U.S. CYBER COMMAND 2020 FOIA LOG

Case #	Requester Name	Request Description	Received
20-R016	Patrick O'Neill	I hereby request the following records: I hereby request the following records: The FOIA request log for 2019	1/22/20
20-R017	Patrick O'Neill	I hereby request the following records: National Security Presidential Memorandum 13.	1/22/20
20-R018	Michael Martelle	I hereby request the following records: Any documents or briefings or briefing materials dated 2009 or later containing any of the following words: "arrakis", "houseatreides", "BasharoftheSardaukars", "SalusaSecundus2", "epsiloneridani0". The word may be followed by a two-digit number, ex) "arrakis02". Any documents or briefing material dated 2000 or later containing mention of the Dune series of novels or author Frank Herbert.	1/29/20
20-R019	Patrick O'Neill	I hereby request the following records: Documentation spanning from 1/1/2015 to 1/1/2020 for the Joint Interagency Coordination Process referenced on page 13 of the USCYBERCOM 30-Day Assessment of Operation Glowing Symphony, December 13 2016.	1/29/20
20-R020	Benoit Berthelier	Records related to the Lazarus Group, HIDDEN COBRA, Park Jin-hyok, Chosun Expo or APT38	2/4/20
20-R021	Benoit Berthelier	Records regarding North Korean propaganda activities online	2/4/20
20-R022	Benoit Berthelier	Records related to the North Korean DDoS Botnet infrastructure	2/4/20
20-R023	Benoit Berthelier	Records related to Digital forensics methods used to identify attacks & malware as North Korean	2/4/20
20-R024	Benoit Berthelier	Records related to Records related to the modus operanti of North Korean hackers (communication methods, programming languages & techniques, procurement and/or sale of 0day exploits...)	2/4/20
20-R025	Benoit Berthelier	Records related to Domestic and overseas training of state-sponsored North Korean hackers (Unit 180, Bureau 121)	2/4/20
20-R026	Jurre van Bergen	I hereby request the following records: Any records related to Metasploit including the ETERNALBLUE, EmeraldThread, EternalChampion, EskimoRoll, EternalRomance, EducatedScholar, EternalSynergy, EclipsedWing computer vulnerability exploitation code into the Metasploit framework, developed by Rapid7. This could for example be damage assessments that are being shared with any other government agencies, or received by such agencies. As well as any investigations that could have stemmed into the inclusion of such cyber attack tools into an open source and freely distributive and completely free tool like Metasploit.	2/4/20
20-R027	Rachel Cuccias	for information on a contract for Big Data Platform (BDP). The Prime is Alion Science. The contract #: HB0001-18-C-0001 and we are specifically asking for information on Task Order HC102816F027. We are requesting the contract and any modifications to the contract. We are also requesting the Scope of Work and the Contract value	2/6/20
20-R028	Michael Martelle	I hereby request the following: Any documents related to the investigation into the Equifax data breach.	2/10/20
20-R029	Michael Martelle	I hereby request the following: DRAFT DEFEND THE NATION AGAINST IRANIAN OFFENSE CYBERSPACE OPERATIONS/OPORD 12-XXXX, which is REF/C of EXORD 12-1183, or the final version of the same	2/19/20
20-R030	Michael Martelle	I hereby request the following: Joint Staff Action Processing Form/Cyber Manpower Service Force Mix/Joint Staff JS PBAD, as referenced in USCYBERCOM TASKORD 12-1462.	2/20/20
20-R031	Michael Martelle	I hereby request the following: Warning Order 12-0659, as referenced in USCYBERCOM EXORD 12-1183	2/20/20
20-R032	Michael Martelle	I hereby request the following: Tasking Order 12-1053, as referenced in USCYBERCOM EXORD 12-1183	2/20/20
20-R033	Michael Martelle	I hereby request the following: Fragmentary Order 01 to Tasking Order 12-1053, as referenced in USCYBERCOM EXORD 12-1183.	2/20/20
20-R034	George Johnston	I hereby request the following records: A list of all Mission Rehearsal Exercises (MRE / MRX) 1st IO Command Participated in for the calendar year 2019, and Information Operation products produced for the month of April 2019 at the training site or sites.	2/22/20
20-R035	Michael Martelle	I hereby request the following records: Any after action reviews, reports, or progress reports related to Defend the Nation - Iran (DTN-I) or any operations sharing a cryptonym with DTN-I	2/26/20
