U.S. CYBER COMMAND INSTRUCTION 5000.06

FREEDOM OF INFORMATION ACT PROGRAM

Originating Component:	Special Staff (J0)
Effective:	From date of digital signature.
Releasability:	Cleared for public release. Available on the Command Publications Website at https://intelshare.intelink.gov/sites/uscybercom/Library/SitePages/publications.aspx
Reissues and Cancels:	United States Cyber Command Instruction (USCCI) 5000.06, "Freedom of Information Act Program," April 8, 2019
Applicability:	This Instruction applies to: o All Headquarters (HQ) United States Cyber Command (USCYBERCOM) military, civilian, and contractor personnel. o USCYBERCOM subordinate organizations to include the Service Cyberspace Components, the Joint Force HQ-Cyberspace, the Joint Force HQ-Department of Defense (DoD) Information Network, and designated Joint Task Forces.

VELEZ.DENNIS.[redacted] Digitally signed by VELEZ.DENNIS.[redacted] Date: 2025.01.27 12:44:32 -05'00'

Approved by: DENNIS VELEZ
Rear Admiral, U.S. Navy
Chief of Staff

Purpose: This instruction establishes policies, procedures, roles, and responsibilities for the implementation of the USCYBERCOM Freedom of Information Act (FOIA) Program.

Summary of Changes: The following changes are included:

- Expands and updates the roles and responsibilities of the FOIA Program Manager, the FOIA Case Manager, and the Subject Matter Expert.
- Removes J-Code Directors roles and responsibilities, as this was never implemented.
- Adds roles and responsibilities for all USCYBERCOM personnel.
- Updates, revises, and expands the section "Procedures" to reflect the actual/current FOIA methods and processes.
- Re-titles and expands section titled "FOIA-like review" to the "Mandatory Declassification Review (MDR) Requests."
- Adds the section "Privacy Act Request" not previously included in the previous version of the instruction to ensure completeness of FOIA procedures.
- Adds terms to the Glossary section.
- Re-titles "Informative Websites" to "Links."
- Adds to and updates "References."

TABLE OF CONTENTS

SECTION 1: GENERAL INFORMATION

1.1. BACKROUND INFORMATION.

a. FOIA, United States Code (USC), Title 5, Section 552 and Public Law (PL) 93-579), are the laws that establish the publics' right to request records from federal government agencies. A FOIA request may be filed by any person, including any member of the public (U.S. or foreign citizen/entity), an organization, or a business, but not including a Federal Agency or a fugitive from the law.

b. The FOIA provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that they are protected from disclosure by law.

c. The FOIA promotes public trust by encouraging that the maximum amount of information be made available to the public regarding the operation and activities of the government.

d. The Privacy Act of 1974, codified in Section 552a of Title 5 USC, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

e. The DoD FOIA Program is governed by Part 286 of Title 32, Code of Federal Regulations (CFR) with the rules for Privacy Act protections being established in Part 310 of 32 CFR. These rules apply to all records in Privacy Act systems of records (SORs) maintained by the DoD and describe the procedures by which individuals may request access to records about themselves, request amendment or correction of those records, and request an accounting of disclosures of those records by the DoD to other entities outside the DoD. DoD adherence to Part 310 of 32 CFR for processing all Privacy Act requests for access to records under the FOIA, codified in Section 552 of Title 5 USC, provides individuals the protections of both statutes.

1.2. POLICY.

a. DoD Directive (DoDD) 5400.07 establishes policy and assigns responsibilities for the DoD FOIA Program in accordance with (IAW) the FOIA.

b. DoD Manual (DoDM) 5400.07 implements the DoD FOIA Program pursuant to this directive, supplements Part 286 of 32 CFR and incorporates amendments to Section 552 of Title 5 USC, the Open, Public, Electronic, and Necessary (OPEN) Government Act of 2007 (Public Law 110-175) and the FOIA Improvement Act of 2016 (Public Law 114-185).

c. Due to its size and complexity, the DoD FOIA Program is decentralized, and DoD Components operate their own FOIA offices. USCYBERCOM established its FOIA requester service center in July 2018. The USCYBERCOM FOIA Program is codified in this instruction.

