U.S. CYBER COMMAND 2019 FOIA LOG

Case #	Requester Name	Request Description	Received
19-R030	Mustafa Musawwir	I am requesting (under the Freedom of Information Act) copies of all documents (and electronic documents) involving unicourt.com in any capacity whatsoever.	1/3/19
19-R031	Michael Martelle	I hereby request the following: The CONOPS submitted by USCYBERCOM to the Secretary of Defense regarding plans for retaliation against a foreign power in the case of interference in the 2018 US Election. At a minimum, we request all unclassified paragraphs in the CONOPS.	1/3/19
19-R032	Michael Martelle	I hereby request the following: An index of CONOPS submitted by USCYBERCOM to the Secretary of Defense for pre-approval during September or October of 2018.	1/3/19
19-R033	Charles Piller	This is a request under the Freedom of Information Act (FOIA), 5 U.S.C. § 552 for documents about research involving human subjects that is classified in whole or in part, funded and/or conducted by your department or by any department contractor or grantee, from Jan. 1, 2014 through Dec. 31, 2018. This request includes unclassified versions of the following documents, or, when necessary, documents with properly classified portions redacted. 1) Project lists. 2) Project summaries, progress reports, and final reports. 3) Contract and grant proposals and approvals. 4) Budgets (if separate from above documents). 5) Institutional Review Board (IRB) approval reports. 6) Any documents in the above categories for previously classified human subjects research projects that were declassified during the noted period.	1/9/19
19-R034	Mustafa Musawwir	The records I request can be described as follows: According to the following website, Adam Peter Lanza (of the Sandy Hook Elementary School shooting) possibly spent much time on the Internet in the days immediately prior to the event.URL: https://en.m.wikipedia.org/wiki/Sandy_Hook_Elementary_School_shooting#Perpetrator I would l ke to obtain an idea of what Adam Peter Lanza was doing on the Internet in that immediately prior timeframe. I am requesting (under the Freedom of Information Act) copies of all cyberspace records of Adam Peter Lanza.	1/12/19
19-R035	Travis Downing	I request that copies of the following documentation be provided to me: Information on the procedures for determining a given site is to be blocked. Information on the procedures for determining what “category” is assigned. A complete list of all sites blocked by CYBERCOM. Identification of what office makes the initial nomination for a site to be blocked. Identification of what office adjudicates and officially agrees with the blocking decision. Information on the evidence used to justify the label “hate-and-racism” for the site in question. Information on the evidence used to defend the site against the label of “hate-and-racism”. Documentation of the final deliberations for this label and block decision. Due process and contesting procedures that are in place for these determinations? Notification procedures for those being blocked.	1/15/19
19-R036	Michael Martelle	I hereby request the following: The order activating the Navy Cyber Warfare Development Group Reserve Unit, activated January 4 2019.	1/15/19
19-R037	Michael Martelle	I hereby request the following: Annex C Appendix 6 and Enclosure F (the references list) to OPORD 15-055.	2/13/19
19-R038	Russ Kick	I hereby request the following records: your agency's FOIA request log covering 2018, which includes a field showing the subject of each request and a field for the final disposition.	2/25/19
19-R039	Ken Klippenstein	This is a request under the Freedom of Information Act. I’d l ke to request records concerning the U.S. Cyber Command operation during the 2018 U.S. midterm elections to disrupt the Internet access of the Internet Research Agency — an infamous Russian troll factory.	2/26/19
19-R040	Michael Martelle	I hereby request the following records: Any after-action reports on operations targeting the Russian Internet Research Agency (IRA) around the 2018 midterm elections.	2/27/19
19-R041	Michael Martelle	I hereby request the following records: Each edition (believed to come out each fiscal year) of the TASKORD titled "Cyber Force Implementation Plan" and all associated attachments.	2/28/19

19-R042	Richard Diegel	I request a copy of the following product(s) be provided to me: 1. Unclassified documents pertaining to the initial formation of U.S. Cyber Command (HQDA EXORDs, DoD Directives, policy memos. etc). 2. Unclassified documents pertaining to the agent.btz cyber attacks from 2008-2009, including any cyber actor attribution. 3. Unclassified documents pertaining to the execution of Operation Buckshot Yankee. 4. Unclassified documents pertaining to Russian-attributed cyber attacks leading up to the 2016 presidential election and 20 18 mid-term elections. 5. Any other unclassified documents pertaining to Russian cyber activities directed against U.S. government entities.	3/10/19