20-R036	Christopher Sheats	I hereby request the following records: Copies of internal presentations, reports, studies, memorandum, or proposals created or received by U's Cyber Command concerning software developed by The Tor Project, Inc., including but not limited to: Tor, Tor Browser, Tor bridges, Tor onion sites (v2 or v3, sometimes called "darkweb" or "darknet" sites), Tor onion services (v2 or v3, sometimes called "hidden services"), Tor bandwidth authorities or directory authorities, Tor pluggable transports (obfs4, meek, ScrambleSuit, etc.), Tor relays (also known as "routers" or "nodes", sometimes called "guard", "middle", or "exit" relays)	3/2/20

20-R037	Eric Geller	I hereby request the following records: All Vulnerabilities Equities Process annual reports and other VEP documents distr buted to U.S. Cyber Command in its role as a member of the VEP Equities Review Board	3/3/20
20-R038	Michael Martelle	I hereby request the following: Any orders, briefings, or after-action reports regarding or mentioning Operation Setting Sun	3/13/20
20-R039	Michael Martelle	I hereby request the following: Any documents mentioning or related to "Joint Task Force Galen" or "JTF Galen" from March 1, 2020 onwards	4/8/20
20-R040	Ananda Srethapramote	Russian 2016 hackings	5/2/20
20-R041	Ananda Srethapramote	Tik tok privacy issues	5/3/20
20-R042	Emma Best /Jason Leopold	I hereby request the following: Documents, memos, reports, letters, emails, eChirps and other written, audio-visual or other recorded format mentioning or descr bing the hacktivist known as Phineas Fisher, AKA Phineas Phisher, HackBack and @GammaGroupPR, most famous for the data breaches of Gamma Group, Hacking Team, AKP and Cayman National Bank and Trust (Isle of Man).	5/4/20
20-R043	(b) (6)	I, (b) (6), am submitting a request for electronic copies of all final depositions in support of an investigation of allegations leveled against Mr. (b) (6) United States Cyber Command.	5/18/20
20-R044	Chris Bing	I hereby request the following records: Product brochures, Powerpoint presentations, and other promotional business documents from U.S. defense contractor Raytheon -- also known as Raytheon Intelligence, Information and Services (IIS) and/or Blackbird Technologies -- about products relating to tactical intelligence, surveillance, reconnaissance and cybersecurity. Such product documents may carry terminology/keywords/descriptions that include: Computer Network Operations (CNO), Computer Network Exploitation (CNE) and Computer Network Attacks (CNA). This FOIA is not requesting documents marked as classified, but rather it seeks marketing materials produced by the contractor, Raytheon, to explain/sell their cyber intelligence offerings to the U.S. government between the years 2014 and 2020.	5/21/20
20-R045	Chris Bing	I hereby request the following records: Product brochures, Powerpoint presentations, flyers and other promotional business documents from U.S. defense contractor BlackHorse Solutions, Inc. about products relating to cybersecurity, electronic warfare, virtual operations, artificial intelligence, and machine learning. Such product documents may carry terminology/keywords/descriptions that include: Computer Network Operations (CNO), Computer Network Exploitation (CNE), Computer Network Attacks (CNA), and quick reaction capability (QRC). BlackHorse Solutions, Inc. is a Virginia-headquartered company that specializes in developing technology for Department of Defense agencies. This FOIA seeks materials produced by the contractor to explain/sell/market their offerings to the U.S. government between the years 2014 and 2020 (or this current date of review). Such material would be l kely held by the appropriate business contracting office and other divisions that make purchasing decisions	6/1/20
20-R046	Chris Bing	I hereby request the following records: Product brochures, Powerpoint presentations, flyers and other promotional business documents from U.S. defense contractor ManTech about products or services relating to offensive cybersecurity, electronic warfare, virtual operations, artificial intelligence, and machine learning. Such product documents may carry terminology/keywords/descriptions that include: Computer Network Operations (CNO), Computer Network Exploitation (CNE), Computer Network Attacks (CNA), and quick reaction capability (QRC). ManTech, also known as ManTech International Corporation, is a Virginia-headquartered company that specializes in developing technology solutions for Department of Defense agencies. This FOIA seeks materials produced by the contractor to explain/sell/market their cyber intelligence capabilities/offerings to the U.S. government between the years 2017 and 2020 (or the current date of review). Such material would be likely held/controlled by the appropriate business contracting office within the agency and/or other divisions that make purchase/contracting decisions.	6/1/20

