DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD Suite 6171
FORT GEORGE G. MEADE, MARYLAND 20755

SEP 18 2018

Mr. Malcolm Byrne
The National Security Archive
Gelman Library, Suite 701
2130 H. Street, N.W.
Washington D.C. 20037

Dear Mr. Byrne,

Thank you for your May 29, 2018 Freedom of Information Act request. U.S. Strategic Command (USSTRATCOM) referred you request to U.S. Cyber Command (USCYBERCOM) on May 31, 2018 for processing. After carefully reviewing the enclosed document, I have also determined certain portions no longer meet the classification criteria of E.O. 13526, Section 1.4. As such I have declassified those portions. However, there are portions I am withholding.

As the Initial Denial Authority, I am partially denying portions of the document. The denied information is currently and properly classified in the interest of national defense or foreign policy according to Executive Order 13526, *Classified National Security Information,* Section 1.4(a). I am also denying the release of certain UNCLASSIFIED portions as they meet the standards for classification pursuant to Executive Order 13526, Section 1.7.(e). Specifically, when these UNCLASSIFIED portions are combined, they reveal an additional association or relationship that: 1) meets the standards for classification under Executive Order 13526; and 2) are not otherwise revealed in the individual items of information. I am also denying access to the names and associated individual identifying information of USCYBERCOM and USSTRATCOM personnel. Lastly, I am denying access to certain unclassified information as release could pose a risk of harm to either U.S. Government personnel and/or operations.

In accordance with 5 U.S.C. § 552, Freedom of Information Act, Exemptions 1 and 3, are hereby invoked, and require this information be withheld. The Exemption 3 Federal statute invoked is 10 U.S.C. § 130b, *Personally Identifying Information Regarding Personnel Assigned to an Overseas, Sensitive, or Routinely Deployable Unit*. USCYBERCOM was designated a sensitive unit on 15 January 2015.

If you are not satisfied with this action, you may appeal this response to the appellate authority, Ms. Joo Chung, Director of Oversight and Compliance, Office of the Secretary of Defense. The appellate address is: ODCMO, Director of Oversight and Compliance, 4800 Mark Center Drive ATTN: DPCLTD, FOIA Appeals, Mailbox #24, Alexandria VA 22350-1700. As an alternative, you may use the OSD FOIA request portal at http://pal.whs.mil/palMain.aspx; or e-mail your appeal to OSD.FOIA-APPEAL@mail.mil. Your appeal should be submitted within 90 calendar

days of this letter and cite case number 18-R006, and be clearly marked "Freedom of Information Act Appeal."

Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at (202) 741-5770; toll free at 1-977-684-6448; or facsimile at (202) 741-5769.

Sincerely,

ROSS A. MYERS
Rear Admiral, U.S. Navy
Chief of Staff

DTG 171657Z AUG 15
FROM: USCYBERCOM FT GEORGE G MEADE MD

TO: COMFLTCYBERCOM FT GEORGE G MEADE MD
COMNAVIDFOR SUFFOLK VA
NAVNETWARCOM SUFFOLK VA
NAVCYBERDEFOPSCOM SUFFOLK VA
CDRUSACYBER FT BELVOIR VA
CDRUSACYBER G3 FT BELVOIR VA
CDRUSACYBER G33 FT BELVOIR VA
ARMY FORCES CYBER CMD PETERSON AFB CO
ARMY GNOSC FT BELVOIR VA
MARFORCYBERCOM FT MEADE MD
MCNOSC QUANTICO VA
24AF LACKLAND AFB TX
DISA FT GEORGE G MEADE MD
DIRNSA FT GEORGE G MEADE MD
NSA FT GEORGE G MEADE MD
NSACSS FT GEORGE G MEADE MD
JFHQ DODIN FT GEORGE G MEADE MD
USCYBERCOM CNMF FT GEORGE G MEADE MD

INFO: CDR USSTRATCOM OFFUTT AFB NE
HQ USSTRATCOM OFFUTT AFB NE
USSTRATCOM COMMAND CENTER OFFUTT AFB NE
NCR STRATCOM OFFUTT AFB NE
USCYBERCOM FT GEORGE G MEADE MD

~~SECRET//REL TO USA, FVEY~~

SUBJECT: (U) USCYBERCOM TASKORD 15-0124 ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2015 AND FY 2016

MSGID/ORDER/USCYBERCOM/15-0124 /ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2015 AND FY 2016 /TASKORD/(S//REL TO USA, FVEY)//

REF/A/DOC/(U//~~FOUO~~) DMAG DECISION-COA1B FULL GROWTH (S//REL TO USA, FVEY)/DMAG/11DEC2012/-//

REF/B/DOC/(U//~~FOUO~~) CYBER FORCE CONCEPT OF OPERATIONS & EMPLOYMENT (CFCOE) (S//REL TO USA, FVEY)/USCYBERCOM/22JUL2014/V.4.1//

REF/C/EXORD/(U//~~FOUO~~) CJCS EXECUTE ORDER TO IMPLEMENT CYBERSPACE OPERATIONS COMMAND AND CONTROL (C2) FRAMEWORK (S//REL TO USA, FVEY)/ CJCS/212105ZJUN13/-//

REF/D/TASKORD/(U//~~FOUO~~) ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2013 (S//REL TO USA, FVEY)/USCYBERCOM/060852ZMAR13/13-0244//

REF/E/FRAGORD/(U//~~FOUO~~) FRAGORD 01 TO TASKORD 13-0244 ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2013 (S//REL TO USA, FVEY)/USCYBERCOM/132004ZMAY13 /13-0244/

REF/F/DOC/(U//~~FOUO~~) DCDR MEMORANDUM FOR SERVICE CYBER COMPONENT COMMANDERS ESTABLISHING INITIAL OPERATIONAL CAPABILITY (IOC) DESIGNATION OF JOINT FORCE HEADQUARTERS – CYBER (JFHQ-C) (U//FOUO)/USCYBERCOM/30SEP13/-//