19-R043	Michael Martelle	I hereby request the following: The CDR USCYBERCOM email Joint Force Headquarters Cyber (JFHQ-C) IOC FOC Criteria dated August 28, 2013.	3/19/19
19-R044	Michael Martelle	I hereby request the following: Attachment 1 of the Deputy Commander memorandum for Service Cyber Component Commanders Establishing Initial Operational Capability (IOC) Designation of Joint Force Headquarters - Cyber (JFHQ-C" issued September 30, 2013.)	3/19/19
19-R045	Michael Martelle	I hereby request the following: The draft of the Cyber Force Concept of Operations and Employment (CFCOE) Version 3.3 dated November 20, 2013.	3/19/19
19-R046	Michael Martelle	I hereby request the following: The Joint Information Environment (JIE) Operations concept of operations dated January 24, 2013.	3/19/19
19-R047	Michael Martelle	I hereby request the following: Attachment 2 to the "Current Operations Standard Operating Procedure" dated February 14, 2014.	3/19/19
19-R048	Michael Martelle	I hereby request the following: the draft Joint Force Headquarters DOD Information Network (JFHQ-DODIN) concept of operations (CONOPS) version 48, dated January 3, 2014.	3/19/19
19-R049	Michael Martelle	I hereby request the following: Any EXORDS and After Action Reports (AARs) related to USCYBERCOM's Exercise Cyber Lightning 2019.	3/19/19
19-R050	Michael Martelle	I hereby request the following: Joint Cyberspace Training and Certification Standards (JCT&CS) vl.2	4/10/19
19-R051	Michael Martelle	I hereby request the following: Any planning documents or after-action reviews (AARs) associated with the FY 2013 Cyber Guard 13-1 exercise/wargame.	5/1/19
19-R052	Michael Martelle	I hereby request the following: Any planning documents or after-action reviews (AARs) associated with the FY 2014 Cyber Guard 13-1 exercise/wargame.	5/1/19
19-R053	Michael Martelle	I hereby request the following: Any planning documents or after-action reviews (AARs) associated with the FY 2013 Cyber WarGame	5/1/19
19-R054	Michael Martelle	I hereby request the following: Any planning documents or after-action reviews (AARs) associated with the FY 2013 Cyber Knight 13-1 and 13-2 exercise/wargames	5/1/19
19-R055	Chad osselin	This request seeks any and all information related to: The websites/servers/domains brynn.io, chadg.io, and osasu.com. Complete reasons why my websites (those listed above) were visited by computers or systems related to the DoD. Information regarding Chad Gosselin (the owner of those websites and the author this request). In the event Chad Gosselin is/was not associated with those websites, any information that was obtained to learn more about persons of interest, targets, or subjects associated with the websites listed above. Whether Microsoft or an individual related to Microsoft contacted the DoD or its commands, subsidiaries, affiliates, third-parties, associates, contractors, businesses, or organizations to investigate a security concern on or about October 1, 2018 or October 2, 2018.	5/7/19
19-R056	Joseph Cox	I hereby request the following records: For CYBERCOM: 1. Any slides held by CYBERCOM that explain operation Synthetic Theology. Similar to those released for Operation Burnt Frost that give an overview of the operation. Reference: https://d3gn0r3afghep.cloudfront.net/foia_files/2015/09/28/FOIA_15-095_-_1st_Interim_Response_-_28_Sep_15.PDF 2. Operation Synthetic Theology rules of engagement (ROE). 3. Most recent execute order for operation Synthetic Theology.	5/10/19
19-R057	Chris Bing	I hereby request the following records: Planning documents, memos and/or reports descr bing the US Cyber Command effort in 2018 to counter Russian disinformation operations aimed at the 2018 U.S. midterm election. This effort in some documents will carry the codename: "Synthetic Theology." US Cyber Command Cyber Mission Force teams were central to the U.S. operation to disrupt a Russian government-linked organization, known as the "Internet Research Agency" (IRA), which is known to spread false and/or deceptive material online.	5/13/19

19-R058	Justine Wong	I am looking to incorporate the current gender demographic statistics for the DoD Cyber workforce, such as CYBERCOM, ARCYBER, AFCYBER, MARFORCYBER, Fleet Cyber. If retention rates by gender are also available, I would like to include them as well per each component. An aggregate number or percentage of males and females per each component and overall CYBERCOM for gender ratio and retention rates would suffice.	5/14/19
19-R059	Emma Best	I hereby request the following records: NSO Group Technologies AKA NSO Group, including communications (i.e. emails, memos, letters, etc.) to or from the organization, contracts, bids and invoices to or from the organization.	5/15/19
