or sensitive information when aggregated with other information available via open sources, should report the details, in accordance with Reference (aj), through command channels or to their information security or OPSEC office(r) for evaluation and appropriate action. On security determination, appropriate action includes notifying the DoD owner(s) or operator(s) of the DoD Internet service or information in IbC.

f. Links

(1) Frames and Other Direct Embedding. Potential ethical, legal, and security risks (e.g., advertising, copyright, malware, trademark, other inappropriate or malicious behavior) shall be assessed and mitigated when considering the use of frames and other technology to connect directly to and display content from non-USG sites.

(2) Manual Review. All external links to non-USG sites shall be verified to ensure continued provision of the link quality (i.e., objectivity, utility, integrity) intended by the DoD Component and expected by users. Relying solely on automatic link validation tools is not sufficient, and frequent manual review of the content at external links is required.

g. Mobile Code. DoDI 8552.01 (Reference (ar)) shall govern the dissemination of software modules that are obtained from remote systems, transferred across a network, downloaded, and executed on a local system without explicit installation or execution by a recipient (e.g., JavaScript).

h. Privacy Act Statement (PAS)

(1) When an individual is requested to furnish personal information and the information is to be included in a system of records (i.e., a system in which information about the individual is retrieved by name or other personal identifier), a PAS, consistent with the requirements of Reference (ah), must be posted or provided through a well-marked hyperlink on the page where the information is being requested. Providing the hyperlink via a statement such as "Privacy Act Statement: Please refer to the section in the Privacy Policy that describes why this information is

being collected and how it will be used," is satisfactory when linked directly to the applicable portion of the Privacy Policy required by paragraph 4.d. of this enclosure.

(2) If personal information is to be collected and maintained in a Privacy Act system of records, a Privacy Act system of records notice (SoRN) shall be published in the Federal Register prior to collection. Specific guidance and the location of DoD SoRNs are provided in Reference (ah).

(3) If a PAS would be required for a paper-based solicitation, it is required for online solicitation, regardless of whether the site is a public or private DoD Internet service, or an IbC.

i. Privacy Advisory

(1) When an individual is requested to furnish personal information via a DoD website and the information is not maintained in a Privacy Act system of records, the solicitation of such information requires a privacy advisory be provided. The privacy advisory informs the individual as to why the information is being solicited and how the information will be used.

(2) The privacy advisory shall be posted on the web page where the information is being solicited or provided through a well-marked hyperlink. Providing the hyperlink via a statement, such as "Privacy Advisory: Please refer to the Privacy Policy that describes why this information is being collected and how it will be used," is satisfactory when linked directly to the applicable portion of the Privacy Policy required by paragraph 4.d. of this enclosure.

j. Privacy Impact Assessments (PIAs). A PIA must be completed in accordance with DoDI 5400.16 (Reference (as)) before activating DoD Internet services that interface with new or significantly altered ISs or electronic collections that collect, disseminate, process, or consist of PII from or about members of the public, Federal personnel, contractors, or foreign nationals employed at U.S. military facilities internationally.

(1) Results of the PIAs shall be posted on the DoD Component's principal public website in accordance with Reference (as).

(2) In accordance with OMB Memorandum M-10-23 (Reference (at)), an adapted PIA is required whenever a DoD Component's use of a third-party website or application makes PII available to the DoD Component.

k. Privacy Breach. Any loss, theft, or compromise of PII, actual or suspected, shall be reported in accordance with Reference (aa).

2. PUBLIC AND PRIVATE DoD INTERNET SERVICES

a. DoD De-Militarized Zone (DMZ). Remote access and access to the Internet on DoD ISs supporting external-facing DoD Internet services shall be regulated by employing technical controls such as proxy services and screened subnets (also called DMZs) or through systems that

are isolated from all other DoD ISs by physical means in accordance with References (f) and (g), and DoDI 8551.1 (Reference (au)).

b. Domains. Internet domain names established and approved in compliance with DoDI 8410.01 (Reference (av)) shall be used for all DoD Internet services. The ".mil" Internet domain is established for the exclusive use of the DoD, and should be the primary address for DoD Internet services.

c. Federal Internet Services. DoD collection, dissemination, storage, and other processing of information on Federal-owned, -operated, or -controlled Internet services (e.g., Intellipedia, Data.gov) are subject to the same policies and procedures as when such activities are conducted on DoD Internet services.

d. IA

(1) The confidentiality, integrity, availability, non-repudiation, and authenticity of DoD information shall be ensured through compliance with Reference (h). DoD ISs hosting public or private DoD Internet services must be certified and accredited. Security and management controls must be in place to:

(a) Prevent inappropriate disclosure of sensitive and other non-public information.

(b) Ensure public and non-public information are resistant to tampering.

(c) Provide availability to the information or service as intended by the DoD Component and expected by customers.

(2) An approved, legally sufficient notice and consent banner, in accordance with Reference (g) and available at http://iase.disa.mil/, shall be displayed on private DoD Internet services.

(3) Private DoD Internet services shall be public key enabled in accordance with DoDI 8520.2 (Reference (aw)).

(4) A comprehensive, in-depth IA strategy for the security of web operations shall be implemented in alignment with the current version of DISA's Web Server Security Technical Implementation Guide (Reference (ax)).

e. Search

(1) Duplicative search functions on and across DoD Internet services shall be avoided absent a compelling operational need or documented business case. Components are strongly encouraged to explore integrating the no-fee services of the USASearch.gov Affiliate Program (https://search.usa.gov/affiliates/) on public DoD websites, or in the case of very small sites, place a site map or subject index on public DoD Internet services to assist in locating DoD information.

(2) The content of DoD Internet services shall be made discoverable by and available to the DoD Net Centric Enterprise Services (NCES) Enterprise Search as described in DoD CIO Memorandum (Reference (ay)).

(3) The NCES Enterprise Search shall be linked to or integrated on private DoD websites and ensure that the content of such websites is discoverable by and available to the NCES Enterprise Search.

(4) The content of DoD Internet services shall be made discoverable and available to the JWRAC and the Component Web Risk Assessment Cells as described in Reference (n).

3. PUBLIC DoD INTERNET SERVICES AND IbC

a. Advertising and Endorsement

(1) For the purpose of advertising, public DoD Internet services are USG publications. In accordance with Reference (l), U.S. Congress Senate Publication 101-9, and DoDD 5500.07 (References (az) and (ba)), the credibility of DoD information must not be adversely affected by association with non-USG sponsorships, advertisements, or endorsements.

(a) Any advertisement by or for any private individual, firm, or corporation shall not be inserted or allowed on public DoD Internet services prepared or produced with either appropriated or non-appropriated funds. DoD endorsement shall not be implied in any manner for any specific non-USG service, facility, event, or product.