REF/G/DOC/(U//~~FOUO~~) CRYPTOLOGIC INTELLIGENCE OVERSIGHT IMPLEMENTATION PLAN (S//REL TO USA, FVEY)/USCYBERCOM/13JUN13/-//

REF/H/DOC/(U//~~FOUO~~) CYBER COMPONENTS COMMANDER CONFERENCE (TS//REL TO USA, FVEY)/USCYBERCOM/22OCT13/-//

REF/I/TASKORD/(U//~~FOUO~~) ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2014 (S//REL TO USA,FVEY)/USCYBERCOM /110044ZOCT13/13-0747//

REF/J/DOC/(U//~~FOUO~~) MEMORANDUM FOR J3, UNITED STATES CYBER COMMAND, REGARDING FINAL LOCATION (b)(1) Sec 1.7(e) AT NSA-WASHINGTON (NSAW) (U//FOUO)/UNITED STATES ARMY CYBER COMMAND/06FEB2014/-//

REF/K/DOC/(U//~~FOUO~~) DEPUTY COMMANDER FLEET CYBER COMMAND EMAIL TO USCYBERCOM J3, SUBJECT: (U) MODIFICATION TO THE CYBER FORCES PLANNING MODEL; GO/FO COORD (U//FOUO)/USCYBERCOM//09FEB2014/-//

REF/L/DOC/(U//~~FOUO~~) JFHQ-C CERTIFICATION SLIDE PRESENTATION/USCYBERCOM/ (TS//REL TO USA, FVEY)/USCYBERCOM/03OCT2013/-//

REF/M/FRAGORD/(U//~~FOUO~~) FRAGORD 06 TO TASKORD 13-0747 ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2014/(S//REL TO USA, FVEY)/USCYBERCOM/092250ZMAR15/13-0747//

REF/N/FRAGORD/(U//~~FOUO~~) FRAGORD 05 TO TASKORD 13-0747 ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2014/(S//REL TO USA, FVEY)/USCYBERCOM/250033ZJUN14/13-0747//

REF/O/FRAGORD/(U//~~FOUO~~) FRAGORD 04 TO TASKORD 13-0747 ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2014/(S//REL TO USA, FVEY)/USCYBERCOM/050103ZJUN14/13-0747//

REF/P/FRAGORD/(U//~~FOUO~~) FRAGORD 03 TO TASKORD 13-0747 ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2014/(S//REL TO USA, FVEY)/USCYBERCOM/310329ZMAY14/13-0747//

REF/Q/FRAGORD/(U//~~FOUO~~) FRAGORD 02 TO TASKORD 13-0747 ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2014/(S//REL TO USA, FVEY)/USCYBERCOM/291429ZJAN14/13-0747//

REF/R/FRAGORD/(U//~~FOUO~~) FRAGORD 01 TO TASKORD 13-0747 ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2014/(S//REL TO USA, FVEY)/USCYBERCOM/311009ZOCT13/13-0747//

REF/S/TASKORD/(U//~~FOUO~~) ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS IN FISCAL YEAR (FY) 2014/(S//REL TO USA, FVEY)/USCYBERCOM/ 110044ZOCT13/13-0747//

REF/T/DOC/(U//~~FOUO~~) USSTRATCOM READINESS REPORTING AND ASSESSMENTS (UNCLASSIFIED)/USSTRATCOM/19 MARCH 2012/-//

REF/U/EXORD/(U//~~FOUO~~) MOD 1 TO CJCS EXECUTE ORDER TO IMPLEMENT CYBERSPACE OPERATIONS COMMAND AND CONTROL (C2) FRAMEWORK (S//REL TO USA, FVEY)/CJCS/212105ZJUN13/-//

REF/V/DOC/(U//~~FOUO~~) CYBER MISSION FORCE (CMF) TEAM FULL OPERATIONAL CAPABILITY (FOC) APPROVAL AND CERTIFICATION PROCESS (U//FOUO)/ USCYBERCOM/ 09 APRIL 2015/-//

REF/W/TASKORD/(U//~~FOUO~~) USCYBERCOM OPERATIONAL PROCESSES (U//FOUO)/ USCYBERCOM/131033ZMAR14/14-0061//

REF/X/DOC/(U//~~FOUO~~) ENCLOSURE 1 TO TASKORD 15-0124 (S//REL USA, FVEY)/ USCYBERCOM/-/-//

REF/Y/DOC/(U//~~FOUO~~) ENCLOSURE 2 TO TASKORD 15-0124 (S//REL USA, FVEY)/ USCYBERCOM/-/-//

REF/Z/DOC/(U//~~FOUO~~) ENCLOSURE 3 TO TASKORD 15-0124 (S//REL USA, FVEY)/ USCYBERCOM/-/-//

ORDTYPE/TASKORD/USCYBERCOM//

TIMEZONE/Z//

NARR/ (U//~~FOUO~~) THIS ORDER TASKS SERVICE CYBER COMPONENTS TO EXECUTE BUILDING THE CMF TEAMS WITHIN FY15 AND FY16.//

GENTEXT/SITUATION/1.

1.A. (~~S//REL TO USA, FVEY~~) USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department Of Defense Information Networks (DODIN) and; prepare to, and when directed, conduct full spectrum military Cyberspace Operations (CO) in order to (IOT) enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries. USCYBERCOM accomplishes this mission through 1) Deter or defeat strategic threats to US interests and infrastructure; 2) Ensure DOD mission assurance; and 3) Achieve Joint Force Commander objectives mission areas. The Chairman of the Joint Chiefs of Staff has validated (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) The Joint Staff, Armed Services, and USCYBERCOM and its components are working to establish (b)(1) Sec 1.4(a) rapidly in accordance with (IAW) the Deputy Management Action Group (DMAG) approved plan, ref A, IOT mitigate operational risk.

1.B. (U) GENERAL.