19-R060	Emma Best	I hereby request the following records: Records, reports, emails, memos and other documents mentioning or relating to the Network Crack Program Hacker Group, a Chinese hacker group based out of Zigong in Sichuan Province. iDefense linked the GinWui rootkit, developed by their leader Wicked Rose with attacks on the US Department of Defense in May and June 2006.	5/15/19
19-R061	Emma Best	I hereby request the following records: Records relating to or mentioning Hacking Team, including communications (i.e. emails, memos, letters, etc.) to or from the organization, contracts, bids and invoices to or from the organization, as well as any records relating to the 2015 hack of the organization, the subsequent release of their files and the republication of their emails on the WikiLeaks website.	5/15/19
19-R062	Emma Best	I hereby request the following records: Records, emails, memos and reports relating to or mentioning Bureau 121, a North Korean cyberwarfare agency, which is part of the Reconnaissance General Bureau of North Korea's military.	5/15/19
19-R063	Cian Heasley	I am looking for records or documents you may have on the "FloodNet" denial of service cyber attacks on what was then the main website of the US Department of Defense, defenselink.mil on or around September 1998.	5/25/19
19-R064	Zachary Beal	We are requesting information and activities concerning any investigation, and/or cause, and origin analysis by the Department of Defense concerning the June 27, 2017 Notpetya cyber-attack that impacted Mondelez International Inc., including, but not limited to communications and correspondence between the Department of Defense (and the departments below) and Mondelez International Inc., for the period of June 27, 2017 through July 1, 2018. The DOD departments include the Department of Defense U.S. Cyber Command.	6/19/19
19-R065	Kirsti Jespersen	E-mail and memoranda on the subject of U.S. Government or Department of Defense electronic traffic being mis-directed through non-FIVE EYES networks and data centers by the Border Gateway Protocol (BGP). Temporal scope of this request is from 1 January 2018 to 15 June 2019.	6/24/19
19-R066	(b) (6)	On January 17, 2019 after being referred for the position, I, (b) (6), SSN# (b) (6), was not selected for the Announcement: WTST193134175291 . I am trying to find out why was I not selected?	7/3/19
19-R067	Michael Martelle	I hereby request the following: The CONOPS for countering Russian malicious cyber actors (MCA) proposed by JCS and OSD Action Officers on or around November 30, 2015.	7/1/19
19-R068	Michael Martelle	I hereby request the following: All releasable portions of "The Russian Playbook".	7/1/19
19-R069	Michael Martelle	I hereby request the following: All materials prepared by USCYBERCOM for the Deputy Secretary of Defense Advanced Capability and Deterrence Panel.	7/1/19
19-R070	Michael Martelle	I hereby request the following: Any request for CYBERCOM support by EUCOM, or CONOPS for CYBERCOM support to EUCOM, between 2012 and 2018.	7/1/19
19-R071	Michael Martelle	I hereby request the following: Any materials prepared for, or as a product of, the August 2016 Cyber Summit hosted by the USCYBERCOM J5	7/1/19
19-R072	Michael Martelle	I hereby request the following: Any after action review materials resulting from the Baltic Ghost series of exercises.	7/1/19
19-R073	Chris Bing	I hereby request the following records: Planning documents, memos and/or reports descr bing US Cyber Command's private sector engagement effort known as "Pathfinder," which has helped "select critical infrastructure partners to share threat information, conduct collaborative analysis of vulnerabilities and threats, and mitigate those risks," according to past congressional testimony by Gen. Paul Nakasone. I am seeking emails and communications discussing partnerships between US Cyber Command and U.S. financial and energy firms.	7/16/19

19-R074	Chris Bing	I hereby request the following records: Planning documents, contracts, email communication, memos and/or reports describing US Cyber Command's "MAGETOWER" program. This program includes but is not limited to the Command's "Project VOLTRON" efforts -- which are happening in USCC J9 in coordination with Cyber National Mission Forces (CNMF) and DoD Defense Innovation Unit Experimental (DIUx). I am seeking information explaining the goal and purpose of MAGETOWER and Project Voltron, including details regarding program partners and related entities.	7/16/19
19-R075	Chris Bing	I hereby request the following records: Planning documents, contracts, email communication, memos and/or reports describing US Cyber Command's partnership with DreamPort, a technical innovation facility located in Columbia, MD. I am seeking information related to the Command's work with DreamPort to facilitate the development of technologies and as a manager of private sector engagements. DreamPort is a company led by Karl Gumtow.	7/16/19
