

U.S. CYBER COMMAND 2021 FOIA LOG

Case #	Requester Name	Request Description	Received
21-R019	Runa Sandvik	All briefs, emails, records, and any other documents on, about, mentioning, or concerning the creation of the 2020 ComRATv4 illustration, as seen here: https://twitter.com/CNMF_CyberAlert/status/1321863548486770689 .	01/01/21
21-R020	John Antill	I am requesting the Powerpoint Introduction to USCYBERCOM Battle Rhythm through the Freedom of Information Act.	01/06/21
21-R021	Michelle Broder Van Dyke	Information or records on "watertown chronicles." I'm requesting all finished intelligence on "watertown chronicles" from 1947 to 2011.	01/07/21
21-R022	Malcolm Byrne	A copy of any reports, assessments, analyses, and other records relating to the Iranian government's attempt to shut down nation-wide access to the Internet in November 2019 in response to large-scale public protests.	02/04/21
21-R023	Malcolm Byrne	A copy of any reports, assessments, analyses, and other records relating to the June 20, 2019, downing of a US surveillance UAV flying over the Persian Gulf. The time period for this request is 06/20/19-08/01/19.	02/05/21
21-R024	Malcolm Byrne	Any and all reports, assessments, and similar documents pertaining to Iranian cyberattacks against US government agencies on October 13-14, 2020. The Iranian government announced the attacks in state media on Oct. 15.	02/17/21
21-R025	Malcolm Byrne	Any and all reports, assessments, and similar documents pertaining to the background, motives, activities, and effectiveness of the "Silent Librarian" cyber group and its threat against U.S. assets and interests. The time period for this request is 08/01/2018-present.	02/18/21
21-R026	Parker Yesko	A list of all alleged war crimes perpetrated by members of CYBERCOM from 2001 through present, including dates, locations and narrative descriptions of the incidents, names/ages of victims, names/ranks/units of alleged perpetrators and all other details contained in CYBERCOM's central collection of reportable incidents. Please interpret the term "war crimes" in the broadest possible sense, to include the types of crimes defined in 18 U.S.C. § 2441, the Law of Armed Conflict, the Geneva Conventions and other commonly accepted frameworks for international humanitarian law.	02/18/21
21-R027	Gilberto Pineda	a) All Briefings, reports, memorándums, transcripts, presentations, policy statements, legal opinions, and emails related to Russian interference in the US elections of 2016, the disinformation campaigns carried out by Russian intelligence operatives in social networks, and the intrusion and late publishing of stolen materials from the Democratic National Committee, and any other records that describes the assessing by the CYBERCOM of such events.	01/17/21
21-R028	Gilberto Pineda	All briefings, reports, memoranda, transcripts, presentations, policy statements, legal opinions and manuals regarding quantum computing and quantum information science, from 2010 to 2021.	01/17/21
21-R029	Gilberto Pineda	All records such as presentations, legal opinions, technical assessments, memoranda, reports, and emails related to the "hacktivist" movement, "Anonymous" from the creation of the US CYBERCOM to this date.	01/17/21
21-R030	Joseph Cox	All invoices, purchases orders, contracts, loan agreements, procurement documents (but not limited to solicitation documents or notices of proposed contracts, proposed bids, unsolicited proposals, and/or documents justifying contracting without full and open competition), about, concerning, or related to the following companies and products: "Babel Street", "Locate X", "Locate X Premium", "Venntel", "Anomaly Six". All user manuals, instruction manuals, guides, and similar documents about, concerning, or related to the following companies and products: "Babel Street", "Locate X", "Locate X Premium", "Venntel", "Anomaly Six". All slide decks, presentations, Powerpoint Presentations, memos, and similar documents about, concerning, or related to the following companies and products: "Babel Street", "Locate X", "Locate X Premium", "Venntel", "Anomaly Six".	03/07/21