1.B.1. ~~(S//REL TO USA, FVEY)~~ USCYBERCOM continues to work with the Services, Combatant Commands (CCMDs), the National Security Agency/Central Security Service (NSA/CSS), Service Cyber Components (SCC), The Defense Information Systems Agency (DISA), Joint Force Headquarters-Cyber (JFHQ-C), Cyber National Mission Force Headquarters (CNMF-HQ), and Joint Forces Headquarters DODIN (JFHQ-DODIN) to coordinate (b)(1) Sec 1.4(a) in support of (ISO) operational priorities. This TASKORD is subject to modification at the discretion of the Commander, USCYBERCOM (CDRUSCYBERCOM).

1.B.2. (U//~~FOUO~~) ADVERSARY FORCES. Worldwide threats, ranging from criminal elements to Non-State and Nation-State Actors seek persistent access to Department Of Defense (DOD) information systems and United States Critical Infrastructure and Key Resources (CIKR) for, diplomatic, informational, military, and economic advantage. Adversaries have the capability to remotely penetrate access-controlled U.S. information systems and networks, and they actively conduct cyberspace Intelligence, Surveillance, and Reconnaissance (ISR) actions ISO their interests. A few nations possess advanced capabilities for insider or close-access cyberspace operations (CO), as well as operations targeting supply chains and industrial control systems.

1.C. (U) FRIENDLY FORCES.

1.C.1. (U//~~FOUO~~) Departments of the Army, Navy, Marine Corps, and Air Force support building of FY15 and FY16 CMF teams and allocating resources, through support agreements if necessary, to ensure teams are organized, trained, equipped, and employed to meet Initial Operational Capability (IOC) requirements. Commanders are expected to man the formations (b)(1) Sec 1.7(e) and to take maximum advantage of available training resources.

1.C.2. (U//~~FOUO~~) Geographical and functional CCMD support efforts to assign missions, identify critical assets and develop targets and Cyber Key Terrain. As required, CCMDs coordinate with USCYBERCOM, NSA or supporting JFHQ-C or JFHQ-DODIN accordingly.

1.C.3. (U) ADJACENT.

1.C.3.A. (U//~~FOUO~~) (b)(1) Sec 1.7(e) on CMF teams at an appropriate time and provides additional direct support personnel, infrastructure, mission support, and mission alignment support for CMF teams.

1.C.4. (U//~~FOUO~~) SUBORDINATE.

1.C.4.A. (U//~~FOUO~~) SCCs providing units to build FY15 and FY16 teams with Operational Readiness reported by CNMF-HQ, JFHQ-Cs, and JFHQ-DODIN ISO the tasks and mission objectives outlined in this TASKORD.

1.C.4.B. ~~(S//REL TO USA, FVEY)~~ Cyber National Mission Forces (CNMF) teams are operationally aligned under the CNMF-HQ and conduct CO (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

1.C.4.C. (U//~~FOUO~~) Cyber Combat Mission Force (CCMF). CCMF teams are operationally aligned under JFHQ-C. SCCs established the four JFHQ-C to provide support to the CCMDs. USCYBERCOM continues to

support CCMDS with cyber planning via the Cyber Support Elements (CSE) and liaison officers and In Coordination With (ICW) their respective JFHQ-C, CSE/LNO, and CCMF support designed CCMD plans. 1.C.4.D. ~~(S//REL TO USA, FVEY)~~ Cyber Protection Force (CPF). The CPF supports the second mission area – secure, operate, and defend the DODIN. The CPF are organized into four types of CPTs (CCMD, National, Service, DODIN) that are operationally aligned with a CCMD, CNMF-HQ, SCC or JFHQ-DODIN. Each CPT is comprised of five squads: Mission Protection, Discovery and Counter Infiltration, Cyber Threat Emulation, Cyber Readiness, and Cyber Support. When required and authorized, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

GENTEXT/MISSION/2. (U//~~FOUO~~) USCYBERCOM coordinates Cyber Mission Force (CMF) generation IOT organize, train, equip, and employ FY15 and FY16 CMF teams ISO USCYBERCOM mission areas; 1) Deter or defeat strategic threats to US interests and infrastructure; 2) Ensure DOD mission assurance; and 3) Achieve Joint Force Commander objectives.//

GENTEXT/EXECUTION/3.

3.A. (U) CONCEPT OF OPERATIONS.

3.A.1. (U) COMMANDER'S INTENT.

3.A.1.A. ~~(S//REL TO USA, FVEY)~~ PURPOSE. To provide an established, capable CMF as expeditiously as possible to conduct full-spectrum cyberspace operations in all three mission areas against increasing threats to our nation's critical infrastructure and DoD networks. The CMF will be (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to, offensive and defensive cyberspace operations.

3.A.1.B. ~~(S//REL TO USA, FVEY)~~ METHOD. Continued expansion of operational capability in FY15 and FY16 in order to build a combat-ready CMF, positioned in the best locations for mission success and with a Command and Control (C2) structure in place to successfully direct operations. To accomplish this, 34 CMF teams in FY15 and 28 CMF teams in FY16 will be built. Throughout this build process, SCC commanders creatively and aggressively establish the maximum operational capability (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) the end-state force model will be kept in mind and incrementally used to annually increase our forces until completion. SCCs will conduct continuous and close coordination with their service headquarters and all USCYBERCOM directorates throughout the build process.

3.A.1.C. (U//~~FOUO~~) END STATE. 34 FY15 and 28 FY16 CMF teams are organized, trained, and equipped for employment ISO USCYBERCOM mission areas: 1) Deter or defeat strategic threats to US interests and infrastructure; 2) Ensure DOD mission assurance; and 3) Achieve Joint Force Commander objectives.

3.A.2. (U) KEY TASKS.

3.A.2.A. (U//~~FOUO~~) SCCs work with USCYBERCOM and their service headquarters to accomplish the following:

3.A.2.A.1. (U//~~FOUO~~) By 30 September 2015, the objective is to organize, train, and equip 34 CMF teams assigned for FY15 to IOC.
3.A.2.A.2. (U//~~FOUO~~) By 30 September 2016, the objective is to organize, train, and equip 28 CMF teams assigned for FY16 to IOC.