(b) Stand-alone non-USG graphics, logos, or aggrandizing statements such as "Powered by …," "Serviced by …," and "Designed by …" shall not be inserted or allowed on public DoD Internet services, or the DoD-controlled content area of an IbC prepared or produced with either appropriated or non-appropriated funds. Proprietary rights notices (including copyright and trademark notices) are not aggrandizing statements. Copyright notices are required as described in paragraph 1.c. of this enclosure. Factual acknowledgement of partners, software, technology, and services used on a public DoD Internet service may be included in descriptive information about the service or the organization, such as an "About Us" page; however, such acknowledgement should be carefully considered in the security risk assessment and risk mitigation measures for the service, and may not be used in any manner that supports the appearance of endorsement. Factual acknowledgement may include a corresponding non-USG graphic, logo, or trademark. This graphic, logo, or trademark may be used as a hyperlink to the corresponding non-USG website or service; however, the link must be disclaimed as described in subparagraph 3.c.(2) of this enclosure.

(c) Users shall not be required or encouraged to choose any specific brand of browser software or other client applications to access public DoD Internet services and IbC. DoD websites must be designed in accordance with accepted standards of the World Wide Web Consortium (http://www.w3.org/standards/) to ensure browser compatibility.

(d) Remuneration of any kind (e.g., payment, reimbursement, reduced prices, gifts) shall not be accepted in exchange for advertising, acknowledgement, or endorsement without specific statutory authority to do so. Accepting remuneration may constitute an improper augmentation of appropriations in violation of chapters 13 and 15 of title 31, U.S.C. (Reference (bb)).

(2) Non-USG advertising in electronic versions of morale, welfare, and recreation products is governed by Enclosure 12, paragraph 2.d. of DoDI 1015.10 (Reference (bc)). Such advertising must only be displayed via private DoD Internet services that ensure distribution is limited to authorized customers.

(3) Advertising in electronic versions of DoD newspapers, magazines, and civilian enterprise publications is governed by DoDI 5120.4 (Reference (bd)).

(4) Subparagraph 5.c.(4) of this enclosure provides additional guidance on advertisements in IbC.

b. Data.gov. The information review process requirements in the Appendix of this enclosure and due diligence shall be followed to ensure that all data is thoroughly reviewed for public release prior to display on Data.gov. The DoD Component is the authoritative source for all datasets and is responsible for submitting changes to the dataset's metadata and uniform resource locators (URLs) in a timely manner.

c. Links

(1) Criteria. Only links to information or services related to the performance of the DoD Component's function or mission and the purpose of the DoD Internet service or DoD use of the IbC shall be established. Objective, supportable criteria and guidelines for the selection and maintenance of links to external information shall be established and published along with the external links disclaimer, as appropriate, following the guidance in subparagraph 3.c.(2) of this enclosure.

(2) External Links Disclaimer. Links to USG Internet services shall not be disclaimed. The quoted disclaimer in Figure 1 shall be displayed or linked to on public DoD Internet services that have non-USG links, or through an intermediate "exit notice" page generated by the server whenever a request is made for any non-USG link.

Figure 1. External Links Disclaimer

"The appearance of hyperlinks does not constitute endorsement by the [insert sponsoring organization, i.e., Department of Defense, U.S. Army, U.S. Navy, U.S. Air Force, or U.S. Marine Corps] of non-U.S. Government sites or the information, products, or services contained therein. Although the [insert sponsoring organization] may or may not use these sites as additional distribution channels for Department of Defense information, it does not exercise editorial control over all of the information that you may find at these locations. Such links are provided consistent with the stated purpose of this website."

(3) Links to Private DoD Internet Services. Links or references to private DoD Internet services shall not be placed on public DoD Internet services or IbC; however, under certain circumstances it may be appropriate to establish a link to a log-on page, provided that details about the contents are not revealed.

d. Quality and Principles of Public Information. Consistent with the principles of information provided in DoDD 5122.05 (Reference (be)), the quality (e.g., objectivity, utility, integrity) of information shall be ensured and maximized, appropriate to the nature and timeliness of information disseminated to the public in accordance with DepSecDef Memorandum (Reference (bf)). In addition, contact information shall be provided as described in subparagraph 4.b. of this enclosure.

e. Registration. The Internet addresses and contact information for all public DoD Internet services, EOP, and other official uses of IbC shall be registered in the registration system(s) hosted by the Office of the ASD(PA) on Defense.gov.

f. Web Measurement and Customization Technologies (WMCT). In accordance with OMB Memorandum M-10-22 (Reference (bg)), the DoD Components may use WMCT (e.g., cookies) for the purpose of improving DoD services online through conducting measurement and analysis of usage or through customization of the user's experience.

(1) Regardless of circumstances, the DoD Components shall not use such technologies:

(a) To track user individual-level activity on the Internet outside of the DoD Internet service from which the technology originates.

(b) To share the data obtained through such technologies, without the user's explicit consent, with other Federal agencies, the DoD Components, or other organizations. Explicit consent must include a notice of the purpose and ramifications of the technology being used, as well as an opt-in function to allow the users to signify they have read and understand the information and agree to the technology's use. For example, this could be achieved with a pop-up box and "agree" button that link to privacy policies and terms of use statements.

(c) To cross-reference, without the user's explicit consent, any data gathered from WMCT against PII to determine individual-level online activity.

(d) To collect PII without the user's explicit consent in any fashion.

(e) For any like usages so designated by OMB.

(2) Usage Tiers. The defined tiers for authorized use of WMCT are:

(a) Tier 1 – Single Session. This tier encompasses any use of single session WMCT.

(b) Tier 2 – Multi-session Without PII. This tier encompasses any use of multi-session WMCT when no PII is collected or processed (including when the component is unable to identify an individual as a result of its use of such technologies).

(c) Tier 3 – Multi-session With PII. This tier encompasses any use of multi-session WMCT when PII is collected or processed (including when the component is able to identify an individual as a result of its use of such technologies).

(3) Clear Notice and Personal Choice. The DoD Components must not use WMCT from which it is not easy for the public to opt out. The DoD Components shall explain in their Privacy Policy the decision to enable WMCT by default or not, and require users to make an opt-out or opt-in decision. The DoD Components must provide users who decide to opt out with access to information that is comparable to the information available to users who opt in.

(a) DoD Component Side Opt Out. The DoD Components are encouraged and authorized, where appropriate, to use WMCT in order to establish that a user has opted out of all other uses of such technologies on the relevant domain or application. Such uses are considered Tier 2.

(b) Client Side Opt Out. If DoD Component side opt-out mechanisms are not appropriate or available, instructions on how to enable client side opt-out mechanisms may be used. Client side opt-out mechanisms allow the public to opt out of WMCT by changing the settings of a specific application or program on the public user's local computer. For example, public users may be able to disable persistent cookies by changing the settings on commonly used web browsers. In the site's Privacy Policy, DoD Components should link to http://www.usa.gov/optout_instructions.shtml, which contains general instructions on how the public can opt out of some of the most commonly used WMCT.

