



UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6171
FORT. GEORGE G. MEADE, MARYLAND 20755

Re: 23-R063

JUL 24 2025

Colin Aamot



Dear Mr. Aamot,

This letter responds to the enclosed Freedom of Information Act (FOIA) request, submitted to U.S. Cyber Command on September 15, 2023.

We have located and reviewed 41 pages of material responsive to your request. We are releasing this information to you in its entirety.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the Department of Defense (DoD) FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Contact information for each resource is enclosed.

A handwritten signature in black ink, appearing to read "K. Lenox", is written over the typed name and title.

KEVIN P. LENOX
Rear Admiral, U.S. Navy
Acting Chief of Staff

Enclosures:
a/s

JUL 24 2025

Re: 23-R063

DoD FOIA Public Liaison:

Ms. Virginia Burke
Phone: (571) 372-0462
Email: osd.mc-alex.oatsd-pclt.mbx.foia-liaison@mail.mil

Office of Government Information Services:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road – OGIS
College Park, MD 20740-6001
Email: ogis@nara.gov
Phone: (202) 741-5770
Toll Free: 1-877-684-6448
Fax: (202) 741-5769

Administrative Appeal: *

Mr. Michael Kremlacek
Acting Assistant to the Secretary of Defense
for Privacy, Civil Liberties, and Transparency
(PCLT)
Office of the Secretary of Defense
4800 Mark Center Drive
ATTN: PCLFD, FOIA Appeals
Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

* Appeal should cite case number above, be clearly marked "FOIA Appeal" and filed within 90 calendar days from the date of this letter.

FOIA Request 859446

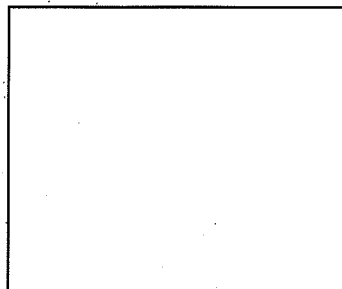
The following list contains the entire submission submitted September 15, 2023 10:50:18am ET, and is formatted for ease of viewing and printing.

Contact information**First name**

Colin

Last name

Aamot

Mailing Address**City****State/Province****Postal Code****Country****Phone****Email**A large rectangular box with a black border, used to redact contact information. It covers the fields for Mailing Address, City, State/Province, Postal Code, Country, Phone, and Email.**Request****Request ID**

859446

Confirmation ID

858866

23-R063

Dear FOIA Officer, Pursuant to the Freedom of Information Act, 5 U.S.C. § 552, and the implementing FOIA regulations of the agency, I respectfully request the following:

A copy of all internal policy documents, memorandums or guidance pertaining to FOIA processing and procedures, FOIA Appeal processing and procedures, and Mandatory Declassification Review (MDR) processing Policy and Procedures between 2018 and present. Please include any and all documents relating to steps the agency takes when processing or deconflicting with other agencies when processing FOIA requests, Appeals, or MDR requests.

I also hereby request a list of the oldest 50 FOIA's still open with the Agency including the request date, request body/text, and requestor. I am amicable to a rolling production as records are available. To further narrow down the scope of the request, requester does not seek correspondence that merely forwards press clippings, such as news accounts or opinion pieces, newsletters, and published or docketed materials, if that correspondence has no comment or no substantive comment added by any party in the thread. The terms "pertaining to," "referring," "relating," or "concerning" with respect to any given subject means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with, or is in any manner whatsoever pertinent to that subject. The term "record" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (emails), MMS or SMS text messages, instant messages, messaging systems (such as iMessage, Microsoft Teams, WhatsApp, Telegram, Signal, Google Chat, Twitter direct messages, Lync, Slack, and Facebook Messenger), contracts, cables, telexes, notations of any type of conversation, telephone call, voicemail, meeting or other communication. Please comply fully with 5 U.S.C. § 552(b). To further narrow down the scope of the request, the requester does not seek correspondence that merely forwards press clippings, such as news accounts or opinion pieces, newsletters, and published or docketed materials, if that correspondence has no comment or no substantive comment added by any party in the thread. Accordingly, without limitation to the foregoing, if any portion of this request is denied for any reason, please provide written notice of the records or portions of

Request description

Supporting documentation

Fees**Request category ID**

media

Fee waiver

yes

This request is primarily and fundamentally for non-commercial purposes. The requested information is in the public interest because there trust in government is at historic lows, and the American people deserve transparency with regards to the agency's operations and disclosure of core information. Because this is a request by a member of the news media for information of public interest, made in my capacity as an investigative journalist and author , I actively gather information of potential interest to my audiences, and I use my editorial skills to turn raw materials into a distinct work. I furthermore distribute that work to my audience through podcasts or articles through multiple outlets. I request that you waive all applicable fees associated with this request. If you deny this request for a fee waiver, please advise me in advance of the estimated charges if they are to exceed . Please send me a detailed and itemized explanation of those charges. If you have any questions, or feel you need clarification of this request please contact me at

Explanation**Willing to pay**

50

Expedited processing**Expedited Processing**

no

UNCLASSIFIED



United States Cyber Command Instruction (USCCI)

OPR: J070
DISTRIBUTION: A

USCCI 5000-06
17 April 2018

Freedom of Information Act (FOIA) Program

1. Purpose. This United States Cyber Command (USCYBERCOM) Instruction (USCCI) establishes policies, procedures, requirements and responsibilities for releasing requested records in accordance with Section 552 of Title 5, United States Code (USC), *Freedom of Information Act* (hereafter, FOIA) and within statutory time limits.

2. Supersedes/Cancellation. This is the first issuance.

3. Applicability. This instruction applies to USCYBERCOM personnel assigned to USCYBERCOM and its subordinate units to include the Headquarters (HQ) Cyber National Mission Force (CNMF), the Service Component Commands (SCC), the Joint Force Headquarters-Cyber (JFHQ-C), the Joint Force Headquarters – Department of Defense Information Networks (JFHQ-DODIN) and designated Joint Task Forces (JTF). However, the SCCs will follow their Service regulations for information that is purely Service unique or generated apart from USCYBERCOM's joint mission.

4. Responsibilities. Responsibilities are outlined in Enclosure 1.

5. Procedures. Procedures are outlined in Enclosure 2.

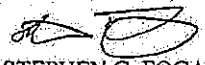
6. Summary of Changes. None.

7. Releasability. Cleared for public release. This instruction is approved for public release; distribution is unlimited. Department of Defense (DOD) Components, other Federal agencies and the public may obtain copies of this directive.

UNCLASSIFIED

UNCLASSIFIED

8. Effective Date. This instruction is effective upon receipt.



STEPHEN G. FOGARTY
Major General, USA
Chief of Staff

Enclosures:

Enclosure 1 – Roles and Responsibilities

Enclosure 2 – Procedures

Attachment 1 – Glossary of References and Supporting Information

Attachment 2 – DD Form 2086

UNCLASSIFIED

UNCLASSIFIED

ENCLOSURE 1

1. Roles and Responsibilities.

1.1. Chief of Staff (CoS).

1.1.1. Oversee the implementation of the Command's FOIA Program.

1.1.2. Serve as the USCYBERCOM Initial Denial Authority (IDA).

1.2. Chief Knowledge Officer (CKO) (J070).

1.2.1. Direct, manage and administer the Command FOIA program.

1.2.2. Designate the FOIA Program Manager (PM) in writing.

1.3. FOIA PM (FPM). Reporting to the CoS and CKO, lead the USCYBERCOM FOIA Program Office (FPO)/J070. Depending on workload, the USCYBERCOM FPO may also include one or more FOIA Case Managers (FCM) to assist the FPM in the processing and redaction with each FOIA request. The FPM is ultimately responsible for the following actions within the FPO.

