DoD Directive 3115.18

DoD Access to and Use of Publicly Available Information (PAI)

Originating Component:	Office of the Under Secretary of Defense for Policy Office of the Under Secretary of Defense for Intelligence and Security
Effective:	June 11, 2019
Change 1 Effective:	August 20, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Approved by:	David L. Norquist, Performing the Duties of the Deputy Secretary of Defense
Change 1 (Administrative) Approved by:	Christopher R. Choate, Chief, Directives Division

Purpose: This issuance establishes policy and assigns responsibilities for DoD access to and use of PAI and establishes the DoD PAI Advisory Council (PAC).

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION 3
1.1. Applicability. 3
1.2. Policy. 3
1.3. Summary of Change 1. 4
SECTION 2: RESPONSIBILITIES 5
2.1. Under Secretary of Defense for Intelligence and Security (USD(I&S)). 5
2.2. USD(P). 5
2.3. Assistant Secretary of Defense for Special Operations and Low-intensity Conflict. 5
2.4. Chief Management Officer of the Department of Defense. 5
2.5. USD(R&E). 6
2.6. USD(A&S). 6
2.7. DoD Chief Information Officer. 7
2.8. General Counsel of the Department of Defense. 7
2.9. Assistant to the Secretary of Defense for Public Affairs. 7
2.10. DoD Component Heads. 8
2.11. Secretaries of the Military Departments. 9
2.12. CJCS. 9
SECTION 3: DOD PAC PURPOSE AND ORGANIZATION 10
3.1. Purpose. 10
3.2. Organization and Membership. 10
3.3. Meetings. 11
GLOSSARY 12
G.1. Acronyms. 12
G.2. Definitions. 12
REFERENCES 14

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) 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 (referred to collectively in this issuance as the "DoD Components").

b. This issuance should not be construed to prevent the free flow of news and information to the news media, the general public, internal DoD audiences, and other applicable forums, by DoD public affairs organizations in accordance with DoD Directive (DoDD) 5122.05, DoD Instruction (DoDI) 5400.13, and DoDI 5400.14, or the communication of DoD policies, strategies, and budget information to Congress by the Assistant Secretary of Defense for Legislative Affairs in accordance with DoDD 5142.01.

1.2. POLICY.

a. It is DoD policy to allow for lawful and appropriate access to and use of PAI, subject to the restrictions in this issuance and in accordance with law, policy, and regulations, including those governing privacy, civil liberties, research involving human subjects, records management and disposition, and acquisition of information concerning persons and organizations not affiliated with DoD.

b. DoD may access, obtain, and use PAI to plan, inform, enable, execute, and support the full spectrum of DoD missions.

(1) DoD Intelligence Components as defined in DoD Manual (DoDM) 5240.01 will comply with that manual when conducting intelligence activities.

(2) Except as otherwise specified by this policy, DoD Components not covered by DoDM 5240.01 will comply with DoDD 5200.27 when accessing and using PAI related to persons and organizations not affiliated with DoD for the purposes outlined in this issuance.

c. DoD will enable and support the use of PAI through the DoD PAC.

d. Access to and use of PAI for DoD purposes through DoD information systems must be conducted in accordance with appropriate operations security, information security, and cyber security policies, including DoDD 5205.02E; Volumes 1 through 4 of DoDM 5200.01; DoDI 8500.01; and DoDI 8170.01.

e. DoD should share PAI and PAI tools with federal, State, local, tribal, and foreign partners in accordance with applicable laws, regulations, international agreements, and policies, including those governing disclosure; dissemination of intelligence; protection of sensitive sources and methods; Section 1535 of Title 31, United States Code, also known as the "Economy Act;"

defense support to civil authorities; individuals' personally identifiable information; intellectual property; and contracts, terms of service, export controls, and international and technology transfer, including DoDI 2040.02.

f. DoD will share capabilities and data across the DoD Components when feasible (e.g., by using enterprise subscriptions and licenses) to reduce duplication and increase integration for lower costs and increased efficiencies.