20-R047	Chris Bing	I hereby request the following records: Product brochures, Powerpoint presentations, flyers and other promotional business documents from U.S. defense contractor Booz Allen Hamilton about products or services relating to offensive cybersecurity, electronic warfare, virtual operations, artificial intelligence, and machine learning. The focus of the requests involves product documents that carry terminology/keywords/descriptions such as: Computer Network Operations (CNO), Computer Network Exploitation (CNE), Computer Network Attacks (CNA), quick reaction capability (QRC), signals intelligence (SIGINT), and cyber intelligence. Booz Allen Hamilton, also known as Booz Allen and BAH , is a Virginia-headquartered company that specializes in offer services and developing technology solutions for U.S. government agencies. This FOIA seeks materials produced by the contractor to explain/sell/market their cyber intelligence capabilities/offerings to the U.S. government between the years 2017 and 2020 (or the current date of review). Such material would be likely held/controlled by the appropriate business contracting office within the agency and/or other divisions that make purchase/contracting decisions.	6/1/20
20-R048	Chris Bing	I hereby request the following records: Product brochures, Powerpoint presentations, flyers and other promotional business documents from defense and technology company Verint Systems -- also known as "Verint" or "Verint Cyber Intelligence" or "Verint CIS" -- about products or services relating to offensive cybersecurity, surveillance, electronic warfare, virtual operations, artificial intelligence, and machine learning. The focus of the requests involves product documents that carry terminology/keywords/descriptions such as: Computer Network Operations (CNO), Computer Network Exploitation (CNE), Computer Network Attacks (CNA), and cyber intelligence. Verint is a technology contractor that sells surveillance technologies and internet monitoring capabilities. The firm is headquartered in the United States, but is primarily managed from Israel. Verint is known for producing high-tech products for national security and law enforcement agencies to help conduct surveillance against threats, including terrorism and criminal entities. This FOIA seeks materials produced by the contractor to explain/sell/market their cyber intelligence capabilities/offerings to the U.S. government between the years 2015 and 2020 (or the current date of review). Such material would be likely held/controlled by the appropriate business contracting office within the agency and/or other divisions that make purchase/contracting decisions	6/1/20
20-R049	Emily Crose	I hereby request the following records: Documentation associated with Operation GLOWINGSYMPHONY as outlined in the attached news article on the project. Please include any powerpoint slideshows, operational notes, recorded audio/video data and after action/Battle Damage Assessment reporting that may also be releasable	6/9/20
20-R050	Daniel Ekern	Any records on contracts, research agreements, personnel, or projects involving Carnegie Mellon University, specifically related to the areas of Artificial Intelligence, Robotics, and Psychology.	6/17/20
20-R051	Nataliya Gerasimova	I am seeking a list of correspondences between the U.S. Cyber Command and members of Congress and their offices. Specifically, I would l ke to know what Congressional offices contacted the U.S. Cyber Command from 01.01.2001 to 12.31.2019. An entry in such a log generally includes: 1) The name of the member of Congress who contacted the U.S. Cyber Command 2) The date the U.S. Cyber Command was contacted 3) The subject of the inquiry. (i.e. What kind of information did the member request? Or what was the correspondence about?) 4) When (and if) the request was completed.	6/18/20
20-R052	Cameron Oakes	I request access to and copies of: All letters, investigative files, memos, and emails (from 01/01/00 onward) with the terms "Omegle.com ," "Omegle," or "Omegle.com LLC" appearing in the subject or body of the document.	6/19/20
20-R053	Pavithra Rajesh	The analysis related to the TikTok app, including the analysis related to the decision to advise military personnel of the potential risk associated with using the T kTok app	7/10/20