3.A.2.A.3. (U//~~FOUO~~) NLT 15 days from release date of this TASKORD, provide the IOC and FOC projection dates for all FY15 and FY16 teams and FOC projection dates for all FY13 and FY14 teams that have not been declared FOC. Provide projections to CMF coordination element Points of Contact (POC) listed in section 5.D.1.

3.B. (U) TASKS.

3.B.1. (U) USCYBERCOM DIRECTORATES.

3.B.1.A. (U) J2.

3. B.1.A.1. (U//~~FOUO~~) ICW USCYBERCOM/J3 and the CNMF-HQ determine through mission analysis a prioritized list of operational targets for alignment to CNMF teams.

3.B.1.A.2. (U//~~FOUO~~) Build out the CMF IAW the established (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Cyber Mission Forces that require (b)(1) Sec 1.7(e) MOAs are currently signed and in effect for the CNMF, CCMF and the CPF.

3.B.1.B. (U) J3.

3.B.1.B.1. (U//~~FOUO~~) Track IOC and FOC team build progress for all CMF teams through FY16, to include personnel, training, space (facilities and workspaces), and mission. (POC: J338, DL_USCC_J338@NSA.IC.GOV)

3.C.1.B.2. (U//~~FOUO~~) Coordinate with J6 for threshold and objective CEE requirements NLT 01 October 2015.

3.B.1.B.3. (U//~~FOUO~~) Assess the ability of CMF to satisfy operational contingency plan requirements.

3.B.1.C. (U//~~FOUO~~) J4. ICW CCMD/J4, NSA/CSS Installation and Logistics Directorate, SCCs, and DISA determine solutions for facilities and seating for CMF teams and JFHQ-C Staff that (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) 30 September 2015. (POC (b)(3) @nsa.ic.gov)

3.B.1.D. (U) J5.

3.B.1.D.1. (U//~~FOUO~~) Provide cyberspace operations strategy, policy, and doctrinal guidance ISO the CMF build.

3.B.1.D.1.A. (U//~~FOUO~~) Work ICW higher headquarters to prioritize change-recommendations and advocate policy modifications required to improve CMF capabilities.

3.B.1.D.2. (U/~~FOUO~~) Conduct deliberate planning ISO HHQ and other GCC planning efforts that provide strategic guidance and an operational framework for the CMF IOT achieve US military objectives in and through cyberspace.
3.B.1.D.3. (U/~~FOUO~~) Work ICW USCYBERCOM J3, HQ-CNMF, and JFHQ-Cs, and JFHQ-DODIN IOT develop command policies that provide direction and guidance for reoccurring operational support and sustainment activities and ensure proper alignment with DoD cyberspace policy framework.

3.B.1.D.4. (U/~~FOUO~~) Provide partnership guidance to inform CMF capabilities development IAW contingency plan priorities.

3.B.1.D.4.A. (U/~~FOUO~~) Work ICW NSA/CSS corporate policy stakeholders IOT develop command policies and deconflict any CMF issues that have an adverse impact on NSA/CSS equities.

3.B.1.E. (U) J6.

3.B.1.E.1. (~~S//REL TO USA, FVEY~~) ICW J4, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) determine combat support requirements to support mission objectives (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

3.B.1.E.2. (U//~~FOUO~~) ICW J3, and NLT 30 September 2015, identify, plan/design and implement future combat support solutions to allow for full-spectrum CO for CMF teams and JFHQ-C.

3.B.1.E.3. (U//~~FOUO~~) ICW SCCs develop requirements that entail (b)(1) Sec 1.7(e) implementation.

3.B.1.F. (U//~~FOUO~~) J7. ICW NSA/CSS, SCCs, JFHQ-DODIN, CNMF-HQ, and DISA determine solutions for training (b)(1) Sec 1.7(e) FY15 and FY16 teams. As part of this effort, develop and promulgate a formal process that enables SCCs to anticipate training schedules and seat availability IOT inform CMF team build (POC (b)(3) @nsa.ic.gov).

3.B.2. SERVICE CYBER COMPONENTS. Execute team build as outlined in Enclosure 1 to this order.

3.B.2.E. (U) REQUEST FOR SUPPORT.

3.B.2.E.1. (U) NATIONAL SECURITY AGENCY (NSA) / CENTRAL SECURITY SERVICE (CSS).

3.B.2.E.1.A. (U//~~FOUO~~) Request NSA/CSS continue planning to support CMF build-out to include delegation of SIGINT mission authority to appropriate CMF elements IAW ref C.

3.B.2.E.1.B. (U//~~FOUO~~) Request NSA/CSS coordinate with USCYBERCOM J4 to determine solutions for facilities and seating for CMF teams and JFHQ-C staff planned to (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) NLT 30 September 2015 (POC (b)(3) @nsa.ic.gov)

3.B.2.E.1.C. (U//~~FOUO~~) Request NSA/CSS coordinate with USCYBERCOM J6 to determine interim and long term solutions for information technology (b)(1) Sec 1.7(e) for CMF teams planned to (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) as appropriate. Interim solutions, to include insight regarding (b)(1) Sec 1.7(e) plans for National CPTS, due NLT 01 September 2015. Long term solutions due NLT 30 September 2015.

3.B.2.E.2. (U) DEFENSE INFORMATION SYSTEMS AGENCY (DISA).
3.B.2.E.2.A. (U//~~FOUO~~) Conduct analysis to determine infrastructure and workspace requirements necessary to support DODIN CPTs.

3.B.2.E.2.B. (U//~~FOUO~~) Request DISA assign workspace to meet CPT requirements. Additionally, develop MOAs and support agreements with the SCCs to cover the cost of CPT employment (e.g., stationing CPTs at Enterprise Operation Centers reduces TDY costs.)

3.C. (U) COORDINATING INSTRUCTIONS.

3.C.1. (U) DIRLAUTH for SCCs, CNMF HQ, JFHQ-C, JFHQ-DODIN, and DISA with supported commands to coordinate the location and positioning of CMF teams for planning purposes.

3.C.1.A. (U//~~FOUO~~) Coordinate with supported CCMDs to determine CMT mission alignment and optimal location of CCMD CPTS.

