



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

SEP 17 2018

Ms. Divya Hosangadi
Johns Hopkins Center for Health Security
621 E. Pratt Street, Suite 210
Baltimore, MD 21202

Dear Ms. Hosangadi,

Thank you for your 19 June 2018 Freedom of Information Act request. U.S. Strategic Command (USSTRATCOM) referred your request to U.S. Cyber Command (USCYBERCOM) on 19 June 2018 for processing. Our office located two responsive documents.

After carefully reviewing the enclosed documents, 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.

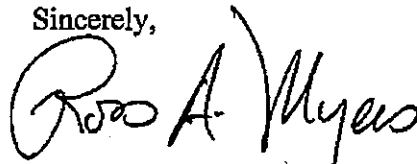
As the Initial Denial Authority, I am partially denying portions of the document. The denied information is currently and properly classified in the interest of national defense or foreign policy according to Executive Order 13526, *Classified National Security Information*, Section 1.4(a) and b(7)(e). 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. 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.

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 should cite case number 18-059, 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,

A handwritten signature in black ink, reading "Ross A. Myers". The signature is written in a cursive style with a large, stylized "R" and "M".

ROSS A. MYERS
Rear Admiral, U.S. Navy
Commander

From: National FOIA Portal <National.FOIAPortal@usdoj.gov>
Sent: Tuesday, June 19, 2018 12:10 PM
To: STRATCOM Offutt AFB J006 Mailbox FOIA PA
Subject: [Non-DoD Source] New FOIA request received for U.S. Cyber Command

Hello,

A new FOIA request was submitted to your agency component:

The following list contains the entire submission, and is formatted for ease of viewing and printing.

| | |
|--------------------------------|---|
| request_id | 14421 |
| confirmation_id | 13896 |
| address_city | Baltimore |
| address_country | United States |
| address_line1 | Johns Hopkins Center for Health Security |
| address_line2 | 621 E. Pratt Street, Suite 210 |
| address_state_province | MD |
| address_zip_postal_code | 21202 |
| company_organization | Johns Hopkins Center for Health Security |
| email | [REDACTED] |
| expedited_processing | no |
| fee_amount_willing | 50.00 |
| fee_waiver | yes |
| fee_waiver_explanation | This request is for records that are essential for academic research currently being conducted by the Johns Hopkins Center for Health Security, for educational purposes designed to contribute to public understanding of operations and activities of the government. |
| name_first | Divya |
| name_last | Hosangadi |
| phone_number | [REDACTED] |
| request_category | educational |
| request_description | Requesting the most current continuity of operations plan (COOP) for US Cyber Command. The COOP we request is for one that would be enacted during a large scale national emergency, such as a large scale natural disaster or pandemic situation. If the COOP plan(s) is determined to be exempt from FOIA disclosure, I request lists of primary mission essential functions (PMEF) for the US Cyber Command and any of its subcomponents, if applicable. Because we are requesting only the most current plan, we suggest searching for documents developed between 01/01/2016 and present day (06/19/2018). If the COOP requested was developed prior to 2016, we request expanding the search dates to range from 2014 (01/01/2014) to 2016 (01/01/2016), and to continue expanding the date range if the most recent document was developed prior to 2014. The same suggestion for dates applies for lists of PMEFS, if the COOP is deemed exempt from FOIA disclosure. I have already contacted OSD and spoken to Jim Hogan and Aaron Graves. If the requested COOP information for the US Cyber Command is only available by contacting OSD, please let me know. Federal Preparedness Circular 65 requires that departments and agencies maintain lists of PMEFS as part of their continuity of operations plans. Records to be used in educational/research pursuits associated with the Johns Hopkins Bloomberg School of Public Health Please let me know if you have any questions. |

(b) (6)

The following table contains the entire submission, and is formatted for ease of copy/pasting into a spreadsheet.

| request_i | confirmation_i | address_cit | address_countr | address_line | address_line | address_state_provin | address |
|-----------|----------------|-------------|----------------|--------------|--------------|----------------------|---------|
| d | d | y | y | 1 | 2 | ce | |

| | | | | | | | |
|-------|-------|-----------|---------------|--|--------------------------------------|----|-------|
| 14421 | 13896 | Baltimore | United States | Johns Hopkins Center for Health Security | 621 E. Pratt Street, Suite 210 | MD | 21202 |
|-------|-------|-----------|---------------|--|--------------------------------------|----|-------|

~~SECRET~~

USCYBERCOM

**CONTINUITY OF OPERATIONS
(COOP) PLAN (U)**

DATE: 1 March 2017



**USCYBERCOM
9800 SAVAGE ROAD
FORT GEORGE G. MEADE, MD 20755**

Classified By: (b)(3)

Derived From: USCYBERCOM Classification Guide

Dated: 20150415

Declassify On: 20400416

~~SECRET~~

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

~~SECRET~~



USCYBERCOM
9800 Savage Road
Fort George G. Meade, MD 20755

Reply ZIP Code: 20755

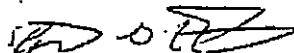
1 March 2017

MEMORANDUM FOR: Distribution List

SUBJECT: USCYBERCOM CONTINUITY OPERATIONS (COOP) PLAN for
USCYBERCOM (S)

1. (U) This USCYBERCOM Continuity of Operations Plan provides the details for USCYBERCOM efforts to satisfy the DOD 3020.26 "Department of Defense Continuity Programs" requirement for all DOD Components (USCYBERCOM) to develop, coordinate, and maintain continuity plans.
2. (U) The USCYBERCOM COOP Plan is effective for planning purposes upon receipt and for expansion into an Operations Order (OPORD) when directed.
3. (U) The USCYBERCOM COOP Plan was coordinated with USCYBERCOM Components, USSTRATCOM Headquarters staff, and the Joint Staff.
4. (U) Forward any recommended changes to USCYBERCOM J3, 9800 Savage Road, Fort George G. Meade, MD 20755.

FOR THE COMMANDER


STEPHEN G. FOGARTY
Major General, USA
Chief of Staff

Encl

USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX (S)
USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN ANNEX C (S)

iii

~~SECRET~~

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

~~SECRET~~

USCYBERCOM COOP Plan
1 March 2017

USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX
RECORD OF CHANGES

In the event the issuing authority distributes changes to this plan, ensure the changes are made and recorded in the table below.

| Change Number/ Message DTG | Posted Date | Effective Date | Printed Name/ Signature of Change Verifier |
|-------------------------------------|----------------|-------------------|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

v
~~SECRET~~

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

~~SECRET~~

USCYBERCOM COOP Plan
1 March 2017

USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX (U)
SECURITY INSTRUCTIONS

1. (U) The long title of this plan is "Continuity of Operations Plan for United States Cyber Command (U)." The short title is "USCYBERCOM COOP Plan (U)." Both titles are UNCLASSIFIED.

2. (U) The overall classification of this document is SECRET. Pages are classified SECRET to protect information classified at that level or the compilation of sensitive (but not necessarily classified) individual entries which, when aggregated, may convey information of a classified nature.

3. (U) Reproducing, extracting, and/or paraphrasing in whole or in part is authorized only when necessary to satisfy military requirements, provided the original classification of the affected portion is maintained. The distribution of this plan, or portions thereof, is restricted to those agencies and personnel whose duties specifically require knowledge of the contents.

4. (U) This document contains information affecting the national defense of the United States within the meaning of the Espionage Laws, Title 18, United States Code, sections 793 and 794. The law prohibits the transmission or revelation of information contained within the document to unauthorized personnel.

~~SECRET~~

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

~~SECRET~~

USCYBERCOM COOP Plan
1 March 2017

USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX (U)

TABLE OF CONTENTS

| <u>CONTENTS</u> | <u>PAGE</u> |
|--|-------------|
| RECORD OF CHANGES | v |
| SECURITY INSTRUCTIONS | vii |
| TABLE OF CONTENTS | ix |
| USCYBERCOM COOP PLAN SUMMARY | xi |
| BASIC OPERATIONS ORDER | 1 |
| ANNEX A, TASK ORGANIZATION | A-1 |
| APPENDIX 1 – Command Relocation Group (CRG) Organization | A-1-1 |
| ANNEX B, THREATS AND INTELLIGENCE | B-1 |
| ANNEX C, OPERATIONS | C-1 |
| APPENDIX 1 – Execution Authority, Options, and Responses | C-1-1 |
| APPENDIX 2 – Staff Reconstitution..... | C-2-1 |
| APPENDIX 3 – (CCMD has a section that is responsible for COOP) | C-3-1 |
| APPENDIX 4 – CNMF..... | C-4-1 |
| APPENDIX 5 – Augmentation Mission Staff Operations..... | C-5-1 |
| APPENDIX 6 – Command Mission Essential Functions | C-6-1 |
| ANNEX D, LOGISTICS..... | D-1 |
| APPENDIX 1 – Logistics Support | D-1-1 |
| APPENDIX 2 – Transportation and Mobility | D-2-1 |
| APPENDIX 3 – Site Logistics Support..... | D-3-1 |
| ANNEX E, PERSONNEL AND ADMINISTRATION..... | E-1 |
| ANNEX F, PUBLIC AFFAIRS | F-1 |
| ANNEX J, COMMAND RELATIONSHIPS | J-1 |
| ANNEX K, COMMUNICATIONS AND INFORMATION..... | K-1 |
| APPENDIX 1 – Emergency Phone Contact List | K-1-1 |
| APPENDIX 2 – Joint Staff Phone Contact List for COOP site | K-2-1 |
| APPENDIX 3 – Key C4IT Systems | K-3-1 |
| APPENDIX 4 – Communications Suite descriptions for sites | K-4-1 |
| ANNEX L, ENVIRONMENTAL CONSIDERATIONS | L-1 |
| ANNEX M, COOP TESTS, TRAINING, AND EXERCISES..... | M-1 |
| ANNEX P, HOST NATION SUPPORT | |
| ANNEX Q, MEDICAL SERVICES..... | Q-1 |
| ANNEX X, EXECUTION CHECKLIST..... | X-1 |
| ANNEX Y, COMMUNICATIONS SYNCHRONIZATION | Y-1 |
| ANNEX Z, DISTRIBUTION | Z-1 |
| GLOSSARY..... | Glossary-1 |

~~SECRET~~

~~SECRET~~

FIGURES

PAGE

TABLES

PAGE

x
~~SECRET~~

~~SECRET~~

USCYBERCOM COOP PLAN
1 March 2017

USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX
SUMMARY (U)

1. (U) PURPOSE. The USCYBERCOM COOP Plan provides the Commander of USCYBERCOM the means to continue USCYBERCOM Mission Essential Functions (MEFs) during national security emergencies or when normal operations conditions have been impaired or made impossible. This plan fulfills the requirement provided by National Security Presidential Directive (NSPD)-51 and DODD 3020.26 which stipulate the requirements for both a comprehensive continuity program and plan development, respectively. This plan will update perishable information as needed.

- a. (U) Support National and DOD policy directives.
- b. (U) Implement Secretary of Defense (SecDef) and Chairman of the Joint Chiefs of Staff (CJCS) directives.
- c. (U) Detail the concept of operations.
- d. (U) Define the decision authority for execution.
- e. (U) Describe conditions for implementation.
- f. (U) Identify execution criteria.
- g. (U) Identify primary COOP functions, procedures, and capabilities required to execute those functions.
- h. (U) Define a minimum level of readiness.
- i. (U) Assign responsibilities to the USCYBERCOM Staff, and USCYBERCOM Military Service and Functional Components.
- j. (U) Provide planning capabilities necessary to perform MEFs during national security emergencies or other emergencies that affect the ability to execute the USCYBERCOM mission.
- k. (U) Provide guidance to reconstitute the positions of CDRUSCYBERCOM and personnel assigned to USCYBERCOM, to include active duty military, DOD civilian, and contractors as appropriate.

2. (U) APPLICABILITY. This plan is effective upon receipt and applies to all personnel assigned to USCYBERCOM.

~~SECRET~~

~~SECRET~~

3. (U) POLICY. USCYBERCOM will ensure continuous operations of USCYBERCOM's Mission Essential Functions (MEFs) according to National and DOD Policy referring to Continuity of Operations.

- a. (U) An identifiable command authority.
- b. (U) A surviving USCYBERCOM staff, able to accomplish USCYBERCOM MEFs and adequate to task and manage MEFs accomplishment.
- c. (U) A secure, survivable, and redundant operational communications system with access (receive and transmit) to all appropriate data and voice communication systems.
- d. (U) MISSION. On order, CDRUSCYBERCOM and designated elements of the Command relocate as part of a USG-wide continuity of operations (COOP) program in order to ensure the Command maintains the ability to perform all Unified Command Plan-directed missions and responsibilities in times of peace, crisis, or conflict.

e. (U) Commander's Intent. USCYBERCOM will be prepared to conduct COOP to ensure continuous operations of USCYBERCOM's MEFs, with or without warning, in a manner that insures seamless C2 of global cyberspace operations and uninterrupted support to Combatant Commands, Services and Agencies in accordance with the standards specified in this plan for a

(b)(1) Sec 1.4(a) This will be accomplished through the Command Relocation Group (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(1) (U//~~FOUO~~) Purpose. USCYBERCOM remains able to accomplish MEFs in the event that relocation from the (b)(1) Sec 1.7(e) is ordered, anticipated, or necessary.

(2) (U//~~FOUO~~) Method. Alert and deploy Command Relocation Group personnel to select COOP site(s). Personnel will stand up selected USCYBERCOM COOP sites and commence cyberspace operations in support of USCYBERCOM MEFs.

(3) (U//~~FOUO~~) End State. USCYBERCOM maintain continuous operations at the USCYBERCOM COOP site(s) until operations resume in the (b)(1) Sec 1.7(e) or a follow-on plan has been approved by the Commander.

4. (U) MISSION ESSENTIAL FUNCTIONS (MEFs). Certain USCYBERCOM functions have been identified as Mission Essential Functions for the purpose of this plan. Interruption or loss of these functions will have serious impact within days of interruption. MEFs are the most critical tasks associated with the success of USCYBERCOM's operational mission. See APPENDIX XX to

~~SECRET~~

ANNEX C, "OPERATIONS."

5. (U) ESSENTIAL ELEMENTS OF INFORMATION (EEI). The USCYBERCOM COOP Plan execution is based on an assessment of the potential magnitude of the threat, duration of the threat or attack, potential for facility loss, and readiness concerns.

- a. (U) Is there a credible threat to continuous operations or key personnel?
- b. (U) How specific and/or imminent is the threat? How much available warning time exists to execute COOP plans and relocate operations?
- c. (U) How grave are the potential consequences of the threat?
- d. (S) Is there a (b)(1) Sec 1.4(a) at USCYBERCOM HQ?
- e. (S) Given the threat, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) remain in place or relocate to another location?
- f. (S) Is clandestine (b)(1) Sec 1.4(a)

6. (U) CONCEPT OF OPERATIONS.

a. (S) Purpose. This plan is designed to increase the survivability of essential USCYBERCOM personnel and provide flexible MEFs execution during the pre-, trans-, and post-event phases of a COOP contingency. Survivability and continuity are accomplished (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) AAW the DODD 3020.26.

b. (U) The Concept of Operation supports:

(1) (S) The continuous tailoring of the Command Relocation Group (b)(1) Sec 1.4(a) to meet existing threat conditions.