20-R054	Michael Leiter	1. All records relating to or referring to the March 13, 2020, letter from William Dunlap, Director of the Information Technology Directorate for the Defense Advanced Research Projects Agency ("DARPA"), to Drew Hayden, Agile Defense Program Manager, notifying Agile Defense that "the U.S. Government has disqualified the vendor Fortinet" and directing "the removal of the platform (CyberSponse)" from all DARPA networks (attached), including but not limited to records explaining the factual and legal basis for the decision to "disqualify" Fortinet and require the removal of CyberSponse from all DARPA networks. 2. All records relating to CCB case DMSS-07945-3 referenced in Mr. Dunlap's letter of March 13, 2020, identified in Request No. 1 above that refer or relate to Fortinet or the decision to disqualify Fortinet as a vendor in connection with the prime contract awarded to Agile Defense. 3. All records relating to or referring to the potential or actual disqualification, suspension, or debarment of Fortinet by the Department of Defense, any Department of Defense component, or any other United States government agency, including but not limited to any communications, memoranda, risk assessments, findings, or notifications regarding Fortinet or any of its products or services. 4. To the extent not included in Requests Nos. 1, 2 or 3, above, all records received by the Department of Defense from any third party or. other government agency or any communications and other written correspondence between the Department of Defense and third parties or other governmental agency regarding Fortinet or any of its products or services. 5. To the extent not included in 1, 2, or 3, above, all records reflecting or memorializing any contacts, meetings, or communications regarding or in connection with the decision to disqualify, suspend, or debar Fortinet (1) between any agents, employees, or contractors of the Department of Defense; (2) between any agent, employee, or contractor of the Department of Defense and any agent, employee, or contractor of another U.S. government agency; and (3) between any agent, employee, or contractor of the Department of Defense and any third party. 6. All records from on or after January 15, 2020, regarding Fortinet that were prepared by U.S. Cyber Command or distr buted by U.S. Cyber Command to any U.S. government agency or other third party.	7/13/20
20-R055	Byron Tau	I request the department provide the following records within 20 business days: - Any prepared remarks, notes, transcriptions, audio recording or video recordings of the remarks that David Luber, Executive Director, United States Cyber Command, made at the 2019 GEOINT Symposium, as well as any other records pertaining to his remarks. - To assist in the agency's search, please note that Mr. Luber is listed as delivering a keynote address to the symposium on June 4, 2019:http://geoint2019.com/agenda?day=4 - Please search for records between Jan 1., 2019 and Jan 1., 2020	7/14/20
20-R056	Eric Geller	I hereby request the following records: All records of classified and unclassified war games, tabletop exercises, and simulations related to election security (including but not limited to election infrastructure cyberattacks, disinformation, and other forms of election interference) in which U.S. Cyber Command has participated since the 2016 election.	7/20/20
20-R057	Cristin Monahan	I hereby request the following: Any documents or communications pertaining to Xi'an Tianhe Defense Technology Company Limited, or to any of its subsidiaries.	7/27/20
20-R058	Cristin Monahan	I hereby request the following: Any documents, including correspondence and after-action reports, pertaining to the "Zbellion" component of the 2018 Joint Land, Air, and Sea Special Strategic Program (JLASS).	7/27/20
20-R059	Cian Heasley	I hereby request the following: I am writing to request documents, records or recordings (audio or video) or other information media you may hold on the hacking group known as "TeaMp0isoN" aka "Team Poison" aka "Team P0ison" and its member "TriCk" aka Junaid Hussein and the August 11th release of US military personnel records by Hussein on Twitter.	8/15/20
20-R060	Chris Bing	Emails sent from these addresses to Cyber Command: kgumtow@cyberpointllc.com and kgumtow@dreamport.tech, Search terms: Project Raven, Reuters, Raven, UAE, United Arab Emirates, Lori Stroud, Karma	8/17/20