SECTION 2: ROLES & RESPONSIBILITIES

2.1. CHIEF OF STAFF (COS).

a. Oversees the command FOIA program.

b. Serves as the Initial Denial Authority (IDA).

(1) The Commander, USCYBERCOM, delegated IDA to the CoS on July 2, 2019.

(2) The CoS may authorize additional personnel to deny FOIA requests for reasons other than exemptions IAW DoDM 5400.07 section 6.3.b.

2.2. CHIEF KNOWLEDGE OFFICER.

a. Directs, manages, and administers the command FOIA program.

b. Designates the FOIA program manager in writing.

c. Is authorized to deny FOIA requests for reasons other than exemptions.

2.3. FOIA PROGRAM MANAGER (FPM).

a. Leads the command FOIA program office (FPO). The FPM leads analysis of FOIA requests submitted to HQ USCYBERCOM and its subordinate components. As the command's principal FOIA technical authority, provides guidance on interpretation and application of statutes and regulations to the command's leadership and to colleagues responsible for generating and managing information for which FOIA requests have been made.

b. Determines program requirements, based on analysis of statutes and regulations, and insights into FOIA requests and resources likely to be required to address them. Develops and codifies disclosure policies and procedures implemented throughout USCYBERCOM and its components.

c. Supports Commander-delegated IDA to grant or deny official requests to obtain information from and to gain access to records and automated systems. Exercises delegated authority to make independent judgments concerning discretionary releases of information on a case-by-case basis and is authorized to deny FOIA requests for reasons other than exemptions.

d. Coordinates inter-agency FOIA matters with the National Security Agency (NSA), Department of Justice (DOJ), Office of the Defense Department Chief Management Officer, military services, and other U.S. Government agencies.

e. Assists FOIA case managers (FCMs) assigned to the FPO.

f. Leads and facilitates discussions and negotiations with requesters to achieve an optimal balance between the command's need to protect information that is vital to its operations with the objectives of the FOIA program to provide information to the public.

g. Confers with legal counsel, the DoD, or DoJ attorneys if the command is served with a complaint concerning a FOIA request.

h. Creates and conducts training for USCYBERCOM personnel on FOIA policies, procedures, and responsibilities. Creates and distributes training and reference material for USCYBERCOM personnel.

i. Represents the USCYBERCOM at both interagency and intra-agency meetings covering information management programs. Functions as the command spokesperson in intra-agency coordination meetings or symposia concerning government implementation of the FOIA.

j. Evaluates and determines customer needs for USCYBERCOM FOIA internal websites and the public FOIA reading room and makes necessary updates.

k. Submits quarterly, annual, and special FOIA reports to the DoD Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties and Transparency (OATSD(PCLT)).

l. Maintains Classification Advisory Officer certifications IAW USCCI 5900.04.

2.4. FOIA CASE MANAGER (FCM).

a. Processes FOIA requests IAW the FOIA, DoDD 5400.07, DoDM 5400.07, and Title 32, CFR, Part 286, DoD FOIA Program.

b. Manages the USCYBERCOM FOIA requester service center.

c. Tasks the USCYBERCOM directorates through the Workflow Management System (WMS) to search for and/or review records that are responsive to FOIA requests.

(1) Provides ample processing instructions.