(2) (S) The relocation of Command Relocation Group (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to the USCYBERCOM COOP sites commensurate with the size, skills, and ranks necessary to support the USCYBERCOM Staff and provide support to the MEFs restoration operations.

(3) (S) USCYBERCOM's COOP plan for devolment (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) is currently being coordinated (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) for COOP space so that mission essential personnel (b)(1) Sec 1.4(a)

~~SECRET~~

(4) (U) Phase 3 Post-Event (Reconstitution). The USCYBERCOM Staff reconstitutes, using surviving USCYBERCOM personnel and, if required, personnel from the Military Services, and USCYBERCOM Subordinate Component Commands. Should the USCYBERCOM HQ (b)(7)(e) (b)(7)(e) not be functional, the USCYBERCOM Staff will reconstitute at a location designated by the acting CDRUSCYBERCOM. See APPENDIX XX, "STAFF RECONSTITUTION," to ANNEX C, "OPERATIONS."

7. (U) CONDITIONS FOR EXECUTION. A decision to execute any portion of the USCYBERCOM COOP may occur during duty and non-duty hours, with little or no warning. COOP execution is explained in detail in ANNEX C Paragraph 3.

8. (S) EXECUTION AUTHORITY. Execution of aspects of this plan requires consultation with and approval by the Commander, USCYBERCOM, his representative, or higher authority. The Director of Operations (USCYBERCOM

(b)(1) Sec 1.4(a)

9. (U) TIME TO COMMENCE EFFECTIVE OPERATIONS. See "BASE PLAN," Paragraph 3 Execution, "PLANNING FACTORS."

10. (U) KEY ASSUMPTION AND THREATS.

a. (S) Threats to operations of the USCYBERCOM (b)(1) Sec 1.4(a) facilities range from natural disasters and infrastructure failures to terrorist attacks and attacks during times of war. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) highly visible symbols of the United States, to include government facilities such as USCYBERCOM (b)(1) Sec 1.4(a) Possible threats to USCYBERCOM (b)(1) Sec 1.4(a) operations include, but are not limited to:

- (1) (U) Natural disaster (e.g. earthquake, hurricane)
- (2) (U) Manmade disaster or emergency (e.g. accidental disruption, and/or cyber attack)
- (3) (U) Technological emergency (e.g. Power failure, fire)
- (4) (U) Acts of terrorism involving attacks utilizing conventional, nuclear,

~~SECRET~~

biological, and chemical materials weapons, as well as conventional or cyber attacks on (b)(7)(e)

b. (U) Unconventional. Coordinated military attack on the United States involving conventional, nuclear, biological, chemical materials and/or weapons.

11. (U) OPERATIONAL CONSTRAINTS.

a. (S) The overall number of personnel relocating (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) the relocation site.

b. (S) The command must retain the ability (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

during all phases of the plan execution.

c. (C) Nuclear, biological, or chemical attack directed at USCYBERCOM

(b)(1) Sec 1.4(a)

d. (C) (b)(1) Sec 1.4(a)

relocation and/or reconstitution efforts.

e. (C) During relocation, the group may encounter (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

to the designated relocation points.

f. (U) The relocation and reconstitution of designated personnel may not be

(b)(7)(e)

(b)(7)(e)

to perform the MEF's functions.

12. (U) COMMAND RELATIONSHIPS. Command relationships remain the same as prior to plan implementation. Successions of command lines for command of USCYBERCOM are outlined in ANNEX J. USCYBERCOM may elect to reconstitute at any location possessing the capability to support requirements.

13. (U) TASKS. See USCYBERCOM COOP BASE Plan, "COORDINATING INSTRUCTIONS".

14. (U) COMMUNICATION APPRAISAL. See ANNEX K, "COMMUNICATIONS AND INFORMATION."

15. (U) LOGISTICS APPRAISAL. The logistics appraisal of this plan focuses on the three essential elements of logistical assessments: feasibility; supportability; and sustainability. The assessment analysis considers core capabilities in terms of critical items, limitations, logistics, outsourcing, and threats to logistic capabilities prior to and during a COOP event. The

~~SECRET~~

~~SECRET~~

assessment also highlights deficiencies or gaps and any associated risks; it proposes mitigation strategies to reduce or contain identified risks. COOP support is dependent upon the determination of alternate locations/sites and flexibility for the delivery of services and support. See ANNEX D, "LOGISTICS AND SUSTAINMENT" for execution procedures for logistics support to COOP.

16. (U) PERSONNEL APPRAISAL.

a. (U) There are currently enough USCYBERCOM personnel to meet requirements. There is the potential that an event could occur where a significant number of personnel [REDACTED] (b)(7)(e)

[REDACTED] (b)(7)(e)

b. (S) Personnel requirements and processes to achieve rapid reconstitution of USCYBERCOM [REDACTED] (b)(1) Sec 1.4(a)

[REDACTED] (b)(1) Sec 1.4(a)

c. (S) Personnel assigned to the Command Relocation Group [REDACTED] (b)(1) Sec 1.4(a) shall be trained, qualified, certified, and exercised to ensure readiness to execute assigned MEFs, to include operations supporting USCYBERCOM, under all conditions.

OFFICIAL

<F. M. LNAME>
RANK, SERVICE
POSITION, J-3

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX (U)
BASE PLAN (U)

(U) REFERENCES.

a. (U) National Security Presidential Directive 51 (NSPD 51) / Homeland Security Presidential Directive 20 (HSPD 20), National Continuity Policy, 9 May 07 (U)

b. (U) Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Programs and Requirements, Oct 12 (U)

c. (U) Federal Continuity Directive 2 (FCD 2), Federal Executive Branch Mission Essential Function and Primary Mission Essential Function and Identification and Submission Process, Feb 08 (U)

d. (U) DOD Directive 3020.26, Department of Defense Continuity Programs, 9 Jan 09 (U)

e. (U) DOD Directive 3020.26P, Secretary of Defense Continuity of Operations Plan, 21 Mar 07 (S)

f. (U) DOD Instruction 3020.42, Defense Continuity Plan Development, 27 Apr 11 (U)

g. (U) Chairman of the Joint Chiefs of Staff Operation Order 3-12, Continuity of Operations (COOP) for the Chairman of the Joint Chiefs of Staff, 30 Nov 12 (S)

h. (U) National Continuity Policy Implementation Plan, 27 Sep 07 (U)

i. (U) Department of Defense Implementation of National Continuity Policy, 18 Jan 12 (TS)

j. (U) Department of Defense Directive 7730.65, Defense Readiness Reporting System (DRRS), 11 May 15 (U)

k. (U) National Terrorist Advisory System Public Guide, DHS website (U)

l. (U) USSTRATCOM Continuity of Operation (COOP), 1 August 2014 (S)

1. (U) Situation.

a. (U) General. Crises may occur that negatively affect or prevent

operations from continuing in USCYBERCOM facilities. The USCYBERCOM Continuity of Operations Plan (USCYBERCOM COOP Plan) describes the processes and steps in order to continue Mission Essential Functions (MEFs) without unacceptable interruption during a national security emergency. National security emergencies are any occurrence of disruptive conditions that seriously degrade or threaten the national security of the United States. In addition, the USCYBERCOM COOP Plan provides for the timely and orderly devolvement, relocation and/or reconstitution of key staff during an emergency or other event affecting the ability to execute the USCYBERCOM mission from current facilities. Consideration is given to executing relocation of MEFs as a precautionary measure. This will be performed by the Command Relocation Group: (b)(7)(e) as determined by the situation.

b. (U) Enemy. See ANNEX B, "THREATS AND INTELLIGENCE," and current intelligence reports as appropriate.

(1) (U//~~FOUO~~) Threat. Threats to operations of the USCYBERCOM range from natural disasters to terrorist attacks and attacks during times of war. The following threats to USCYBERCOM will meet the threshold for executing COOP.

(a) (U//~~FOUO~~) Natural Disaster

(b) (U//~~FOUO~~) Manmade disaster or emergency

(c) (U//~~FOUO~~) Technological emergency.

(d) (U//~~FOUO~~) Acts of terrorism involving Chemical, Biological, Radiological, Nuclear, or High-yield Explosive (CBRNE) materials

(e) (U//~~FOUO~~) Coordinated military attack on the UNITED States involving conventional, nuclear, biological, or chemical materials or weapons.

(2) (U//~~FOUO~~) Intelligence Operations. USCYBERCOM J2 will be responsible for providing and/or coordinating all intelligence required by the commander, staff judge advocate, staff planners, operators to plan and execute all assigned missions. It is the details of the assigned cyberspace operations mission that drive the details of the J2 organization and processes, which are briefly explained below.

c. (U) Friendly. U.S. forces and other components identified by current operations report.

d. (U) Facts.

✓

(1) (C) USCYBERCOM Headquarters Facility, (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) variety of threats that may interrupt
essential operations and functions.

(2) (U) Enemy forces are capable of launching attacks against Fort Meade, MD and other major US military facilities with little or no advanced warning.

(3) (U) This COOP Plan is executable with or without warning, during duty or non-duty hours.

(4) Emergency funding will be made available to facilitate COOP.

(5) There will be situational event-driven disruption to normal operations.

e. (U) Assumptions.

(1) (C) USCYBERCOM may receive (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(2) (C) (b)(1) Sec 1.4(a) to and from local
COOP sites.

(3) (C) (b)(1) Sec 1.4(a) COOP sites will be available.

(4) (C) (b)(1) Sec 1.4(a) can be modified
as required if (b)(1) Sec 1.4(a) determined to be
mission essential and subject to COOP.

(5) (C) Command Relocation Group: (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) capable of performing the functions
of the USCYBERCOM MEFs.

(6) (C) The COOP site(s) (b)(1) Sec 1.4(a) support and
logistics for the Command Relocation Group.

(7) (C) The COOP site(s) (b)(1) Sec 1.4(a) supporting the Command
Relocation Group in its performance of the USCYBERCOM MEFs.

(8) (C) USCYBERCOM (b)(1) Sec 1.4(a) will function during COOP and
will be accessible by USCYBERCOM from the COOP site(s).

(9) (C) USCYBERCOM remains in communication with higher
headquarters, (b)(1) Sec 1.4(a) Combatant Commands
(CCMDs), Services, and Agencies at the COOP site(s).

(10) (C) All designated USCYBERCOM personnel [redacted] (b)(1) Sec 1.4(a) site(s).

(11) (C) Non-COOP personnel [redacted] (b)(1) Sec 1.4(a) [redacted] (b)(1) Sec 1.4(a) planned and directed.

(12) (C) The [redacted] (b)(1) Sec 1.4(a) [redacted] (b)(1) Sec 1.4(a) full range of natural and/or man made disasters and may require devolvement and/or relocation to alternate facilities to perform the USCYBERCOM MEFs.

(13) (C) The Commander USCYBERCOM [redacted] (b)(1) Sec 1.4(a) [redacted] (b)(1) Sec 1.4(a) as long as possible.

(14) (C) USCYBERCOM will retain [redacted] (b)(1) Sec 1.4(a) authorities.

f. (U) Planning Factors.

(1) (U) Purpose. This plan is executable in both a "with warning" and "no-warning" scenario, during duty or non-duty hours. For the USCYBERCOM COOP Plan, duty hours are considered to be [redacted] (b)(7)(e) hours Eastern Time, Monday-Friday except federal holidays.

(2) (U) Staffing Considerations. The rank, skill sets, and number of personnel assigned to the Command Relocation Group are determined by space limitations and MEFs to be performed. Due to these space limitations, the Command Relocation Group by necessity represents a fraction of the full USCYBERCOM staff. To meet these staffing limitations and in order to support the MEFs, the USCYBERCOM directorates will prioritize their directorate functions and select the most knowledgeable and experienced personnel for assignment to the Command Relocation Group. The assignments for USCYBERCOM directorates are provided in APPENDIX 1, "COMMAND RELOCATION GROUP ORGANIZATION," to ANNEX A, "TASK ORGANIZATION."

(3) (U) Essential Elements of Information. USCYBERCOM COOP Plan execution is contingent on an assessment of the potential magnitude of the threat, duration of the threat or attack, potential for facility loss, and readiness concerns.

(a) (U) Is there a credible threat to continuous operations or key personnel?

(b) (U) How specific and/or imminent is the threat? How much available warning time exists to execute COOP plans and relocate operations?

(c) (U) How grave are the potential consequences of the threat?

(d) (S) Is [redacted (b)(1) Sec 1.4(a)] USCYBERCOM HQ?

(e) (S) Given the threat, [redacted (b)(1) Sec 1.4(a)]
[redacted (b)(1) Sec 1.4(a)] relocate to another location?

(f) (S) [redacted (b)(1) Sec 1.4(a)] not to cause additional
unrest within the community?

2. (S) Mission. On order, CDRUSCYBERCOM and designated elements of the Command [redacted (b)(1) Sec 1.4(a)] program in order to ensure the Command maintains the ability to perform all Unified Command Plan-directed missions and responsibilities in times of peace, crisis, or conflict.

a. (U) MEFs. The MEFs and tasks are discussed in APPENDIX XX "MISSION ESSENTIAL FUNCTIONS," to ANNEX C, "OPERATIONS."

3. (U) Execution. This plan is designed to increase the survivability of essential USCYBERCOM personnel to enable flexible MEF execution during the pre-, trans-, and post-event phases of a COOP contingency. Survivability and continuity are accomplished [redacted (b)(7)(e)]
[redacted (b)(7)(e)] while maintaining the ability to perform succession.

a. (S) COOP Concept of Operations. Personnel will relocate to one of the USCYBERCOM COOP locations (Command Relocation Group: [redacted (b)(1) Sec 1.4(a)]
[redacted (b)(1) Sec 1.4(a)] as determined by the situation. Alternate or additional sites may be used if available at implementation. USCYBERCOM COOP execution [redacted (b)(1) Sec 1.4(a)]

b. (U) Execution Authority. Execution aspects of this plan requires consultation with, and approval by, the Commander, USCYBERCOM, his representative, or higher authority. The Director of Operations (USCYBERCOM J3) is responsible for the execution of this plan.

c. (U) Conditions for Execution. The following conditions may cause execution of USCYBERCOM COOP. This plan is designed to support continuity of operations given war, terrorist attack, natural or technological disaster, or at the direction of the President or Secretary of Defense. These conditions may occur during duty and non-duty hours, with or without warning, and may cause disruptions to normal USCYBERCOM operations.

(1) (U) War conditions. Conditions may exist when the United States is engaged in hostilities against another country. The hostilities may or may not be conducted under a formal declaration.

(2) (U) Terrorist Attacks. Attacks may be executed by a foreign national

or U.S. citizen and are characterized by a deliberate, planned effort to attack key infrastructure USCYBERCOM relies on.