1.3.1. Track and process FOIA requests for USCYBERCOM in accordance with the FOIA, Department of Defense Directive (DODD) 5400.07 and DoD Manual (DODM) 5400.07. All USCYBERCOM FOIA actions are processed through the HQ US Strategic Command (USSTRATCOM) FPO that functions as USCYBERCOM's FOIA Requestor Service Center (RSC). (Note: All current roles and responsibilities assigned to USSTRATCOM that assist the USCYBERCOM FPO are expected to transfer to USCYBERCOM within four months after USCYBERCOM achieves Initial Operational Capability designation.)

1.3.2. Task the appropriate USCYBERCOM organizations, via the USCYBERCOM Workflow Management System (WMS), to identify, search for and/or review responsive records for each FOIA request. Provide ample processing instructions. Conduct an initial review of identified documents to confirm their responsiveness to a given FOIA request.

1.3.3. Within 20 workdays of the original FOIA request, or a referral or consultation request from another DOD or U.S. Government (USG) agency, provide the USSTRATCOM FPO the responsive records with either zero or some redactions, a response of zero responsive records, or an estimated date as to when responsive records can be realistically processed. Include the signed USCYBERCOM IDA memorandum for completed FOIA cases.

1.3.4. Either accomplish the redaction of responsive records or review the proposed redactions of the appropriate organizations for FOIA compliance.

1.3.5. If a FOIA request implicates the equities of other USG agencies, to include other military organizations, forward the portion of the proposed response that includes records related to that agency to the implicated agency, via the USSTRATCOM FOIA PM.

1.3.6. Prepare staffing packages per USCYBERCOM Instruction (USCCI) 5000-01 for CoS review and/or approval to submit to the USSTRATCOM FPO. Formal staffing

UNCLASSIFIED

UNCLASSIFIED

coordination should include, but is not limited to, a FOIA Monitor (FMon) or Subject Matter Expert (SME), a Classification Advisory Officer (CAO), an Operations Security (OPSEC) Coordinator, a Staff Judge Advocate (SJA) member, and a Public Affairs Officer (PAO).

1.3.7. Provide FOIA processing initial and/or recurring training to appointed FMons and SMEs.

1.3.8. Co-chair the combined FOIA and Privacy & Civil Liberties Working Group (FPC&L WG). Keep FMons and SMEs apprised of updates to FOIA processing guidance. Maintain a FOIA wiki page or similar forum on the unclassified USCYBERCOM portal.

1.3.9. Notify the CoS and the Office of the Staff Judge Advocate (OSJA) of requests for records of a controversial or sensitive nature.

1.3.10. Notify the USCYBERCOM PAO if there is potential for news media interest or involvement in the case.

1.3.11. Maintain appropriate electronic and hard copy records pursuant to Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5760.01A, Volume I; CJCSM 5760.01A, Volume II; DoDD 5400.07 and DoDM 5400.07 and USSTRATCOM Strategic Instruction (SI) 900-6.

1.3.12. Submit annual and special FOIA report inputs to the USSTRATCOM FOIA PM, as required.

1.3.13. Maintain USCYBERCOM's FOIA Standard Operating Procedures (SOP).

1.3.14. Maintain CAO certification per USCCI 5900-04.

1.3.15. Serve as the alternate FMon for the USCYBERCOM J0, J1 and J4 Directorates and any current or subsequently established JTF.

1.4. FOIA Monitors (FMon). Designated in writing by the Director or subordinate organization equivalent, the FMons accomplish the following.

1.4.1. Be familiar with the nine FOIA exemptions.

1.4.2. Monitor the FOIA program within their directorate or equivalent subordinate organization to ensure a reasonable search of electronic and physical files occurs for each applicable FOIA request. Provide relevant status updates directly to the FPO or through WMS, as appropriate.

1.4.3. Task organizational leadership to identify SME(s) to respond to each FOIA request.

1.4.4. Either complete the FOIA task or monitor SME progress in order to meet each FOIA tasking deadline.

1.4.5. Provide FOIA processing advice and assistance to the SMEs. Seek advice from the USCYBERCOM FPM, when necessary.

UNCLASSIFIED

UNCLASSIFIED

1.4.6. Notify the USCYBERCOM FPO of responsive records to a controversial or sensitive subject or cases where the existence or nonexistence of a record may in itself be classified (Glomar Response).

1.4.7. Track and provide to the USCYBERCOM FPO the time spent processing each FOIA request on the DD Form 2086, *Record of Freedom of Information (FOI) Processing Cost* (see Attachment 2).

1.4.8. Serve as the organization's representative to the FP&CL WG.

1.5. Subject Matter Expert (SME).

1.5.1. Respond to FOIA requests according to processing instructions contained in the tasking guidance provided by the USCYBERCOM FPM and/or FMon.

1.5.2. Process FOIA actions through the organization's FMon.

1.6. Director (or equivalent at a subordinate organization).

1.6.1. Appoint an individual to serve as the directorate's FMon and provide the FMon a copy of the appointing memorandum.

1.6.2. Ensure respective FMon(s) understand FOIA procedures and are afforded training opportunities, as required, to learn and execute assigned duties.

1.7. Office of the Staff Judge Advocate (OSJA).

1.7.1. Review and evaluate recommendations to withhold all or part of a record using one or more of the FOIA exemptions.

1.7.2. At his or her discretion, identify additional items for withholding or disclosure.

1.8. Public Affairs Officer (PAO).

1.8.1. Remain cognizant of FOIA requests that possess USCYBERCOM equities, especially those with known media interest.

1.8.2. Provide insight on what information is already publicly available.

1.8.3. Provide recommendations on withholding all or part of a responsive record.

1.9. Operations Security (OPSEC) Coordinator provides recommendations on withholding all or part of a record based on OPSEC considerations.

1.10. Classification Advisory Officer (CAO).

1.10.1. Confirm information being withheld under FOIA exemption (b)(1) is properly and currently classified pursuant to an existing executive order.

1.10.2. Confirm information recommended for disclosure is unclassified. Inform the FPM if information recommended for disclosure should be classified if it is not.

UNCLASSIFIED

UNCLASSIFIED

ENCLOSURE 2

2. Procedures.

2.1. The Commander, USCYBERCOM (CDRUSCYBERCOM) ensures USCYBERCOM personnel comply with the FOIA by making releasable information available to the public, as requested, by responding through USSTRATCOM to perfected FOIA requests within the statutory time limits.

2.2. Until designated as a DoD FOIA Program Component, USCYBERCOM responds to FOIA requests through USSTRATCOM and does not communicate directly with FOIA requestors as USSTRATCOM maintains a FOIA Requestor Service Center (RSC). USCYBERCOM must forward any FOIA request (electronic or hardcopy) received directly from a requestor to the USSTRATCOM FOIA PM for processing.

2.3. USCYBERCOM CoS serves as the Command's IDA. USCYBERCOM provides to USSTRATCOM complete FOIA responses for dissemination to the FOIA requestor.