g. DoD Components will have the ability to access PAI relevant to their missions through the Non-classified Internet Protocol Router Network on the DoD Information Network (DODIN) or other DoD-provided network in accordance with the risk management framework prescribed in DoDI 8510.01.

h. DoD personnel will not use false assertions of identity or organizational affiliation for official purposes to access, acquire, or use PAI without complying with cover policies including DoDD S-5205.61, DoDI S-5105.63, and other DoD guidance and issuances on the use of cover.

i. Managed attribution solutions and other security measures appropriate for the activity to mitigate risk and protect personnel, equipment, facilities, organizations, activities, mission equities, and programs. DoD personnel will only use managed attribution solutions:

(1) To perform authorized activities. Use of these solutions requires appropriate training, risk assessment, and DoD Component approval, which includes documenting the need for managed attribution solutions.

(2) With DoD or U.S. Government-approved devices or information systems, including approved hardware, software, networks, methods, and security measures appropriate to the mission and risk unless granted a waiver from a DoD Component head.

j. DoD personnel will comply with terms of service, e.g., those of social media providers, and other contractual obligations and not provide false information to the service provider unless approved in accordance with this issuance and other DoD policies.

k. No unfavorable personnel actions may be taken based solely on uncorroborated or unverified PAI.

1.3. SUMMARY OF CHANGE 1.

This administrative change updates:

a. The title of the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Intelligence and Security (USD(I&S)) in accordance with Public Law 116-92.

b. References for accuracy.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)). The USD(I&S) will:

a. Coordinate with the DoD Component heads to develop policy and guidance on DoD's access to and use of PAI for matters related to USD(I&S) responsibilities and functions in collaboration with other members of the DoD PAC.

b. Establish policy, issues guidance, provide direction, and oversee access to, and use of PAI for intelligence, counterintelligence, security, insider threat, sensitive activities, and intelligence-related purposes, consistent with assigned responsibilities and functions in DoDD 5143.01.

c. Coordinate with the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), the Under Secretary of Defense Research and Engineering (USD(R&E)), and the relevant DoD Component heads to develop and implement measures to synchronize DoD's access to and use of PAI tools, data, acquisition, automated analysis, storage, utilization, and final disposition.

d. Co-chair the DoD PAC with the USD(P).

2.2. USD(P). The USD(P) will:

a. In collaboration with other members of the DoD PAC, coordinate with the DoD Component heads to develop policy and guidance on DoD's access to and use of PAI for matters related to USD(P) responsibilities and functions.

b. Establish policy, issue guidance, provide direction, and conduct oversight on the use of PAI to fulfill assigned responsibilities and functions, in accordance with DoDD 5111.01.

c. Coordinate with the USD(I&S), the USD(A&S), the USD(R&E), and relevant DoD Component heads to develop and implement measures to synchronize DoD's access to and use of PAI tools, data, acquisition, automated analysis, storage, utilization, and final disposition.

d. Co-chair the DoD PAC with the USD(I&S).

2.3. ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS AND LOW-INTENSITY CONFLICT. Under the authority, direction, and control of the USD(P), the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict will advise and support the USD(P) at the PAC.

2.4. CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE. The Chief Management Officer of the Department of Defense will:

a. Ensure DoD PAI policy and procedures adequately consider and address privacy and civil liberty issues in accordance with the DoD privacy and civil liberties program and

DoDD 5105.53, DoDI 5400.11 and, subject to Paragraph 1.2.b.(2) of this issuance, with DoDD 5200.27.

b. Participate in and assist the DoD PAC in coordinating and enabling the appropriate access to and use of PAI in support of DoD missions.