(3) (U) Natural and Technological Disasters. Any number of events may require a partial or total administrative and operational relocation to an alternate site. Factors for initiating relocation include, but are not limited to: hurricanes, fire, toxic emissions, earthquake, hazardous nuclear power plant emissions, sewer or power failures, contamination of water sources, health hazards, structural instability, or other disruptions to operations during which USCYBERCOM or USCYBERCOM facilities, are rendered unusable for normal operations.

(4) (U) By Direction. Commander, USCYBERCOM or his designated representative will activate all or specific portion(s) of this plan.

d. (U) Operations to be conducted.

(1) (U) COOP Phases. Since the exact nature, timing, or extent of a crisis cannot be precisely determined in advance, this directive outlines flexible options that can be adapted to any crisis situation. COOP planning and execution span four phases: Phase 0 - Pre-event, Phase 1 - Trans-event, Phase 2 - Continuity Operations, and Phase 3 - Post-event.

(a) (S) Phase 0 - Pre-Event Phase (Readiness and Preparedness). This phase consists of all tasks accomplished prior to execution of COOP plans. Actions are taken to decide, prepare, coordinate, and train to readiness standards. Plans and actions are coordinated, reviewed and staffed. In addition, timely alert, notification, coordination, and decision-making exercises are conducted to prepare personnel for a COOP event. USCYBERCOM J3 is the catalyst for pre-event activities. During this phase, consideration is given to phasing the relocation of personnel and resources to a USCYBERCOM COOP site. To reduce the vulnerability of the staff to a surprise attack or terrorist activity, the decision to relocate (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) personnel significantly minimizes the (b)(1) Sec 1.4(a) of a (b)(1) Sec 1.4(a) This phase ends with (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) event requiring COOP to be activated.

(b) (S) Phase 1 - Trans-Event Phase (Activation and Relocation) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) This phase commences with identification of a threat or event that may require a COOP response (b)(1) Sec 1.4(a) Actions are taken to decide, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) are critical during this phase. Notification of senior leaders is completed, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Succession to command decisions (b)(1) Sec 1.4(a) if necessary, the temporary

| | | |
|-------------------|------------------------------|-------------------|
| (b)(1) Sec 1.4(a) | Actions in this phase enable | (b)(1) Sec 1.4(a) |
| (b)(1) Sec 1.4(a) | This phase ends upon | (b)(1) Sec 1.4(a) |
| (b)(1) Sec 1.4(a) | | |

(c) (S) Phase 2 – Continuity Operations. During this phase, the

| | | |
|-------------------|-------------------|--|
| (b)(1) Sec 1.4(a) | | |
| for a | (b)(1) Sec 1.4(a) | leadership, directorate, and / or component leads will assist in coordinating and sustaining deployed staff requirements. During this phase, decision-makers will assess the impact of the event and determine the duration of operations from an alternate site(s). Actions include managing communications, logistics, transportation, personnel augmentation and rotation, as well as site and / or platform activities. This phase ends when planning is completed for the return (recovery) of deployed personnel, their functions, and C2 to a permanent site. |
| | | (b)(1) Sec 1.4(a) |
| (b)(1) Sec 1.4(a) | | |

(d) (S) Phase 3 - Post-Event (Reconstitution). During this phase, plans may be implemented for the return (recovery) of the MEFs, their functions, and C2 to a permanent operating location,

| | |
|-------------------|---|
| | (b)(1) Sec 1.4(a) |
| (b)(1) Sec 1.4(a) | Decision-makers will continue to assess the impact of the event and any emerging threats and determine the duration of conducting operations from alternate operating facilities. This concept of operations recognizes the need to function for a |
| (b)(1) Sec 1.4(a) | During this (b)(1) Sec 1.4(a) reconstitution actions will interlace with the operational performance of the MEFs. An estimate of the level and duration of the incident that required COOP plan implementation will be based on, but not limited to, the type and continued existence of threats, the severity of the damage, the ability to reconstitute the full staff, and the reliability of communications. If facilities are not available, they will, in turn contact other local bases, federal facilities, or begin searching for other real estate options to support the Command |
| (b)(1) Sec 1.4(a) | |

(b)(1) Sec 1.4(a) Depending on the amount of HQ Staff affected, CDRUSCYBERCOM or his designated representative can select directorates/special staff to relocate based on a given priority for the situation. While Phase 1 and 2 activities may be of short duration, Phase 3 activities may continue for an extended period of time. This phase ends when the USCYBERCOM Commander or his/her designated representative determines whether to reconstitute at the HQs facility (if conditions permit) or at an alternate site.

(2) (U) COOP Tiers. COOP implementation and mission offset revolve around a five-tiered concept of response based on the magnitude of the threat or impact of an actual event. While specific responses are associated with each of these five tiers for planning purposes, this is not intended to restrict the Commander's flexibility to respond to an actual situation using the best available means. The nature and scope of the emergency will dictate the appropriate response to any situation.

(a) (S) Tier 1 USCYBERCOM HQs Impaired. USCYBERCOM HQs in the (b)(1) Sec 1.4(a) has sustained some damage and parts are unusable such as localized flooding, fire, or structural damage (example: Virginia Earth Quake 2012). Individual directorates may be affected, but the HQs is still usable in some areas. The command will relocate and use unaffected areas within the HQs. In addition, personnel and functions may relocate to local COOP facilities in accordance with (IAW) directorate / component plans or as directed by the command. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) may have to execute their COOP Plan. Some personnel may be directed to go home and wait for further instructions.

(b) (S) Tier 2 HQs Unusable. Event renders USCYBERCOM HQ - (b)(1) Sec 1.4(a) completely unusable (example: Hurricane, Fire or Terrorist Attack). If USCYBERCOM is not able to perform MEFs and supporting tasks then CDR USCYBERCOM or his designed representative will determine if a devolment and/or transition of MEFs and supporting tasks to subordinate commands with augmentation considered. Sites will be determined based on the extent of damage and/or the impact resulting from events. This will also determine the decision for COOP. Affected personnel will relocate to COOP facilities IAW COOP or command guidance.

(c) (S) Tier 3 Installation Inaccessible. The threat or event renders USCYBERCOM - (b)(1) Sec 1.4(a) inaccessible and unusable (example: Chlorine release or Hurricane damage). All MEFs, and supporting tasks will be transitioned to alternate and / or COOP operating facilities. The transition of MEFs, and supporting tasks to subordinate commands with the level of augmentation considered. Sites will be coordinated with COOP plan development IOT achieve a successful relocation of selected missions, operations and personnel. Affected personnel will relocate to designated COOP facilities IAW directorate guidance or as directed by the command.

(d) (S) Tier 4 USCYBERCOM area (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

The MEFs, and supporting tasks will be

transitioned and performed as appropriate at the designated COOP facilities. The transition of MEFs, and support tasks to subordinate commands with augmentation will be considered. Sites will be determined based on the extent of damage and impact resulting from events requiring COOP. Affected personnel will relocate to COOP facilities IAW directorate guidance or as directed by the command.

(e) (S) Tier 5 (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
The MEFs will be transitioned as appropriate to the COOP site(s) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) The transfer of MEFs and supporting tasks to subordinate commands with augmentation will be considered. (b)(1) Sec 1.4(a) and coordinated (b)(1) Sec 1.4(a) IAW directorate or as directed by the command.

e. (U) Tasks.

(1) (U) All Directorates and Subordinate Commands.

(a) (U) Support USCYBERCOM J3 efforts to revise and maintain COOP Plan IAW DOD guidelines.

(b) (U) Participate in COOP Working Group (CWG) meetings.

(c) (U) With or without notice, be prepared to (BPT) execute the command COOP in order to be operational (b)(7)(e) or as specified in each individual MEF, after disruption by any event across the spectrum of (b)(7)(e) Units geographically separated from USCYBERCOM Headquarters (b)(7)(e) will independently execute COOP plans, as required, in response to events in their respective geographic locations.

(d) (U) BPT maintain contact with all personnel not included in the COOP for follow on orders and accountability.

(e) (U) Conduct biennial reviews:

1. (U) This Plan and respective Annex's, Appendixes, Tabs, and Exhibits.

2. (U) Coordinate or validate MOUs and/or MOAs with relocation facility hosts. This includes internal coordination with J3 approval for use of a distant relocation facility.

(f) (U) Annually provide COOP training to personnel, and within the first (b)(7)(e) new employee's arrival. Training will include (but not be limited to) the following:

1. (U) Emergency evacuation procedures.
2. (U) Directorate specific COOP responsibilities and actions.
3. (U) Recall procedures; update recall rosters as needed.

(g) (U) [redacted] (b)(7)(e) (or more frequently, as required), update and maintain MEFs.

(h) (U) Advise all MEF Personnel to develop/review/update family plans and emergency data forms. Continue to maintain / update MEF Personnel Rosters as needed.

(i) (U) Participate in Exercise COOP events [redacted] (b)(7)(e) as directed in order to:

1. (U) Validate current COOP actions and procedures.
2. (U) Verify required IT and communications capability, connectivity, accesses and collaboration tools at alternate locations.
3. (U) Train and exercise personnel on COOP actions, procedures and capabilities at the relocation sites.

(j) (U) Assign and maintain COOP POCs IAW the COOP Working Group (CWG) Charter.

(k) (S) Test COOP [redacted] (b)(1) Sec 1.4(a) procedures.

(2) (U) USCYBERCOM Directorates.

(a) (U) The USCYBERCOM Chief of Staff will: BPT stand-up the [redacted] (b)(7)(e)

(b) (U) Director USCYBERCOM J1 will: Provide required personnel, establish programs, and support the execution of this plan. Additional information is provided in Annex E.

(c) (U) Director USCYBERCOM J2 will: Provide CDRUSCYBERCOM and the Joint Operations Center (JOC) with COOP planning related intelligence situational awareness to include strategic and tactical indications and warning of threats to continuous USCYBERCOM operations.

(d) (U) Director USCYBERCOM J3 will:

1. (U) Be (Office of Primary Responsibility (OPR) for the USCYBERCOM COOP program.

2. (U) Maintain and update this plan as required.
3. (U) Provide all command personnel with an annual COOP awareness briefing.
4. (U) Ensure execution of J3 MEF's during COOP execution as described in ANNEX C.

(e) (U) Director USCYBERCOM J4 will:

1. (U) BPT Support the redeployment/movement of personnel to and from distributive locations.
2. (U) BPT to initiate 24 hour operations as needed.
3. (U) Provide logistics support in accordance with Annex D.

(f) (U) Director USCYBERCOM J5 will: BPT execute applicable parts of the COOP.

(g) (U) Director USCYBERCOM Capabilities Development Group (CDG) will:

1. (S) Develop and maintain a plan [REDACTED] (b)(1) Sec 1.4(a)

[REDACTED] (b)(1) Sec 1.4(a)

2. (U) BPT execute directorate COOP.

3. (S) Provide updates on [REDACTED] (b)(1) Sec 1.4(a)

[REDACTED] (b)(1) Sec 1.4(a) survivability and redundancy.

(h) (U) Director USCYBERCOM J7 will:

1. (U) Ensure COOP events and activities are incorporated into USCYBERCOM and other Combatant Command Tier 1 exercises and training events.

(i) (U) Director USCYBERCOM J8 will:

1. (U) Coordinate with appropriate organization to ensure emergency contracting and purchasing support.
2. (U) Identify deploying personnel to maintain COOP Government Purchasing Card (GPC) capability.
3. (U) Identify deploying personnel that can engage with appropriate contract authority on behalf of USCYBERCOM.

4. (U) Provide Headquarters contracting guidance and fund-site information upon COOP activation. Subordinate Command funding will be provided by their funding organization.

(3) (U) All USCYBERCOM Subordinate Commands, JFHQ-Cs, Service Components, and Task Forces.

(a) (U) Develop and maintain COOP plans. Completed plans will be provided to HQ USCYBERCOM J3 [redacted (b)(7)(e)] of headquarters plan approval dates and subsequent revision approval dates.

(b) (S) BPT accept the transfer of those HQ USCYBERCOM MEFs that have been [redacted (b)(1) Sec 1.4(a)] to a Sub-unified, JFCC, Component, or Task Force.

(c) (S) BPT to provide operational facilities and support to ensure COOP for HQ USCYBERCOM [redacted (b)(1) Sec 1.4(a)] as needed.

4. (U) Administration and Logistics.

a. (U) Concept of Support. See Concept of Operations in Annex C.

b. (U) Logistics

(1) (U) No-Warning Relocation. This situation could occur when an attack or incident is imminent, in progress, or there is a contingency precluding continued use of the USCYBERCOM facilities.

(2) (U) With Warning Relocation. Decision to relocate may be contingent on the same trigger event that drives an increase in tensions and Defense Readiness Condition (DEFCON), Force Protection Condition (FPCON), Information Operations Condition (INFOCON), Continuity of Government Readiness Conditions (COGCON), and/or Homeland Security National Terrorism Advisory System (NTAS) Alerts.

(3) (S) Personnel designated to relocate as part of this plan during a COOP contingency [redacted (b)(1) Sec 1.4(a)]

[redacted (b)(1) Sec 1.4(a)]
Personnel relocation may be conducted all at once or in phases as relocation options are implemented.

(4) (U) As relocation options are implemented and movements directed by senior leadership, the specific transportation requirements [redacted (b)(7)(e)] [redacted (b)(7)(e)] will be forwarded by their directorate to USCYBERCOM J4 for coordination. These requirements will be presented in writing from the proper approval authority. If an individual directorate is

unable to contact J4, then that organization will coordinate their own transportation (b)(7)(e)

(5) (U) Where possible, applicable memorandums of understanding and/or agreements should attempt to have host facilities provide all logistics support to implement this plan, to include housekeeping, facilities maintenance, billeting (where applicable), messing facilities, local transportation, medical, chemical warfare defense, security, services, and civil engineering support. J4 will coordinate an update to the Command Arrangement Agreement (CAA) with USTRANSCOM to address short-notice transportation and other mission support requirements.

(6) (U) Transportation plans are executable during duty and non-duty hours, with or without warning. Emergency short-notice relocation of key personnel may be directed by the CDRUSCYBERCOM at any time in order to enhance survivability of key personnel.

c. (U) Personnel. Many annex's and MEF documents establish essential personnel and administrative functions designed to meet USCYBERCOM needs in the event of a large-scale relocation or staff reconstitution.

d. (U) Public Affairs. The Office of Public Affairs (JO) is USCYBERCOM's office with primary responsibility for all Public Affairs (PA) actions that support CDRUSCYBERCOM and will provide information and recommendations on answers to the press on significant PA matters for COOP.

(1) (U) PA will work closely with the DOD, Joint Staff, and other agencies to provide PA planning for continuation of operations; develop contingency public statements and response to media queries, with supporting questions and answers, provide support for media briefings, establish a combined media center or a Joint Information Bureau as required, and develop internal information products and strategies to inform USCYBERCOM personnel and family members of COOP.

(2) (U) All queries received from the public, media organizations, or other organizations involved in gathering and disseminating information will be referred without comment to USCYBERCOM Public Affairs.