2.4. The Directorate for Oversight and Compliance (DO&C), Office of the Deputy Chief Management Officer (ODCMO) serves as the FOIA Public Liaison for USSTRATCOM, and hence, USCYBERCOM. Likewise, the Director of Administration and Management (DA&M) serves as the FOIA appellate authority for USSTRATCOM, and hence, USCYBERCOM.

2.5. The USCYBERCOM FPO responds to perfected FOIA requests received from the USSTRATCOM FOIA PM in either of two following manners: 1) request from the FOIA requestor to USCYBERCOM via the USSTRATCOM FOIA PM; or 2) referral from another USG agency to USCYBERCOM via the USSTRATCOM FOIA PM. The typical flow of actions is as follows.

2.5.1. Upon receipt, the USCYBERCOM FPO reviews the written FOIA request for clarity. Any questions or desired clarifications about the FOIA request for the requestor are routed back through the USSTRATCOM FOIA PM. In addition, any procedural questions on that particular FOIA request (e.g., application of exemptions or release determinations in similar previous FOIAs) are resolved to minimize processing time of any responsive records. Finally, the USCYBERCOM FPO determines whether the request properly belongs to USCYBERCOM or whether the request should be referred to a different USG agency based on the subject of the FOIA.

2.5.2. Based on the requested records, the USCYBERCOM FPO determines which organizations to task to search for responsive records. The task can either be distributed via WMS or in certain cases where a specific record(s) is/are requested, may be directly tasked to an organization (e.g., J7 for exercise related records) or an office (e.g., Command Historian for historical records). All correspondence will include the USSTRATCOM assigned FOIA case number (e.g., 18-065 [the 65th case for Fiscal Year 2018]).

2.5.3. In order to meet the FOIA timeline to release records within twenty (20) business days of receipt of the FOIA request, tasked organizations must complete an electronic and hard copy search for responsive records, and provide access to these records to the USCYBERCOM FPO, preferably in an electronic form, within five (5) business days.

UNCLASSIFIED

UNCLASSIFIED

Whether zero, one or multiple records are found, each tasked organization's FMon ensures all personnel involved with a FOIA case provide a brief description of the extent of the search and the time spent completing the search. The FPO annotates this time on the DD Form 2086 to reflect the level of effort required to answer the FOIA request.

2.5.4. The USCYBERCOM FPO then validates whether the records identified by each organization are responsive to the actual request, and provides the USSTRATCOM FOIA PM an estimated date when all of the records can be sufficiently processed. Depending on the number, length and/or complexity of the records found, the estimated time to review/redact each record may take significantly longer than twenty (20) business days. The USSTRATCOM PM must communicate with the FOIA requestor when there are delays.

2.5.4.1. Option 1. Pending the FOIA requester's concurrence, the FOIA requestor receives two or more interim releases of reviewed records versus waiting for the review and release of all responsive records. For example, instead of releasing ten (10) responsive records at the ninety (90) business day mark, four (4) of ten (10) responsive records are reviewed and released at the forty-five (45) business day mark. The remaining six (6) records are released at the ninety (90) business day mark.

2.5.4.2. Option 2. In cases where the number of responsive records is significant, the USCYBERCOM FPM negotiates, via the USSTRATCOM FOIA PM, a refined FOIA request that better identifies the desired information, and hence limits the number of records to a more manageable level that can be processed within acceptable timelines. For example, USCYBERCOM reviews an exercise After Action Report and the corresponding PowerPoint presentation versus reviewing those two records plus a plethora of e-mails that even remotely address the exercise and its aftermath. The FOIA requestor receives the desired information in a reasonable time without unnecessarily overburdening the FPO.

2.5.5. While tasked organization's FMons and SMEs are not required to redact each responsive record under their purview, insight into what portions of each of the records is recommended for withholding, especially from a classified (i.e., FOIA exemption (b)(1)) perspective, is beneficial as the USCYBERCOM FPO processes each record and applies the appropriate FOIA exemptions.

2.5.6. Upon completion of the proposed redactions, the USCYBERCOM FPO coordinates the proposed response with multiple organizations and offices. At each step, the USCYBERCOM FPO attempts to adjudicate any recommended additional disclosures or withholdings. At the end of this staffing, if differences remain, the FPO annotates those items on the USSTRATCOM Form 915 to codify the various staffing actions and decisions. The organization and offices involved in this staffing include, but are not limited to, the following.

2.5.6.1. The FMon and/or SME from the organizations that provided the responsive records to focus on the proposed redactions.

2.5.6.2. An OPSEC Coordinator or the Command OPSEC PM to look at each FOIA response and determine whether OPSEC concerns exist, especially from a mosaic

UNCLASSIFIED

UNCLASSIFIED

and compilation perspective, prior to forwarding the responsive records to USSTRATCOM.

2.5.6.3. A CAO to verify information recommended for disclosure is unclassified.

2.5.6.4. The OSJA to provide legal advice on the application of FOIA exemptions to the USCYBERCOM CoS.

2.5.6.5. A PAO to maintain oversight on what records have been requested via FOIA and what information is recommended for disclosure to the FOIA requestor. The PAO also provides insight to the FPM on what applicable open source information already exists. This guidance could affect the application of FOIA exemptions.

2.5.6.6. The J070 for concurrence to submit the completed staffing package to the USCYBERCOM Command Secretariat (CmdSec) for staffing up to the USCYBERCOM CoS.

2.5.7. The CmdSec logs each package, and reviews it for any formatting discrepancies. Upon completion of their review, the CmdSec forwards the package to the USCYBERCOM CoS Executive Assistant. Typically, the Deputy CoS also reviews the package for situational awareness and completeness. Then the USCYBERCOM CoS may choose to approve the FOIA package as is, approve with additional redactions, or return the package to the FPM for additional staffing and a resubmission.

2.5.8. Upon CoS approval (signature of the IDA memorandum), the USCYBERCOM FPO electronically provides the USCYBERCOM response and a completed DD Form 2086 to the USSTRATCOM FPO. While this concludes USCYBERCOM's actions, the USCYBERCOM FPO continues to track the FOIA case until the USSTRATCOM FPO forwards the records to the FOIA requestor and formally closes the FOIA case in their log.

2.6. There are two additional situations where the USCYBERCOM FPO reviews records prior to FOIA release. In each of these scenarios, the actual records for processing are forwarded to the USCYBERCOM FPO by the USSTRATCOM FOIA PM.

2.6.1. Consultation. Based on the material in responsive record(s) under review by another agency, USCYBERCOM is determined to have equities in at least one section of a record. USCYBERCOM FPO strictly reviews those portion(s) to determine whether FOIA exemption(s) apply to the information. Depending on the extent of the consultation, the USCYBERCOM FPO initiates actions consistent with Section 2.5.6. above. Based on the extent of the consultation, the CKO/J070 may sign out USCYBERCOM's response.

2.6.2. FOIA-like Review. Occasionally USCYBERCOM is asked by another DoD agency via the USSTRATCOM FOIA PM, to complete a Mandatory Declassification Review/FOIA-like review for a select record(s). Again, the USCYBERCOM FPO initiates actions consistent with Section 2.5.6. above. Based on the extent of this FOIA-like review, the CKO/J070 may sign out USCYBERCOM's response.