(c) Tier 3 Restrictions. The DoD Components employing Tier 3 uses shall use opt-in functionality.

(4) Data Safeguarding and Privacy. All uses of WMCT shall comply with References (ah) and (aq).

(5) Process for the DoD Components' Use of WMCT

(a) Privacy Policy. The DoD Components using WMCT in a manner subject to Tier 1 or Tier 2 are authorized to use such technologies as long as the DoD Components:

1. Are in compliance with Reference (bg) and all other relevant policies.

2. Provide clear and conspicuous notice in their online Privacy Policy citing the use of such technologies, as specified in Attachment 3 of Reference (bg).

3. Comply with DoD and DoD Component internal policies governing the use of such technologies.

(b) Privacy Office Review. All proposals by the DoD Components to engage in Tier 3 uses must be reviewed by the DoD Senior Agency Official for Privacy (SAOP) within the Defense Privacy and Civil Liberties Office (DPCLO) before implementation.

(c) Notice and Comment. Following DoD SAOP review for new proposals of Tier 3 uses or substantive changes to existing uses of such technologies, the DoD Components shall:

1. Solicit comment through the DoD Open Government Website at http://open.dodlive.mil/ for a minimum of 30 days. This notice and comment shall include the DoD Component's proposal to use such technologies and a description of how they will be used, which should at a minimum address the items in the Privacy Policy as described in Attachment 3 of Reference (bg). With written approval from the DoD CIO, the DoD Components are exempt from this requirement if the notice-and-comment process is reasonably likely to result in serious public harm.

2. Review and consider substantive comments and make changes to their intended use of WMCT where appropriate.

3. Obtain explicit written approval from the DoD CIO. This approval must be cited in the DoD Component's online Privacy Policy. After this approval has been obtained and after notice and comment, as specified in subparagraph f.(5)(c) of this section, has been completed, the DoD Components are authorized to use Tier 3 WMCT.

4. PUBLIC DoD INTERNET SERVICES

a. Authority, Mission, and Organization. A description of the DoD or the DoD Component's organizational structure, mission, and statutory authority shall be linked from major entry points (including homepages) on the DoD Federal Agency Public Website (http://www.defense.gov/) and the principal, public websites of the DoD Components consistent with Reference (c).

b. Contact Information. Contact information shall be linked from all major entry points on the DoD Component's principal public websites consistent with Reference (c). Consolidating this information on a single "Contact Us" page is recommended. Contact information must contain:

(1) Organization's postal address.

(2) Street addresses for any regional or local offices that have a function requiring interaction with the public.

(3) Office telephone number(s), including numbers for any regional or local offices or toll-free numbers and telephone device for the deaf (TDD) numbers, if available. If TDD lines are not available, use appropriate relay such as the Federal Relay Service as needed.

(4) Means to communicate by electronic mail (e.g., e-mail addresses, group mailbox).

(5) The policy, procedures, and time for responding to e-mail inquiries.

(6) Contact information to report data problems as required in Reference (bf).

(7) How to request information through section 552 of Reference (ae) pursuant to DoDD 5400.07 and DoD 5400.7-R (References (bh) and (bi)); and link to information made available specifically under FOIA. (DoD FOIA guidance is posted on the DoD Federal Agency Public Website.)

(8) Contact information for or link to the DoD or the DoD Component's office that promotes small business participation in defense acquisition pursuant to Reference (c) and PL 107-198 (Reference (bj)).

(9) Contact information to report both technical and information problems regarding the website specifically, including accessibility problems.

(10) A PAS or privacy advisory, as appropriate for the method of contact, in accordance with References (ah) and (aq). Subparagraphs 1.h. and 1.i. of this enclosure provide additional information.

c. "No Fear Act" Data. A link specifically labeled "No Fear Act Data" shall be placed on home pages of the DoD Federal Agency Public Website and the principal public websites of the DoD Components. This specific label must link to summary statistical data about equal employment opportunity complaints filed with DoD or with the DoD Components, as applicable, and written notification of whistleblower rights and protections pursuant to Reference (c) and PL 107-174 (also known as "The No Fear Act" (Reference (bk))).

d. Privacy Policy

(1) Clear privacy policies shall be posted or linked to on public DoD Internet services in compliance with References (c) and (ao) at major entry points and at those points or pages where personal information is collected from the public. Use the specific label "Privacy Policy." The privacy and security notice provided in Figure 2 may be tailored in the spaces indicated by square brackets ([…]) as shown in that figure's example.

Figure 2. Privacy and Security Notice

PRIVACY AND SECURITY NOTICE

1. [Name of service (e.g., "Website Title")] is provided as a public service by [name of the DoD Component(s)].

2. Information presented on this service not identified as protected by copyright is considered public information and may be distributed or copied. Use of appropriate byline, photo, and image credits is requested.

3. For site management, information is collected [Link "information is collected" to description of specific information. An example is provided after paragraph 8. in this figure] for statistical purposes. This U.S. Government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, software programs are employed to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations and national security purposes, no other attempts are made to identify individual users or their usage habits beyond DoD websites. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration Guidelines. [Agencies subject to Reference (o) shall add the following sentence to this paragraph: "All data collection activities are in strict accordance with DoD Directive 5240.01."]

6. Web measurement and customization technologies (WMCT) may be used on this site to remember your online interactions, to conduct measurement and analysis of usage, or to customize your experience. The Department of Defense does not use the information associated with WMCT to track individual user activity on the Internet outside of Defense Department websites, nor does it share the data obtained through such technologies, without your explicit consent, with other departments or agencies. The Department of Defense does not keep a database of information obtained from the use of WMCT. [If the DoD CIO has provided explicit written approval to use Tier III WMCT, cite that approval here.] General instructions for how you may opt out of some of the most commonly used WMCT is available at http://www.usa.gov/optout_instructions.shtml.

7. Unauthorized attempts to upload information or change information on this site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act (18 U.S.C. § 1030).

8. If you have any questions or comments about the information presented here, please forward them to [contact information to report both technical and information problems with the website specifically, including accessibility problems].

Figure 2 continued on next page

Figure 2. Privacy and Security Notice, Continued

EXAMPLE
Information Collected from [Name of site or "This website"] for Statistical Purposes

xxx.yyy.com -- [28/Jan/2008:00:00:01 -0500] "GET /Defense/news/nr012708.html HTTP/1.0" 200 16704 Mozilla 3.0/www.google.com

xxx.yyy.com (or 123.123.23.12)-- this is the host name (or Internet protocol (IP) address) associated with the requester (you as the visitor). In this case, the requester is coming from the xxx.yyy.net address. Depending on the requester's method of network connection, the host name (or IP address) may or may not identify the user's specific computer. Connections via many Internet Service Providers (ISP) assign different IP addresses for each session, or only connect to the Internet via proxy servers, so the host name may only identify the ISP. The host name (or IP address) may identify a specific computer if that computer has a fixed IP address.