20-R061	Taylor Matthews	I request that a copy of the following document(s) be provided to me: · All contracts between the Department of Defense (or any subdivision or component thereof) and Atigeo; · All communications regarding Atigeo's performance or lack of performance under any contract with the Department of Defense (or any subdivision or component thereof); · All communications regarding problems implementing Atigeo's software (including xPatterns) and problems normalizing and ingesting data to be analyzed by Atigeo's software (including xPatterns); · All communications regarding the performance or lack of performance of any cyber-security solutions or software provided by Atigeo, including but not limited to its xPatterns product; · Documents sufficient to show the payments made to Atigeo; and · All communications regarding evaluation of Atigeo's performance, including but not limited to any communications regarding breach of any contract with the Department of Defense (or any subdivision or component thereof).	8/20/20
20-R062	Cian Heasley	I am requesting information, documents, records or recordings (audio or visual) you may hold relating to a computer malware "botnet" known as "BrickerBot" and the internet nickname associated with its author "Janit0r".	8/21/20
20-R063	Emma Johanningsmeier	I request that all records held by the U.S. Cyber Command related to the Telegram app and its founder, Pavel Durov, be provided to me.	8/22/20
20-R064	Cristin Monahan	I hereby request the following: Any documents, including but not limited to, official correspondence, incident reporting, assessments, or briefing material related to the 2019 investigation into cyber attacks attr buted to Advanced Persistent Threat 28 on the Montenegro government's networks.	9/21/20
21-R001	Cristin Monahan	I hereby request the following: For the time period between January 2017 and October 2020, any correspondence, reports or assessments regarding Chinese cybersecurity parks, also known as Information Security Industrial Parks, in Beijing, Tianjin, and Chengdu.	10/2/20
21-R002	Eric Reusche	I would l ke to receive any documentation related tot he mission of the Military Auxiliary Radio System	10/20/20
21-R003	Carsten Beyer	I am requesting the following information; 1) Any intelligence that was captured from Operation Glowing Symphony conducted by JTF-ARES in 2016 against ISIL media production units, or a summary of the intelligence thereof.	10/17/20
21-R004	Juan Morillo	1. The following Documents and Communications relating to Facebook: a. All Documents and Communications relating to any requests by the United States Cyber Command ("Cyber Command") to Facebook for information or assistance; b. All Documents and Communications relating to Facebook's responses to any Cyber Command requests for information or assistance; c. All Documents and Communications relating to the use of Facebook by law enforcement targets or other individuals suspected of engaging in a crime or other act of misconduct; d. All Documents and Communications discussing any Facebook policy or practice of surveilling its users; e. All Documents and Communications relating to any breaches of Facebook's security policies by third parties, including hacking of Facebook by a third party or other data breaches at Facebook; f. All Documents and Communications relating to Facebook's security vulnerabilities; g. All Documents and Communications relating to Facebook's knowledge or awareness of the use of Facebook in furtherance of any crime or other act of misconduct; and h. Any Documents and Communications containing information Facebook has disclosed to the Cyber Command that relates to NSO Group Technologies ("NSO Group"). 2. The following Documents and Communications relating to WhatsApp, a. All Documents and Communications relating to any requests by the Cyber Command to WhatsApp for information or assistance; b. All Documents and Communications relating to WhatsApp's responses to any Cyber Command requests for information or assistance; c. All Documents and Communications relating to the use of WhatsApp by law enforcement targets or other individuals suspected of engaging in a crime or other act of misconduct; d. All Documents and Communications discussing any WhatsApp policy or practice of surveilling its users; e. All Documents and Communications relating to any breaches of WhatsApp's security policies by third parties, including hacking of WhatsApp by a third party or other data breaches at WhatsApp; f. All Documents and Communications relating to WhatsApp's security vulnerabilities; g. All Documents and Communications relating to WhatsApp's knowledge or awareness of the use of WhatsApp in furtherance of any crime or other act of misconduct; and h. Any Documents and Communications containing information WhatsApp has disclosed to the Cyber Command that relates to NSO Group	10/26/20