UNCLASSIFIED

UNCLASSIFIED

ATTACHMENT 1

Glossary of References and Supporting Information.

References

5 USC § 552, *The Freedom of Information Act*, as amended

DODD 5400.07, *DoD Freedom of Information Act (FOIA) Program*, 2 January 2008, certified current through 2 January 2015

DODM 5400.07, *DoD Freedom of Information Act (FOIA) Program*, 25 January 2017

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5760.01A, *Joint Staff and Combatant Command Records Management Manual: Volume I--Procedures*, 7 February 2008, Incorporating Change 2, 13 July 2009

CJCSM 5760.01A, *Joint Staff and Combatant Command Records Management Manual: Volume II--Disposition Schedule*, 13 July 2012, Directive current as of 15 September 2014

SI 900-6, *Freedom of Information Act (FOIA) Program*, 15 May 2006

USCCI 5000-01, *Correspondence Instruction*, 22 April 2016

USCCI 5900-04, *Classification Advisory Officer Program*, 2 December 2016

Informative Websites

USG: <https://FOIA.gov/>

Department of Justice (DOJ): <https://www.justice.gov/oip/doj-guide-freedom-information-act-0>

DOD: <http://open.defense.gov/Transparency/FOIA/>

USSTRATCOM: <http://www.stratcom.mil/Contact/Freedom-of-Information-Act/>

Abbreviations and Acronyms

CAO—Classification Advisory Officer

CDG—Capabilities Development Group

CDRUSCYBERCOM—Commander, United States Cyber Command

CJCSM—Chairman of the Joint Chiefs of Staff Manual

CKO—Chief Knowledge Officer

CmdSec—Command Secretariat

CNMF—Cyber National Mission Force

CoS—Chief of Staff

CUI—Controlled Unclassified Information

DA&M—Director of Administration and Management

DO&C—Directorate for Oversight and Compliance

DOD—Department of Defense

UNCLASSIFIED

UNCLASSIFIED

DODD—Department of Defense Directive
DODM—Department of Defense Manual
FCM—FOIA Case Manager
FMon—FOIA Monitor
FOI—Freedom of Information
FOIA—Freedom of Information Act
FOUO—For Official Use Only
FP&CL WG—FOIA and Privacy and Civil Liberties Working Group
FPM—FOIA Program Manager
FPO—FOIA Program Office
GO/FO—General Officer/Flag Officer
HQ—Headquarters
IDA—Initial Denial Authority
JFHQ-C—Joint Force Headquarters-Cyber
JFHQ-DODIN—Joint Force Headquarters-Department of Defense Information Networks
JTF—Joint Task Force
NSA/CSS—National Security Agency/Central Security Service
ODCMO—Office of the Deputy Chief Management Officer
OPSEC—Operations Security
OSJA—Office of the Staff Judge Advocate
PAO—Public Affairs Office
PM—Program Manager
RSC—Requestor Service Center
SCC—Service Component Command
SES—Senior Executive Service
SI—Strategic Instruction
SID—System Identifier
SME—Subject Matter Expert
SOP—Standard Operating Procedure
USC—United States Code
USCCI—United States Cyber Command Instruction
USCYBERCOM—United States Cyber Command
USG—United States Government
USSTRATCOM—United States Strategic Command
WMS—Workflow Management System

UNCLASSIFIED

UNCLASSIFIED

Glossary of Terms (Note: the following definitions are taken from DODM 5400.07 (Ref c). The word "document" equates to "record", which is used throughout the USCCI).

Agency Record [record] - Includes all documents or records created or obtained by a USG agency that are in the agency's possession and control at the time a FOIA request is received.

Four factors determine an agency's control:

1. The intent of the creator of the document to retain control over the record
2. The ability of the agency to use and dispose of the record as it sees fit
3. The extent to which agency personnel have read or relied upon the document
4. The degree to which the document was integrated into the agency's record systems or files

Records maintained by a government contractor for records management purposes are considered in the DOD Component's possession. Records created by an agency employee during employment, including e-mails, may be either agency records or personal files. [DODM 5400.07 further defines an agency record from a FOIA perspective]

Consultation - The process whereby, in certain situations, a federal agency transfers a FOIA responsive record to another federal agency to obtain recommendations on the releasability of the document. After review, the document is returned to the original agency for response to the FOIA requestor or further review.

FOIA Request - A written request for agency records that reasonably describes the records sought, enabling a DOD Component employee familiar with the files to locate the records with a reasonable amount of effort.

FOIA Requester - Any person, including a partnership, corporation, association, State or State agency, foreign government, foreign national, or a lawyer or other representative acting on behalf of any person who submits a FOIA request. This definition specifically excludes agencies within the Executive Branch of the USG.

IDA - An official who has been granted authority by a DOD Component head to withhold information requested pursuant to the FOIA for one or more of the nine categories of records exempt from mandatory disclosure.

Perfected FOIA Request - A FOIA request that arrives at the FOIA RSC of the DOD Component in possession of the records. The statutory time limit for responding to a FOIA request does not begin until it is perfected.

Responsive - Information or agency records requested by a FOIA requester.

UNCLASSIFIED

UNCLASSIFIED

ATTACHMENT 2 DD Form 2086

RECORD OF FREEDOM OF INFORMATION (FOI) PROCESSING COST				REPORT CONTROL SYMBOL DD-DA-634(A)1365	
Please read instructions on back before completing form.					
1. REQUEST NUMBER	2. TYPE OF REQUEST (X one) a. INITIAL b. APPEAL	3. DATE COMPLETED (YYYYMMDD)	4. ACTION OFFICE		
5. CLERICAL HOURS (E-9/GS 8 and below)		FEB. CODE	(1) TOTAL HOURS	(2) HOURLY RATE	(3) COST
a. SEARCH	1				
b. REVIEW/EXCISING	2		X	\$20.00	-
c. OTHER ADMINISTRATIVE COSTS	3				
6. PROFESSIONAL HOURS (D-1 - D-6/GS 9-GS-15)/CONTRACTOR			(1) TOTAL HOURS	(2) HOURLY RATE	(3) COST
a. SEARCH	1				
b. REVIEW/EXCISING	2		X	\$44.00	-
c. OTHER/COORDINATION/DENIAL	3				
7. EXECUTIVE HOURS (D-7 - GS 1 and above)			(1) TOTAL HOURS	(2) HOURLY RATE	(3) COST
a. SEARCH	1				
b. REVIEW/EXCISING	2		X	\$75.00	-
c. OTHER/COORDINATION/DENIAL	3				
8. COMPUTER SEARCH			(1) TOTAL TIME	(2) RATE	(3) COST
a. MACHINE TIME (Not PC, desktop, laptop)	4				
b. PROGRAMMER/OPERATOR TIME (Human)			X		
(1) Clerical Hours	1			\$20.00/hr	
(2) Professional Hours	1			\$44.00/hr	
9. OFFICE MACHINE COPY REPRODUCTION			(1) NUMBER	(2) RATE	(3) COST
a. PAGES REPRODUCED FOR FILE COPY	2			.15	
b. PAGES RELEASED	5		X	.15	-
10. PRE-PRINTED PUBLICATIONS			(1) TOTAL PAGES	(2) RATE	(3) COST
a. PAGES PRINTED	6		X	.02	-
11. COMPUTER PRODUCT OUTPUT/ACTUAL COST CHARGES			(1) NUMBER	(2) ACTUAL COST	(3) COST
a. TAPE/DISC/CD	8		X		-
b. PAPER PRINTOUT	3				
12. OTHER ADMINISTRATIVE FEES			(1) NUMBER	(2) ACTUAL COST	(3) COST
a. ALL POSTAGE/ADMINISTRATIVE (See instructions)	2		X		-
13. AUDIOVISUAL MATERIALS			(1) NUMBER	(2) ACTUAL COST	(3) COST
a. MATERIALS REPRODUCED	4		X		-
14. SPECIAL SERVICES			(1) NUMBER	(2) ACTUAL COST	(3) COST
a. ALL SPECIAL SERVICES (See instructions)	6		X		-
15. MICROFICHE REPRODUCED					
			X	.25	-
FEE CODES			16. FOR FOI OFFICE USE ONLY		
1. Chargeable to "commercial" requesters. Chargeable to "other" requesters after deducting 2 hours.			a. TOTAL COLLECTABLE FEES		
2. Chargeable to "commercial" requesters only.			b. TOTAL PROCESSING FEES		
3. Not chargeable to any fee category.			c. TOTAL CHARGED		
4. Chargeable to "commercial". Chargeable to "other" after deduction of the equivalent of 2 hours. (Example: deduct \$88.00 professional rate.)			d. FEES WAIVED/REDUCED (X one)		
5. Chargeable to all fee categories after deduction of 100 pages (DOES NOT include "commercial").			Yes No		
6. Chargeable to all fee categories. No deductions.			Yes No		
			e. FEES NOT APPLICABLE (X one)		
			Yes No		
			See Chapter 5, Fee Schedule, DoD 5400.7-R, to determine appropriate assessment of fees.		