[28/Jan/2008:00:00:01 -0500] -- this is the date and time of the request

"GET /Defense/news/nr012708.html HTTP/1.0" -- this is the location of the requested file

200 -- this is the status code - 200 is OK - the request was filled

16704 -- this is the size of the requested file in bytes

Mozilla 3.0 -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages

www.google.com -- this indicates the last site the person visited, which indicates how people find the requested file.

Requests for other types of documents use similar information. Unless otherwise stated, no personally-identifiable information is collected.

(2) Provide privacy policies in a standard machine-readable format on public websites in addition to the human-readable text version. Section IV of Reference (ao) provides specific guidance.

e. Strategic and Annual Performance Plans. Link to the DoD or the DoD Component's strategic plan and annual performance plans from major entry points to the DoD Federal Agency Public Website and the principal public websites of the DoD Components, consistent with Reference (c).

f. USA.gov. Link to the USG's Official Web Portal, USA.gov, from major entry points to the DoD Federal Agency Public Website and, if deemed necessary, the principal public websites of the DoD Components, consistent with Reference (c).

5. IbC

a. General Provisions. Longstanding guidance on personal communication ethics and the handling and dissemination of DoD information continues to apply when using IbC. Policies and laws related to the protection, control, and release of DoD information, such as OPSEC, information security, and PII apply.

(1) Non-public or sensitive information shall not be collected, disseminated, stored, or otherwise processed via IbC unless directed to do so in statute, regulation, or Executive order. IbC are not subject to Federal or DoD IA standards, controls, or enforcement, and therefore may not consistently provide the protections necessary to prevent disclosure to inappropriate or unintended audiences.

(2) Authorized users are prohibited from installing unapproved software or applications on DoD-furnished equipment. Additionally, some IbC may offer mobile code that is prohibited from being executed on DoD furnished equipment in accordance with Reference (ar) or third party applications not covered by the signed DoD ToS with the IbC. Such offers should not be used or installed without approval. Third party applications include, but are not limited to, games, hobbies, photography tools, or mobile code as categorized in Reference (ar).

(3) DoD policy prohibits authorized users from using, installing, or configuring peer-to-peer file-sharing applications, unless these actions are approved for mission enhancing functions consistent with ASD(NII) Memorandum (Reference (bl)).

b. Personal Use. DoD employees are not prohibited from establishing IbC accounts for personal use; however, the following provisions apply:

(1) Contractual Obligation or Agreements. Personal accounts with IbC are not covered by ToS agreements implemented by DoD. The DoD shall not be a party to, nor in any way responsible for, individual obligations or agreements established with IbC for personal use.

(2) Contact Information. Use non-mission related contact information, such as personal telephone numbers or postal and e-mail addresses, to establish personal accounts, when such information is required.

(3) Communication and Standards of Conduct

(a) Barring absence of official communication channels, personal accounts shall not be used to conduct official DoD communication. Personal accounts may be used to participate in activities such as professional networking, development, and collaboration related to, but not directly associated with, official mission activities as a DoD employee or DoD contractor.

(b) Personal communication shall be conducted in compliance with Reference (l). The dissemination and discussion of non-public information shall be avoided and opinions shall be disclaimed as necessary in accordance with paragraphs 2-207 and 2-301 of Reference (l). Sensitive and classified information, and unclassified information that aggregates to reveal sensitive or classified information, shall not be disclosed.

(c) When use of DoD systems for authorized purposes is allowed by the DoD and OSD Component Heads or designees, such communication shall be conducted in compliance with paragraph 2-301(a)(2) of Reference (l).

c. Official Use. In addition to approving the establishment of EOP as described in subparagraph 7.a.(4) of Enclosure 2, and consistent with section 2-301 of Reference (l), the DoD and OSD Component Heads may approve the establishment of IbC accounts by authorized users for public communication related to other assigned duties, such as recruiting, or any other purpose determined necessary in the interest of the Federal government. The following provisions apply to official use:

(1) DoD and OSD Component Heads and official-use account users must be prepared to account fully for exercising sound judgment within the authority and scope of official activities.

(2) Liaison shall be conducted with public affairs and OPSEC staff to ensure organizational awareness of their authorized, mission-related public communication.

(3) The use of IbC for security breaches (e.g., hacking), disclosure of PII, and for fraudulent or objectionable use shall be monitored. If an authorized user posts their PII on IbC, the DoD will not be responsible for negative consequences such as identity theft, public embarrassment, or any other untoward event.

(4) Written requests (letters or emails) shall be submitted to IbC providers to block the display of any commercial advertisements, solicitations, or links on EOP and IbC pages administered with official-use accounts if the IbC provider would otherwise normally display such materials. Use the disclaimer in Figure 1 of this enclosure if required. Refer to paragraphs 3.a. and 5.c.(8) of this enclosure for additional guidance.

(5) Establishing an official presence on, or use of, an IbC may require acceptance of a ToS agreement. The "standard" ToS used by the IbC provider may contain legally objectionable terms and conditions, which must be amended or otherwise addressed for DoD use. Additionally, IbC providers may agree only to such amended terms and conditions for limited portions of their products and services.

(a) DoD employees and DoD contractors who establish an EOP or other official uses on an IbC shall verify whether a ToS for that IbC has been signed and approved by the DoD CIO. Such ToS apply to DoD-wide use and operation of EOP and other official uses. In this case, there is no need for additional ToS at the Component level. Signed and approved ToS are listed at http://www.defense.gov/socialmedia/terms-of-service.aspx.

(b) If a ToS agreement for an IbC has not been signed by the DoD CIO, establish, in coordination with the DoD CIO, a ToS agreement signed at either the DoD CIO or the DoD Component level. The General Services Administration (GSA) provides ToS templates appropriate for Federal government use at https://www.apps.gov/ that shall be adapted for DoD use if available for the desired IbC. Initiate coordination with the DoD CIO via digitally-signed

e-mail to ToS-Application@osd.mil. Coordination with the DoD CIO will include determination of appropriate coordination with CDRUSSTRATCOM and with Component or DoD General Counsel.

(6) Contact Information and Identification

(a) Use mission related contact information, such as official duty telephone numbers or postal and e-mail addresses, to establish official-use accounts when such information is required.

(b) Depending on the requirements of the specific IbC, official-use account pages for individuals and pages representing DoD organizations shall be established in the category "Government," and registered to organization names that begin with, "U.S. Department of Defense/[insert name of organization or name of component]." This requirement does not apply to creation of a specific account name, handle, or nickname.