2.5. USD(R&E). The USD(R&E) will:

a. In collaboration with other members of the DoD PAC, advise the DoD Components on research and engineering policy and guidance to support DoD research priorities for PAI for matters related to USD(R&E) responsibilities and functions.

b. Advocate and support the use and production of PAI for research and engineering. This includes technology development, technology transfer, prototyping, experimentation, and developmental testing for DoD. Facilitate the rapid development and transition of urgently needed technology and tools in support of DoD missions.

c. Support sustainment of PAI tools used for research and related resources, infrastructure, data sources, licenses, subscriptions, and services used by DoD.

d. Coordinate with the USD(I&S), the USD(P), the USD(A&S), and other DoD Component heads to develop and implement measures to synchronize DoD's acquisition of PAI tools and management of associated data, automated analysis, storage, and utilization.

e. Enable DoD capabilities through science and engineering applications to enhance the use of PAI.

f. Participate in and assist the DoD PAC in coordinating and enabling the appropriate access to and use of PAI in support of DoD missions.

2.6. USD(A&S). The USD(A&S) will:

a. In collaboration with other members of the DoD PAC, advise the DoD Components regarding acquisition policy and guidance on DoD acquisition of PAI for matters related to USD(A&S) responsibilities and functions.

b. Advocate and support the use and production of PAI for acquisition, procurement, and sustainment for the DoD.

c. Facilitate the acquisition of urgently needed technology and tools in support of DoD missions.

d. Support sustainment of PAI tools, data acquisition, and related resources, infrastructure, data sources, licenses, subscriptions, and services used by the DoD to combine requirements and acquisition efforts and reduce duplication of effort.

e. Coordinate with the USD(I&S), the USD(P), and other DoD Component heads to develop and implement measures to synchronize DoD acquisition of PAI tools and management of associated data, automated analysis, storage, and utilization.

f. Participate in and assist the DoD PAC in coordinating and enabling the appropriate access to and use of PAI in support of DoD missions.

2.7. DOD CHIEF INFORMATION OFFICER. The DoD Chief Information Officer will:

a. Set standards and establish policy to ensure access to PAI in the DoD information enterprise and DoD information and communication network in accordance with DoDD 5144.02.

b. Ensure DoD PAI policy and procedures adequately consider and address records management issues in accordance with DoDI 5015.02.

c. Participate in and assist the DoD PAC in coordinating and enabling the appropriate access to and use of PAI in support of DoD missions.

2.8. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. The General Counsel of the Department of Defense will:

a. Advise OSD organizations on the lawful access to, use of, and storage of PAI.

b. Support the Inspector General of the Department of Defense investigations of alleged violations pertaining to the access to, use of, and storage of PAI to ensure compliance with this issuance and applicable laws and regulations, in accordance with DoDD 5145.01.

c. Conduct legal reviews of PAI matters in coordination with the USD(I&S), the USD(P), and the CJCS.

d. Participate in and assist the DoD PAC in coordinating and enabling the lawful access to, use of, and storage of PAI in support of DoD missions.

2.9. ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS. The Assistant to the Secretary of Defense for Public Affairs will:

a. Establish policy, issue guidance, provide direction, and oversee public affairs access to and use of PAI to fulfill assigned responsibilities and functions in DoDD 5122.05.

b. Coordinate the release and dissemination of official public information to the news media.

c. In coordination with the DoD Chief Information Officer and affected DoD Component heads, provide public affairs guidance and best practices for official use of social media and the oversight and maintenance of official DoD social media accounts, in accordance with DoDI 8170.01.

d. Monitor the news media environment and other PAI to support DoD's mission, inform DoD public affairs operations, and respond to events with DoD equities.

e. Participate in and assist the DoD PAC in coordinating and enabling the appropriate access to and use of PAI in support of DoD missions.

2.10. DOD COMPONENT HEADS. The DoD Component heads:

a. May issue implementing guidance to their respective components and subordinate organizations for access to and use of PAI as necessary, consistent with the policy in this directive.

b. Plan, program, and budget for PAI capabilities to meet mission requirements.

c. Approve use of managed attribution solutions and other actions requiring approval for accessing and using PAI.

d. Are designated to approve exceptions for their respective components to Paragraphs 5.6. and 5.7. of DoDD 5200.27.

e. As necessary, train personnel to DoD standards and on appropriate use of PAI for force protection, warning, and other missions to protect personnel and mitigate foreign intelligence, counterintelligence, terrorist, and other threats.