DD FORM 2086, JAN 2003

PREVIOUS EDITION IS OBSOLETE.

UNCLASSIFIED

UNCLASSIFIED



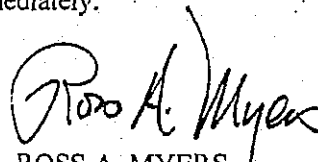
United States Cyber Command Instruction (USCCI)

OPR: J070
DISTRIBUTION: B

USCCI 5000-06
APR 08 2019

Freedom of Information Act Program

1. Purpose. This United States Cyber Command (USCYBERCOM) Instruction (USCCI) establishes policies, procedures, requirements and responsibilities for releasing requested records in accordance with (IAW) Section 552 of Title 5, United States Code (USC), *Freedom of Information Act* (FOIA) and within statutory time limits.
2. Supersedes/Cancellation. This revision supersedes USCCI 5000-06, *Freedom of Information Act (FOIA) Program*, 17 April 2018.
3. Applicability. This instruction applies to USCYBERCOM personnel and subordinate units including the Headquarters Cyber National Mission Force, Service Component Commands (SCC), Joint Force Headquarters-Cyber, Joint Force Headquarters – Department of Defense Information Network, and designated Joint Task Forces (JTF). SCCs will follow Service regulations for any FOIA request that is Service specific or separated from the joint mission area.
4. Responsibilities. Responsibilities are outlined in Enclosure 1.
5. Procedures. Procedures are outlined in Enclosure 2.
6. Summary of Changes. This revision reflects command elevation to a Combatant Command and its designation as a Department of Defense (DOD) FOIA Program Component. Changes of importance include the removal of all FOIA responsibilities previously conducted by United States Strategic Command as the command's DOD FOIA Program Component.
7. Releasability. Cleared for Public Release. This instruction is approved for public release; distribution is unlimited. DOD Components, other Federal agencies, and the public may obtain copies of this directive.
8. Effective Date. This instruction is effective immediately.


ROSS A. MYERS
Rear Admiral, USN
Chief of Staff

UNCLASSIFIED

UNCLASSIFIED

USCCI 5000-06

Enclosures:

Enclosure 1 – Roles and Responsibilities

Enclosure 2 – Procedures

Attachment 1 – Glossary of References and Supporting Information

Attachment 2 – DD Form 2086, *Record of Freedom of Information (FOI) Processing Cost*

UNCLASSIFIED

ENCLOSURE 1**1. Roles and Responsibilities.****1.1. Chief of Staff (CoS).**

- 1.1.1. Oversees the command FOIA Program.
- 1.1.2. Serves as the Initial Denial Authority (IDA).
- 1.1.3. Delegates IDA for select FOIA cases.

1.2. Chief Knowledge Officer (CKO). Assigned to USCYBERCOM J070, Information Management Defense.

- 1.2.1. Directs, manages, and administers the command FOIA program.
- 1.2.2. Designates the FOIA Program Manager in writing.

1.3. FOIA Program Manager (FPM). Reports matters to the CoS and CKO. Leads the command FOIA Program Office (FPO)/J070. Supervises all FOIA Case Managers (FCM) assigned full-time to the FPO to assist in the processing and redaction of each FOIA request. Maintains responsibility for FPO actions listed in paragraphs 1.3.1.-1.3.18.

1.3.1. Tracks and processes FOIA requests IAW the FOIA, DOD Directive (DODD) 5400.07, *DOD Freedom of Information Act (FOIA) Program* and DOD Manual (DODM) 5400.07, *DOD Freedom of Information Act Program*.

1.3.2. Manages the command FOIA Requestor Service Center (RSC).

1.3.3. In coordination with the command Public Affairs Office, maintains content on the public facing FOIA website on the non-classified internet protocol router network (NIPRNET) at www.cybercom.mil.

1.3.4. Tasks the appropriate organizations via the USCYBERCOM Workflow Management System (WMS), to identify, search for and/or review responsive records for each FOIA request. Provide ample processing instructions. Conduct an initial review of identified documents to confirm responsiveness to a specific FOIA request.

1.3.5. Determines the responsible directorate to task for search and/or document review. Via a USCYBERCOM FCM:

1.3.5.1. Identifies a Subject Matter Expert (SME) and tasks the responsible parties directly, when possible, as a direct FOIA tasking approach is paramount to shorten the coordination efforts and ease the burden to the mission.

1.3.5.2. On a case-by-case basis, determines the SMEs' level of effort on the request.

1.3.5.3. Determines when to task FOIA requests in WMS.

1.3.6. Unless categorized under "unique circumstances," within twenty (20) workdays of the original FOIA request, or a referral or consultation request from another DOD or US Government

UNCLASSIFIED

USCCI 5000-06

(USG) agency, provides to the FOIA requester the responsive records with or without redactions, a response of zero responsive records, a Glomar response (IAW DODM 5400.07, para 5.1.f.(1)) or an estimated date as to when responsive records can be realistically processed. Includes the USCYBERCOM IDA-signed memorandum for completed FOIA cases.

1.3.7. Accomplishes the redaction of responsive records or reviews the proposed redactions of the appropriate organizations for FOIA compliance.

1.3.8. If a FOIA request implicates other USG agencies, to include other military organizations, forwards the portion of the proposed response that includes records related to that agency to the implicated agency.

1.3.9. Prepares staffing packages for CoS review and/or approval to submit to the FOIA requester IAW USCCI 5000-01, *Correspondence Management*. Ensures formal coordination includes the offices described in paragraph 2.3.6.

1.3.10. Provides FOIA processing initial and/or recurring training to appointed FOIA Monitors (FMon) and, as required, SMEs.