(c) When using an IbC for official use, the transparency banner described in Figure 3 shall be posted, as possible, to ensure clear distinction between the collaborative forum or discussion board of the IbC and the official information available on the DoD Component's website.

Figure 3. Transparency Banner

"Welcome to the [name of DoD Component]'s [name of IbC] page/presence. If you are looking for the official source of information about the [name of DoD Component], please visit [address of official website or other official information].

The [name of DoD Component] is pleased to participate in this open forum in order to increase government transparency, promote public participation, and encourage collaboration.
Please note that the [name of DoD Component] does not endorse the comments or opinions provided by visitors to this site. The protection, control, and legal aspects of any information that you provided to establish your account or information that you may choose to share here is governed by the terms of service or use between you and the [name of IbC].

Visit the [name of DoD Component] contact page at [address of official website or other official information] for information on how to send official correspondence."

(7) Communication

(a) Sensitive and classified information, and unclassified information that aggregates to reveal sensitive or classified information, shall not be disclosed.

(b) Official-use accounts shall not be used to conduct communication not related to assigned duties, functions, or activities.

(c) IbC shall be used as supplemental communication or distribution channels for DoD information. Do not establish or represent official-use accounts or pages as primary sources of DoD information.

(d) A clear description of the purpose for using the IbC and that DoD is the content provider shall be posted, as possible.

(e) Links to official DoD content hosted on DoD-owned, -operated, or -controlled sites shall be posted, where applicable and possible, when official use of an IbC references materials originating from an official DoD website.

(f) Links shall be posted to the organization's official public website.

(g) Specific steps to protect individual privacy whenever third-party websites and applications are used to engage with the public shall be implemented in compliance with Reference (at).

(8) Disclaimers

(a) "For official information from or about the U.S. Department of Defense/[insert name of organization], please visit our [insert homepage or other official information source] at [insert address]." shall be placed in a prominent location on each authorized page as workable.

(b) If the IbC provider is unwilling or unable to block the display of commercial advertisements, the following message shall be placed in a prominent location on each authorized page as workable: "The appearance of commercial advertising and hyperlinks inserted by the host of this service does not constitute endorsement by the U.S. Department of Defense/[insert name of organization]."

(9) Transparency Banner. As workable, the standard transparency banner in Figure 3 shall be displayed on EOP and other official uses of IbC.

(10) Internet Address Shortening. Some IbC services (e.g., Twitter, Facebook) encourage shortened address links to fit text and character limitations. Go.USA.gov is available to create short .gov address links for official government addresses in the .gov and .mil domains. For official government addresses in other domains, commercial address shorteners may be used.

6. SPECIFIC EOP REQUIREMENTS. EOP activities must be conducted in compliance with the general requirements listed in sections 1 through 5 of this enclosure as workable. Additional requirements, specific to EOP, include:

a. Approval shall be obtained from the responsible DoD Component Head before establishing EOP.

b. Official branding shall be used in accordance with DoDD 5535.09 (Reference (bm)) and other guidance that may be issued by the ASD(PA).

c. Clear identification that a DoD Component provides the content for the EOP shall be provided.

d. The DoD Component under which the EOP is managed, the mission of that Component, and the purpose of the EOP shall be provided, as workable.

Appendix
Information Review Process

APPENDIX TO ENCLOSURE 3

INFORMATION REVIEW PROCESS

1. PURPOSE. This appendix is an overview of the process to determine appropriate application of IA, information security, and OPSEC for DoD information. This process must be applied to all DoD information proposed for dissemination. The process results in clearance approval that verifies information is appropriate for release to the public and dissemination via public DoD Internet services and IbC, or that the information is not appropriate for release to the public and must be disseminated via a private DoD Internet service. Clearance approval supports the final authorization for release and dissemination of DoD information.

2. REQUIREMENTS

a. DoD and OSD Component Heads and subordinate organizations that disseminate DoD information via unclassified DoD Internet services and IbC are responsible for instituting an information review process. The process in this Appendix represents DoD best practices and should be implemented to the greatest extent possible. However, DoD and OSD Component Heads may authorize modification of this process to serve the requirements of their Component's mission or need most effectively, including the requirement to support government transparency, collaboration, and accountability by making the maximum amount of useful information available to the public.

b. All information proposed for dissemination must be reviewed internally and be compliant with the provisions described in this appendix prior to clearance approval, release authorization, and subsequent dissemination.

c. When information proposed for public release meets the criteria provided in Reference (j), it must additionally be reviewed by the DoD Office of Security Review (OSR).

3. INFORMATION REVIEW

a. Information review is the evaluation of information intended for dissemination beyond the control of the originating organization. It determines whether the information may be disseminated outside the organization's control and the scope of such dissemination, including information being disseminated to the public. The information review process must take into account multiple equities:

(1) The disseminating organization whose interests are focused on providing information efficiently and effectively to meet mission requirements. (These interests must be balanced against the need to minimize risk to personnel and the ability to execute the mission. If the organization that intends to disseminate the information is not the originating office, the

originator will be included in the review process as required by subparagraph 4.c. of this appendix.)

(2) Information security, which is focused on protecting and safeguarding classified and controlled unclassified information (CUI).

(3) OPSEC, which is focused on the protection of unclassified critical information that may individually or in aggregate lead to the compromise of classified information, operational missions, and sensitive activities.

(4) IA, which is focused on ensuring the confidentiality, integrity, and availability of the information through operational procedures and secure configuration of the DoD Internet service and the IS supporting the DoD Internet service, including access controls and other technical measures to restrict access to intended audiences.

(5) DoD principles of information and quality of information disseminated to the public consistent with References (be) and (bf).

(6) Other functions or offices as designated by the DoD Component.

b. The information review process established by each DoD or OSD Component Head shall, at a minimum:

(1) Hold subordinate organizations or officials responsible for ensuring that there is a valid mission need to disseminate the information and that information review procedures are implemented and consistently followed.

(2) Designate individuals to review all information intended for dissemination, and determine the appropriate and intended audience and access, distribution, or release controls. Designated individuals shall be educated in related IA, OPSEC, information security, and release requirements.

(3) Designate individuals who are authorized to determine clearance approval for unclassified DoD information.

(4) Evaluate information for OPSEC concerns and other sensitivity (e.g., classification, identification as For Official Use Only (FOUO) or other CUI category), including sensitivity in the aggregate.