(2) Conducts an initial review of records to confirm responsiveness to the criteria of the request.

d. Incorporates the recommendations of subject matter experts (SMEs) and ensures compliance with the FOIA when reviewing and redacting responsive records.

e. Coordinates, consults, or refers records to other DoD Components or federal agencies when responsive records contain information regarding these organizations.

f. Enters and tracks data in a formal control system to enable the FPM to complete reports for OATSD(PCLT) described in section 2.3.k.

g. Maintains awareness of OATSD(PCLT) FOIA litigation coordination process and Department Level Interest topics.

h. Reviews and considers current FOIA decisions disseminated by the DOJ Office of Information Policy (OIP) and OATSD(PCLT).

i. Preserves all correspondence pertaining to requests received, as well as copies of all requested records, until disposition or destruction is authorized pursuant to Title 44 USC or the General Records Schedule 4.2 of the National Archives and Records Administration. Records shall not be disposed of or destroyed while they are the subject of a pending request, appeal, or lawsuit under the FOIA.

j. Provides FOIA training to USCYBERCOM personnel when FPM is unable to do so.

2.5. SUBJECT MATTER EXPERT (SME).

a. Responds to FOIA tasks in WMS according to processing instructions provided by the FCM.

b. Conducts searches for records that are reasonably calculated to uncover relevant material in response to a FOIA request.

(1) Consults the FCM with questions regarding the scope of the request.

(2) Completes USCYBERCOM Form 510, "Freedom of Information Act Search Form", to document the search effort.

c. Provides relevant material to the FCM to determine which records meet the criteria of the request.

d. Reviews information responsive to a FOIA request and determines whether disclosure would harm an interest protected by one or more of the FOIA exemptions, or disclosure is prohibited by law.

(1) Consults the FCM regarding the applicability of FOIA exemptions.

(2) Provides closeout remarks in WMS and uploads redacted records.

e. Familiarizes themselves with the foundational laws, policies, and guidance, as referenced in paragraphs 1.1.a-e., 1.2.a.-b., Attorney General Memorandum, "Freedom of Information Act Guidelines," March 15, 2022, and the nine FOIA exemptions.

2.6. OFFICE OF THE STAFF JUDGE ADVOCATE.

a. Reviews and evaluates proposed responses to FOIA requests to determine consistency with applicable law.

b. Identifies and addresses any potential legal errors.

c. Provides legal guidance to the IDA concerning the discharge of their responsibilities.

2.7. PUBLIC AFFAIRS OFFICER.

a. Maintains awareness of FOIA requests that have USCYBERCOM equities, with special consideration to those with known or potential media interests.

b. Provides insight on publicly available information and information that has been officially acknowledged.

2.8. OPERATIONS SECURITY COORDINATOR.

a. Maintains awareness of FOIA requests that may have Operations Security implications.

b. Provides recommendations regarding the suitability for disclosure of all or part of a record based on Operations Security considerations.

2.9. CLASSIFICATION ADVISORY OFFICER.

a. Confirms withheld information is properly and currently classified pursuant to an existing executive order, classification guide, or its aggregation under FOIA exemption 1.

b. Confirms information recommended for disclosure is unclassified or, if the information is not unclassified, informs the FPM.

c. Coordinates with the USCYBERCOM Information Security Program Manager for declassification of USCYBERCOM-originated material.

2.10. HEADQUARTERS USCYBERCOM PERSONNEL.

a. Complete FOIA training within 60 days of onboarding via one of the following courses or training methods:

(1) USCYBERCOM Newcomers Orientation.

(2) Joint Knowledge Online portal at https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf. Search for the DOJ -US00l-DOJ Freedom of Information Act (FOIA) Training for Federal Employees, course number DHA-US1278.

(3) Department of Justice Office of Information Policy portal at https://www.justice.gov/oip/training under the Digital FOIA Training Resources title. For General Schedule 14 or above personnel, take the Freedom of Information Act Training for Executives. For General Schedule 13 and below personnel, take the Freedom of Information Act Training for Federal Employees.

(4) MyGovLearn portal at https://elm.mygovlearn.com/psp/ps/?cmd=login (self-paced learning MGL_ELM Account option). Search for the Freedom of Information Act, course labeled "fgov_01_a47_le_enus".

(5) Directorate, program office, or one-on-one training with the FPM.