3.C.1.B. (U//~~FOUO~~) Assist USCYBERCOM J3/J4/J6/J8/J9 with coordination at (b)(1) Sec 1.7(e) centers to determine facility, workspace and combat mission support requirements for each team; conduct analysis of available resources and identify gaps to USCYBERCOM J4 NLT 30 September 2015.

3.C.1.C. ~~(S//REL TO USA, FVEY)~~ Identify Special Technical Operations (STO) and Special Access Programs (SAPs) requirements and (b)(1) Sec 1.4(a)

3.C.1.C.1. ~~(S//REL TO USA, FVEY)~~ Conduct analysis to determine potential manning issues and provide proposed STO billet structures for all respective teams to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) costs associated with the increase in manning, and costs associated with increased infrastructure requirements.

3.C.1.C.2. (U//~~FOUO~~) As necessary, and when critical to mission accomplishment, identify (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) the CMF teams to USCYBERCOM J39. This should include (b)(1) Sec 1.7(e) security paperwork necessary to enable support from the USCYBERCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e). (POC (b)(3) @nsa.ic.gov)

3.C.1.D. (U//~~FOUO~~) Provide feedback on plans, policy, doctrinal, and partnership issues to USCYBERCOM J5.

3.C.1.E. (U//~~FOUO~~) TEAM READINESS REPORTING REQUIREMENTS . SCC designated POCs or Team Leads provide information on each team member and update on team mission alignment, approved mission essential tasks, IOC/FOC build status, and readiness assessment data (personnel, training, and space) to USCYBERCOM by close of business each Wednesday. Maintain reports on the USCYBERCOM CMF SIPRNET Intelink SharePoint portal (aka: Battle Roster): (http://intelshare.intelink.sgov.gov/sites/uscybercom/nmf/cmf/sitepages/home.aspx). Full details of this requirement are outlined in Enclosure 2, to this order.

3.C.1.F. (U//~~FOUO~~) Identify individual training requirements for team members and prospective team members to USCYBERCOM J7. After training requirements have been identified and validated at the

quarterly USCYBERCOM J7 CMF training summits, they may be submitted as follows: for National Cryptologic School (NCS) courses, submit training requirements via the NSA/CSS ADET portal. For non-NCS courses, submit training requirements via email to: cmf_non_ncs@nsa.ic.gov. Training plans and standards are provided in ref B.

3.C.1.G. (U//~~FOUO~~) Utilize the Individual Training Equivalency Board (ITEB) to request relief from the approved CMF training pipeline for individuals with an appropriate level of prior training, education, and experience. The ITEB consists of a panel of subject matter experts in the CMF work roles that consider ITEB packets submitted by the SCCs to make an equivalency determination. CMF team leaders submit ITEB packets requesting course exemption through their SCC leadership to USCYBERCOM J7 at cmf_tng_equiv@nsa.ic.gov.

3.C.1.H. (U//~~FOUO~~) ICW service training institutions, utilize the CMF course equivalency process to determine what service training solutions could provide an alternative to training identified on the CMF training pipeline. Individuals completing the approved service courses would then be excused from the equivalent course in the CMF training pipeline. Services request course equivalency through coordination with USCYBERCOM J7.

3.C.1.I. (U//~~FOUO~~) Complete the build of the CMF FY13 and FY14 teams tasked in ref D thru S respectively.

3.C.1.J. (U//~~FOUO~~) Build CMF teams as tasked in paragraphs 3.C.2 through 3.C.5 and transfer C2 of those teams to respective operational headquarters (i.e., CNMF HQ, JFHQ-C, JFHQ-DODIN, CCMD, SCC commands) IAW conditions stated in ref E and the following guidance.

3.C.1.J.1. (U//~~FOUO~~) The SCC officially informs gaining operational HQ that CMF team is prepared to enter mission alignment and mission delegation processes. It is the responsibility of the gaining HQ to manage each process through completion.

3.C.1.J.2. (U//~~FOUO~~) JFHQ-C assume Operational Control (OPCON) of CMTs and CSTs IAW ref E.

3.C.1.J.3. (U//~~FOUO~~) JFHQ-DODIN assume OPCON of DODIN CPTS (D-CPT).

3.C.1.J.4. (U//~~FOUO~~) CNMF-HQ assumes OPCON of NMTs, NSTs, N-CPTs IAW ref E.

3.C.1.J.5. (U//~~FOUO~~) CCMDs assume OPCON of CCMD CPTs (C-CPT) IAW ref E.

3.C.1.J.6. (U//~~FOUO~~) SCC Commands assume OPCON of Service CPTs (S-CPT) IAW ref E.

3.C.1.K. (~~S//REL TO USA, FVEY~~) To meet CMF team IOC criteria, the SCC is authorized to determine individual qualifications to fill a given work role. This determination should be based upon the individual, established standards, and the commander's operational risk assessment. SCC will coordinate with CDR CNMF-HQ for teams OPCON to CNMF, CDR JFHQ-C for teams OPCON to JFHQ-C, and JFHQ-DODIN for teams OPCON to JFHQ-DODIN. Individuals deemed qualified must possess the requisite knowledge, skills, and abilities (KSA) to execute assigned tasks to standard. Additionally, for positions that require

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) certification processes will be used.

3.C.1.L. (~~S//REL TO USA, FVEY~~) The CMF employs (b)(1) Sec 1.4(a) developers within the CSTs and NSTs. CSTs employ (b)(1) Sec 1.4(a) per team and NSTs employ (b)(1) Sec 1.4(a) per team. All developers will be pooled (b)(1) Sec 1.4(a) Any changes to the current plan for pooling developers (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) will be addressed via a FRAGO to this TASKORD. USCYBERCOM J7 is in the process of developing a capability developer training pipeline with an expected approval date NLT 01 October 2015. USCYBERCOM J9 is in the process of developing a capability developer implementation plan with expected approval date NLT 01 October 2015. (POCs (b)(3) @nsa.ic.gov / (b)(3) (b)(3) @nsa.ic.gov). NST capability developers will be located at NSAW and NSAT.