21-R031	Elias Moukal	I request that a copy of any, if not all documents (including emails) relating to the following Twitter post (including cross references) and its content to be provided to me in a pdf format. https://twitter.com/CNMF_CyberAlert/status/1228309409694134272?s=19	03/25/21
21-R032	Elias Moukal	I request that a copy of any, if not all documents (including emails) relating to the investigation & the disclosure of the Kimsuky APT group be provided to me in a pdf format.	03/25/21
21-R033	Elias Moukal	I request that a copy of any, if not all documents (including emails) relating to the investigation & the disclosure of the BeagleBoyz APT group be provided to me in a pdf format.	03/25/21

21-R034	Sean Lyngaas	Copies of any and all email correspondence between Cyber Command public affairs officers (to include, but not limited to (b) (6)) and other Cyber Command staff from March 20, 2021 to April 5, 2021 mentioning "MAR 10327841.rl.vl" or "MAR I 0327841" or "MAR" or "Mal ware Analysis Report." 2. All draft copies of MAR 10327841.rl.vl, or MAR 10327841, prepared between March 1, 2021 and March 31, 2021. 3. All revised copies of MAR 10327841.rl.vl, or MAR 10327841, prepared between March 31, 2021 and April 5, 2021.	04/05/21
21-R035	Harm Venhuizen	Any and all reports of cyber-attacks against Department of Defense systems, both attempted and successful. Any and all attachments and enclosures to said reports.	04/05/21
21-R036	Jurre van Bergen	Any records dealing with Russian companies/organisations: ARinteg (ООО "АРИНТЕР") (https://arinteg.ru/), Federal Service for Technical and Export Control (FSTEC / FSTEK) (https://fstec.ru/), JSC NPO Echelon (npo-echelon.ru), Axoft Oб Axoft (http://axoft.ru), Infotecs, АО "Инфотекс (https://infotecs.ru/) As well as persons: Alexey Markov and Dmitry Slobodenyuk	04/07/21
21-R037	Jurre van Bergen	The FOIA request log for 2020 and for January 2021, February 2021 and March 2021	04/07/21
21-R038	Mark Pomerleau	I request all documents from Jan. 1, 2012 to present related whole or in part to: The creation of the Capabilities Development Group (CDG), the CDG's roles, goals and missions and oversight of requirements CDG issued for capabilities.	04/05/21
21-R039	Mark Pomerleau	I request all documents from Jan. 1, 2012 to present related whole or in part to: The CDG's yearly budget for each year it existed and the number of personnel assigned to CDG for each year it existed as well as names, titles and job descriptions of such personnel.	04/05/21
21-R040	Mark Pomerleau	I request all documents from Jan. 1, 2012 to present related whole or in part to: Dissolution of CDG and reabsorption back into the J9.	04/05/21
21-R041	Mark Pomerleau	I request all documents from Jan. 1, 2012 to present related whole or in part to: J9's roles, goals and missions as they relate to requirements and capability development since the CDG was reabsorbed and the J9's budget as it applies to capability development and requirements since the CDG was reabsorbed	04/05/21
21-R042	Derek Bernsen	I request a copy of the following: product(s) be provided to me: Quarterly briefings from service cryptologic components on capabilities and readiness to USCYBERCOM. Specifically, manning numbers and retention rates as well as rough estimates for the number of capabilities produced by each service and by USCYBERCOM.	04/08/21
21-R043	Elisabeth Holmes	This FOIA/PA request is for any and all records, documents, and communications created since June 19, 2003 referring to, relating to, mentioning, or concerning: 1. Civil Liberties Defense Center (EIN 58-2670951, a 501(c)(3) nonprofit public benefit organization established in 2003 and based in Eugene, Oregon which provides legal representation, legal support, and educational resources to the public); 2. (b) (6) (see enclosed Privacy Act waiver enclosed for personal identifying information); 3. (b) (6) (see enclosed Privacy Act waiver enclosed for personal identifying information); 4. (b) (6) (see enclosed Privacy Act waiver enclosed for personal identifying information); 5. (b) (6) (see enclosed Privacy Act waiver enclosed for personal identifying information); 6. (b) (6) (see enclosed Privacy Act waiver enclosed for personal identifying information); 7. (b) (6) (see enclosed Privacy Act waiver enclosed for personal identifying information); 8. (b) (6) (see enclosed Privacy Act waiver enclosed for personal identifying information).	05/06/21