SECTION 3: PROCEDURES

3.1. RECEIVING FOIA REQUESTS.

a. The FPO typically receives FOIA requests by email to cybercom_foia@cybercom.mil, or through https://www.foia.gov, the federal government's central website for FOIA.

(1) The FPO occasionally receives FOIA requests by postal mail or by phone at (301) 688-3585.

(2) If a requester calls to submit a FOIA request, the FPO should direct the requester to https://www.foia.gov.

b. The FPO also receives consultations and referrals ofFOIA requests from other agencies.

(1) The FPO receives these actions by email to the mailbox on the network appropriate for the classification of the material. The mailbox on the Non-secure Internet Protocol Router Network is cybercom_foia@cybercom.mil. The mailbox on the Secure Internet Protocol Router Network is cybercom_foia@cybercom.smil.mil. The mailbox on the top-secret network is cybercom_foia@nsa.ic.gov.

(2) The FCM should consult Part 286.7 (d) of Title 32 CFR for guidance on the consultation and referral process.

3.2. REVIEWING FOIA REQUESTS.

a. Upon receipt, the FCM reviews the FOIA request to determine whether it is reasonably described.

(1) The FCM consults Part 286.5, Title 32 CFR and DoDM 5400.07, Section 3.6, for guidance on what is considered a reasonable description of requested records.

(2) The FCM should be familiar with the DOJ Guide to FOIA chapter on proper FOIA requests at https://www.justice.gov/oip/doj-guide-freedom-information-act-O.

b. If the request is reasonably described, the FCM assigns the request a tracking number and issues an acknowledgment letter to the requester.

(1) The FPO must make this determination within 20 working days, or 10 calendar days if the requester has asked for expedited processing.

(a) The FPO refers to Part 286 (e), Title 32 CFR and consults the Office of the Staff Judge Advocate to determine whether to grant expedited processing.

(b} The tracking number for requests is the two-digit fiscal year, followed by the letter "R", followed by the number indicating the order in which the request was received (e.g., 24-R010 would be the tenth request received in fiscal year 24).

{c) The tracking number for consultations and referrals is the designation assigned by the consulting or referring agency. The FPO does not assign a new tracking number for consultations and referrals.

(2) The FCM refers to Title 32, CFR subpart 268.8 for information regarding general timing ofresponses to FOIA requests.

c. Ifthe FOIA request is not reasonably described, the FCM seeks clarification from the requester.

(1) The FPO attempts to make all FOIA requests actionable unless they are not made in accordance with published regulations, or they are clearly unreasonable.

(2) The FCM refers to subpart 286.9 oftitle 32, CFR for information regarding responses to FOIA requests and adverse determinations ofFOIA requests.

d. Ifthe FOIA request is for records clearly originating with another agency, the FPO will advise the requester to submit the request to the correct agency.

(1) The FCM refers to Title 32, CFR subpart 268.8 for information regarding misdirected requests.

(2) The FCM follows procedures outlined in subpart 286.7(d)(3) oftitle 32, CFR for coordination with other agencies prior to consultation or referral.

3.3. PROCESSING FOIA REQUESTS.

a. The FCM preserves all correspondence pertaining to the request.

(1) The FCM creates an email subfolder for each request to capture communication with the requester and staffthat contribute to the processing ofthe request.

(2) The FCM creates a shared folder to maintain files pertinent to the request (e.g. background, letters, responsive documents, etc.).

b. The FCM creates a WMS task IAW United States Cyber Command Manual (USCCM) 5000.01, "Task Management Program," to ensure accountability ofall FOIA request processing.

(1) The FCM assigns the WMS task to the office(s) that has a nexus to the topic ofthe request. For example, ifthe request is for records regarding plans and policy, J5 may be an appropriate office to engage. Or, ifthe request relates to exercises and training, the FCM may consider assigning the task to J7.

{a} In accordance with USCCM 5000.01, *Task Management Program,* all tasks require a suspense ofat least 10 working days.

(b) The FCM provides clear and concise guidance in the instructions field ofthe WMS task to ensure that the SME understands the assignment.