3.C.1.M. (U//~~FOUO~~) CMF teams established by one SCC and allocated to another HQ (e.g., FLTCYBER establishes the (b)(1) Sec 1.7(a) and it is apportioned to JFHQ-C ARCYBER) are to be transferred as follows:

3.C.1.M.1. (U//~~FOUO~~) PRESENTATION OF FORCES. Upon meeting IOC criteria, the establishing SCC coordinates with the gaining force HQ. With approval from the gaining force HQ, the SCC will declare IOC of that team and the gaining force HQ assumes OPCON.

3.C.1.M.2. (U//~~FOUO~~) REPORTING OF FORCES. SCCs maintain reporting responsibility over teams tasked via ref D and ref I until they are transferred to the gaining force HQ.

3.C.2. (U//~~FOUO~~) SCCs are authorized DIRLAUTH with supported commands to coordinate the location and positioning of CPTs for planning purposes.

3.C.3. (U//~~FOUO~~) SCCs are authorized DIRLAUTH with NSA/CSS ADET for coordination of NSA-provided training, SCCs are required to keep USCYBERCOM J7 informed IAW 3.D.1.E.

3.C.4. (U//~~FOUO~~) SCCs coordinate CEE and information technology requirements through the USCYBERCOM Capability Requirements Investment Board (CRIB), Cyber Operational Capability Board (COCB), and Enterprise Engineering Review Board (EERB) processes.

3.C.5. (U//~~FOUO~~) All responses and change requests regarding this order, including inability to reach IOC/FOC, should be sent via message format with supporting documentation to CMF coordination element POCs listed in section 5.C.1.

3.C.6. (U//~~FOUO~~) CDRUSCYBERCOM is the approval authority for any changes to the assigned number of teams, types of teams, mission, or location.

3.C.7. (~~S//REL USA, FVEY~~) The DMAG decision, CDRUSCYBERCOM intent, NSA/CSS resource planning, and current C2 assumptions are based upon NMTs, CMTs, associated NSTs, CSTs, and National Mission CPTs (b)(1) Sec 1.4(a) IAW mission requirements. Non-national CPTs (b)(1) Sec 1.4(a) upon CDRUSCYBERCOM/DIRNSA'S approval at service's expense and conditions based on space availability, furthermore, CDRUSCYBERCOM has approved (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

3.C.8. (U//~~FOUO~~) SCCs organize and employ CMF teams as units IAW ref B.

3.C.9. (~~S//REL TO USA, FVEY~~) SCC personnel currently in training (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) This does not apply to normal service rotations IAW service administrative control (ADCON) of personnel.

3.C.10. (U//~~FOUO~~) IAW USCYBERCOM Command Policy Memorandum 2013-01 and the Memorandum Of Understanding (MOU) between NSA/CSS and USSTRATCOM regarding support to USCYBERCOM, personnel (b)(1) Sec 1.7(e) will be in compliance with applicable DoD and NSA/CSS policies and procedures. The policies and procedures apply to initial and continued access to NSA/CSS information, facilities, spaces and/or systems. These include, but are not limited to the following: visitor control procedures, unofficial foreign travel, security incident reporting, foreign association, intelligence oversight, and assumption of responsibility and accountability for all classified materials and equipment provided by NSA/CSS.//

GENTEXT/ADMIN AND LOGISTICS/4.

4.A. (U//~~FOUO~~) USCYBERCOM J4 is the single point of coordination for CMF facilities based on the (b)(1) Sec 1.7(e) All CMF team headquarters (CNMF-HQ, JFHQ-C and JFHQ-DODIN) ICW CMF team leads are responsible to notify J4 of space and NSA/CSS co-location requirements. JFHQ-DODIN will coordinate with DISA for DODIN CPT NSA/CSS co-location requirements. J4 will aggregate initial FY15 space and NSA/CSS co-location requirements based on FY14 rosters and team requirements and provide to NSA/CSS for space requests with distributed execution by JFHQ-C at each location.

4.A.1. (U//~~FOUO~~) After initial requirements are provided to NSA/CSS by J4, J4 submits consolidated space and co-location requirements (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) The request will include detailed breakdowns of expected CMF teams, including specific space requirements and how many personnel are required to co-locate with each NSA/CSS mission area. This approved SPF will direct NSA/CSS allocation of spaces across enterprise.

4.A.2. (U//~~FOUO~~) SCC and JFHQ-C locating at NSA/CSS facilities are required to coordinate with USCYBERCOM J4 and J8 to assist with the establishment of any interservice support agreements (ISA) for reimbursable support and/or an MOU/ MOA for non-reimbursable support.

4.A.3. (U//~~FOUO~~) Permanent stationing of CMF teams and JFHQ-C at installations (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) to support USCYBERCOM requires the appropriate stationing documents be submitted to DoD. CMF teams permanently stationed (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) as required by the supported commands will be submitted as appropriate to DoD.

4.A.4. (U//~~FOUO~~) Requests for support from NSA/CSS (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) shall be coordinated with USCYBERCOM via the ICRWG/EERB and submitted to NSA/CSS.

4.B. (U//~~FOUO~~) IOC AND FOC REQUIREMENTS.

4.B.1. (U//~~FOUO~~) IOC and FOC manning and training standards are effective on the release date of this TASKORD for FY15 and FY16 teams.

4.B.2. (U//~~FOUO~~) IOC. CMF teams will be declared IOC after team meets the following criteria:

4.B.2.A. (~~S//REL TO USA, FVEY~~) (b)(1) Sec 1.4(a) of the team is on-hand, to include a core number of personnel in specified work roles; a sub-set of these core personnel must be fully trained IAW ref B annex C and the following (first number indicates required number on team <<slash>>/ second number indicates required number fully trained). The position titles below have been updated to reflect those defined in the Joint Cyber Training and Certification Standards (JCT&CS) and supersede guidance provided in ref N, 4.B.1.A.1 through 4.B.1.A.5.

4.B.2.A.1. (U) POSITION TITLES. See Enclosure 3 to this order.