21-R044	Joseph Cox	I hereby request the following records: Any presentation slides, slide decks, or memorandum, that refer to, or are related to, about, or concerning Intrusion Truth, from January 1st 2018 to the date this request is processed.	05/11/21
21-R045	Jane Evans	Please send any possible information on any, all sonic attacks on people. For example, on diplomats working in Cuban embassy. If i am able to know the name of the agents who worked on the case, this would be extremely helpful. Also please send any possible information on anyone experiencing mind reading, as in having their thoughts decoded and known, without their consent, through the use of infrasound, (high n low frequencies usually inaudible). Being accomplished most likely through the use of maybe satellites, frequencies, towers, electromagnetics ect.	05/11/21
21-R046	Brad Heath	Please provide me copies of any authorizations or reports describing the two-dozen operations to disrupt 2020 election interference described on May 14 by Gen. Paul M. Nakasone.	05/14/21

21-R047	Eleanor Eagan	Request description The Revolving Door Project requests that your agency produce within twenty business days the following information for all entries from all agency transmissions to the Office of Personnel Management for inclusion in the Enterprise Human Resources Integration (EHRI) warehouse completed between January 1, 2017 and the date on which this request is fulfilled: Status Data Submission ID Name Agency/Subelement Adjusted Basic Pay Current Appointment Authority Duty Station Pay Plan Grade, Level, Class, Rank, or Pay Band Position Occupied Type of Appointment Work schedule Supervisory status Effective Date Location Occupation Occupational category Age Education Level Dynamics Data Submission: ID Name Agency/Subelement Current Appointment Authority Accession/Separation Indicator Effective Date Age Range Pay Plan Grade LOS Level Duty Station Occupation Occupational Category Adjusted Basic Pay Type of Appointment Work Schedule The Revolving Door Project seeks all responsive records regardless of format, medium, or physical characteristics. In conducting your search, please understand the terms "record," "document," and "information" in their broadest sense, to include any written, typed, recorded, graphic, printed, or audio material of any kind. To ensure that this request is properly construed, that searches are conducted in an adequate but efficient manner, and that extraneous costs are not incurred, the Revolving Door Project welcomes an opportunity to discuss its request with you before you undertake your search or incur search or duplication costs. By working together at the outset, the Revolving Door Project hopes to decrease the likelihood of costly and time-consuming litigation in the future. Where possible, please provide responsive material in electronic format by email or in PDF. Please send any responsive material being sent by mail to the Revolving Door Project, 1611 Connecticut Avenue NW, Suite 400, Washington, DC 20009. If it will accelerate release of responsive records to the Revolving Door Project, please also provide responsive material on a rolling basis.	05/19/21
21-R048	Mark Pomerleau	I request all documents related whole or in part to: After action reviews from exercises U.S. Cyber Command participated in or conducted from Jan. 1, 2018 to present prepared by U.S. Cyber Command and analysis from exercises U.S. Cyber Command participated in or conducted from Jan. 1, 2018 to present prepared by U.S. Cyber Command.	05/24/21
21-R049	Aaron Schaffer	I hereby request the following: A copy of all documents, including but not limited to unclassified memoranda, prepared under 10 USC 484 (as amended by the FY 2021 NDAA) to the date of your search.	06/15/21