(2) If the task is to search for records, the FCM provides resources that will help the SME conduct an adequate search. The FCM should be familiar with the DOJ Guide to FOIA chapter on searching for responsive records. See the Glossary for a link to the DOJ Guide to FOIA.

(a) The SME completes USCYBERCOM Form 510 provided in the WMS task to document the search effort.

(b) The SME should not commence review of any records located until the FPO validates whether the records are in fact responsive to the criteria of the request.

(3) If the task is to review records located in response to a request, the FCM provides resources to help the SME understand the process of identifying exempt information, segregating non-exempt information, and applying the foreseeable harm standard.

(a) The FCM consults DoDM 5400.07, section 5, for general provisions of the nine FOIA exemptions.

(b) The DOJ Guide to FOIA offers an analysis of the "reasonably segregable" obligation that the SME considers when conducting reviews. When reviewing records that contain classified information, the SME consults relevant security classification guides, classification working aids, and Executive Order (EO) 13526, Classified National Security Information, with special consideration to sections 1.4 and 1.7(e).

(c) When reviewing records that contain sensitive information that does not meet the criteria of classification but must still be protected, the SME consults the DoD Controlled Unclassified Information (CUI) registry and the USCYBERCOM Critical Information List. The SME will refer to https://www.dodcui.mil for information on CUI and USCCM 5200.01 for information on unclassified critical information.

(d) The FCM works with the SME conducting the review to ensure that USCYBERCOM is withholding information responsive to a FOIA request only if disclosure would harm an interest protected by one or more of the FOIA exemptions, or disclosure is prohibited by law.

(4) Upon completion of the search or review task assigned through WMS, the SME attaches files (e.g. USCYBERCOM Form 510, responsive records, redacted records), provides remarks, and closes the task. The SME should refer to USCCM 5000.01 and the WMS User Guides for instructions on how to complete WMS tasks. See the Glossary for links to the WMS User Guides.

c. When the FCM receives the required responses to WMS tasks, the FCM adjudicates all comments and recommendations and prepares a staffing package for coordination with the relevant personnel outlined in Section 2.

(1) The FCM may forego coordination with certain personnel if their role is irrelevant to a specific determination. For example, if no records are located or no search is undertaken, review by the Classification Advisory Officer is not required because there are no records to

review. Or, if a record is denied in full, Public Affairs Office review is unnecessary because information is not being released that may generate media interest.

(2) The FCM completes USCYBERCOM Form e506 to succinctly explain the action, justify the final recommendation, and memorialize coordination with all relevant stakeholders. Tabs to USCYBERCOM Form e506 will include all pertinent records and information that shaped the decision.

3.4. RESPONDING TO FOIA REQUESTS.

a. The FPO follows guidance outlined in DoDM 5400.07 Section 6.3.c. and Part 286.9 of Title 32 CFR when responding to FOIA requesters.

b. OATSD(PCLT) will notify the FPO if a FOIA requester appeals the initial USCYBERCOM determination.

(1) The FOIA appellate authority for USCYBERCOM is the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency per Part 286.11 (b)(2) of Title 32 CFR.

(2) If a FOIA requester appeals the initial USCYBERCOM determination, the FPO will be contacted by OATSD(PCLT) and asked to provide the complete administrative record of the action to the assigned appeals analyst.

(3) OATSD(PCLT) reviews the appeal and either upholds the USCYBERCOM determination or remands the decision. If a decision is remanded, USCYBERCOM will further process the request IAW the appeal determination.

c. FOIA requesters may file a lawsuit seeking to compel the disclosure of information.

(1) Per DoDM 5400.07, section 6.7.b., if USCYBERCOM is served with a complaint concerning a FOIA request that is still open, it will administratively close the FOIA request after consultation with legal counsel.

(2) In the event of a FOIA litigation, the FPO works with the Office of the General Counsel of the Department of Defense to establish centralized processing of FOIA litigation documents when necessary (per DoDD 5400.07, Section 2.4.b).