19-R076	Nathan Tempey	I hereby request copies of the following records: All documents regarding modeling of "crowd control" and "SMS messaging" deployment generated pursuant to a contract with Deloitte Consulting LLP (W15QKN-17-D-0032) between July 1, 2013 and the present. Such documents should include but not be limited to the text of contracts with Deloitte for the services of its Advanced Analytics and Modeling team involving SMS technology, and any reports, proposals, presentations, data, or video or audio recordings generated in fulfillment of such contracts.	7/19/19
19-R077	Michael Martelle	I hereby request the following: Any materials, including but not limited to orders or briefings, regarding USCYBERCOM support to the NSA/CSS Cybersecurity Directorate.	7/26/19
19-R078	Joseph Cox	All slides, memos, briefs, instruction manuals, guidelines, related to CYBERCOM's use of VirusTotal, from 1st June 2018 to the present.	7/26/19
19-R079	Jonathan Heath	Unclassified and declassified reports and analysis of the Russian compatriot policy or cootechestvenn ki policy, specifically but not limited to any reports or products that analyze the policy as a whole, reports, publications or products that pertain to the policy as it pertains to the 2014 invasion of Ukraine by Russian Federation, reports, publications or products that pertain to the policy as it pertains to the Russian Federation's military invasion of South Ossetia; any analysis, reports, publications or products regarding the Russian compatriot policy or cootechestvenniki policy as it pertains to activities of the Russian Federation in the United States.	8/2/19

19-R080	Christopher Ayers	I hereby request that a copy of the following Documents and Communications, or Documents and Communications containing the following information, be made available to me: 1.From January 1, 201 7 to date, all Documents and Communications related to Intel or Intel's CPUs, including, but not limited to, documents and communications related to any investigation(s), evaluation, or assessment of any actual, alleged, or suspected Defect or potential Defect. 2.From January 1, 2017 to date, all Documents and communications related to Meltdown, Foreshadow, Spectre, Fallout, RIDL, ZombieLoad, or other Side Channel Attack related to or directed at any Defect in Intel's CPUs. 3.From January 1, 2017 to date, all Documents and Communications related to any data breach attendant to Meltdown, Foreshadow, Spectre, Fallout, RIDL, ZombieLoad, or other Side Channel Attack related to or directed at any Defect in Intel's CPUs, whether in testing/simulation or in a live user setting, including, but not limited to, any report(s), assessments, and the like. 4.From January 1, 2017 to date, all Documents and Communications relating to the design, development, testing, or other consideration of any actual or contemplated fix, repair, mitigation, remedial measure, or means of redressing, in whole or part, (a) Meltdown, Foreshadow, Spectre, Fallout, RIDL, ZombieLoad, or other Side Channel Attack related to or directed at any Defect in Intel's CPUs or (b) any actual, alleged, or suspected Defect in Intel's CPUs. 5. From January 1, 201 7 to date, all Documents and Communications related to Google, Apple, Microsoft, Amazon, AMD, ARM, Linux, and other industry-leading companies that studied any Defect or Side Channel Attack including Meltdown, Foreshadow, Spectre, Fallout, RIDL, ZombieLoad, or other Side Channel Attack related to or directed at any Defect in Intel's CPUs, and/ or collaborated on the development of mitigations of the any actual, alleged, or suspected Defect potential Defect or risk of Side Channel Attacks. 6.From January 1, 2017 to date, all Documents and communications related to the performance impact of Intel's CPUs or AMD' s CPUs relating to mitigation of any Defect and risks of Side Channel Attacks, including, but not limited to: a. All benchmarking tests for performance impact of mitigation devices, patches, and software updates to address Meltdown, Foreshadow, Spectre, Fallout, RIDL, ZombieLoad, or other Side Channel Attack related to or directed at any Defect in Intel's CPUs; b.The impact of mitigation devices, patches, and software updates on the performance of Intel's or AMD's CPUs, including the interoperability of software programs; and c. The strengths, weaknesses, and efficacy of mitigation devices, patches, and software updates with respect to mitigating security risks to Intel's or AMD's CPUs.7.Documents and communications relating to the development, design, or engineering of any of Intel's CPUs (or any actual or potential modifications), including, but not limited to: a.Copies of the microarchitecture specifications (MAS) and each redbook related to any CPU; and b.Each version of register-transfer language (RTL) code or hardware description language (HDL) code, such as Verilog HDL, VHSIC HDL, or Intel internal HDL, used to model, synthesize or construct any CPU.	8/2/19