21-R050	Aaron Schaffer	I hereby request the following: Documentation associated with Operation Synthetic Theology. Please include any PowerPoint slideshows, operational notes and memos, recorded audio/video data and after action/Battle Damage Assessment reporting that may also be releasable.	06/17/21
21-R051	Cristin Monahan	I hereby request the following: Any correspondence between the Louisiana National Guard and USCYBERCOM regarding a series of cyberattacks targeting the Louisiana state government offices in October 2020.	06/24/21
21-R052	Raquel Poy	In 2017? 2018? I tried to make a direct FOIA request from CyberCom. US military. I'd like to make a FOIA request for all data available about me held with the US Military. Since they should have none beyond my identifying info because I would never be in the military. its like a Catfish Episode joke waiting to happen by the "strongest military in the world". (hysterical! lmao)	07/05/21
21-R053	Mark Pomerleau	I request all documents related whole or in part to: After action reviews from Cyber National Mission Force collective training events U.S. CyberCommand conducted from Jan. 1, 2018 to present prepared by U.S. Cyber Command and analysis from Cyber National Mission Force collective training events U.S. Cyber Command participated in or conducted from Jan. 1, 2018 to present prepared by U.S. Cyber Command	07/12/21
21-R054	Aaron Schaffer	Documentation associated with the Election Security Group. Please include any PowerPoint slideshows, operational notes and memos, recorded audio/video data and after action/Battle Damage Assessment reporting that may also be releasable.	06/17/21
21-R055	Joseph Cox	All slides, memos, briefs, instruction manuals, guidelines, related to PREVALENTCHEF, from 1st January 2020 to the present.	08/03/21
21-R056	Joseph Cox	All slides, memos, briefs, instruction manuals, guidelines, related to WOLFDOOR 2.0, from 1st January 2020 to the present.	08/03/21
21-R057	Joseph Cox	All slides, memos, briefs, instruction manuals, guidelines, related to GREENMONKEY, from 1st January 2020 to the present.	08/03/21

21-R058	(b) (6)	I request all confidential and pertinent records related to myself, (b) (6), Social Security # (b) (6). The records are to include any and all documents related to me, especially documents related to me being the subject of directed energy experimentation, or the similar, that is ran out of Luke Airforce Base, Shriever Air Force Base, Shriever Space Force Base, Peterson Space Force Base, and Peterson-Shriever Garrison. If easiest, an email with all documents is sufficient. Also, include any and all documents related to the Cyber Command knowledge of impersonation of Cyber Command personnel by United States Air Force personnel during USAF's Directed Energy Weapons experimentation of subject (b) (6).	08/24/21
21-R059	Emma North-Best	I hereby request the following records: Records mentioning or describing the Chinese hacking group sometimes known as BYZANTINE FOOTHOLD.	09/01/21
21-R060	Emma North-Best	I hereby request the following records: Records mentioning or describing PLA Unit 61398 AKA BYZANTINE CANDOR, APT1 (Mandiant), Beijing Group (Secureworks), Comment Crew/Comment Group, Comment Panda (CrowdStrike), Elderwood Group (Symantec), Shanghai Group (Secureworks), Sneaky Panda (CrowdStrike) and TITAN RAIN III. You may limit this search to records generated since January 1, 2002.	09/01/21
21-R061	Emma North-Best	I hereby request the following records: Records mentioning or describing the hacker group sometimes referred to as BISHOP KNIGHT.	09/02/21
21-R062	Olivia Fines	Emails and Instant Messages (using any platform such as Skype, TEAMS, AIM, etc.) to or from Dr. Laura Callahan, Deputy Director (acting), C4 Systems Directorate, from 1 September 2019 to Present which reference singularly or in any combination of any of the following search terms (b)(3) and (b)(6)	09/13/21

21-R063	Antonio Perez-Marques	<p>I hereby request that the United States Cyber Command make available copies of:</p> <p>1. Communications between individuals at the United States Cyber Command responsible for or with authority to make decisions regarding the procurement of cybersecurity and/or counterterrorism tools or products and (b)(3) and (b)(6)</p> <p>[REDACTED]</p>	09/14/21