(3) (U) Command members shall not give information to the public even if material is unclassified or cleared through security and policy review and operational security channels unless the Commander, through PA, approves the release. This process avoids the release of potentially sensitive information or releases out of context, which could mislead the public.

e. (S) Medical. Medical support will be provided through local public First Aid Station/Clinics located near alternate facilities. Personnel are highly

encouraged to maintain a copy of their medical record, as access to the medical records on short notice may be difficult. Fly-away and MEF personnel will ensure they maintain an adequate quantity of prescription medicines on hand

(b)(1) Sec 1.4(a)

5. (U) Command and Control.

a. (U) Command.

(1) (U) Command Relationships. For planning purposes, it is assumed that the current command organizational structure, including all command relationships, will not change. Each annex or appendix will identify all command arrangement agreements, Memorandums of Agreement (MOA) and memorandums of understanding (MOUs) used and those that require development.

(a) (S) Additional Measure: If relocating to a pre-planned location, the

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

different locations depending on the event.

(2) (U) Succession to Command. The order of succession, the individuals responsible for assuming command will follow already established USCYBERCOM regulations and procedures and guidance. For positions other than the Commander, date of rank or position within that organization will determine who is in charge.

(a) (U) Orders of succession. Organizations and agencies are responsible for establishing, promulgating, and maintaining orders of succession to key positions. Such orders of succession are an essential part of an agency's COOP plan. Orders should be of sufficient depth to ensure the agency's ability to perform essential functions while remaining a viable part of the Federal Government through any emergency.

(b) (U) Command, Control, Communications, and Computer [C4] Systems. C4 systems play a critical role in the accomplishment of COOP activities. In general, we can assume that there has been significant disruption in C4 and that only basic C4 systems are functional. Each annex and appendix will cover what specific C4 requirements are needed to accomplish their MEFs.

b. (U) USCYBERCOM Support to Other Federal COOP Plans. USCYBERCOM could be required to provide support to other select government COOP plans during a COOP contingency. Support required by USCYBERCOM will be addressed in separately staffed agreements.

c. (U) Coordinating Instructions.

(1) (U) All tasked directorates and agencies will develop, coordinate, and forward to J3 procedures in the form of Annexes to support the USCYBERCOM COOP within 90-120 days of publication approval.

(2) (U) See ANNEXES for additional coordinating instructions and responsibilities.

(3) (U) Universal Coordinated Time (ZULU) will be used.

OFFICIAL

<F. M. LNAME>
RANK, SERVICE
POSITION, J-3



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 your 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.

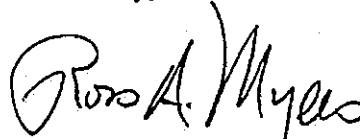
In accordance with 5 U.S.C. § 552, Freedom of Information Act, Exemptions 1 and 3, are hereby invoked, and require this information be withheld. The Exemption 3 Federal statute invoked is 10 U.S.C. § 130b, *Personally Identifying Information Regarding Personnel Assigned to an Overseas, Sensitive, or 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,

A handwritten signature in black ink, appearing to read "Ross A. Myers". The signature is written in a cursive, flowing style with a large initial "R".

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

18-R006

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

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

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

TO: COMFLT CYBERCOM FT GEORGE G MEADE MD
COMNAVIDFOR SUFFOLK VA
NAVNETWARCOM SUFFOLK VA
NAV CYBERDEFOPSCOM 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//

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

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/311009Z OCT13/13-0747//

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/ 110044Z OCT13/13-0747//

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/212105Z JUN13/-//

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/131033Z MAR14/14-0061//

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 (b)(1) Sec 1.4(a) 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) 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) (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 TO 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 mission essential tasks, with associated mission critical functions, as well as integrating (b)(1) Sec 1.7(e) critical 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) 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/uscycbercom/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/uscycbercom/Pages/RFI.aspx>)
JWICS: (<https://intelshare.intelink.ic.gov/sites/uscycbercom/request/Pages/RFI.aspx>)

5.F. (U//~~FOUO~~) USCYBERCOM CMF SIPRNET Intelink SharePoint portal (aka: Battle Roster):
(<http://intelshare.intelink.sgov.gov/sites/uscycbercom/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//



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

September 18, 2018

Susan Maret, PH.D
School of Information
Clark Hall
San Jose, CA, 95192

(b) (6)



Subject: FOIA Request (18-R016)

Dear Ms. Maret,

After conducting a thorough search in the J3 directorate at U.S. Cyber Command for your September 06, 2018 FOIA request. We did not locate records responsive to your request, nor have we created or maintained such records.

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 should cite case number 18-R016, and be clearly marked "Freedom of Information Act Appeal."

JOHN H. WILEY III
USCYBERCOM FOIA
Action Officer

USCYBERCOM/J0 FOIA
 9800 Savage Road, Suite 6171
 Fort George G. Meade, MD 20755

Dear FOIA officer,

Under the provisions of the Freedom of Information Act (FOIA), 5 U.S.C. §552, I request all records pertaining to

- USCYBERCOM's participation, including any staff training, in the YouTube Trusted Flagger program (see <https://support.google.com/youtube/answer/7554338?hl=en>).
- USCYBERCOM's reporting history under the YouTube Trusted Flagger program (see https://support.google.com/youtube/answer/7687979?hl=en&ref_topic=2803138).
- Any records pertaining to USCYBERCOM's communication with NGOs (nongovernmental organizations) who are involved with the Trusted Flagger program.

The Trusted Flagger program is described as "developed by YouTube to help provide robust tools for individuals, government agencies, and non-governmental organizations (NGOs) that are particularly effective at notifying YouTube of online content that violates Youtube's *Community Guidelines* (see <https://www.youtube.com/yt/about/policies/#community-guidelines>).

To assist your agency in assessing any fees, I am an academic researcher who is working on a project related to the above request and will widely share information in an upcoming publication. Release of these records is not primarily in my commercial interest. Furthermore, release of these records is of scholarly and public interest, and greatly enhances knowledge of USCYBERCOM's domestic activities as it relates to moderating content on the YouTube platform. Therefore, I respectfully request a waiver of fees under 5 U.S.C. Section 552(a) (4) (A) (iii).

Please note that 5 U.S.C. Section 552(a) (4) (A) (iv) (II) requires that you provide the first 100 copies to me at no charge and remainder of materials at 10 cents per page. If there are any agency fees assessed for searching, reviewing, or copying materials, I would like to be contacted before your agency tasks my request. I am happy to receive information in various formats (e.g., .pdf, .doc, DVD, email).

Thank you,

Susan

Susan Maret, Ph.D.
School of Information
Clark Hall
San Jose State University
San Jose, CA, 95192



(b) (6)



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

October 4, 2018

Michael Martelle
The National Security Archive
The George Washington University
Gelman, Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037

Subject: FOIA Request (18-R017)

Dear Mr. Martelle,

After conducting a thorough search in the J3 directorate and corresponding directly with Dr. Stephen Orr, referencing FOIA request 18-R017, we did not locate responsive records nor have we created or maintained such records.

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 should cite case number 18-R016, and be clearly marked "Freedom of Information Act Appeal."

A handwritten signature in black ink, reading "John H. Wiley III", followed by a stylized flourish.

JOHN H. WILEY III
USCYBERCOM FOIA
Action Officer

Michael Martelle

18-R017

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

USCYBERCOM/IO FOIA
9800 Savage Road, Suite 6171
Fort George G. Meade, MD 20755

Re: Request under the FOIA, in reply refer to Archive# **20181017CYB005**

Dear :

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

Any materials prepared for the following presentations to the Defense Science Board Task Force on Cyber as a Strategic Capability:

1. *Perspective on USCYBERCOM Capabilities and Modalities given by Dr. Stephen Or IV on 05-06 Oct 2016*
2. *USCYBERCOM Perspective given by RADAM T.J. White on 05-06 Oct 2016*
- ✓ 3. *Briefing on Operational Strategy given by Dr. Richard Harknett on 05-06 Oct 2016*
4. *Briefing on the Joint Intelligence Operations Center given by CAPT Mike Studeman on 30 Nov-1 Dec 2016*
- ✓ 5. *Briefing on Global Cyberspace Operations Synchronization(GCOS) given by COL Stephen Letcher on 21-22 Feb 2017*
6. *Briefing on the USCYBERCOM Excursion-Cyber Innovation Lab given by Col Mike Burke of the Cyber National Mission Force on 21-22 Feb 2017*
7. *The USCYBERCOM-CIO Perspective presented by Mr. G. Dennis Bartko of the USCYBERCOM Capabilities Development Group on 04-05 Apr. 2017*
- 8). *Briefing on Operation GLOWING SYMPHONY given by Brig Gen. Tim Haugh and Capt Steve Donald of JTF-Ares on 30 Nov-1 Dec 2016*

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.



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

NOV 07 2018

Michael Martelle
The National Security Archive
Gelman Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037

Dear Mr. Martelle,

Thank you for your September 9, 2018 Freedom of Information Act (FOIA) request for the "USCYBERCOM-CIO Perspective" presented by the Capabilities Development Group (CDG) on April 4-5, 2017.

After a thorough search of our files, U.S. Cyber Command did not locate the requested record.

If you are not satisfied with our action on this request, you may file an administrative appeal within 90 calendar days from the date of this letter by U.S. mail or email. If you submit your appeal in writing, please address it to ODCMO, Director of Oversight and Compliance, 4800 Mark Center Drive, ATTN: DPCLTD, FOIA Appeals, Mailbox #24, Alexandria VA 22350-1700. If you submit your appeal by email please send it to OSD.FOIA-APPEAL@mail.mil. All correspondence should reference U.S. Cyber Command case tracking number 19-R015.

Additionally, you may contact the Office of Government Information Services (OGIS), which provides mediation services to help resolve disputes between FOIA requesters and Federal agencies. Contact information is 8601 Adelphi Road – OGIS, College Park, MD 20740-6001. OGIS may also be reached at ogis@nara.gov, 202-741-5770, and 1-877-684-6448.

Sincerely,

A handwritten signature in black ink, reading "Paul R. Guevin III".

PAUL R. GUEVIN III, GG15, DAF
Chief Knowledge Officer

Michael Martelle

18-R023

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

USCYBERCOM/JO FOIA
9800 Savage Road, Suite 6171
Fort George G. Meade, MD 20755

Re: Request under the FOIA, in reply refer to Archive# **20181017CYB005**

Dear :

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

Any materials prepared for the following presentations to the Defense Science Board Task Force on Cyber as a Strategic Capability:

1. *Perspective on USCYBERCOM Capabilities and Modalities given by Dr. Stephen Or IV on 05-06 Oct 2016*
2. *USCYBERCOM Perspective given by RADAM T.J. White on 05-06 Oct 2016*
- ✓ 3. *Briefing on Operational Strategy given by Dr. Richard Harknett on 05-06 Oct 2016*
4. *Briefing on the Joint Intelligence Operations Center given by CAPT Mike Studeman on 30 Nov-1 Dec 2016*
- ✓ 5. *Briefing on Global Cyberspace Operations Synchronization(GCOS) given by COL Stephen Letcher on 21-22 Feb 2017*
6. *Briefing on the USCYBERCOM Excursion-Cyber Innovation Lab given by Col Mike Burke of the Cyber National Mission Force on 21-22 Feb 2017*
7. *The USCYBERCOM-CIO Perspective presented by Mr. G. Dennis Bartko of the USCYBERCOM Capabilities Development Group on 04-05 Apr. 2017*
8. *Briefing on Operation GLOWING SYMPHONY given by Brig Gen. Tim Haugh and Capt Steve Donald of JTF-Ares on 30 Nov-1 Dec 2016*

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.



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

NOV 11 2018

Michael Martelle
The National Security Archive
Gelman Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037

Dear Mr. Martelle,

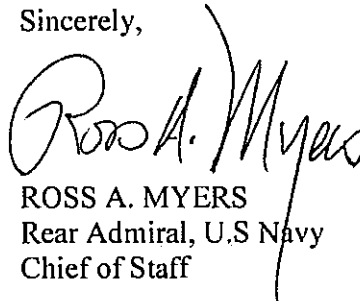
Thank you for your September 21, 2018 Freedom of Information Act (FOIA) request for materials related to the Cyber Components Commander Conference on October 22, 2013.

As the initial denial authority, I am partially denying portions of the document under 5 U.S.C. §§ 552(b)(1) and (b)(3). The denied portions include classified national security information under the criteria of Executive Order 13526 (labeled as (b)(1)) and personally identifying information regarding personnel assigned to a sensitive unit exempt from disclosure under 10 U.S.C. § 130b (labeled as (b)(3)). U.S. Cyber Command is a sensitive unit.

If you are not satisfied with our action on this request, you may file an administrative appeal within 90 calendar days from the date of this letter by U.S. mail or email. If you submit your appeal in writing, please address it to ODCMO, Director of Oversight and Compliance, 4800 Mark Center Drive, ATTN: DPCLTD, FOIA Appeals, Mailbox #24, Alexandria VA 22350-1700. If you submit your appeal by email please send it to OSD.FOIA-APPEAL@mail.mil. All correspondence should reference U.S. Cyber Command case tracking number 19-R021.

Additionally, you may contact the Office of Government Information Services (OGIS), which provides mediation services to help resolve disputes between FOIA requesters and Federal agencies. Contact information is 8601 Adelphi Road – OGIS, College Park, MD 20740-6001. OGIS may also be reached at ogis@nara.gov, 202-741-5770, and 1-877-684-6448.

Sincerely,


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

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

Friday, September 21, 2018

9800 Savage Road, Suite 6171
Fort George G. Meade, MD 20755

Re: Request under the FOIA, in reply refer to Archive# **20181232CYB013**

Dear :

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

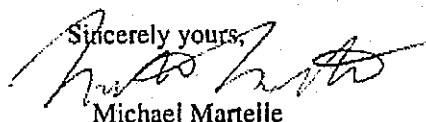
Any materials related to the Cyber Components Commander Conference on October 22, 2013 including but not limited to conference proceedings or briefing material.