4.B.2.B. (U) (~~S//REL TO USA, FVEY~~) (b)(1) Sec 1.4(a) is completed as follows:

4.B.2.B.1. (U//~~FOUO~~) Team Mission(s) Identified.

4.B.2.B.2. (U//~~FOUO~~) All available personnel have been placed in work roles as specified in par. 4.B.2.A.1. and mission alignment is complete ICW USCYBERCOM J3F (POC (b)(3) @nsa.ic.gov).

4.B.2.B.3. (U//~~FOUO~~) NST or CST is identified and aligned or identified for build (not applicable to CPT).

4.B.2.B.4. (U//~~FOUO~~) Team Leader is in receipt of mission.

4.B.2.C. (U//~~FOUO~~) Training requirements have been identified for all available team members and provided to USCYBERCOM J7 and higher HQs.

4.B.2.D. (U//~~FOUO~~) All personnel in work roles as specified in para 4.B.2.A.1. are allocated space to perform duties and have access to CEE and appropriate networks and data (mission support) to accomplish assigned missions.

4.B.2.E. (U//~~FOUO~~) CMF TEAM IOC DECLARATION PROCESS. Establishing SCC Commander (CDR) certifies their CMF team has achieved all IOC criteria, and then initiates the IOC declaration process. SCC CDR coordinates with the gaining operational CDR to accept OPCON transfer. Upon acceptance of OPCON, service cyber component CDR declares team IOC.

4.B.2.F. (U//~~FOUO~~) IOC WAIVERS. The gaining operational CDR has the option to waive team's IOC declaration IOT gain OPCON of the team for operational advantage and mission requirement. An operational or functional justification is required for waiver approval. Upon accepting OPCON of the pre-IOC team, the operational CDR will continue coordination with service cyber component CDR to ensure team achieves IOC criteria and is declared IOC. The operational CDR assumes the responsibility for ensuring the team achieves FOC. The IOC waiver is not intended to change the projected IOC dates and the teams' expected IOC dates shall be included in the waiver memo.

4.B.3. (U//~~FOUO~~) IAW ref F, SCC JFHQ-C'S are IOC, capable of executing (b)(1) Sec 1.7(e) mission essential tasks, with associated mission critical functions, as well as integrating (b)(1) Sec 1.7(e) ritical USCYBERCOM operational processes (see ref L).

4.B.4. (U//~~FOUO~~) FOC. CMF teams, having first achieved IOC, will be declared FOC when a team achieves compliance with ref I and meets the following criteria:

4.B.4.A. (U//~~FOUO~~) Successful completion of the Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities (DOTMLPF) process.

4.B.4.A.1. (U//~~FOUO~~) DOCTRINE. Concept Of Operation (CONOP) and implementation plans applicable to specified unit types provided to and approved by USCYBERCOM.

4.B.4.A.2. (U//~~FOUO~~) ORGANIZATION. Specific missions for each team identified and approved; initial review/assessment of unit size and structure complete; all personnel are properly aligned by function and are working mission.

4.B.4.A.3. (~~S//REL TO USA, FVEY~~) TRAINING (IAW REF B, Annex C). Mission Essential Task List (METL) established and approved; Job Qualification Requirements (JQR) identified for work roles where applicable; (b)(1) Sec 1.4(a) personnel are individually trained, qualified, and certified when applicable; collective/unit training complete; or as assessed by the SCC commander.

4.B.4.A.4. (U//~~FOUO~~) MATERIAL. Reporting vehicles designed, approved, and operational; team has access to applicable existing equipment/ capabilities necessary for mission accomplishment; additional equipment needs/requirements and gaps identified.

4.B.4.A.5. (U//~~FOUO~~) LEADERSHIP AND EDUCATION. All professional military education (PME) and civilian-equivalent Leadership and Education (L&E) programs identified.

4.B.4.A.6. (~~S//REL TO USA, FVEY~~) PERSONNEL. Team filled (b)(1) Sec 1.4(a) direct support personnel are filling authorized positions, on-hand, and properly aligned as applicable.

4.B.4.A.7. (U//~~FOUO~~) FACILITIES. Physical space/workstations and access to required data (Mission Support) for all personnel identified and available.

4.B.4.B. (U//~~FOUO~~) Successful completion of a joint or service assessment in which the CMF team accomplishes its mission and demonstrates proficiency in all areas noted in this paragraph (4.B.4.)

4.B.4.C. (U//~~FOUO~~) CMF team FOC declaration process IAW ref V. Operational CDR, in coordination with the establishing service cyber component commander, verifies their CMF team (all CMF teams except S-CPTs) has achieved all FOC criteria, and then routes the FOC request to DCDRUSCYBERCOM. For S-CPTs, the SCC CDR routes the FOC request to DCDR USCYBERCOM. DCDR USCYBERCOM declares all CMF teams FOC IAW ref V.

4.B.5. (U//~~FOUO~~) (U//~~FOUO~~) IAW Ref O and Ref W, JFHQ-C FOC is achieved when the following conditions are met. FOC will be achieved NLT 30 September 2015.

4.B.5.A. (U//~~FOUO~~) The JFHQ-C demonstrates proficiency in the USCYBERCOM-directed JFHQ-C (b)(1) Sec 1.7(e) mission essential tasks (JMETs – as defined by the USCYBERCOM JFHQ-C certification framework to operationalize the JFHQ), associated critical functions, and integration with USCYBERCOM associated processes necessary to conduct (b)(1) Sec 1.7(e) operations.

4.B.5.B. (U//~~FOUO~~) The JFHQ-C commander requests FOC following successful completion of a joint or service event in which the JFHQ-C successfully accomplishes its mission and demonstrates proficiency in (b)(1) Sec 1.7(e) directed JMETs, all applicable (b)(1) Sec 1.7(e) JMETs, critical functions, and associated processes as assessed by an external assessment team.

4.B.6. (U) POLICY.

4.B.6.A. (~~S//REL TO USA, FVEY~~) Specific personnel / units will conduct (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) consistent with mission needs.