22-R001	Adam Janofsky	Emails, memos, powerpoint presentations, and other documents sent to or held by US Cyber Command that reference the word "BlackMatter" between the years 2016 and 2021 (most recent date available). Such documents may include mention of "ransomware".	10/01/21
22-R002	Aaron Schaffer	I hereby request the following: A copy of the listing of U.S. Cyber Command Office of Inspector General Investigations closed during Calendar Years 2019, 2020 and 2021 (through Sept. 2021).	10/19/21
22-R003	Aaron Schaffer	I hereby request the following: A copy of each report produced for Congress by U.S. Cyber Command during the past three years, and which are not posted on the Command's public internet website.	10/19/21
22-R004	Aaron Schaffer	I hereby request the following: A digital/electronic copy of any transition briefing document(s) (late 2020) prepared by U.S. Cyber Command for the incoming Biden Administration.	10/19/21
22-R005	Aaron Schaffer	I hereby request the following: A copy of all procurement and planning documents related to PAPERWASP. Please include all contracts and emails associated with PAPERWASP, any modification, and any subaward.	10/19/21
22-R006	(b) (6)	My Archival SF86	10/24/21

22-R007	Stefan Soesanto	Information on the deployment of NATO's Cyber Rapid Reaction Teams (RRTs): (1) Number of cyber incidents or cyber attacks that led to the activation of a NATO RRT (2012-2021) (2) Country or location where these cyber incidents or cyber attacks took place / RRT missions were carried out (3) Duration of the RRT missions (average of all and/or duration of the individual RRT missions) (3) Descriptions of the information and communication systems affected (4) Information on any attribution assessments made ("who done it?") (5) After-action reports / NATO RRT performance evaluations	10/29/21
22-R008	Cristin Monahan	I hereby request the following: REF A of USCYBERCOM EXORD 12-1183: "CRISIS ACTION PLANNING TO DEFEND THE NATION FROM IRANIAN CYBER ATTACKS," WARNORD 12-0659, published June 11, 2012.	11/15/21
22-R009	(b) (6)	All travel approved by US CYBERCOM for (b) (6) from 01 Jan 2017 to 01 May 2021. This request is due to the amount of travel that (b) (6) supposedly did with US CYBERCOM.	11/16/21
22-R010	(b) (6)	Contact information for the Joint Exercise Planner USCYBERCOM J-7 Security Manager. I would like the contact information for the security office/officer in charge in order to contact them regarding (b) (6) admission of misconduct.	11/16/21
22-R011	Cristin Monahan	I hereby request the following: For the period from June 2017 to present, any records referencing the malware known as "Industroyer" or "Crash Override." This malware was employed in the December 2016 attack on Ukraine's national grid operator, Ukrenergo.	11/17/21
22-R012	(b) (6)	All documents relating to any/all sexual affairs (b) (6) had during her marriage to (b) (6). I know she admitted to at least one sexual affair with a coworker US Air Force (b) (6), as well as admitted to her Security Officer others. Date range 01 Jan 2017- 01 May 2021.	11/17/21
22-R013	(b) (6)	All travel dates approved by U.S. CYBERCOM for travel for (b) (6). I would prefer the location as well as travel dates, however if the travel locations are not available then just the dates of travel that were approved for "work related" travel.	11/17/21
22-R014	Cian Heasley	I am looking for any records or information you may hold on hacking related to computer intrusions that took place in late 1997 or early 1998 that involved Netdex, a California based ISP and Department of Defense systems. A Wired article from the time quotes the CEO of Netdex as saying "10 San Francisco-based FBI agents are devoted to the case, and that the investigation has involved the National Security Agency, the Air Force, the Pentagon, and "dozens, if not hundreds, of system admins." At the time the hack that was most prominently mentioned was Lawrence Livermore National Laboratories, although many other systems were affected. At the time Deputy Defense Secretary John Hamre described the "organized and systematic" attack as having "the potential to disrupt military communications throughout the world." I am requesting these records from December 1st 1997 through to July 30th 1998.	11/30/21