SECTION 4: NON-FOIA REQUESTS

4.1. MANDATORY DECLASSIFICATION REVIEW (MDR) REQUESTS.

a. Members of the public may request a declassification review of records classified under the provisions of EO 13526, or predecessor orders. Declassification requests in full or in part must be approved by a declassification authority.

b. The FCM will refer to DoDM 5230.30, *DoD Mandatory Declassification Review Program,* and Part 222 of Title 32 CFR for MDR processing procedures. The MDR process is similar to the FOIA process.

(1) When the FPO receives an MDR request, it coordinates a "FOIA-like review" of the requested record with the personnel outlined in Section 2 of this instruction.

(2) The FCM clearly marks any portions to be redacted, citing the appropriate exemptions from section 1.4 and 6.2 of EO 13526.

(a) EO 13526, section 3.5(c), states that agencies shall release the requested information unless withholding is otherwise authorized and warranted under applicable law.

(b) EO 13526, section 6.2(d), states that nothing in this order limits the protection afforded any information by other provisions of law, including FOIA exemptions. The review of each record will determine if the record:

1- No longer meets the standards for classification as established by EO 13526 and is therefore declassified in full.

2- Contains portions still meeting the standards for classification and is therefore declassified in part and denied in part.

3. Still meets the standards for classification in its entirety and is therefore denied in full.

(c) DoD Components shall not release any unclassified information exempt from public release pursuant to Exemption 2 through 9 of the FOIA.

c. The FCM assigns tracking numbers to MDR requests, enters MDR data into a formal control system, tasks MDR reviews through WMS, and preserves all correspondence pertaining to MDR processing.

4.2. PRIVACY ACT REQUESTS.

a. Individuals may request access to records about themselves under the Privacy Act, Title 5 USC § 552(a).

b. The right of access under the Privacy Act is similar to that of the FOIA, and the statutes do overlap, but not entirely.

(1) The Privacy Act allows individuals to access records about themselves, while the FOIA allows the public to access government information.

(2) The primary difference between the FOIA and the access provision of the Privacy Act is the scope of information accessible under each statute.

(3) The FPO considers an individual's access request under both the Privacy Act and the FOIA.

(a) The FCM consults DoDM 5400.07 Section 3.9 for information regarding the relationship between the FOIA and the Privacy Act.

(b) The FCM refers to Part 310 of Title 32 CFR_for Privacy Act processing guidance and the DOJ Overview of the Privacy Act, with special consideration to the individual's right of access at https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/access.

(c) The FCM refers to https://dpcld.defense.gov/privacy/soms/ for information about SORs and system ofrecord notices (SORN).

c. DoD Privacy Act SORs are decentralized, and USCYBERCOM is often not the DoD Component that maintains the requested record. Therefore, the FPO frequently advises a Privacy Act requester to submit his or her request to the address listed in the record access procedures of the SORN containing the record.

d. The FCM assigns tracking numbers to Privacy Act requests, enters Privacy Act data into a formal control system, and preserves all correspondence pertaining to Privacy Act request processing.

(1) The FCM does not task Privacy Act reviews through WMS due to privacy concerns.

(2) The FCM works closely with Office of the Staff Judge Advocate on all Privacy Act requests to ensure that the privacy of third parties is not violated.

GLOSSARY

Acronyms

CFR	Code of Federal Regulations
COS	Chief of Staff
CUI	Controlled Unclassified Information
DOD	Department of Defense
DODD	Department of Defense Directive
DODM	Department of Defense Manual
DOJ	Department of Justice
EO	Executive Order
FCM	FOIA Case Manager
FOIA	Freedom of Information Act
FPM	FOIA Program Manager
FPO	FOIA Program Office
HQ	Headquarters
IAW	in accordance with
IDA	Initial Denial Authority
MDR	Mandatory Declassification Review
NSA	National Security Agency
OATSD(PCLT)	Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency
OIP	Office of Information Policy
OPEN	Open, Public, Electronic, and Necessary
SME	Subject Matter Expert
SOR	System of Record
SORN	System of Record Notice
WMS	Workflow Management System
USC	United States Code
USCYBERCOM	United States Cyber Command
USCCI	United States Cyber Command Instruction
USCCM	United States Cyber Command Manual

Terms

System of records: any group of records under the control of the Department of Defense from which information is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to the individual as defined in the Privacy Act.