1.3.11. Co-chairs the combined FOIA and Privacy & Civil Liberties Working Group (FP&CL WG). Keeps all FMons and SMEs apprised of FOIA processing guidance updates. Maintains a FOIA wiki page or similar forum on an internal NIPRNET primary key infrastructure (PKI) enabled command portal.

1.3.12. Promptly notifies the CoS and the Office of the Staff Judge Advocate (OSJA) of FOIA requests for records of a controversial or sensitive nature.

1.3.13. Promptly notifies the Public Affairs Office if there is potential for media interest or involvement in the case.

1.3.14. Maintains appropriate electronic and hard copy records pursuant to Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5760.01A, *Joint Staff and Combatant Command Records Management Manual: Volume I--Procedures*, and *Volume II--Disposition Schedule*; DODD 5400.07; DODM 5400.07; USCCI 5000-01 and the appropriate records management program laws/directives.

1.3.15. Submits annual and special FOIA report requirements to higher headquarters, as directed.

1.3.16. Develops and maintains a command FOIA Standard Operating Procedures.

1.3.17. Maintains Classification Advisory Officer (CAO) certifications IAW USCCI 5900-04, *Classification Advisory Officer Program*.

1.3.18. Serves as the alternate representative to the FP&CL WG for J0 (Special Staff), J1 (Manpower and Personnel) and J4 (Logistics) Directorates, and current or subsequently established JTFs.

1.4. **FOIA Monitors (FMon).** Appointed in writing by the J-Code Director or subordinate organization equivalent.

UNCLASSIFIED

1.4.1. Be familiar with the nine FOIA exemptions and the Intelligence Oversight requirements of USCCI 5200-02, *Intelligence Oversight*.

1.4.2. Monitor the FOIA program within respective directorates or equivalent subordinate organizations to ensure a reasonable search of electronic and physical files occurs for each applicable FOIA request. Provide relevant status updates directly to the FPO or through WMS, as appropriate.

1.4.3. Task organizational leadership to identify SME(s) to respond to each FOIA request.

1.4.4. Complete the FOIA task or monitor SME progress in order to meet each FOIA tasking deadline.

1.4.5. Provide FOIA processing advice and assistance to the SME. Seek advice from the FPM, when necessary.

1.4.6. Notify the FPO regarding responsive records to a controversial or sensitive subject or cases where the existence or nonexistence of a record may in itself be classified (Glomar Response).

1.4.7. Track and provide the time spent processing each FOIA request on the DD Form 2086, *Record of Freedom of Information (FOI) Processing Cost* (see Attachment 2) to the FPO.

1.4.8. Serve as the organization's primary representative to the FP&CL WG.

1.5. Subject Matter Expert (SME).

1.5.1. Responds to FOIA requests according to processing instructions contained in the tasking guidance provided by the FPM and/or FMon.

1.5.2. Processes FOIA actions through the organization's FMon.

1.5.3. Serves as the organization's alternate representative to the FP&CL WG. This task is not applicable to J0, J1, J4 and JTF.

1.6. J-Code Directors (or equivalent at a subordinate organization).

1.6.1. Appoint an individual to serve as the directorate's FMon and provide the FMon a copy of the appointing memorandum.

1.6.2. Designate a SME to serve as alternate representative to the FP&CL WG. This task is not applicable to J0, J1, J4 and JTF.

1.6.3. Ensure respective FMon (s) understand FOIA procedures and enable training opportunities, as required, to execute assigned duties.

1.7. Office of the Staff Judge Advocate (OSJA).

1.7.1. Reviews and evaluates recommendations to withhold all or part of a record using one or more of the FOIA exemptions.

1.7.2. At their discretion, identifies additional items for withholding or disclosure.

1.8. Public Affairs Officer (PAO).

UNCLASSIFIED

USCCI 5000-06

1.8.1. Remains cognizant of FOIA requests that possess command equities, with special consideration to those with known or potential media interests.

1.8.2. Provides insight on publicly available information.

1.8.3. Provides recommendations on withholding all or part of a responsive record.

1.9. **Operations Security (OPSEC) Coordinator.** Provides recommendations on withholding all or part of a record based on OPSEC considerations.

1.10. **Classification Advisory Officer (CAO).**

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

1.10.2. Confirms information recommended for disclosure is unclassified. Inform the FPM if information recommended for disclosure should be classified, but is not.

UNCLASSIFIED

ENCLOSURE 2**2. Procedures.**

2.1. The Commander, USCYBERCOM ensures personnel comply with the FOIA by making releasable information available to the public, as requested, and by responding to perfected FOIA requests within the statutory time limits.

2.2. The command responds to FOIA requests as a FOIA RSC and processes all FOIA requests (electronic or hardcopy) received directly from a requestor. Refer to DODM 5400.07:

2.2.1. Para 3.4.b. for the FOIA Public Liaison function.

2.2.2. Para 6.5 for FOIA appeal processing guidance.

2.3. The FPO responds to perfected FOIA requests 1) received directly from a FOIA requestor or 2) referred from another DOD agency. The typical flow of actions is as follows.

2.3.1. Upon receipt, the FPO reviews the written FOIA request for clarity. Direct any questions or desired clarifications about the FOIA request to the requestor. In addition, any procedural questions on that particular FOIA request (e.g., application of exemptions or release determinations in similar previous FOIAs) are resolved to minimize processing time of any responsive records. Finally, the FPO determines whether the request properly belongs to the command or whether the command should refer the request to a different DOD agency based on the subject of the FOIA.

2.3.2. Based on the requested records, the FPO determines which organizations to task to search for responsive records. The FPO either can distribute the task via WMS or, in certain cases where the requested record is a specific record, may directly task an organization (e.g., J7 (Exercises and Training) for exercise related records) or an office (e.g., Command Historian for historical records). All correspondence will include the command assigned FOIA case number (e.g., 19-010, the 10th case for Fiscal Year 2019).

2.3.3. To meet the FOIA timeline to release records within twenty (20) business days of receipt of the FOIA, tasked organizations must complete an electronic and hard copy search for responsive records and provide access to these records to the FPO, preferably in an electronic form, within seven (7) business days. Whether the tasked organization finds none, one, or multiple records, each tasked organization's FMon ensures all personnel involved with a FOIA case provide a brief description of the extent of the search and the time spent completing the search. The FPO annotates this time on the DD Form 2086 to reflect the level of effort required to answer the FOIA request.

2.3.4. The FPO then validates whether the records identified by each organization are responsive to the actual request, and provides the requester an estimated date when the FPO can sufficiently process all of the records. Depending on the number, length and/or complexity of the records found, the estimated time to review/redact each record may take significantly longer than twenty (20) business days. The RSC communicates with the FOIA requestor when there are delays.

2.3.4.1. Option 1. Pending the FOIA requester's concurrence, the FOIA requestor receives two or more interim releases of reviewed records versus waiting for the review and

release of all responsive records. For example, instead of releasing ten (10) responsive records at the ninety (90) business-day mark, the command reviews and releases four (4) of ten (10) responsive records at the forty-five (45) business day mark. The command would release the remaining six (6) records at the ninety (90) business-day mark.