22-R015	Cristin Monahan	After action reports, participant lists, exercise scenarios or inject materials, or budgetary documents related to exercise Cyber Guard 15 from September 2014 to January 2016	12/01/21
22-R016	Aaron Schaffer	Reports associated with Inspector General investigative inquiries IO-2021-001 and 2021-049	12/03/21
22-R017	Nick Turse	30 minute FOIA presentation mentioned in the 2021 DoD Chief FOIA Officer Report	12/05/21
22-R018	Nick Turse	U.S. Cyber Command FOIA request log from January 1, 2021, to present.	12/05/21
22-R019	Nick Turse	I request a copy of the Standing Operating Procedures (SOPs) referred to in this document: https://open.defense.gov/Portals/23/Documents/FOIA/CFO/2021_DoD_Chief_FOIA_Officer_Report.pdf ("Standing Operating Procedures (SOPs) can improve the consistency and quality of an agency's FOIA process. Eighty-eight percent of DoD's Components have SOPs. Sixty four percent of DoD Components describe their FOIA process on their websites to show that DoD has effective systems in place. The majority of components review the accuracy of their procedures, on an annual basis, some components review SOPs montly, biannually, or on an "as needed basis.")	12/05/21
22-R020	Elias Moukal	USCYBERCOM FOIA statistics for 2021	12/6/21
22-R021	Nick Turse	I request copies of individual "self assessment" agency reports and RMSA surveys from 2016 to the date that this request is perfected	12/11/21
22-R022	Elias Moukal	Regarding my request on Red Star, I am afraid this is as specified as I can go. I am interested in records by CYBERCOM describing the operation, the history & the functionality of the operating system, specifically version 2.0 and 4.0.	12/13/21

22-R023	Cristin Monahan	I hereby request the following: Any charter documents, meeting minutes, briefings, or presentations produced by the "Implementation Team," a team of four officers, including then-Colonel Paul Nakasone and Lt. Colonel Jen Easterly, tasked by Keith Alexander with developing an initial framework for a cyber command.	12/21/21
22-R024	Kathleen Casey	I am requesting copies of the following records: FOIA Requests On The Topic Of "Senator Bennet," And/or "Michael Bennet" (December 2016 – Present). Freedom of Information Act (FOIA) requests and the responsive materials thereof filed December 2016 to the present date of this request on the topic of "Michael Bennet," "Senator Bennet," or the staff or representatives of Senator Michael Bennet, in both his capacity as a United States Senator and as a private citizen. Direct correspondence should include letters, emails, reports, and other relevant material. I am not seeking any secondary material such as phone logs, notations of conversation, etc. FOIA requests made by America Rising and/or Allan Blustein: I am requesting copies of all FOIA requests made by America Rising and/or Allan Blustein (a.blustein@americarisingllc.com) to U.S. Department of Defense- U.S. Cyber Command from December 1, 2016, to	12/18/21
22-R025	Cristin Monahan	I hereby request the following: Any briefings, memoranda, presentations or assessments, regarding the following Israel-based companies: Cobwebs, Cognyte, Black Cube, and Bluehawk CI. Meta (formerly Facebook, Inc.) released a report (https://about.fb.com/wpcontent/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf) linking these companies to the surveillance-for-hire industry.	12/22/21

22-R026	Antonio Perez-Marques	<p>I hereby request that the United States Cyber Command make available copies of: Communications between individuals at the United States Cyber Command responsible for or with authority to make decisions regarding the procurement of cybersecurity and/or counterterrorism tools or products and (b)(3) and (b)(6)</p> 	12/23/21
---------	-----------------------	---	----------