4.B.6.B. (~~S//REL TO USA, FVEY~~) (b)(1) Sec 1.4(a) program is established IAW ref G and functional within each team as applicable.//

GENTEXT/COMMAND AND CONTROL/5.

5.A. (U//~~FOUO~~) USCYBERCOM is the supported command. All others are the supporting commands.

5.B. (U//~~FOUO~~) SCC will maintain ADCON over personnel assigned to the CMF. NSA/CSS will maintain ADCON over personnel aligned to provide direct support to the CMF.

5.C. (U//~~FOUO~~) Copies of this order and all enclosures will be maintained at:
https://www.cybercom.smil.mil.j3/orders/default.aspx

5.D. (U//~~FOUO~~) All DoD components will acknowledge receipt and understanding of this TASKORD within 24 hours to the following site:
(https://intelshare.intelink.sgov.gov/sites/uscybercom/JOC/Orders/Lists/Orders%20Acknowledgement/AllItems.aspx).//

5.E. (U) Request for information regarding execution of this order, amplifying guidance, and/or additional details are to be submitted at the below links
SIPRNET: (https://intelshare.intelink.sgov.gov/sites/uscybercom/Pages/RFI.aspx)
JWICS: (https://intelshare.intelink.ic.gov/sites/uscybercom/request/Pages/RFI.aspx)

5.F. (U//~~FOUO~~) USCYBERCOM CMF SIPRNET Intelink SharePoint portal (aka: Battle Roster):
(http://intelshare.intelink.sgov.gov/sites/uscybercom/nmf/cmf/sitepages/home.aspx).

5.G. (U) POINTS OF CONTACT (POCS):

5.G.1. (U//~~FOUO~~) USCYBERCOM J338 Cyber Mission Force Coordination Element:
NSANet: USCC_CMF_READINESS@NSA.IC.GOV.

5.G.2. (U//~~FOUO~~) USCYBERCOM J2: (b)(3) USMC and (b)(3)
NSTS 969-4163
NSANet (b)(3) @nsa.ic.gov and (b)(3) @nsa.ic.gov.

5.G.3. (U//~~FOUO~~) USCYBERCOM J3F: (b)(3) USA
NSTS: 969-3465
NSAnet: (b)(3) @nsa.ic.gov.

5.G.4. (U//~~FOUO~~) USCYBERCOM J39, (b)(3) USA
NSTS: 963-6125
NSANet: (b)(3) @nsa.ic.gov.

5.G.5. (U//~~FOUO~~) USCYBERCOM J4, (b)(3)
NSTS: 969-5726/5721
NSANet: (b)(3) @nsa.ic.gov.

5.G.6. (U//~~FOUO~~) USCYBERCOM J5: (b)(3)
NSTS: 969-8360
NSANet: (b)(3) @nsa.ic.gov.

5.G.7. (U//~~FOUO~~) USCYBERCOM J6: (b)(3) USAF
NSTS: 969-1829
NSANet: (b)(3) @NSA.IC.GOV.

5.G.8. (U//~~FOUO~~) USCYBERCOM J7: (b)(3)
NSTS: 969-4191
NSANet: (b)(3) @nsa.ic.gov.

5.G.9. (U//~~FOUO~~) USCYBERCOM J8: (b)(3)
NSTS: 992-2573
NSANet: (b)(3) @nsa.ic.gov.

5.G.10. (U//~~FOUO~~) USCYBERCOM SPECIAL SECURITY OFFICER (SSO): (b)(3)
NSTS: 767-2154
NSANet: (b)(3)) @nsa.ic.gov

5.G.11. (U) After Hours POC: USCYBERCOM JOC Duty Officer (JDO)
NSTS: 969-1645
COMM: (443) 654-4804
NIPR: jocops@CYBERCOM.MIL
SIPR: jocops@CYBERCOM.SMIL.MIL.//

GENTEXT/AUTHENTICATION/FOR THE CDR, (b)(3) RADM, USN, USCYBERCOM J3, DIRECTOR OF OPERATIONS//

AKNLDG/YES//

53

18-F-1080

The National Security Archive

The George Washington University
Gelman Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037

Phone: 202/994-7000
Fax: 202/994-7005
nsarchiv@gwu.edu
www.nsarchive.org

Tuesday, May 29, 2018

Office of Freedom of Information
1155 Defense Pentagon
Washington, DC 203011155

Re: Request under the FOIA, in reply refer to Archive# ***20180515DOD071***

Dear Information Officer :

Pursuant to the Freedom of Information Act (FOIA), I hereby request the following:

In connection with the recent (May 17, 2018) announcement that all 133 of U.S. Cyber Command's Cyber Mission Force teams have achieved Full Operational Capability (FOC), a copy of any records specifying in full the standards or requirements that must be met to reach FOC.

If you regard any of these documents as potentially exempt from the FOIA's disclosure requirements, I request that you nonetheless exercise your discretion to disclose them. As the FOIA requires, please release all reasonably segregable non exempt portions of documents. To permit me to reach an intelligent and informed decision whether or not to file an administrative appeal of any denied material, please describe any withheld records (or portions thereof) and explain the basis for your exemption claims.

As a representative of the news media, the National Security Archive qualifies for "representative of the news media" status under 5 U.S.C. Sec. 552(a)(4)(A)(ii)(II) and, therefore, may not be charged search and review fees. (See *National Security Archive v. U.S. Department of Defense,* 880 F.2d 1381 (D.C. Cir. 1989), *cert denied,* 110 S Ct. 1478 (1990)). This request is made as part of a scholarly and news research project that is intended for publication and is not for commercial use. For details on the Archive's research and extensive publication activities please see our website at www.nsarchive.org.

To expedite the release of the requested documents, please disclose them on an interim basis as they become available to you, without waiting until all the documents have been processed. Please notify me before incurring any photocopying costs over $100. If you have any questions regarding the identity of the records, their location, the scope of the request or any other matters, please call me at (202) 994-7000 or email me at foiamail@gwu.edu. I look forward to receiving your response within the twenty day statutory time period.

Sincerely yours,

Malcolm Byrne