19-R081	Michael Martelle	I hereby request the following: Any documents related to an operation producing effects on a network used by the Iranian Revolutionary Guard Corps on June 20, 2019 including but not limited to: - Concept of Operations (CONOP) - Execute/Operation Order (EXORD/OPORD) - Joint Tactical Cyber Request (JTCR) - Cyberspace Effects Request Form (CERF) - Cyber Operations Directive (CYOD) - Master Cyber Operations Plan (MCOP) - Integrated Tasking Order (ITOJ - Cyber Control Order (CCO) - Cyberspace Strike Package - Target Validation	8/28/19
19-R082	Michael Martelle	I hereby request the following: Any documents related to USCYBERCOM support to Operation Sentinel.	8/28/19
19-R083	Akhil Acharya	I would l ke any and all information available regarding the DoD Cyber Command use of the 757-200 aircraft registered to "COMCO". These aircraft are noted by their registration codes: - N610G - N226G	9/9/19
19-R084	Michael Martelle	I hereby request the following: Any after-action or progress reports, or updates, relating to Join Task Force ARES or Operation Glowing Symphony.	9/16/19
19-R085	Jurre van Bergen	I hereby request the following records: Records relating to or mentioning Finfisher and/or Gamma Group, including communications (i.e. emails, memos, letters, etc.) to or from the organization, contracts, bids and invoices to or from the organization, as well as any records relating to the 2014 hack of the FinFisher organization, the subsequent release of their files and the republication of the hack on the WikiLeaks website as 'spyfiles4'.	9/25/19
19-R086	Jurre van Bergen	I hereby request the following records: Any talking points considering reports of Reuters news articles about Cyberpoint LLC a firm in Baltimore, MA, Dark Matter, a firm in the United Arab Emirates and the Kingdom of the United Arab Emirates as well as NESA, National Electronic Security Authority, of the year 2019.	9/25/19

19-R087	Jurre van Bergen	I hereby request the following records: Planning documents, contracts, email communication, memos and/or reports describing Dark Matter's collaboration with NESA and/or Cyberpoint LLC collaboration with NESA in the UAE. I'm specifically looking for documents in the year of 2014. I'd also like to request any e-mail correspondence, memo's, contracts and reports in 2014 between Cyberpoint LLC. If this is too voluminous, i'd like to focus on the first half year of 2014.I am seeking information explaining the goal and purpose of the collaboration between Cyberpoint LLC and Dark Matter collaboration with NESA in the United Arab Emirates and what the role of the United States is.	9/25/19
19-R088	Jurre van Bergen	I would l ke to request any notes, ta king points, memo's, e-mails or any other documents about a meeting of Gen. Paul M. Nakasone with the President where Iran and cyber was the scope of the discussion. I would assume this discussion took place in either August or September of 2019.	9/25/19
19-R089	Alexander Budzyn	The role of Alexander Budzyn in the defense of the USA cyberspace.	9/25/19
20-R001	Eric Levai	Documents related to W kistrat, the private intelligence firm, including, but not limited to, simulations, war games, analysis, etc.	10/05/19
20-R002	David Fowler	Request current organization charts, including both directorates, and component commands, sub-unified commands, joint task forces, etc.	10/15/19
20-R003	Michael Martelle	I hereby request the following: Any documents related to an operation producing effects on Iranian communications/propaganda capabilities beginning September 14, 2019 including but not limited to: Concept of Operations, (CONOP), Execute/Operation Order (EXORD/OPORD), Joint Tactical Cyber Request (JTCR), Cyberspace Effects Request Form (CERF), Cyber Operations Directive (CYOD), Master Cyber Operations Plan (MCOP), Integrated Tasking Order (ITO), Cyber Control Order (CCO), Cyberspace Strike Package, Target Validation	10/16/19
20-R004	Har krishnan Gokul	I am contacting you in order to look for information on the topic we are debating "Resolved: The Benefits of the United States Federal Government's Use of Offensive Cyber Operations Outweigh the Harm" in my research on this topic I came across an operation conducted by JTF Ares called Operation Glowing Symphony. I was wondering if you could point me towards some declassified information or articles regarding Operation Glowing Symphony and its effects.	10/19/19
20-R005	Andrew Davis	Any and all documents or files referencing myself, Andrew Watson Davis, from 1990 to 1999	11/20/19
20-R006	Michael Martelle	I hereby request the following: The Trilateral Memorandum of Agreement among the DOD, DOJ and Intelligence Community Regarding Computer Network Attack (CNA) and Computer Network Exploitation (CNE) dated May, 2007.	11/20/19
20-R007	Michael Martelle	I hereby request the following: Any documents related to the Cyber Offensive and Defensive Exercises (CODE) conducted in November 2019.	11/06/19