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,



Michael Martelle



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

AGENDA

Cyber Component Commanders Meeting
22 October 2013
1300-1630

Protocol:
CAG Rep:

(b)(3) 130b

969-2951s or
969-3791s /

(b)(3) 130b

969-2540s /

(b)(3) 130b

AS OF: 21OCT13

UNIFORM:

MILITARY: DUTY UNIFORM

CIVILIAN: BUSINESS

| Time | Presentation Title and Presenter | Location |
|-----------|--|----------|
| 1300-1315 | (U// FOUO) Welcome and Opening Remarks GEN Keith B. Alexander, USA, CDR USCYBERCOM/DIRNSA/CHCSS | DSCR |
| 1315-1345 | (U// FOUO) Cyberspace Operations and Planning Update (b)(3) 130b USAF, USCYBERCOM J3 | DSCR |
| 1345-1400 | (U// FOUO) CMF Training and Exercises Update (b)(3) 130b USAF, USCYBERCOM J7 | DSCR |
| 1400-1410 | (U// FOUO) Break | |
| 1410-1530 | (U// FOUO) Component Commander Updates on CMF/JFHQ Builds and Service-Specific Shutdown/Sequestration Issues | DSCR |
| 1530-1615 | (U// FOUO) Component Commander Discussions <i>Topics Include:</i> (b)(1) Sec 1.7(e) -Impact of Shutdown on Operations and CMF Builds -Joint Cyber Warrior Education Program (JCWEP) Feedback | DSCR |
| 1615-1630 | (U// FOUO) Closing Remarks GEN Keith B. Alexander, USA, CDR USCYBERCOM/DIRNSA/CHCSS | DSCR |
| 1630 | Depart | |

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



Cyber Mission Force Training & Cyber Flag Update

22 October 2013

(b)(3) 130b

Director of Joint Exercises and Training (J7), USCYBERCOM

The overall classification of this briefing is: UNCLASSIFIED//~~FOUO~~



Shutdown Impact on CMF Training

UNCLASSIFIED

Furlough Impact on 1st Qtr FY14 CMF Training Schedule:

- **17x** FY13-funded courses **delayed minimum of 21 days** (impacts ~323 students & 219,640hrs lost)
 - Re-starts beginning 21 Oct...(rescheduled classes will retain original rosters)
 - Courses: CYBR3800 /CYEC2200/ NETO4012 /CRSK1000/ CYBR1010 /NETA1030 /COMP1100/ CYBR3100 /COMP2050/ NETA2008
- **8x** FY13-funded courses **require additional funding** to be rescheduled (impacts ~166 students & 53,120hrs)
 - Earliest can resume 28 Oct, if original students are available to attend training--otherwise minimum of 28 day delay to restart (Still verifying original student availability)
 - Contracting Officer working with Vendors to assess specific contract penalties/costs for rescheduling
 - Courses: CYBR1200/CYBR1040/NETW3006 /CYBR2005 /NETO4000 /NETW1002 /NETW3004 /NETO4000
- **44x** FY14-funded courses now **delayed until FY14 funds received** (impacts ~913 students & 5,384hrs)
- JCWEP was **delayed 5 days** and the CYBR2005 (Advanced Security Essentials -5 days) block postponed
- **25x** students **delayed Joint Network Attack Course (JNAC)** by 2 weeks
 - Rescheduling 15 Oct class with 28 Oct start (25 CMF attendees) forces 19 Nov class to require swing shift and will run second shift through 22 Nov--goes back to normal day shift 25 Nov
- **19x** students for one full **Mission Commanders Course lost opportunity** (2 week course & 1,520hrs) due to shift in schedule and conflicting instructor commitments
- Shutdown potentially impacting FY14 Battle Rostered names--currently only 66 names against FY14 teams and minimal training requirements scheduled

UNCLASSIFIED



Cyber Flag 14-1 Update

- BLUF: "Reduced Scope" Exercise--20% redux in attendees and schedule...canx'd DV Day 6 Nov
- **Changes to footprint** ~72pax of 490 (~20%): Focused on keeping Blue & OPFOR intact
 - Keep # of teams as planned (no cuts to on-keyboard blue players, just some "overhead" trimming)
 - Cut White Cell by 50 (~40% reduction)
 - Cut Assessors by 12
 - Cut Support staff by 10
- **Timeline:** Cutting 4 days off the front end of schedule (Execution now 1-7 Nov)
 - 13 Oct - Advanced Team/Prep depart
 - 14 Oct - Projected equipment arrival date
 - 14-29 Oct - Local Network Build/Integration/Testing/Final Snapshots
 - 29 Oct - Main Body Travel
 - 30 Oct - Registration/Academics
 - 31 Oct - Range Familiarization/Dress Rehearsal
 - 1-7 Nov - Execution/Vulnerability windows (no intermission/mission planning at halfway point)
 - 8 Nov - Hotwash SVTC (TBD)
- **As of 22 Oct:**
 - **29 Personnel Advanced Team** on site performing setup/test
 - **Equipment successfully shipped/received**--still awaiting 2GB TACLANes from JIOR (Norfolk) ETA Wednesday, 23 Oct
 - **Local Network/Exercise build** 90% complete external connectivity testing begins 23 Oct
 - Showstoppers: None



UNCLASSIFIED

Questions/Discussion?

UNCLASSIFIED



Back Up Slides

Training Pipeline and Training Status Templates



POC and Reference Links

UNCLASSIFIED//~~FOUO~~

- J7 POCs

- NMTs/NSTs/CSTs (b)(3) 130b
- CMTs (b)(3) 130b
- NMTs/CPTs (b)(3) 130b
- CPTs (b)(3) 130b

Other references on NSANet:
• “Go ELM” for pre-requisites
• “Go ITP”

- ADET Scheduling POCs

- (b)(3) 130b
- (b)(3) 130b (CYEC/NETW/NETO/COMP/CYBR)
- (b)(3) 130b (NETA/CRSK/RPTG/ANSK)
- (b)(3) 130b (NETO3200/CYBR3800)

- J7 Portal – Standards, workrole pipelines, Cyber Development Plans, JQRs, etc...

[http://intelshare.intelink.ic.gov/sites/uscypercom/j7/CMF Training/Training/Form s/AllItems.aspx](http://intelshare.intelink.ic.gov/sites/uscypercom/j7/CMF%20Training/Training/Form%20s/AllItems.aspx)

- ADET Portal – Training Schedule, Service Requirements Spreadsheet, etc...

<https://ls.icrf.nsa.ic.gov/adet/org/college-cryptology/cno/cmfsite/CMF%20Training%20Seat%20Requirements/Forms/AllItems.aspx>

UNCLASSIFIED//~~FOUO~~

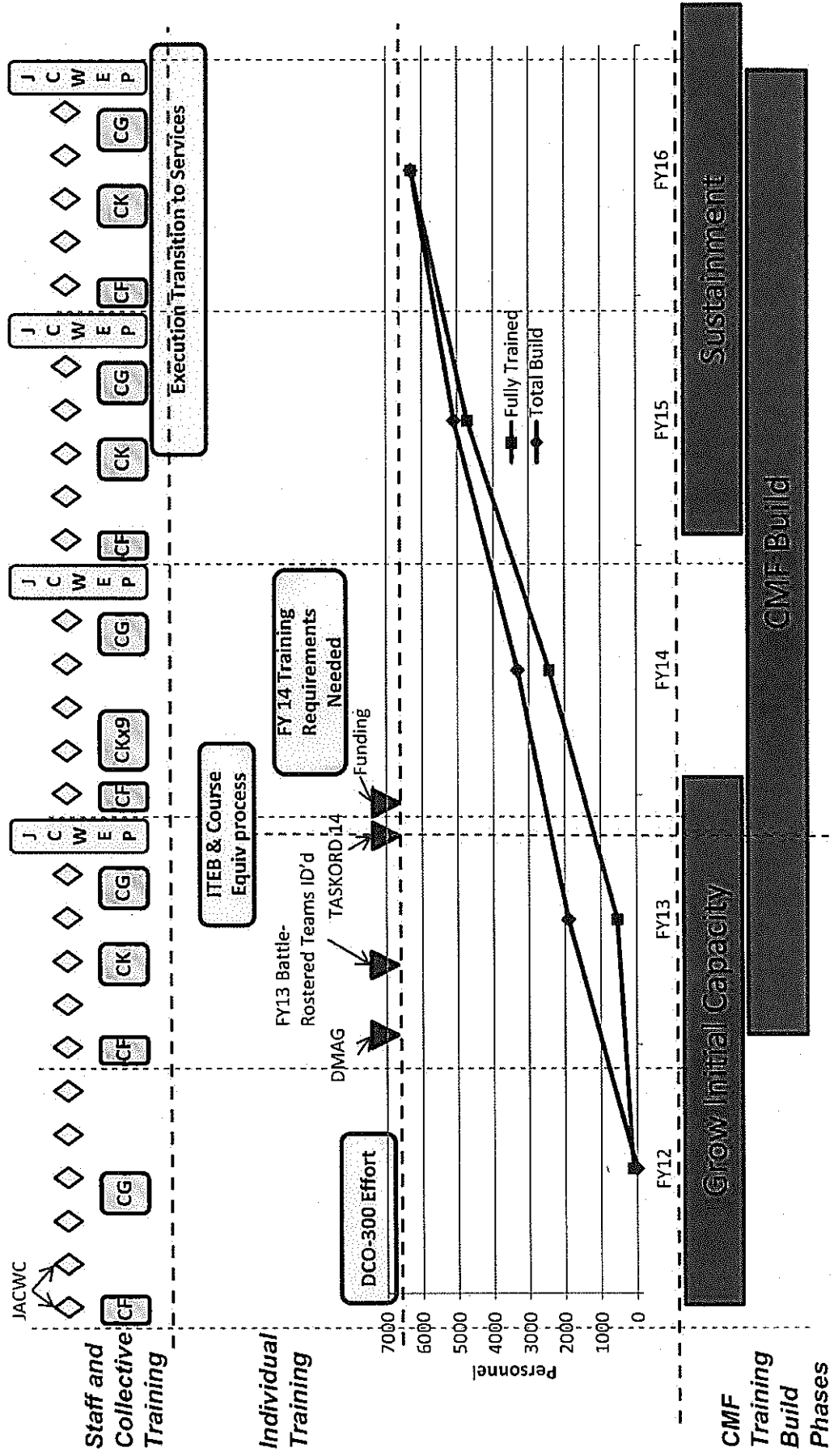


CMF Training Challenges/Mitigations

| Challenges | Mitigations |
|--|--|
| <ul style="list-style-type: none"> • Course Requirements Scheduling & Throughput • Training Pipeline Stabilization • Grandfathering experience/training • Intermediate Cyber Core (ICC) for CPT • JACWC (CMF leadership training) • Red/Blue/Hunt Methodologies Training (for non-National CPTs) | <ul style="list-style-type: none"> • Training products locked 17 Jul and posted to CMF Training Portal • Individual Training Equivalency Board and Course Equivalency processes easing demands on training pipeline • Alternate ICC (ALTICC) and ALTICC Cohorts built/offered along with Service course equivalency process (e.g. 24th AF's INWT) • Approved PACWC variant/pilot and priority for CMF in Oct & FY14 classes • Working with J34/5 to identify specific methodology requirements; training development effort will follow |
| <ul style="list-style-type: none"> • Workrole/Functional Job Qualification Requirements (JQRs) | <ul style="list-style-type: none"> • JQR team completed writing/staffing of all 28 CPT JQRs • CMF JQR TASKORD (19 Sep) for remainder of CMF non-CPT positions • Developed IOO and Auditor JQRs for staffing to alleviate sponsorship |
| <ul style="list-style-type: none"> • Mission Assignment/Alignment Training Impacts | <ul style="list-style-type: none"> • Working in concert with J2/J3/CNMF/NSA on Mission Alignment Board process to ensure ability to attend sponsorship-required training |
| <ul style="list-style-type: none"> • Collective training standards • Tasks, Conditions & Standards identified • Team Certification • JF HQ Certification • CNMF HQ Certification | <ul style="list-style-type: none"> • Build of Training & Readiness (T&R) Manual captures CMF-specific training standards for individual thru collective training--est Feb 14 • Cyber Knight/Guard/Flag w/Svc Cyber Components inform T&R Manual task, conditions, and standards • CFIST developing Joint Mission Essential Tasks (JMETS) for JF HQ • Expanding "Cyber" series of events in FY14 to inform Service presentation of forces |
| <ul style="list-style-type: none"> • Career planning and retention | <ul style="list-style-type: none"> • Work force development working group working with services on identifying critical work roles for retention |
| <ul style="list-style-type: none"> • Funding • Projected RMD funding estimate • TDY Funding | <ul style="list-style-type: none"> • RMD funded, but "fragile" based on fiscal environment • Mitigated by leveraging 4 National Cryptologic System (NCS) centers--USCYBERCOM TDY funding provided by exception for non-NCS courses |



CMF Training History...getting to glideslope



Joint Advanced Cyber Warfare Course (JACWC)



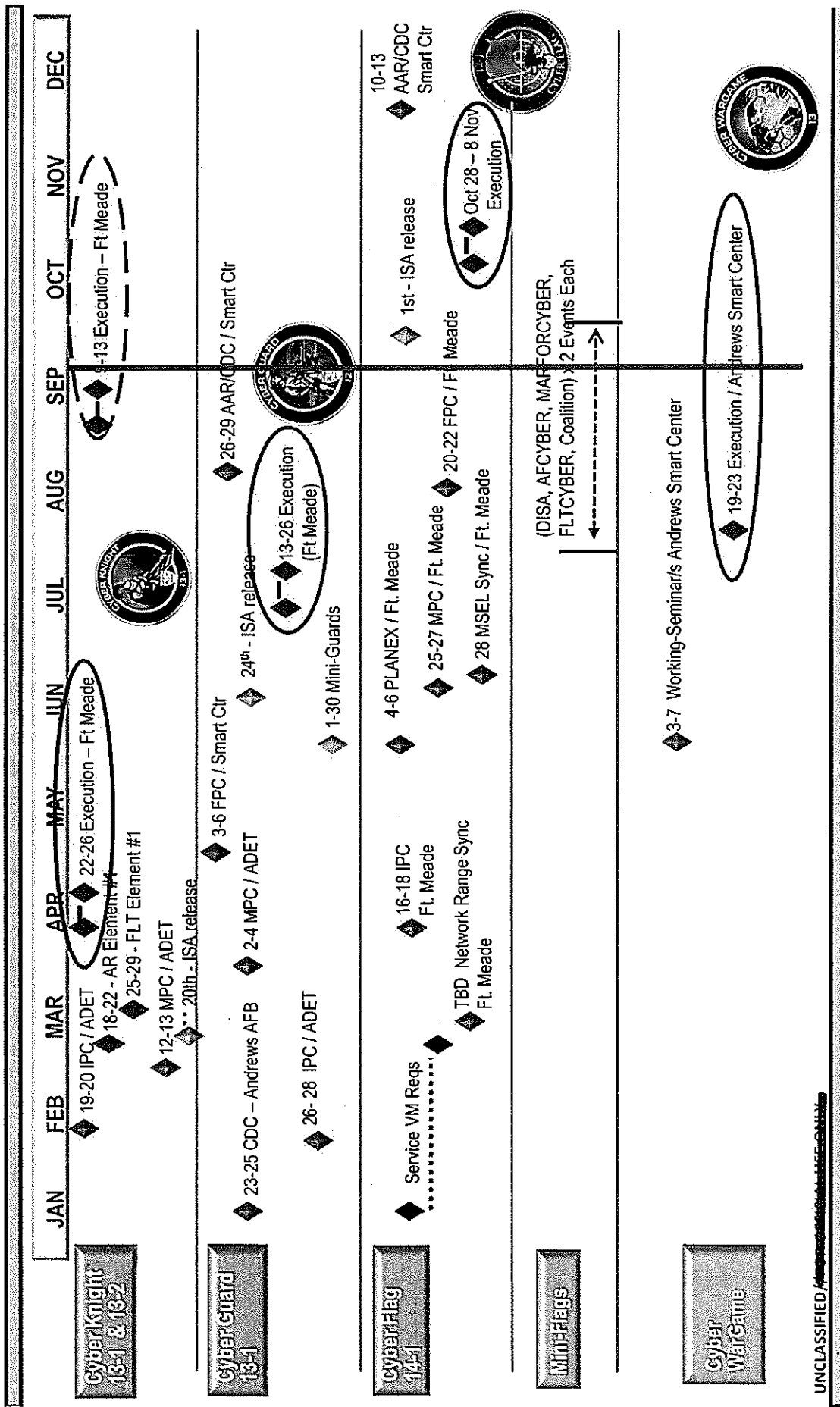
CMF Training "Template"