2.3.4.2. Option 2. In cases where the number of responsive records is significant, the FPM negotiates a refined FOIA request that better identifies the desired information, and hence limits the number of records to a more manageable level that the command can process within acceptable timelines. For example, USCYBERCOM reviews an exercise After Action Report and the corresponding presentation versus reviewing those two records plus a plethora of e-mail that barely address the exercise and its aftermath. The FOIA requester receives the desired information in a reasonable time without unnecessarily overburdening the FPO.

2.3.5. While tasked organization's FMon and SME are not required to redact each responsive record under their purview, insight into what portions of each of the records is recommended for withholding, especially from a classified (i.e., FOIA exemption (b)(1)) perspective, is beneficial as the FPO processes each record and applies the appropriate FOIA exemptions.

2.3.6. Upon completion of the proposed redactions, the FPO coordinates the proposed response with multiple organizations and offices. At each step, the FPO attempts to adjudicate any recommended additional disclosures or withholdings. At the end of this staffing, if differences remain, the FPO annotates those items on the USCYBERCOM Form 915 to codify the various staffing actions and decisions. The organization and offices involved in this staffing include, but are not limited to, the following.

2.3.6.1. The FMon and/or SME from the organizations that provided the responsive records to focus on the proposed redactions.

2.3.6.2. An OPSEC Coordinator or the command OPSEC Program Manager to look at each FOIA response and determine whether OPSEC concerns exist, especially from a mosaic and compilation perspective.

2.3.6.3. A CAO to verify information recommended for disclosure is unclassified.

2.3.6.4. The OSJA to provide legal advice on the application of FOIA exemptions to the USCYBERCOM CoS.

2.3.6.5. A PAO to maintain oversight of requested records and information recommended for disclosure to the FOIA requestor. The PAO provides insight to the FPM regarding existing applicable open source information. This guidance could affect the application of FOIA exemptions.

2.3.6.6. The CKO for concurrence to submit the completed staffing package to the J010 (Command Secretariat (CmdSec)) for staffing to the CoS. Pending CoS delegation, the staffing of select FOIA cases may vary from this norm.

2.3.7. The CmdSec logs each package and reviews it for formatting discrepancies. Upon completion of review, the CmdSec forwards the package to the USCYBERCOM CoS Executive Assistant. The Deputy CoS review is not mandated. The CoS may choose to approve the FOIA

UNCLASSIFIED

USCCI 5000-06

package as is, approve with additional redactions or return the package to the FPM for additional staffing and a resubmission.

2.3.8. Upon CoS approval (signature of the IDA memorandum), the FPO electronically provides the command response to the FOIA requestor and maintains the completed DD Form 2086 for fee collection and/or reporting purposes. This concludes command actions unless the FOIA requestor invokes appeal rights.

2.4. There are two additional situations where the FPO reviews records prior to FOIA release. In both scenarios, based on IDA delegation guidance, the CKO or lower may sign out USCYBERCOM's response.

2.4.1. **Consultation.** Based on the material in responsive record(s) under review by another agency, USCYBERCOM is determined to have equities in at least one section of a record. The FPO only reviews those portion(s) to determine whether FOIA exemption(s) apply to the information, then initiates actions consistent with paragraph 2.3.6. depending on the extent of the consultation.

2.4.2. **FOIA-like Review.** When the command receives a request to complete a Mandatory Declassification Review (i.e., FOIA-like review) for a select record(s), the FPO initiates actions consistent with paragraph 2.3.6.

UNCLASSIFIED

ATTACHMENT 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

5 USC § 552, *The Freedom of Information Act*, as amended
 DODD 5400.07, *DOD Freedom of Information Act (FOIA) Program*, 2 January 2008, certified current through 2 January 2015
 DODM 5400.07, *DOD Freedom of Information Act (FOIA) Program*, 25 January 2017
 Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5760.01A, *Joint Staff and Combatant Command Records Management Manual: Volume I--Procedures*, 7 February 2008, incorporating Change 2, 13 July 2009
 CJCSM 5760.01A, *Joint Staff and Combatant Command Records Management Manual: Volume II -- Disposition Schedule*, 13 July 2012, directive current as of 15 September 2014
 USCCI 5000-01, *Correspondence Management*, 22 April 2016
 USCCI 5200-02, *Intelligence Oversight*, 29 May 2014
 USCCI 5900-04, *Classification Advisory Officer Program*, 2 December 2016

Informative Websites

USG: <https://FOIA.gov/>
 Department of Justice (DOJ): <https://www.justice.gov/oip/doj-guide-freedom-information-act-0>
 DOD: <http://open.defense.gov/Transparency/FOIA/>
 USCYBERCOM: <https://www.cybercom.mil/FOIA/>

Acronyms

CAO	Classification Advisory Officer
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CKO	Chief Knowledge Officer
CmdSec	Command Secretariat
CoS	Chief of Staff
DOD	Department of Defense
DODD	Department of Defense Directive
DODM	Department of Defense Manual
FCM	FOIA Case Manager
FMon	FOIA Monitor
FOIA	Freedom of Information Act
FP&CL WG	FOIA and Privacy and Civil Liberties Working Group
FPM	FOIA Program Manager
FPO	FOIA Program Office
IAW	in accordance with
IDA	Initial Denial Authority
JTF	Joint Task Force
NIPRNET	Non-classified Internet Protocol Router Network
OPSEC	Operations Security

PAO	Public Affairs Office
RSC	Requestor Service Center
SCC	Service Component Command
SME	Subject Matter Expert
USCCI	United States Cyber Command Instruction
USCYBERCOM	United States Cyber Command
USG	United States Government
WMS	Workflow Management System

Terms [Definitions are from DODM 5400.07 (Ref c). The word "document" equates to "record," which is used throughout this USCCI.]

Agency Record [record]. Includes all documents or records created or obtained by a USG agency that are in the agency's possession and control at the time a FOIA request is received. Four factors determine an agency's control: C-S&R

1. The intent of the creator of the document to retain control over the record.
2. The ability of the agency to use and dispose of the record as it sees fit.
3. The extent to which agency personnel have read or relied upon the document.
4. The degree to which the document was integrated into the agency's record systems or files.

Records maintained by a government contractor for records management purposes are considered in the DOD Component's possession. Records created by an agency employee during employment, including e-mails, may be either agency records or personal files. [DODM 5400.07 further defines an agency record from a FOIA perspective]

Consultation. The process whereby, in certain situations, a federal agency transfers a FOIA responsive record to another federal agency to obtain recommendations on the releasability of the document. After review, the document is returned to the original agency for response to the FOIA requestor or further review.

FOIA Request. A written request for agency records that reasonably describes the records sought, enabling a DOD Component employee familiar with the files to locate the records with a reasonable amount of effort.

FOIA Requester. Any person, including a partnership, corporation, association, State or State agency, foreign government, foreign national, or a lawyer or other representative acting on behalf of any person who submits a FOIA request. This definition specifically excludes agencies within the Executive Branch of the USG.

IDA. An official who has been granted authority by a DOD Component head to withhold information requested pursuant to the FOIA for one or more of the nine categories of records exempt from mandatory disclosure.

Perfected FOIA Request. A FOIA request that arrives at the FOIA RSC of the DOD Component in possession of the records. The statutory time limit for responding to a FOIA request does not begin until it is perfected.

Responsive. Information or agency records requested by a FOIA requester.