20-R008	Shannon Vavra	I request that the following be provided to me: a copy of records, including but not limited to documents, briefings, reports, cables, operations, guidance, and orders, mentioning "EternalDarkness," "Eternal Darkness,'"ETERNALDARKNESS' "ETERNAL DARKNESS" or other aliases and names meant to encompass EternalDarkness, including but not limited to those related to advanced component development and prototypes, cyber operations technology development, operation and maintenance, and Air Force operating forces	11/22/19
20-R009	Shannon Vavra	I request that the following be provided to me: a copy of records, including but not limited to documents, briefings, reports, cables, operations, guidance, and orders, mentioning "Hunt Forward" and or the Cyber National Mission Force Mobile & Modular Hunt Forward Kit.	11/22/19
20-R010	Shannon Vavra	I request that the following be provided to me: a copy of records, including but not limited to documents, briefings, reports, cables, operations, guidance, and orders, mentioning 333 packages including but not limited to the related security cooperation, education, training, cyber infrastructure, military to military support, and travel.	12/10/19

20-R011	Muira McCammon	The records I request include, but are not limited to: 1. Records of all tweets deleted by the Twitter handle associated with U.S. Cyber Command (@US_CYBERCOM), including: a. Any tweets that were published on Twitter and subsequently deleted for any reason; and b. Any tweets published by other accounts that were retweeted by @US_CYBERCOM and subsequently deleted for any reason. 2. Records of all tweets that have been kept in draft form beyond their expected date and time of publication, on Twitter or in a third-party social media management platform, for any reason. 3. Records related to the drafting or deletion of tweets, including: a. Any correspondence or record of correspondence regarding the drafting or deletion of specific tweets i. including correspondence sent through official government email addresses or messaging services; and ii. including correspondence sent through private third-party services such as Gmail or Slack; and iii. Including any messages, notes, or annotations created on a third-party social media management platform. b. Documentation of the agency's existing policy regarding the preservation and maintenance of tweets as per the Federal Records Act, and Federal Records Management Bulletin 2014-02 (available at https://www.archives.gov/records-mgmt/bulletins/2014/2014-02.htm), which stated that "social media content may be a Federal record when the use of social media provides added functionality, such as enhanced searchability, opportunities for public comment, or other collaboration… A complete Federal record must have content, context, and structure along with associated metadata (e.g., author, date of creation). The complete record must be maintained to ensure reliability and authenticity." c. Any briefings, reports, memoranda, legal opinions, policy statements, or ta king points used or disseminated within the Agency regarding the drafting or deletion of tweets.	12/10/19
20-R012	Tully Rinckey	This firm represents Mr. (b) (6) A signed power of attorney authorizing us to act on his behalf in this Privacy Act request is attached. Our client requests a copy of records indexed to his name, to include but not limited to copies of documents used to support the basis of denial. His request includes – but is not limited to – reports of investigation; results of database records checks; statements obtained by investigators from people who know him; and, internal correspondence about him case.	12/13/19
20-R013	(b) (6)	I would l ke a copy of my report that was submitted to (b) (3) during the J83 Command Investigation which began on 10/15/19 and which I was a participating witness. I have attached her email regarding the Interview appointment. I would also like a copy of the full investigation to assist me in my ongoing pursuit to find relief which involves currently seeking a reasonable accommodation and my doctor needs a copy to help with her diagnosis to what I have been subjected to since being employed since July 2018 and to the extent of my timeline of information.	12/17/19
20-R014	(b) (6)	I request a copy of the following product(s) be provided to me: Copy of: USCYBERCOM IG and/or other investigation report of disparate treatment/harassment/retaliation of myself, (b) (6) (investigation regarding retaliation against me). Investigation was between May- August 2019, regarding my employment in the J3, Operations Directorate.	12/20/19
20-R015	(b) (6)	I would l ke my emails in regards to the ONI and taking off for a day. I let me manager know and the Admin office and they made me change my time card to vacation time. This was a USERRA violation and I would l ke those emails to start.	12/23/19