- Training Template is a Leadership Tool to help track each individual teams training progress
- Will help forecast future training requirements (i.e. people, \$, schedule)
- Aggregated data will answer the "glide slope" question

(b)(1) Sec 1.7(e), (b)(3) 130b



USCYBERCOM 2013 Exercises & Wargame





Cyber Component Commanders Meeting (22 October 2013)

The overall classification of this briefing is: ~~TOP SECRET//SI//NOFORN~~

Classified By (b)(3) 130b
Derived From: USCYBERCOM/SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380901



Cyber Component Commanders Meeting (22 October 2013) *Cyberspace Operations*

(b)(3) 130b

USCYBERCOM J3

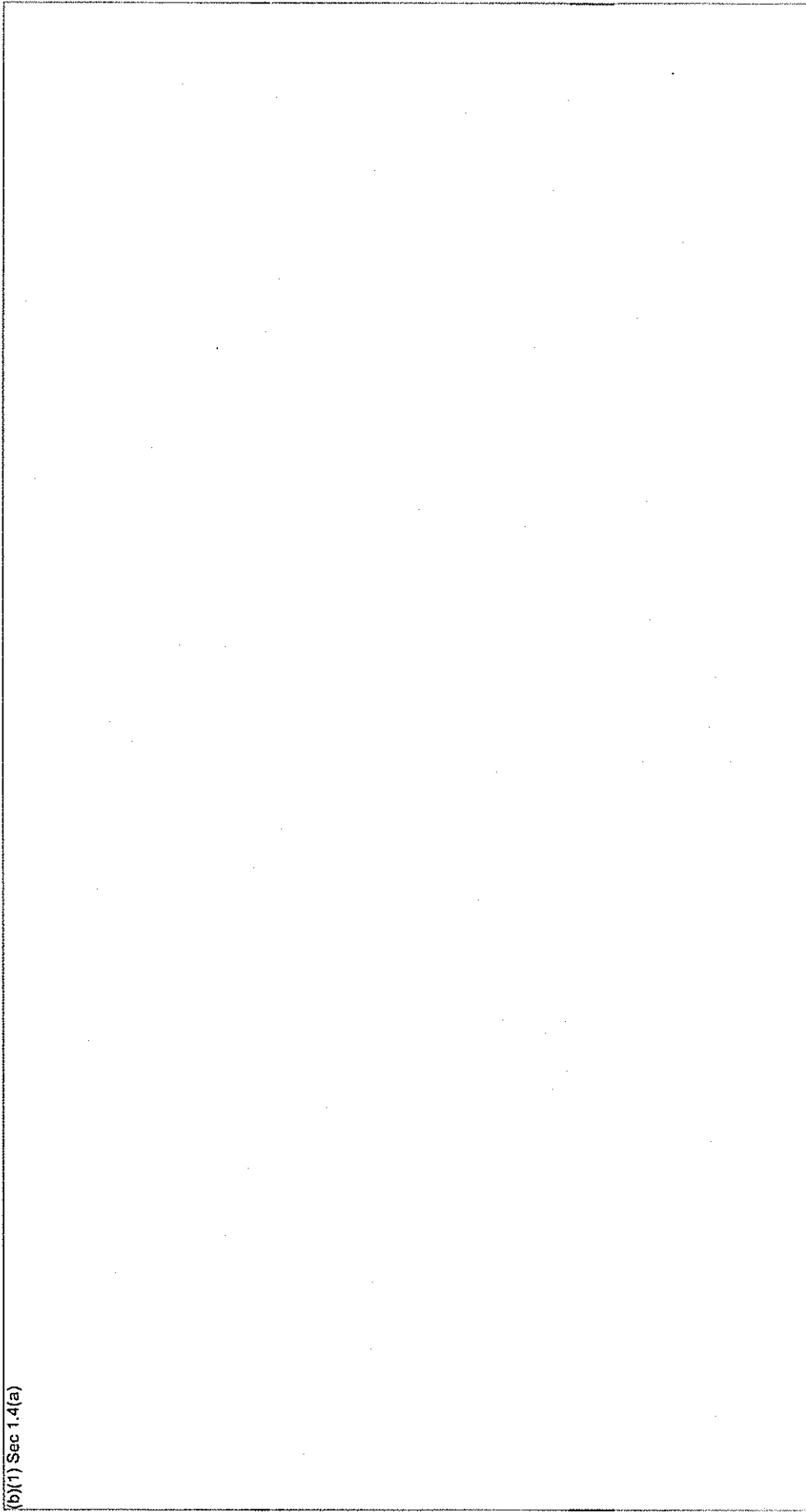
The overall classification of this briefing is: ~~TOP SECRET//SI//~~FOUO~~~~

Classified By: (b)(3) 130b
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380901



(U) Operations & Planning Update

(b)(1) Sec 1.4(a)



(b)(3) 130b

•(U//~~FOUO~~) Presentation brief to J3

DISA) scheduled 24 Oct, STRATCOM on

28OCT



Cyber Mission Force: FY13 – FY14 Build

(b)(1) Sec 1.4(a)

USA = ☐ USAF = ☐ USMC = ☐ USN = ☐

National Mission Teams

National Support Teams

National Cyber Protection Teams

DoDIN Cyber Protection Teams

(b)(1) Sec 1.4(a)

Combat Mission Teams

Combat Support Teams

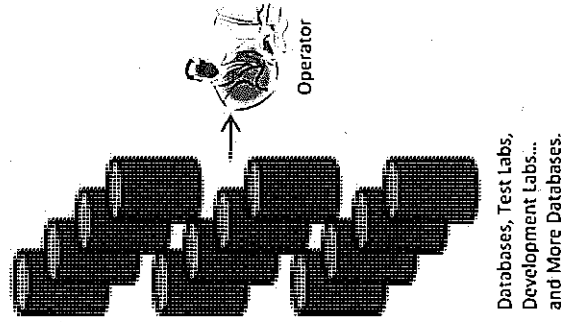
CCMD Cyber Protection Teams

Service Cyber Protection Teams

(b)(1) Sec 1.4(a)



Current State – Intelligence Centric Platform



(b)(1) Sec 1.4(a)

Planners,
Targeteers, Linguists,
TOPIs, R&T Analysts,
Developers, Testers,
Fires Support
Personnel,
Etc.

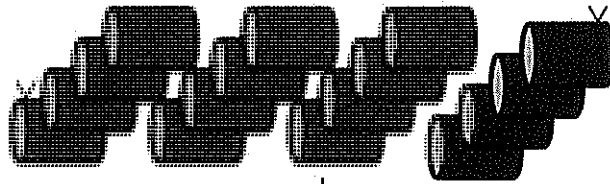
(b)(1) Sec 1.4(a)



Future Strategy



Planners,
Targeteers, Linguists,
TOPIs, R&T Analysts,
Developers, Testers,
Fires Support
Personnel,
Etc.



Databases, Test Labs,
Development Labs
etc.

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)



Cyber Component Commanders Meeting

(22 October 2013)

Cyber Mission Force Training and Cyber Flag Update

(b)(3) 130b

USCYBERCOM J7

The overall classification of this briefing is: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Classified By: (b)(3)

Derived From: USCYBERCOM SCG

Dated: 20111011

AND

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380901



Shutdown Impact on CMF Training

UNCLASSIFIED

Furlough Impact on 1st Qtr FY14 CMF Training Schedule:

- **17x** FY13-funded courses **delayed minimum or 21 days** (impacts ~323 students & 219,640hrs lost)
 - Re-starts beginning 21 Oct...(rescheduled classes will retain original rosters)
 - Courses: CYBR3800 /CYEC2200/ NETO4012 /CRSK1000/ CYBR1010 /NETA1030 /COMP1100/ CYBR3100 /COMP2050/ NETA2008
- **8x** FY13-funded courses **require additional funding** to be rescheduled (impacts ~166 students & 53,120hrs)
 - Earliest can resume 28 Oct, if original students are available to attend training--otherwise minimum of 28 day delay to restart (Still verifying original student availability)
 - Contracting Officer working with Vendors to assess specific contract penalties/costs for rescheduling
 - Courses: CYBR1200/CYBR1040/NETW3006 /CYBR2005 /NETO4000 /NETW1002 /NETW3004 /NETO4000
- **44x** FY14-funded courses now **delayed until FY14 funds received** (impacts ~913 students & 1,606,880 hrs)
- JCWEP was **delayed 5 days** and the CYBR2005 (Advanced Security Essentials -5 days) block postponed
- **25x** students **delayed Joint Network Attack Course (JNAC)** by 2 weeks
 - Rescheduling 15 Oct class with 28 Oct start (25 CMF attendees) forces 19 Nov class to require swing shift and will run second shift through 22 Nov--goes back to normal day shift 25 Nov
- **19x** students for one full **Mission Commanders Course lost opportunity** (2 week course & 1,520hrs) due to shift in schedule and conflicting instructor commitments
- Shutdown potentially impacting FY14 Battle Rostered names--currently only 66 names against FY14 teams and minimal training requirements scheduled

UNCLASSIFIED

8



Cyber Flag 14-1 Update

- BLUF: "Reduced Scope" Exercise--20% redux in attendees and schedule...canx'd DV Day 6 Nov
- **Changes to footprint** ~72pax of 490 (~20%): Focused on keeping Blue & OPFOR intact
 - Keep # of teams as planned (no cuts to on-keyboard blue players, just some "overhead" trimming)
 - Cut White Cell by 50 (~40% reduction)
 - Cut Assessors by 12
 - Cut Support staff by 10
- **Timeline:** Cutting 4 days off the front end of schedule (Execution now 1-7 Nov)
 - 13 Oct - Advanced Team/Prep depart
 - 14 Oct - Projected equipment arrival date
 - 14-29 Oct - Local Network Build/Integration/Testing/Final Snapshots
 - 29 Oct - Main Body Travel
 - 30 Oct - Registration/Academics
 - 31 Oct - Range Familiarization/Dress Rehearsal
 - 1-7 Nov - Execution/Vulnerability windows (no intermission/mission planning at halfway point)
 - 8 Nov - Hotwash SVTC (TBD)
- **As of 22 Oct:**
 - **29 Personnel Advanced Team** on site performing setup/test
 - **Equipment successfully shipped/received**--still awaiting 2GB TACLANes from JIOR (Norfolk) ETA Wednesday, 23 Oct
 - **Local Network/Exercise build** 90% complete external connectivity testing begins 23 Oct
 - Showstoppers: None



UNCLASSIFIED

Questions/Discussion?

UNCLASSIFIED

10



Cyber Component Commanders Meeting (22 October 2013)

**Next Meeting:
22 November 2013, 0830-1300**

The overall classification of this briefing is: ~~TOP SECRET//SI//FOUO~~

Classified By: (b)(3) 130b
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380901



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

NOV 11 2018

Michael Martelle
The National Security Archive
Gelman Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037

Dear Mr. Martelle,

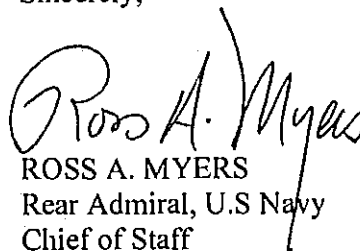
Thank you for your September 21, 2018 Freedom of Information Act (FOIA) request for the Deputy Commander's memorandum establishing Initial Operational Capability (IOC) Designation of Joint Force Headquarters Cyber (JFHQ-C).

As the initial denial authority, I am partially denying portions of the document under 5 U.S.C. § 552(b)(3). The denied portions contain personally identifying information regarding personnel assigned to a sensitive unit exempt from disclosure under 10 U.S.C. § 130b (labeled as (b)(3)). U.S. Cyber Command is a sensitive unit.

If you are not satisfied with our action on this request, you may file an administrative appeal within 90 calendar days from the date of this letter by U.S. mail or email. If you submit your appeal in writing, please address it to ODCMO, Director of Oversight and Compliance, 4800 Mark Center Drive, ATTN: DPCLTD, FOIA Appeals, Mailbox #24, Alexandria VA 22350-1700. If you submit your appeal by email please send it to OSD.FOIA-APPEAL@mail.mil. All correspondence should reference U.S. Cyber Command case tracking number 19-R023.

Additionally, you may contact the Office of Government Information Services (OGIS), which provides mediation services to help resolve disputes between FOIA requesters and Federal agencies. Contact information is 8601 Adelphi Road – OGIS, College Park, MD 20740-6001. OGIS may also be reached at ogis@nara.gov, 202-741-5770, and 1-877-684-6448.

Sincerely,


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

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

Friday, September 21, 2018

9800 Savage Road, Suite 6171
Fort George G. Meade, MD 20755

Re: Request under the FOIA, in reply refer to Archive# **20181229CYB010**

Dear :

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

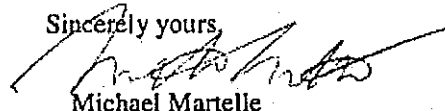
"The Deputy Commander memorandum for Service Cyber Component Commanders Establishing Initial Operational Capability (IOC) Designation of Joint Force Headquarters - Cyber (JFHQ-C)" issued September 30, 2013.

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,



Michael Martelle

~~UNCLASSIFIED FOR OFFICIAL USE ONLY~~



DEPARTMENT OF DEFENSE

Reply to
USCYBERCOM DCDR
9800 SAVAGE RD, STE 6477
Ft Meade, Maryland 20755

001032013

MEMORANDUM FOR COMMANDER, ARMY CYBER COMMAND
COMMANDER, FLEET CYBER COMMAND
COMMANDER, AIR FORCE CYBER COMMAND
COMMANDER, MARINE FORCES CYBER COMMAND

Subject: (U) Initial Operational Capability (IOC) Designation of Joint Force Headquarters
Cyber (JFHQ-C)

References: (a) (U) GEN Alexander's Email to Service Component Commanders,
dated 28 Aug 13 (U FOUO)
(b) (U) Joint Publication 3-12 (U FOUO)

1. (U ~~FOUO~~) Per ref (a), declare IOC for JFHQ-C as soon as the headquarters is capable of executing the tasks, functions, and processes contained in Enclosure A. Notify this command of your decision to declare IOC.

2. (U ~~FOUO~~) Notification certifies the JFHQ-C can execute the six mission essential tasks with associated mission critical functions, as well as integrate with the seven critical U.S. Cyber Command (USCYBERCOM) operational processes described in Enclosure A and ref (b). Formal codification of individual and collective training certification standards for Full Operational Capability will be collaboratively developed and promulgated in a Training & Readiness Manual.