f. Develop and implement a structure to ensure effective and appropriate oversight for the use of PAI, as appropriate, consistent with DoD policy and PAC guidance.

g. Develop criteria as necessary to meet DoD standards for mission-related access to PAI via non-DODIN infrastructure. Ensure DoD Components and subordinate organizations have the ability to access PAI through the DODIN and non-DODIN infrastructure, as required, and ensure appropriate security procedures are in place.

h. Apply operations security processes, in accordance with DoDD 5205.02E, to ensure threat-based risk mitigation measures and countermeasures when accessing PAI, as appropriate.

i. Collaborate with other DoD Components, as appropriate, for access to and use of PAI in support of the full spectrum of DoD missions, as necessary using established procedures and processes.

(1) The DoD Components share relevant PAI with other DoD Components for maximum utility.

(2) The DoD Components specify PAI-related intelligence requirements and request support from Defense Intelligence Components.

j. Support the rapid disclosure to and sharing of PAI and PAI tools with federal, State, local, tribal, and foreign allies and partners using established disclosure, information sharing, technology transfer, and other processes when necessary to support a DoD mission.

k. Enable, as appropriate, identity management processes to reduce vulnerabilities of DoD personnel to adversarial and criminal use of PAI consistent with applicable legal and policy requirements.

l. Identify applicable standards and required training, as appropriate, for personnel; approve an exploitation plan or concept of operations, as appropriate, for missions that carry risks associated with accessing PAI. The plan or concept of operations will address:

(1) Purpose, mission, and authority.

(2) Operations security requirements.

(3) Risk mitigation procedures.

(4) Appropriate oversight requirements.

m. Document component best practices for accessing, using, and assessing PAI. Share best practices with other DoD Components and, as practical and appropriate, with federal, State, local, tribal, and foreign allies and partners to help define legally acceptable and manageable PAI processes.

2.11. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in Paragraph 2.10., the Secretaries of the Military Departments will participate in and assist the DoD PAC in coordinating and enabling the appropriate access to and use of PAI in support of DoD missions.

2.12. CJCS. In addition to the responsibilities in Paragraph 2.10., the CJCS will:

a. In collaboration with other members of the PAC, issue guidance on joint force access to and use of PAI.

b. In coordination with the USD(I&S) and the USD(P), document and disseminate best practices for collecting, using, and accessing PAI from across DoD, interagency organizations, allied nations, and coalition partners, to assist DoD Components in defining acceptable and manageable PAI-related processes.

c. In coordination with the DoD Components, develop training standards to protect DoD personnel from counterintelligence, foreign intelligence, terrorist, and other threats, especially for use when accessing PAI on the internet.

d. Participate in and assist the DoD PAC in coordinating and enabling the appropriate access to and use of PAI in support of DoD missions.

SECTION 3: DOD PAC PURPOSE AND ORGANIZATION

3.1. PURPOSE. The DoD PAC serves as the senior DoD deliberative body to address DoD policy issues related to PAI. The PAC identifies, recommends, and promotes standard and supporting policies related to the use of PAI (e.g., regarding oversight, training, lexicon, and identity management). The DoD PAC:

a. Is an advisory body. The DoD PAC does not establish policy.

b. Recommends ways to improve the effectiveness of DoD use of PAI and its integration into wider DoD programs. The DoD PAC supports the use of PAI to satisfy the needs of the Military Departments and the Combatant Commands.

c. Establishes a PAI lexicon for DoD.

d. Provides a forum for the involved DoD Components on the coordination and planning for projected resources needed to access and use PAI; mechanisms for acquiring PAI data, analytic tools, and related infrastructure; acquisition; PAI training and certifications; investments in PAI; and risk mitigation related to accessing and using PAI.

e. Establishes working groups, as needed, to facilitate the coordination or execution of specific programs or to address DoD PAI needs, leveraging existing groups when possible.