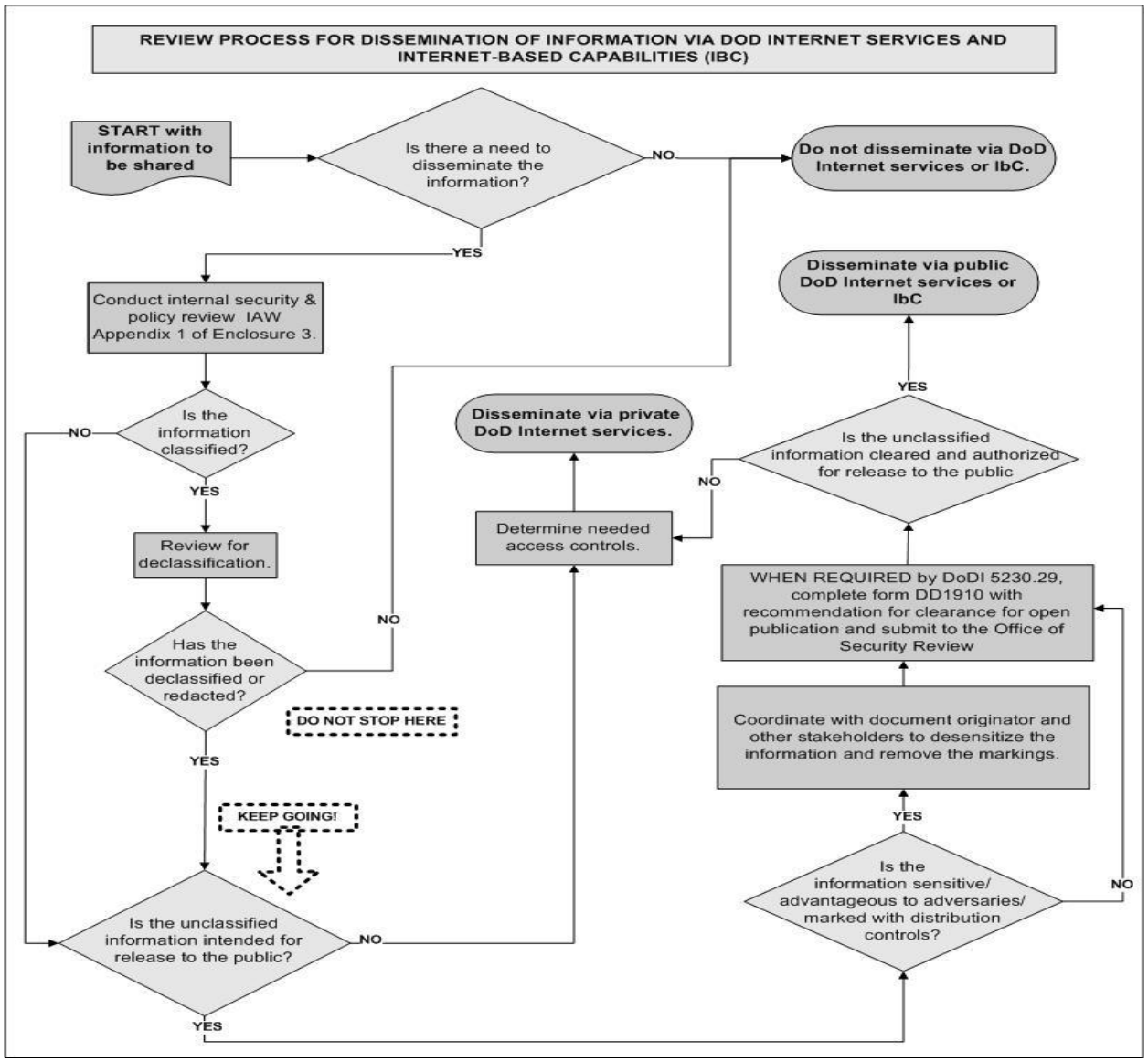
(5) Determine the appropriate and intended audience and access, distribution, or release controls.

(6) Coordinate among the multiple functions with equities and responsibilities in the release of information.

c. Clearance for disseminating information via public DoD Internet services or IbC must be in accordance with the provisions of References (i) and (j) and this Instruction. Clearance can be determined only by an appropriately trained individual specifically delegated that responsibility from the DoD or OSD Component Head or a designee. Approving authorities should verify compliance with applicable requirements of Enclosure 3 and appropriate execution of the procedures in section 4 of this appendix prior to issuing clearance approval.

d. The information review process is outlined in Figure 4.

Figure 4. Information Review Process Flow Chart



4. PROCEDURES

a. Step 1. Identify the purpose for disseminating the information and the target audience. The target audience and proposed scope of dissemination (e.g., public, USG-restricted, internal to the DoD Component, or organizational intranet) shall be identified for each proposed dissemination of information.

(1) Officials disseminating DoD information shall restrict access to the appropriate audience. Only information that is valuable or useful to the general public and that does not require additional protection may be disseminated via public DoD Internet services and IbC. Information requiring additional protection should be disseminated via private DoD Internet services as outlined in Step 4 of these procedures.

(2) Non-public information may not be disseminated via public DoD Internet services or IbC. The lack of classification or control markings alone does not meet the criteria for the public release of unclassified information. Information not specifically cleared and authorized for public release may be disseminated only via non-public means, such as intranets and private DoD Internet services. Examples of non-public information include information of questionable value to the public; information for which dissemination poses an unacceptable risk to the DoD, including information about employees and family members; and information intended only for DoD employees.

(3) Table 3 provides examples of the types of information appropriate for a specific audience and the associated access-control levels that should be used.

Table 3. Audience, Information, and Access Control

AUDIENCE	TYPES OF INFORMATION	INFORMATION SENSITIVITY	ACCESS CONTROL
Public	Documents marked "cleared for public release;" general/news related information; installation/unit history; general mission information; policies authorized for public release.	Non-sensitive; of general interest to the public; cleared and authorized for public release; worldwide dissemination poses limited risk for DoD or DoD personnel, even if aggregated with other information reasonably expected to be in public domain.	None.
Government Only; or DoD and specific partners/ communities/ families	Base/command news, letters, announcements; news summaries; general base/command morale, welfare, and recreation.	Non-sensitive, cleared and authorized for public release, but not of general interest to the public and intended for DoD or other specifically targeted audience, or as defined in Reference (bh).	No mandatory access controls, unless required by other issuances. However, as this information is not intended for the general public access should be limited to target audiences. May be internal-facing with no additional access controls or external-facing with minimal controls such as IP/ domain restriction.
Government Only; or DoD and specific	Non-public conferences; interagency program information; documents	Controlled unclassified information (e.g., FOUO); information sensitive by	Access must be limited to target audience. External-facing with access controls