3. (U) My POC for this matter is (b)(3) 130b

(b)(3)
130b

Jon M Davis
JON M DAVIS
Lieutenant General, USMC
Deputy Commander

Attachment
Enclosure A: (U) JFHQ-C Certification slide presentation (U FOUO)

Copy to
Director, Cyber National Mission Force
Director, Defense Information Systems Agency
USCYBERCOM CoS, All Directorates, Staff Judge Advocate



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

Michael Martelle
The National Security Archive
Gelman Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037

NOV 28 2018

Dear Mr. Martelle,

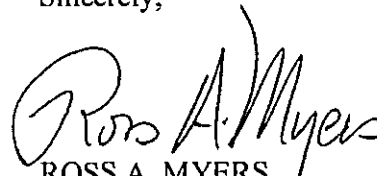
Thank you for your October 4, 2018 Freedom of Information Act (FOIA) request for the JTF-ARES briefing on OPERATION GLOWING SYMPHONY given in November 2016.

After careful consideration, U.S. Cyber Command is withholding the briefing in its entirety. As the initial denial authority, I am denying the information under 5 U.S.C. § 552(b)(1) and (b)(3). The briefing contains classified national security information under the criteria of Executive Order 13526 (labeled as (b)(1)) and defense critical infrastructure security information exempt from disclosure under 10 U.S.C. § 130e (labeled as (b)(3)).

If you are not satisfied with our action on this request, you may file an administrative appeal within 90 calendar days from the date of this letter by U.S. mail or email. If you submit your appeal in writing, please address it to ODCMO, Director of Oversight and Compliance, 4800 Mark Center Drive, ATTN: DPCLTD, FOIA Appeals, Mailbox #24, Alexandria VA 22350-1700. If you submit your appeal by email please send it to OSD.FOIA-APPEAL@mail.mil. All correspondence should reference U.S. Cyber Command case tracking number 19-R016.

Additionally, you may contact the Office of Government Information Services (OGIS), which provides mediation services to help resolve disputes between FOIA requesters and Federal agencies. Contact information is 8601 Adelphi Road – OGIS, College Park, MD 20740-6001. OGIS may also be reached at ogis@nara.gov, 202-741-5770, and 1-877-684-6448.

Sincerely,


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

Michael Martelle

18-R024

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

USCYBERCOM/JO FOIA
9800 Savage Road, Suite 6171
Fort George G. Meade, MD 20755

Re: Request under the FOIA, in reply refer to Archive# **20181017CYB005**

Dear :

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

Any materials prepared for the following presentations to the Defense Science Board Task Force on Cyber as a Strategic Capability:

1. *Perspective on USCYBERCOM Capabilities and Modalities given by Dr. Stephen Or IV on 05-06 Oct 2016*
2. *USCYBERCOM Perspective given by RADAM T.J. White on 05-06 Oct 2016*
- ✓ 3. *Briefing on Operational Strategy given by Dr. Richard Harknett on 05-06 Oct 2016*
4. *Briefing on the Joint Intelligence Operations Center given by CAPT Mike Studeman on 30 Nov-1 Dec 2016*
- ✓ 5. *Briefing on Global Cyberspace Operations Synchronization(GCOS) given by COL Stephen Letcheer on 21-22 Feb 2017*
6. *Briefing on the USCYBERCOM Excursion-Cyber Innovation Lab given by Col Mike Burke of the Cyber National Mission Force on 21-22 Feb 2017*
7. *The USCYBERCOM-CIO Perspective presented by Mr. G. Dennis Bartko of the USCYBERCOM Capabilities Development Group on 04-05 Apr. 2017*
- 8). *Briefing on Operation GLOWING SYMPHONY given by Brig Gen. Tim Haugh and Capt Steve Donald of JTF-Ares on 30 Nov-1 Dec 2016*

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.



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

OCT 10 2019

Jurre van Bergen
MuckRock News
DEPT MR 80877
411A Highland Ave
Somerville, MA 02144

Re: USCC 19-R086

Dear Mr. Van Bergen,

Thank you for your September 25, 2019 Freedom of Information Act (FOIA) request for talking points regarding Reuters news articles about CyberPoint, DarkMatter, and NESA in 2019.

After a thorough search of our files, we did not locate records responsive to your request.

If you are not satisfied with our action on this request, you have the right to seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information regarding these services is enclosed.

Sincerely,

A handwritten signature in black ink, appearing to read "Louis J. Nolan", is positioned above the typed name.

LOUIS J. NOLAN, GG14, DAF
Chief, Command Secretariat

Attachments:
Enclosure a/s

DoD FOIA Public Liaison:

Mr. Darrell Williams

Phone: (571) 371-0462

Email: osd.mc-alex.odcmo.mbx.dod-foia-policy-office@mail.mil

OCT 10 2019

Office of Government Information Services:

Office of Government Information Services
National Archives and Records Administration

8601 Adelphi Road – OGIS

College Park, MD 20740-6001

Email: ogis@nara.gov

Phone: (202) 741-5770

Toll Free: 1-877-684-6448

Fax: (202) 741-5769

Administrative Appeal:

Ms. Joo Chung

ODCMO Director of Oversight and Compliance

4800 Mark Center Drive

ATTN: DPCLTD, FOIA Appeals, Mailbox #24

Alexandria, VA 22350-1700

Email: osd.foia-appeal@mail.mil

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

From: 80877-51043431@requests.muckrock.com
Sent: Wednesday, September 25, 2019 10:59 AM
To: CYBERCOM_FOIA
Subject: [Non-DoD Source] Freedom of Information Act Request: Talking Points UAE

U.S. Cyber Command
FOIA Office
Suite 6171 Fort George G.
9800 Savage Road
Meade, MD 20755

September 25, 2019

To Whom It May Concern:

Pursuant to the Freedom of Information Act, 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 NESAs, National Electronic Security Authority, of the year 2019.

The news article in question: <https://www.reuters.com/investigates/special-report/usa-spying-raven/>

The requested documents will be made available to the general public, and this request is not being made for commercial purposes. I am a member of the press.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter.

I look forward to receiving your response to this request within 20 business days, as the statute requires.

Sincerely,

Jurre van Bergen

jurre@occrp.org

Filed via MuckRock.com

E-mail (Preferred): 80877-51043431@requests.muckrock.com

Upload documents directly:

https://accounts.muckrock.com/accounts/login/?next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fus-cyber-command-17349%252Ftalking-points-uae-

80877%252F%253Femail%253DCYBERCOM_FOIA%252540cybercom.mil&url_auth_token=AABT4M_V2
Y0PK7_s83DY-xf01gc%3A1iD8lK%3A5G3qPx-CRWOnEyet_rul-_oALPk

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News

DEPT MR 80877

411A Highland Ave

Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.

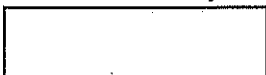


DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6171
FORT GEORGE G. MEADE, MARYLAND 20755

OCT 10 2019

Alexander Budzyn

(b) (6)



Re: USCC 19-R089

Dear Mr. Budzyn,

Thank you for your September 25, 2019 Freedom of Information Act (FOIA) request regarding "the role of Alexander Budzyn in the defense of the USA cyberspace".

After a thorough search of our files, we did not locate records responsive to your request.

If you are not satisfied with our action on this request, you have the right to seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information regarding these services is enclosed.

Sincerely,

LOUIS J. NOLAN, GG14, DAF
Chief, Command Secretariat

Attachments:
Enclosure a/s

DoD FOIA Public Liaison:

Mr. Darrell Williams

Phone: (571) 371-0462

Email: osd.mc-alex.odcmo.mbx.dod-foia-policy-office@mail.mil

OCT 10 2019

Office of Government Information Services:

Office of Government Information Services

National Archives and Records Administration

8601 Adelphi Road – OGIS

College Park, MD 20740-6001

Email: ogis@nara.gov

Phone: (202) 741-5770

Toll Free: 1-877-684-6448

Fax: (202) 741-5769

Administrative Appeal:

Ms. Joo Chung

ODCMO Director of Oversight and Compliance

4800 Mark Center Drive

ATTN: DPCLTD, FOIA Appeals, Mailbox #24

Alexandria, VA 22350-1700

Email: osd.foia-appeal@mail.mil

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

The following list contains the entire submission submitted September 25, 2019 04:50:02pm ET, and is formatted for ease of viewing and printing.

Contact information

| | |
|------------------------|---------------|
| First name | Alexander |
| Last name | Budzyn |
| Mailing Address | <div></div> |
| City | |
| State/Province | |
| Postal Code | |
| Country | United States |
| Phone | <div></div> |
| Email | |

(b) (6)

Request

| | |
|----------------------------|--|
| Request ID | 82711 |
| Confirmation ID | 82186 |
| Request description | The role of Alexander Budzyn in the defense of the USA cyberspace. |

Supporting documentation

Fees

| | |
|----------------------------|--|
| Request category ID | scientific |
| Fee waiver | yes |
| Explanation | This fee waiver is a necessity in bringing transparency to the Citizens of the United States of America. My role in the defense of the cyberspace has reached a new role in the public perception. My character can help keep the vision of the US in line with current goals. |
| Willing to pay | 120.00 |

Expedited processing

| | |
|-----------------------------|----|
| Expedited Processing | no |
|-----------------------------|----|



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

OCT 10 2019

Eric Levai



Re: USCC 20-R001

(b) (6)

Dear Mr. Levai,

Thank you for your October 5, 2019 Freedom of Information Act (FOIA) request for documents regarding the firm Wikistrat.

After a thorough search of our files, we did not locate records responsive to your request.

If you are not satisfied with our action on this request, you have the right to seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information regarding these services is enclosed.

Sincerely,

A handwritten signature in black ink, appearing to read "Louis J. Nolan".

LOUIS J. NOLAN, GG14, DAF
Chief, Command Secretariat

Attachments:
Enclosure a/s

DoD FOIA Public Liaison:

Mr. Darrell Williams

Phone: (571) 371-0462

Email: osd.mc-alex.odcmo.mbx.dod-foia-policy-office@mail.mil

OCT 10 2019

Office of Government Information Services:

Office of Government Information Services
National Archives and Records Administration

8601 Adelphi Road – OGIS

College Park, MD 20740-6001

Email: ogis@nara.gov

Phone: (202) 741-5770

Toll Free: 1-877-684-6448

Fax: (202) 741-5769

Administrative Appeal:

Ms. Joo Chung

ODCMO Director of Oversight and Compliance

4800 Mark Center Drive

ATTN: DPCLTD, FOIA Appeals, Mailbox #24

Alexandria, VA 22350-1700

Email: osd.foia-appeal@mail.mil

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

The following list contains the entire submission submitted October 05, 2019 10:20:02pm ET, and is formatted for ease of viewing and printing.

Contact information

| | |
|-----------------------------|---|
| First name | Eric |
| Last name | Levai |
| Mailing Address | <div data-bbox="787 567 1058 779" style="border: 1px solid black; width: 167px; height: 101px; margin-bottom: 5px;"></div> <div data-bbox="1128 472 1214 504">(b) (6)</div> |
| City | |
| State/Province | |
| Postal Code | |
| Country | United States |
| Company/Organization | Forensic News |
| Email | eric@forensicnews.net |

Request

| | |
|----------------------------|--|
| Request ID | 84691 |
| Confirmation ID | 84166 |
| Request description | Documents related to Wikistrat, the private intelligence firm, including, but not limited to, simulations, war games, analysis, etc. |

Supporting documentation

Fees

| | |
|----------------------------|---------------|
| Request category ID | media |
| Fee waiver | yes |
| Explanation | Media request |

Expedited processing

| | |
|-----------------------------|----|
| Expedited Processing | no |
|-----------------------------|----|



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

OCT 23 2019

Michael Martelle
The National Security Archive
Gelman Library, Suite 701
2130 H Street, NW
Washington, DC 20037

Re: 19-R077

Dear Mr. Martelle,

Thank you for your July 25, 2019 Freedom of Information Act (FOIA) request for material regarding USCYBERCOM support to NSA/CSS Cybersecurity Directorate.

After a thorough search of our files, we did not locate records responsive to your request.

If you are not satisfied with our action on this request, you have the right to seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information regarding these services is enclosed.

Sincerely,

A handwritten signature in black ink, reading "Paul R. Guevin III" with a stylized flourish at the end.

PAUL R. GUEVIN III, GG15, DAF
Chief Knowledge Officer

Attachments:
Enclosure a/s

DoD FOIA Public Liaison:

Mr. Darrell Williams
Phone: (571) 371-0462

Email: osd.mc-alex.odcmo.mbx.dod-foia-policy-office@mail.mil

OCT 23 2019

Office of Government Information Services:

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

Administrative Appeal:

Ms. Joo Chung
ODCMO Director of Oversight and Compliance
4800 Mark Center Drive
ATTN: DPCLTD, FOIA Appeals, Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

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

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

Thursday, July 25, 2019

9800 Savage Road, Suite 617I
Fort George G. Meade, MD 20755

Re: Request under the FOIA, in reply refer to Archive# 20190974CYB023

Dear :

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

Any materials, including but not limited to orders or briefings, regarding USCYBERCOM support to the NSA/CSS Cybersecurity Directorate.

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,



Michael Martelle



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

OCT 31 2019

Jurre van Bergen
MuckRock News
DEPT MR 80877
411A Highland Ave
Somerville, MA 02144

Re: 19-R087

Dear Mr. Van Bergen,

Thank you for your September 25, 2019 Freedom of Information Act (FOIA) request for documents from 2014 regarding CyberPoint and/or DarkMatter collaboration with NESA.

After a thorough search of our files, we did not locate records responsive to your request.

If you are not satisfied with our action on this request, you have the right to seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information about these services is enclosed.

Sincerely,

A handwritten signature in black ink, reading "Paul R. Guevin III" with a stylized flourish at the end.

PAUL R. GUEVIN III, GG15, DAF
Chief Knowledge Officer

Attachments:
Enclosure a/s

DoD FOIA Public Liaison:

Mr. Darrell Williams

Phone: (571) 371-0462

Email: osd.mc-alex.odcmo.mbx.dod-foia-policy-office@mail.mil

OCT 31 2019

Office of Government Information Services:

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

Administrative Appeal:

Ms. Joo Chung
ODCMO Director of Oversight and Compliance
4800 Mark Center Drive
ATTN: DPCLTD, FOIA Appeals, Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

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

From: 80879-74495780@requests.muckrock.com
Sent: Wednesday, September 25, 2019 11:13 AM
To: CYBERCOM_FOIA
Subject: [Non-DoD Source] Freedom of Information Act Request: Dark Matter/NESA

U.S. Cyber Command
FOIA Office
Suite 6171 Fort George G.
9800 Savage Road
Meade, MD 20755

September 25, 2019

To Whom It May Concern:

Pursuant to the Freedom of Information Act, 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.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes. I am a member of the press

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter.

I look forward to receiving your response to this request within 20 business days, as the statute requires.

Sincerely,

Jurre van Bergen

jurre@occrp.org

Filed via MuckRock.com
E-mail (Preferred): 80879-74495780@requests.muckrock.com

Upload documents directly:

https://accounts.muckrock.com/accounts/login/?next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fus-cyber-command-17349%252Fdark-matter%252Femail%253DCYBERCOM_FOIA%252540cybercom.mil&url_auth_token=AABT4M_V2Y0PK7_s83DY-xf01gc%3A1iD8yv%3A2ZZgczPOIBsXCe_aJAVS_pXAiTE

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News
DEPT MR 80879
411A Highland Ave
Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.