21-R005	Ron Hartke	I am requesting: 1. historical PWS/SOW for existing contract - HB000120C0003 2. for existing contract, who is currently assigned: PM (program manager), COR (Contracting Organization Representative), POC (point of contact), CO/KO (contract officer), and CS (contract specialist)	11/4/20
21-R006	John Greenewald	I respectfully request a copy of records, electronic or otherwise, of the following: 1) FOIA Case Log for calendar years 2010-2019 (if your agency operates off of a fiscal year, that is also ok) 2) FOIA Appeals Log for calendar years 2010-2019 (if your agency operates off of a fiscal year, that is also ok) 3) Mandatory Declassification Review (MDR) Log for calendar years 2010-2019 (if your agency operates off of a fiscal year, that is also ok)	11/25/20
21-R007	John Antill	Requesting a FOIA action on this to allow the use in a research paper for Kent State University and posting on the Army MFP process USCCI 5900-04	12/1/20
21-R008	John Antill	Requesting a FOIA action on this to allow the use in a research paper for Kent State University and posting on the Army MFP process USCCI 5200-03	12/1/20
21-R009	John Antill	Requesting the PDF of the Battle Rhythm site that goes over the whole site in detail.	12/3/20
21-R010	Malcolm Byrne	I hereby request the following: A copy of any reports, assessments, analyses, and any other records pertaining to Iranian targeting of dissidents or pro-democracy groups using cyber tools and spyware from November 2019-2020.	12/14/20
21-R011	Malcolm Byrne	I hereby request the following: A copy of any reports, assessments, analyses, and any other records pertaining to U.S. cyber operations against--or infiltration of--Iranian military computer systems in 2019. Media reports cite US officials acknowledging at least one such strike possibly in the wake of the June 2019 downing of a US surveillance UAV.	12/15/20
21-R012	Malcolm Byrne	I hereby request the following: A copy of any reports, assessments, analyses, and other records relating to the background, motivation, tactics, and effectiveness of the Izz ad-Din al-Qassam Cyber Fighters, a group connected to Iran.	12/16/20
21-R013	Malcolm Byrne	I hereby request the following: A copy of any reports, assessments, analyses, and any other records pertaining to Iran's claim that it halted a major cyber attack against unspecified "electronic infrastructure" in December 2019.	12/17/20
21-R014	(b) (6)	I hereby request the following: I would like the notes that the polygrapher took on (b) (6) and the information that he relayed to ARCYBER. This took place on November 20, 2020 at 8:00 AM outside the Whitelaw Campus on Ft. Gordon in the polygraph examiner's office.	12/17/20
21-R015	Michael Thalen	I hereby request the following: I request all agency records between June 2020 and present related to the following tweet made by @US_CYBERCOM on Dec. 22, 2020: https://twitter.com/US_CYBERCOM/status/1341408612942491656 The records I request include, but are not limited to: 1) Any correspondence or record of correspondence regarding the drafting of the tweet. 2) Any correspondence or record of correspondence regarding the creation of the ugly sweater photograph used in the tweet. These include any correspondence sent through official government email addresses, forums, or messaging services as well as any correspondence made through third-party services such as Gmail or Slack.	12/22/20
21-R016	Cristin Monahan	I hereby request the following: All materials, including but not limited to, planning documents, memos, reports and presentation slides related to or explaining Operation Synthetic Theology.	12/28/20
21-R017	Cristin Monahan	I hereby request the following: All policies, procedures and guidance documents addressing the composition, review, posting and deletion processes and criteria for US CYBERCOM-affiliated social media postings (including those by Twitter handles @US_CYBERCOM and @CNMF_CyberAlert).	12/29/20
21-R018	Cristin Monahan	I hereby request the following: Initial Cyber Command work plan and storyboards, developed by General Keith Alexander and General Paul Nakasone and described in Wired article, "The Man Who Speaks Softly--and Commands a Big Cyber Army," by Garrett M. Graff, published October 13, 2020. Graff describes the storyboards as "an illustrated guide to the complex challenges of cyberwar and how to meet them, drawing on an extended metaphor that involved a gated community."	12/31/20