Table 3. Audience, Information, and Access Control, Continued

AUDIENCE	TYPES OF INFORMATION	INFORMATION SENSITIVITY	ACCESS CONTROL
partners/communities	marked with handling/ dissemination restrictions; workflow management systems such as content management systems or document control systems.	aggregation/compilation; information with distribution restrictions; and other non-public information. Information restricted to authorized patrons (e.g., commercial advertising), or as defined in Reference (bh).	such as Common Access Card, UserID + Password, and Personal Identity Verification, used to restrict access to audience. Public Key Enabling shall be completed in accordance with Reference (aw).
DoD only	DoD conference information; reports; security bulletins; operating procedures; non-public events; documents marked with handling/ dissemination restrictions.	Controlled unclassified information; information sensitive by aggregation/ compilation; information with distribution restrictions; and other non-public information. Information restricted to authorized patrons, or as defined in Reference (bh).	Access must be limited to target audience. Internal-facing; may require additional access controls to restrict access to audience.
Internal to DoD Component	Internal office procedures; detailed organizational charts; internal memorandums; documents marked with handling/dissemination restrictions.	Controlled unclassified information, information sensitive by aggregation/ compilation, information with distribution restrictions, and other non-public information, or as defined in Reference (bh).	Access must be limited to target audience. Internal-facing with additional access controls restricting access to the members of the DoD Component.

b. Step 2. Conduct internal review. The organization's subject matter experts (SMEs) shall assess the sensitivity of information proposed for dissemination. The SMEs must be trained and knowledgeable enough to assess the information taking into account:

(1) Rules governing information classification:

(a) Information review procedures for unclassified information about classified programs proposed for release to the public must take into account the likelihood of classification by aggregation. Consulting the program security classification guide (available from the respective program manager or program management office) may be required to determine the likelihood that the information, if aggregated with other information likely to be available on public DoD Internet services or IbC, will reveal an additional association or relationship that meets the standards for classification in accordance with Reference (aa). If such information is posted to a DoD Internet service, it must be afforded effective access controls to prevent such aggregation of information.

(b) In instances where a question arises as to whether information in aggregation requires protection as classified information, and the information has not yet been disseminated, the originating office(s) or the original classification authority for the information shall be contacted to obtain a decision on the matter before the information is disseminated. Where the information has already been disseminated, the information will be withdrawn from the system

and will not be re-posted until a decision is obtained from the originating office(s) or original classification authority for the information. Searches for cached or archived copies of the information should be performed and, where found, removed or otherwise deleted. In instances where there are irresolvable conflicts among the originating offices as to the sensitivity of the information, refer the matter to the next higher level within each of the organizations until a resolution is obtained.

(c) Users of DoD Internet services or IbC who believe that information in compilation or aggregation on a system or systems to which they have access results in classified information, should contact the information owner(s) or, if the information owner(s) is (are) unknown, report the matter to the respective organization's information security office for evaluation and action.

(2) Rules governing CUI, including FOUO and PII. FOUO information, as defined in Reference (bh), shall be protected by access controls as specified in Step 4 (subparagraph 4.d.) of this appendix. Questions about FOUO and other CUI should be referred to the local OPSEC or FOIA office. Types of information that usually meet these criteria include:

(a) Information whose release could substantially hinder the effective performance of DoD military operations and exercises, such as standard operating procedures; tactics, techniques, and procedures (TTPs); information on intelligence, surveillance, and reconnaissance capabilities; command and control and IT architectures and configurations; mobilization, "bed down" or unit movement data and schedules; specificity about unit readiness and unit shortfalls; operation schedules; logistics support requirements, including host nation support; and detailed maps or installation photography.

(b) Proprietary information submitted by a contractor and protected by a limited rights statement or other agreement, trade secrets, and commercial and financial information submitted by an entity outside the government that considers the information to be protected from release to the public.

(c) Test and evaluation information that could result in an unfair advantage or disadvantage to the manufacturer or producer.

(d) Technical information not marked, or otherwise determined to be appropriate for Distribution Statement A as described in Reference (ak). This includes all technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment.

(e) Security classification guides that, if not classified, must be designated FOUO and restricted from dissemination via public DoD Internet services and IbC.

(f) Personal information, as defined in Reference (aq). When posted on DoD Internet services, the requirements of Enclosure 3, subparagraph 1.e.(2) shall be met.

(3) Rules governing OPSEC in accordance with Reference (q). Risk to information related to critical aspects of the organization's operations, including information that may be valuable to an adversary, must be evaluated prior to release. Evaluation of information disseminated via public DoD Internet services and IbC will follow the OPSEC methodology:

(a) Determine the critical information for the activity's operations and plans. Such critical information shall not be publicly accessible, and shall be protected by appropriate access controls. Critical information may include, but is not limited to:

1. Analysis and recommendations concerning lessons learned that would reveal sensitive military operations, exercises, or vulnerabilities.

2. Information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of a military plan or program.

(b) Consider the threat. Identify potential adversaries and their capability to exploit the information to their advantage and our detriment. Assume that any potential adversary has access to public pages and knows how to search the Internet. Search engines can be leveraged as a tool to facilitate data aggregation. Is there an increase in sensitivity of certain information when available electronically or aggregated via data mining?

(c) Assess vulnerabilities. How protected is the DoD Internet service? Are adequate methods of IA, such as access controls, implemented?

(d) Assess the risk. What is the chance of damage if critical information is exploited by an adversary and how great would the damage be? Assessing a higher risk provides justification for the use of protection measures.

(e) Apply protection. Apply the protection needed to minimize potential loss of critical information. Combine information security, IA, and OPSEC measures to minimize information vulnerability.

(f) Adjust content. If the information review process determines that public dissemination of the information would result in an unacceptable level of overall risk, the level of detail in the information must be reduced or access to the information must be restricted by access controls consistent with Step 4 of this appendix.

c. Step 3. Conduct information review for release.

(1) Unclassified information that pertains to military matters, national security issues, subjects of significant concern to DoD, or information proposed for public release in the National Capital Region by senior leaders must be cleared via security and policy reviews and approved by designated authorities within the DoD Components prior to dissemination via public DoD Internet services or IbC. Such information must also be reviewed and cleared by the DoD OSR prior to public release consistent with Reference (j).

(2) Prior to OSR review, organizational SMEs must conduct an internal review as specified in subparagraph 4.b. of this appendix to determine whether the information being considered for clearance falls within the categories listed in Reference (j).

(3) The office or entity that created or sponsored the work that generated the information or received or acquired the information on behalf of DoD (the "originating office") shall be consulted whenever there is doubt with regard to the sensitivity of the information or distribution restrictions on its release. The originating office is responsible for determining:

(a) Any appropriate markings to be applied to the information based on its sensitivity (e.g., classification, distribution control markings for CUI).

(b) The information's releasability to the public.

(c) The approved audience(s) for access (e.g., DoD only, contractors, the public).

(4) Policies and guidance governing release of specific categories of information also apply to information disseminated via unclassified DoD Internet services and IbC.

d. Step 4. Determine appropriate access controls.

(1) Access controls and other IA methods shall be applied in order to restrict access to the target audience effectively. Determinations as to the appropriate access controls and other IA methods to employ are to be based on the sensitivity of the information, the audience for whom the information is intended, and the level of risks to DoD interests (i.e., the outcomes of Steps 1 through 3).