3.2. ORGANIZATION AND MEMBERSHIP.

a. The DoD PAC is co-chaired by the USD(I&S) and the USD(P). Members of the DoD PAC must be Service members or full-time or permanent part-time federal employees.

b. The DoD PAC includes senior level individuals (at the executive or general officer/flag officer-level) designated by the head of each organization, including but not limited to the following DoD and OSD Components:

(1) Office of the USD(R&E).

(2) Office of the USD(A&S).

(3) Office of the Chief Management Officer of the Department of Defense.

(4) Joint Staff.

(5) Office of the Assistant to the Secretary of Defense for Public Affairs.

(6) Office of the DoD Chief Information Officer.

(7) Office of the General Counsel of the Department of Defense.

(8) Military Departments.

(9) Others as invited by the co-chairs.

3.3. MEETINGS.

a. The DoD PAC agenda is established jointly by the co-chairs. Any member of the PAC may nominate agenda items through their respective components.

b. The co-chairs are supported by a co-secretariat designated and provided by the USD(I&S) and the USD(P) who will organize DoD PAC meetings, manage agendas, and fulfill other administrative responsibilities related to the DoD PAC.

c. The DoD PAC will meet at least semiannually or as needed to address DoD mission needs.

d. DoD PAC working group members will support DoD PAC activities.

GLOSSARY

G.1. ACRONYMS.

CJCS	Chairman of the Joint Chiefs of Staff
DoDD	DoD directive
DoDI	DoD instruction
DODIN	DoD Information Network
DoDM	DoD manual
PAI	publicly available information
PAC	PAI Advisory Council
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

cover. The concealment of true identity or organizational affiliation with assertions of false information as part of, or in support of, official duties to carry out authorized activities or lawful operations.

Defense Intelligence Components. Defined in DoDM 5240.01.

identity management. A discipline that seeks to mitigate risks to force, mission, and capabilities through the discovery, examination, analysis, assessment, and management of an individual, organization, or asset's identity elements, characteristics, or other attributes in public or non-public records and databases, and social media or other unstructured data sources.

individual. Defined in DoDI 5400.11.

managed attribution. Actions to control how attributable information appears to an observer.

managed attribution solution. Hardware, software, networks, accounts, or other measures acquired and used to control how attributable information appears to an observer.

operations security. Defined in DoDD 5205.02E.

PAI. Information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by a casual observer, is made available at a

meeting open to the public, or is obtained by visiting a place or attending an event that is open to the public.

PAI tools. Applications or capabilities that mine or derive meaning from PAI data and that acquire, analyze, store, and disseminate PAI. PAI tools and those used for intelligence missions may overlap.

personally identifiable information. Defined in Section 552a of Title 5, United States Code, also known as the "Privacy Act," as amended.

REFERENCES

DoD Directive 5105.53, "Director of Administration and Management," February 26, 2008

DoD Directive 5111.01, "Under Secretary of Defense for Policy (USD(P))," June 23, 2020

DoD Directive 5122.05, "Assistant to the Secretary of Defense for Public Affairs (ATSD(PA))," August 7, 2017

DoD Directive 5142.01, "Assistant Secretary of Defense for Legislative Affairs (ASD(LA))," September 15, 2006

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 24, 2014, as amended

DoD Directive 5145.01, "General Counsel of the Department of Defense (GC DoD)," December 2, 2013, as amended

DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980

DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, as amended

DoD Directive S-5205.61, "(U) DoD Cover and Cover Support Activities," July 15, 2014

DoD Instruction 2040.02, "International Transfer of Technology, Articles, and Services," March 27, 2014, as amended

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Program," January 29, 2019

DoD Instruction 5400.13, "Public Affairs Operations," October 15, 2008

DoD Instruction 5400.14, "Procedures for Joint Public Affairs," November 3, 2014

DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Instruction S-5105.63, "(U) Implementation of Cover and Cover Support Activities," June 20, 2013

DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended

DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information," February 24, 2012, as amended

DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," February 24, 2012, as amended

DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020," December 20, 2019

United States Code, Title 31, Section 1535 (also known as the "Economy Act")

United States Code, Title 5, Section 552a (also known as the "Privacy Act"), as amended