UNCLASSIFIED

USCCI 5000-06

ATTACHMENT 2

DD FORM 2086

RECORD OF FREEDOM OF INFORMATION (FOI) PROCESSING COST				REPORT CONTROL SYMBOL DD-DA&M(A)1365	
Please read instructions on back before completing form.					
1. REQUEST NUMBER	2. TYPE OF REQUEST (X one)		3. DATE COMPLETED (YYYYMMDD)	4. ACTION OFFICE	
	a. INITIAL	b. APPEAL			
6. CLERICAL HOURS (E-9/GS-8 and below)			FEE CODE	(1) TOTAL HOURS	(2) HOURLY RATE
a. SEARCH			1		
b. REVIEW/EXCISING			2		
c. OTHER ADMINISTRATIVE COSTS			3		
6. PROFESSIONAL HOURS (D-1 - D-5/GS-9-GS-15)/CONTRACTOR			(1) TOTAL HOURS	(2) HOURLY RATE	(3) COST
a. SEARCH			1		
b. REVIEW/EXCISING			2		
c. OTHER/COORDINATION/DENIAL			3		
7. EXECUTIVE HOURS (D-7 - ES-1 and above)			(1) TOTAL HOURS	(2) HOURLY RATE	(3) COST
a. SEARCH			1		
b. REVIEW/EXCISING			2		
c. OTHER/COORDINATION/DENIAL			3		
8. COMPUTER SEARCH			(1) TOTAL TIME	(2) RATE	(3) COST
a. MACHINE TIME (Not PC, desktop, laptop)			4		
b. PROGRAMMER/OPERATOR TIME (Human)					
(1) Clerical Hours			1	\$20.00/hr	
(2) Professional Hours			1	\$44.00/hr	
9. OFFICE MACHINE COPY REPRODUCTION			(1) NUMBER	(2) RATE	(3) COST
a. PAGES REPRODUCED FOR FILE COPY			3	.15	
b. PAGES RELEASED			5	.15	
10. PRE-PRINTED PUBLICATIONS			(1) TOTAL PAGES	(2) RATE	(3) COST
a. PAGES PRINTED			5	.02	
11. COMPUTER PRODUCT OUTPUT/ACTUAL COST CHARGES			(1) NUMBER	(2) ACTUAL COST	(3) COST
a. TAPE/DISC/CD			0		
b. PAPER PRINTOUT			3		
12. OTHER ADMINISTRATIVE FEES			(1) NUMBER	(2) ACTUAL COST	(3) COST
a. ALL POSTAGE/ADMINISTRATIVE (See instructions)			3		
13. AUDIOVISUAL MATERIALS			(1) NUMBER	(2) ACTUAL COST	(3) COST
a. MATERIALS REPRODUCED			4		
14. SPECIAL SERVICES			(1) NUMBER	(2) ACTUAL COST	(3) COST
a. ALL SPECIAL SERVICES (See instructions)			6		
15. MICROFICHE REPRODUCED			(1) NUMBER	(2) ACTUAL COST	(3) COST
			5	.25	
FEE CODES			16. FOR FOI OFFICE USE ONLY		
1 Chargeable to "commercial" requesters. Chargeable to "other" requesters after deducting 2 hours.			a. TOTAL COLLECTABLE FEES		
2 Chargeable to "commercial" requesters only.			b. TOTAL PROCESSING FEES		
3 Not chargeable to any fee category.			c. TOTAL CHARGED		
4 Chargeable to "commercial". Chargeable to "other" after deduction of the equivalent of 2 hours. (Example: deduct \$88.00 professional rate.)			d. FEES WAIVED/REDUCED (X one)		
5 Chargeable to all fee categories after deduction of 100 pages (DOES NOT include "commercial").			e. FEES NOT APPLICABLE (X one)		
6 Chargeable to all fee categories. No deductions.			See Chapter 6, Fee Schedule, DoD 5400.7 R, to determine appropriate assessment of fees.		
			Yes No		
			Yes No		

DD FORM 2086, JAN 2003

PREVIOUS EDITION IS OBSOLETE.

UNCLASSIFIED



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/uscycbercom/Library/SitePages/publications.aspx>

Reissues and Cancels: United States Cyber Command Instruction (USCCD) 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.DENNI
S. [REDACTED]

Digitally signed by
VELEZ.DENNI
Date: 2025.01.27 12:44:32
-0500

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:

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

TABLE OF CONTENTS

SECTION 1: GENERAL INFORMATION.....	4
1.1. BACKGROUND INFORMATION.....	4
1.2. POLICY.....	4
SECTION 2: ROLES & RESPONSIBILITIES.....	5
2.1. CHIEF OF STAFF (COS).....	5
2.2. CHIEF KNOWLEDGE OFFICER.....	5
2.3. FOIA PROGRAM MANAGER (FPM).....	5
2.4. FOIA CASE MANAGER (FCM).....	6
2.5. SUBJECT MATTER EXPERT (SME).....	7
2.6. OFFICE OF THE STAFF JUDGE ADVOCATE.....	7
2.7. PUBLIC AFFAIRS OFFICER.....	7
2.8. OPERATIONS SECURITY COORDINATOR.....	8
2.9. CLASSIFICATION ADVISORY OFFICER.....	8
2.10. HEADQUARTERS USCYBERCOM PERSONNEL.....	8
SECTION 3: PROCEDURES.....	9
3.1. RECEIVING FOIA REQUESTS.....	9
3.2. REVIEWING FOIA REQUESTS.....	9
3.3. PROCESSING FOIA REQUESTS.....	10
3.4. RESPONDING TO FOIA REQUESTS.....	12
SECTION 4: NON-FOIA REQUESTS.....	13
4.1. MANDATORY DECLASSIFICATION REVIEW (MDR) REQUESTS.....	13
4.2. PRIVACY ACT REQUESTS.....	13
GLOSSARY.....	15
REFERENCES.....	17

SECTION 1: GENERAL INFORMATION

1.1. BACKGROUND INFORMATION.

- a. FOIA, United States Code (USC), Title 5, Section 552 and Public Law (PL) 93-579, are the laws that establish the public's 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 IA WUSCCI 5900.04.

2.4. FOIA CASE MANAGER (FCM).

- a. Processes FOIA requests IA W 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 -US001-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/ps/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 of FOIA 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 of responses to FOIA requests.

c. If the 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 of title 32, CFR for information regarding responses to FOIA requests and adverse determinations of FOIA requests.

d. If the 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) of title 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 staff that contribute to the processing of the 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 of all FOIA request processing.

(1) The FCM assigns the WMS task to the office(s) that has a nexus to the topic of the request. For example, if the request is for records regarding plans and policy, J5 may be an appropriate office to engage. Or, if the 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 of at least 10 working days.

(b) The FCM provides clear and concise guidance in the instructions field of the 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://dpcl.d.defense.gov/privacy/soms/> for information about SORs and system of record 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/uscycbercom/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>

MyGovLearn Portal: <https://elm.mygovlearn.com/ps/ps/?cmd=login>

Systems of Record and System of Record Notices: <https://dpcl.d.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/uscycbercom/J6/Pages/WMS-UG.aspx>

Secure Internet Protocol Router Network:

<https://intelshare.intelink.sgov.gov/sites/uscycbercom/s-wms-lite/UserGuides/Forms/AllItems.aspx>

NSANet:

<https://wms.cybercom.ic.gov/app/wms/User%20Guide/WMS%202%201%20User%20Guide%20NOV%2017.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