(a) Access controls and other IA methods shall be used to ensure information that requires additional protection is not accessible to the public or other unauthorized persons. Proper functioning of such controls shall be verified annually consistent with Reference (g).

(b) Organizations shall not disseminate, or otherwise make available, CUI or information not specifically cleared and authorized for public dissemination via public DoD Internet services or IbC. Such information must be limited to private DoD Internet services.

(2) Use Table 3 to assist in determining the required access controls. These guidelines are not the only technical options available for appropriately protecting information; check with an IA expert or network administrator regarding other alternatives.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(PA)	Assistant Secretary of Defense for Public Affairs
CI	counterintelligence
CIO	Chief Information Officer
CDRUSSTRATCOM	Commander, United States Strategic Command
CUI	controlled unclassified information
DA&M	Director of Administration and Management
DepSecDef	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DMZ	de-militarized zone
DoDD	DoD Directive
DoDI	DoD Instruction
DTM	Directive-Type Memorandum
EOP	external official presence
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GC, DoD	General Counsel of the DoD
GIG	Global Information Grid
IA	information assurance
IbC	Internet-based capabilities
IP	Internet protocol
IS	information system
ISP	Internet service provider
JWRAC	Joint Web Risk Assessment Cell
LE	law enforcement
NCES	Net Centric Enterprise Services
NIPRNET	Non-classified Internet Protocol Routed Network.
OMB	Office of Management and Budget
OGC, DoD	Office of the General Counsel of the Department of Defense
OPSEC	operations security
OSR	Office of Security Review

PAS	privacy act statement
PIA	privacy impact assessment
PII	personally identifiable information
PL	public law
PM	personnel misconduct
SAOP	Senior Agency Official for Privacy
SME	subject matter expert
SoRN	system of records notice
TDD	telephone device for the deaf
ToS	terms of service
TTP	tactics, techniques, and procedures
URL	uniform resource locator
U.S.C.	United States Code
USD(I)	Under Secretary of Defense for Intelligence
USG	U.S. Government
WMCT	web measurement and customization technologies
WHS	Washington Headquarters Services

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

access control. Technical measure or physical process used to grant or deny specific requests to obtain and use information and related information processing services. Also includes the use of a technical measure to enable customization or enhancement of a single user's experience.

advertisement or advertising. Material or information, regardless of media, disseminated in exchange for any remuneration or intended to promote any service, facility, or product of non-USG entities.

authorized user. Defined in Reference (j).

disseminate. To broadcast, publish, or to take other action to ensure availability beyond the control of the originating source or organization responsible for control of the information.

DoD employee. Defined in Reference (l).

DoD information networks. Defined in Reference (t).

DoD Internet services. All information capabilities and applications available across the Internet in locations owned, operated, or controlled by the DoD. DoD Internet services include collaborative tools such as websites, social networking, social media, user generated content,

social software, e-mail, and instant messaging and discussion forums delivered through a variety of platforms and presentation mediums. This term and its definition are proposed for inclusion in the next edition of Joint Publication 1-02 (Reference (bn)).

DoD website. Any website owned, operated, or controlled by or for DoD, funded with DoD appropriations, or operated by authorized users as part of their official duties. Also includes websites that are operated as outsourced DoD services on non-DoD networks. This term and its definition are proposed for inclusion in the next edition of Reference (bn).

EOP. Official public affairs activities, as defined in DoDI 5400.13 (Reference (bo)), conducted on IbC (e.g., Combatant Commands on Facebook).

external-facing. Available via the Internet to authorized users from any location. A DoD Internet service being external-facing has no bearing on whether it is public or private, i.e., both public and private DoD Internet services may be external-facing.

Federal Agency Public Website. Defined in Reference (c).

high-value. Defined in Reference (k).

IbC. All public information capabilities or applications available across the Internet from locations not directly or indirectly controlled by DoD or the Federal government (i.e., locations not owned or operated by DoD or another Federal agency or by contractors or others on behalf of DoD or another Federal agency).

internal-facing. Existing on DoD ISs for an internal DoD or USG, non-public audience. Not available to or from the general public Internet.

Internet-capable device. Any communication device from which one could access the Internet.

Internet media. Files delivered or acquired using any Internet protocol or supporting technology (e.g., web pages, data or text, e-mail, video, audio, graphic, instant messages, chat).

National Capital Region. Defined in Reference (bn).

non-public information. Information generally not available to the public, obtained in the course of one's official DoD duties or position, that has not been cleared and authorized for release to the public or would normally not be released under the FOIA, if requested. It includes inside information, proprietary information, source selection information, CUI, and other categories of information that are to be withheld from the public. References (aa), (ae), and (bh), Subpart 2635.703 of title 5, Code of Federal Regulations, and sections 3.104-4 and 3.104-5, Federal Acquisition Regulations (References (bp) and (bq)) provide detailed information.

official DoD information. Defined in Reference (i).

official use. Defined in Reference (l), and, for the purposes of this Instruction, includes authorized communication or activities conducted as an assigned DoD employee function.

original classification authority. Defined in Reference (aa).

personal use. Individual communication or activity that is not conducted as an assigned DoD employee function.

PII. Defined in Reference (aq).

private DoD Internet service. A DoD Internet service with access controls in place to limit availability of non-public information or exchanges of non-public information to specific audiences. This term and its definition are proposed for inclusion in the next edition of Reference (bn).

prohibited activity. Download, installation, or use of unauthorized software (e.g., applications, games, peer-to-peer software, movies, music videos, files); accessing pornography; unofficial advertising, selling, or soliciting; improperly handling classified information; using DoD ISs to gain unauthorized access to other systems or networks; endorsing non-USG products or services; participating in any lobbying activity or engaging in any prohibited partisan activity; posting DoD information to external newsgroups, bulletin boards, or other public forums without authorization; other uses incompatible with public service.

prohibited content. Applications, data, documents, files, software, or other information or materials acquired as a result of prohibited activity.

public DoD Internet service. A DoD Internet service used to collect, disseminate, store, or otherwise process information that has been cleared and authorized for release to the public. This term and its definition are proposed for inclusion in the next edition of Reference (bo).

public-facing. See external-facing.

sensitive information. Information, the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Reference (ae) (also known as "The Privacy Act"), but that has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

ToS. An agreement between DoD and an IbC provider establishing the rights and responsibilities of the parties with respect to the official use of the IbC by DoD authorized users. ToS agreements do not include procurement contracts and may not create financial obligations or liabilities on behalf of the U.S. Government. The process for entering into such agreements is outlined in subparagraph 5.c.(5) of Enclosure 3.

website. A set of interconnected pages, services, and associated Internet media available at a URL and prepared and maintained as a collection of information and services by a person, group, or organization.