Links

Command Publications Website:
https://intelshare.intelink.gov/sites/uscybercom/Library/SitePages/publications.aspx

CUI Information: www.dodcui.mil

DoJ Office of Information Policy Portal: https://www.justice.gov/oip/training

DoJ Overview of the Privacy Act: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/access

DOJ Guide to the FOIA: https://www.justice.gov/oip/doj-guide-freedom-information-act-O

Federal Government's central website for FOIA: www.foia.gov

Joint Knowledge Online Portal: https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf

MyGovLeam Portal: https://elm.mygovlearn.com/psp/ps/?cmd=login

Systems of Record and System of Record Notices: https://dpcld.defense.gov/privacy/cs/

USCYBERCOM FOIA Reading Room: https://www.cybercom.mil/FOIA-Privacy-Act/Reading-Room/

WMS User Guide:
Intelink: https://intelshare.intelink.gov/sites/uscybercom/J6/Pages/WMS-UG.aspx
Secure Internet Protocol Router Network:
https://intelshare.intelink.sgov.gov/sites/uscybercom/s-wms-lite/UserGuides/Forms/Allitems.aspx
NSANet:
https://wms.cybercom.ic.gov/app/wms/User%20Guide/WMS%202%201_User%20Guide_NOV_17.pdf

REFERENCES

Executive Order 13526, *Classified National Security Information,* 29 December 2009
Executive Order 13556, Controlled Unclassified Information, 04 November 2010
Title 5 USC §552, *Freedom of Information Act,* 30 June 2016
Title 5 USC §552a, *Privacy Act,* 22 November 2002
Title 32 CFR Part 222, *DOD Mandatory Declassification Review Program,* 01 July 2024
Title 32 CFR Part 286, *DOD Freedom of Information Act Program,* 05 December 2023
Title 32 CFR Part 310, *Protection of Privacy and Access to and Amendment of Individual Records Under the Privacy Act of 1974, 21 April 2023*
Title 44 USC, *Public Printing and Documents,* 22 October 1968
Public Law 110-175, *OPEN Government Act of 2007,* 31 December 2007
Public Law 114-185, *FOIA Improvement Act of 2016,* 30 June 2016
Attorney General Memorandum for Heads of Executive Departments and Agencies regarding FOIA, 15 March 2022
DoDD 5400.07, *DoD Freedom of Information Act (FOIA) Program,* 05 April 2019
DoDM 5400.07, *DoD Freedom of Information Act (FOIA) Program,* 25 January 2017
DoDM 5200.01 Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification,* 24 February 2012
DoDI 5200.48, *Controlled Unclassified Information (CUI),* 6 March 2020
DoDM 5230.30, *DoD Mandatory Declassification Review Program,* 08 February 2022
General Records Schedule 4.2, *Information Access and Protection Records*
Attorney General Memorandum for Heads of Executive Departments and Agencies regarding FOIA, 15 March 2022
USCCI 5200-01, *Operations Security Program,* 18 October 2021
USCCI 5200-10, *Information Security Program,* 2 September 2020
USCCI 5200-17, *Controlled Unclassified Information,* 27 July 2021
USCCI. 5900-04, *Classification Advisory Officer Program,* 15 June 2022
USCCI 5000-07, *Privacy and Civil Liberties Program,* 26 July 2021
USCCM 5000-01, *Task Management Program,* 30 June 2023
USCCM 5200.01, Operations Security Program: *Vol I Critical Information List,* 18 January 2022