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

OCT 05 2020

Cristin Monahan
The National Security Archive
Gelman Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037

Re: 20-R057

Dear Ms. Monahan,

Thank you for your July 27, 2020, Freedom of Information Act (FOIA) request for material pertaining to Xi'an Tian He Defense Technology Co. Ltd. or its subsidiaries.

After a thorough search of our files, we did not locate records responsive to your request.

If you are not satisfied with our action on this request, you have the right to seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information regarding these services is enclosed.

Sincerely,

A handwritten signature in black ink, reading "Paul R. Guevin III", is positioned above the typed name.

PAUL R. GUEVIN III, GG15, DAF
Chief Knowledge Officer

Attachments:
Enclosure a/s

DoD FOIA Public Liaison:

Mr. Darrell Williams

Phone: (571) 371-0462

Email: osd.mc-alex.odcmo.mbx.dod-foia-policy-office@mail.mil

OCT 05 2020

Office of Government Information Services:

Office of Government Information Services
National Archives and Records Administration

8601 Adelphi Road – OGIS

College Park, MD 20740-6001

Email: ogis@nara.gov

Phone: (202) 741-5770

Toll Free: 1-877-684-6448

Fax: (202) 741-5769

Administrative Appeal:

Ms. Joo Chung

ODCMO Director of Oversight and Compliance

4800 Mark Center Drive

ATTN: DPCLTD, FOIA Appeals, Mailbox #24

Alexandria, VA 22350-1700

Email: osd.foia-appeal@mail.mil

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

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

Monday, July 27, 2020

USCYBERCOM/J0 FOIA
9800 Savage Rd., Ste. 6171
Fort George G. Meade, MD 20755

Re: Request under the FOIA, in reply refer to Archive# 20200679CYB012

Dear FOIA Officer :

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

Any documents or communications pertaining to Xi'an Tianhe Defense Technology Company Limited, or to any of its subsidiaries.

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,



Crislin Monahan



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

OCT 05 2020

Taylor Matthews
Lewis Rice LLC
600 Washington Ave, Ste 2500
Saint Louis, MO 63101

Re: 20-R061

Dear Mr. Matthews,

Thank you for your August 20, 2020, Freedom of Information Act (FOIA) request for material regarding Atigeo.

After a thorough search of our files, we did not locate records responsive to your request.

If you are not satisfied with our action on this request, you have the right to seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information regarding these services is enclosed.

Sincerely,

A handwritten signature in black ink, reading "Paul R. Guevin III", is positioned above the typed name.

PAUL R. GUEVIN III, GG15, DAF
Chief Knowledge Officer

Attachments:
Enclosure a/s

DoD FOIA Public Liaison:

Mr. Darrell Williams

Phone: (571) 371-0462

Email: osd.mc-alex.odcmo.mbx.dod-foia-policy-office@mail.mil

OCT 05 2020

Office of Government Information Services:

Office of Government Information Services
National Archives and Records Administration

8601 Adelphi Road – OGIS

College Park, MD 20740-6001

Email: ogis@nara.gov

Phone: (202) 741-5770

Toll Free: 1-877-684-6448

Fax: (202) 741-5769

Administrative Appeal:

Ms. Joo Chung

ODCMO Director of Oversight and Compliance

4800 Mark Center Drive

ATTN: DPCLTD, FOIA Appeals, Mailbox #24

Alexandria, VA 22350-1700

Email: osd.foia-appeal@mail.mil

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

The following list contains the entire submission submitted August 20, 2020 02:40:03pm ET, and is formatted for ease of viewing and printing.

Contact information

| | |
|-----------------------------|--------------------------------|
| First name | Taylor |
| Last name | Matthews |
| Mailing Address | 600 Washington Ave., Ste. 2500 |
| City | Saint Louis |
| State/Province | MO |
| Postal Code | 63101 |
| Country | United States |
| Phone | 314-444-1372 |
| Fax | 314-612-1372 |
| Company/Organization | Lewis Rice LLC |
| Email | tmatthews@lewisrice.com |

Request

| | |
|------------------------|--------|
| Request ID | 153971 |
| Confirmation ID | 153446 |

Request description

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).

Supporting documentation

Fees

Request category ID

commercial

Fee waiver

no

Willing to pay

\$1000

Expedited processing

Expedited Processing

no



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

OCT 21 2020

Eric Geller
Politico
1000 Wilson Blvd, 8th Floor
Arlington, VA 22209

Re: 20-R037

Dear Mr. Geller,

Thank you for your March 3, 2020, Freedom of Information Act (FOIA) request for "all Vulnerabilities Equities Process annual reports and other VEP documents distributed to U.S. Cyber Command in its role as a member of the VEP Equities Review Board."

After a thorough search of our files, we did not locate records responsive to your request.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information regarding these services is enclosed.

Sincerely,

A handwritten signature in black ink, reading "Paul R. Guevin III", is positioned above the typed name.

PAUL R. GUEVIN III, GG15, DAF
Chief Knowledge Officer

Attachments:
Enclosure a/s

Re: 20-R037

DoD FOIA Public Liaison:

Mr. Darrell Williams

Phone: (571) 371-0462

Email: osd.mc-alex.odcmo.mbx.dod-foia-policy-office@mail.mil

OCT 21 2020

Office of Government Information Services:

Office of Government Information Services

National Archives and Records Administration

8601 Adelphi Road – OGIS

College Park, MD 20740-6001

Email: ogis@nara.gov

Phone: (202) 741-5770

Toll Free: 1-877-684-6448

Fax: (202) 741-5769

Administrative Appeal:

Ms. Joo Chung

ODCMO Director of Oversight and Compliance

4800 Mark Center Drive

ATTN: DPCLTD, FOIA Appeals, Mailbox #24

Alexandria, VA 22350-1700

Email: osd.foia-appeal@mail.mil

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

From: Eric Geller <egeller@politico.com>
Sent: Tuesday, March 3, 2020 10:57 AM
To: CYBERCOM_FOIA
Subject: [Non-DoD Source] FOIA request: VEP reports and documents

Hello,

This is a request under the Freedom of Information Act. I hereby request the following records:

All Vulnerabilities Equities Process annual reports and other VEP documents distributed to U.S. Cyber Command in its role as a member of the VEP Equities Review Board. See here for more information:

<https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF> Please search for records since November 15, 2017.

I request a fee waiver as a member of the news media. The requested records are essential to producing journalism that informs the public about government operations. Examples of my work can be found here:

<https://www.politico.com/staff/eric-geller>

If, notwithstanding the waiver, there are any fees for searching, reviewing, or copying the records, please let me know before you task my request. I am willing to pay fees for this request up to a maximum of \$50. If you estimate that the fees will exceed this limit, please inform me first.

If you determine that any of the applicable records is exempt from disclosure, I request a list of those documents as required by *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), cert. denied, 415 U.S. 977 (1972). A "Vaughn index" must describe the withheld documents in enough detail "to permit a reasoned judgment as to whether the material is actually exempt under FOIA." *Founding Church of Scientology v. Bell*, 603 F.2d 945, 949 (D.C. Cir. 1979). In addition, the index must "describe each document or portion thereof withheld, and for each withholding it must discuss the consequences of supplying the sought-after information." *King v. U.S. Dep't of Justice*, 830 F.2d 210, 223-24 (D.C. Cir. 1987). Furthermore, "the withholding agency must supply 'a relatively detailed justification, specifically identifying the reasons why a particular exemption is relevant and correlating those claims with the particular part of a withheld document to which they apply.'" *Id.* at 224 (citing *Mead Data Central v. U.S. Dep't of the Air Force*, 566 F.2d 242, 251 (D.C. Cir. 1977)).

If some of the records I request are exempt from disclosure, please provide to me all reasonably segregable non-exempt sections of these records. See 5 U.S.C. § 552(b). If a document contains such non-exempt sections, but you assert that they are spread out across the document in such a way that segregation would be impossible, please explain which sections of the document are non-exempt and how those sections are spread out across the document. *Mead Data Central*, 566 F.2d at 261. If you make a claim that a section is non-segregable, you must provide the same level of detail as described above for a Vaughn index. If you deny my request entirely, please state that it is not appropriate to segregate sections of the records for disclosure.

I would prefer to receive all correspondence and records electronically, but if that is not possible, my physical address is:

Eric Geller
Politico
1000 Wilson Blvd, 8th Floor
Arlington, VA 22209

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 20 business days, as the statute requires.

—

Eric Geller
Cybersecurity Reporter
POLITICOPro
Cell: (301) 547-6954
Desk: (703) 647-8571
Twitter: @ericgeller



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

OCT 21 2020

Cristin Monahan
The National Security Archive
Gelman Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037

Re: 21-R001

Dear Ms. Monahan,

Thank you for your October 2, 2020, Freedom of Information Act (FOIA) request for material regarding Chinese Cybersecurity Parks, or Information Security Industrial Parks, in Beijing, Tianjin, and Chengdu.

After a thorough search of our files, we did not locate records responsive to your request.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information regarding these services is enclosed.

Sincerely,

A handwritten signature in black ink, reading "Paul R. Guevin III", is positioned above the typed name.

PAUL R. GUEVIN III, GG15, DAF
Chief Knowledge Officer

Attachments:
Enclosure a/s

DoD FOIA Public Liaison:

Mr. Darrell Williams

Phone: (571) 371-0462

Email: osd.mc-alex.odcmo.mbx.dod-foia-policy-office@mail.mil

OCT 21 2020

Office of Government Information Services:

Office of Government Information Services

National Archives and Records Administration

8601 Adelphi Road – OGIS

College Park, MD 20740-6001

Email: ogis@nara.gov

Phone: (202) 741-5770

Toll Free: 1-877-684-6448

Fax: (202) 741-5769

Administrative Appeal:

Ms. Joo Chung

ODCMO Director of Oversight and Compliance

4800 Mark Center Drive

ATTN: DPCLTD, FOIA Appeals, Mailbox #24

Alexandria, VA 22350-1700

Email: osd.foia-appeal@mail.mil

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

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

Friday, October 2, 2020

USCYBERCOM/J0 FOIA
9800 Savage Rd., Ste. 6171
Fort George G. Meade, MD 20755

Re: Request under the FOIA, in reply refer to Archive# **20200900CYB015**

Dear FOIA Officer :

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

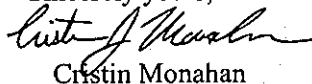
For the time period between January 2017 and October 2020, any correspondence, reports or assessments regarding Chinese cybersecurity parks, also known as Information Security Industrial Parks, in Beijing, Tianjin, and Chengdu.

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,



Cristin Monahan



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

OCT 22 2020

Cristin Monahan
The National Security Archive
Gelman Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037


Re: 19-R068

Dear Ms. Monahan,

Thank you for your July 1, 2019, Freedom of Information Act (FOIA) request for "all releasable portions of 'The Russian Playbook'".

We have located and reviewed 46 pages of material responsive to your request. As the Initial Denial Authority, I have determined that the information is exempt from disclosure under the FOIA, Title 5, United States Code, section 552(b)(1) and (b)(3). Enclosed are details of the specific exemptions cited.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information about these services is enclosed.


DAVID T. ISAACSON
Major General, U.S. Army
Chief of Staff

Attachments:
Enclosure a/s

OCT 22 2020

Re: 19-R068

Exemptions Cited:

- (b)(1) – information properly and currently classified in the interest of national defense or foreign policy, pursuant to Executive Order 13526, Classified National Security Information:
 - Section 1.4(a) – military plans, weapons systems, or operations
 - Section 1.4(c) – intelligence activities (including covert action), intelligence sources or methods, or cryptology
 - Section 1.4(d) – foreign relations or foreign activities of the United States, including confidential sources
 - Section 1.4(g) – vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security
 - Section 1.7(e) – individually unclassified items of information that reveal an additional association or relationship that (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information
- (b)(3) – information specifically exempted from disclosure by statute:
 - 10 U.S.C. § 130b – personally identifying information of DoD personnel in overseas, sensitive, or routinely deployable units
 - 10 U.S.C. § 130e – defense critical infrastructure security information

DoD FOIA Public Liaison:

Mr. Darrell Williams
Phone: (571) 371-0462
Email: osd.mc-alex.odcmo.mbx.dod-foia-policy-office@mail.mil

Office of Government Information Services:

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

Administrative Appeal:

Ms. Joo Chung
ODCMO Director of Oversight and Compliance
4800 Mark Center Drive
ATTN: DPCLTD, FOIA Appeals, Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

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

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

Monday, July 1, 2019

9800 Savage Road, Suite 6171
Fort George G. Meade, MD 20755

Re: Request under the FOIA, in reply refer to Archive# 20190835CYB018

Dear :

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

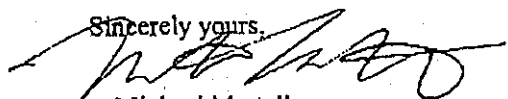
All releasable portions of "The Russian Playbook".

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,



Michael Martelle



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

OCT 06 2021

Jurre van Bergen
MuckRock News
DEPT MR 87401
411A Highland Ave
Somerville, MA 02144-2516

Re: 20-R026

Dear Mr. Van Bergen,

Thank you for your February 4, 2020, Freedom of Information Act (FOIA) request regarding assessments or investigations resulting from security vulnerabilities and exploits shared via Metasploit Project. We clarified the scope of your request with you on February 8, 2020.

We have located and reviewed 6 pages of material responsive to your request. As the Initial Denial Authority, I have determined that the information is exempt from disclosure under the FOIA, title 5, United States Code, section 552(b)(1), (b)(3), and (b)(5). Enclosed are details of the specific exemptions cited.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information about these services is enclosed.

A handwritten signature in black ink, appearing to read "D. Isaacson", with the word "FOR" written in small capital letters to the right.

DAVID T. ISAACSON
Major General, U.S. Army
Chief of Staff

Attachments:
Enclosure a/s

OCT 06 2021

Re: 20-R026

FOIA Exemptions Cited:

(b)(1) – information properly and currently classified in the interest of national defense or foreign policy, pursuant to Executive Order 13526, Classified National Security Information;

Section 1.4(c) – intelligence activities (including covert action), intelligence sources or methods, or cryptology;

Section 1.4(e) – scientific, technological, or economic matters relating to the national security;

Section 1.4(g) – vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security;

Section 1.7(e) – individually unclassified items of information that reveal an additional association or relationship that (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information.

(b)(3) – information specifically exempted from disclosure by statute:

10 U.S.C. § 130b, personally identifying information of DoD personnel in sensitive units;

10 U.S.C. § 130e, defense critical infrastructure security information;

50 U.S.C. § 3024(i)(1), information pertaining to intelligence sources and methods pursuant to the National Security Act of 1947.

(b)(5) – intra-agency memoranda containing information that qualifies for deliberative process privilege.

DoD FOIA Public Liaison:

Ms. Tonya Fuentes
Phone: (571) 371-0462
Email: osd.mc-alex.ocmo.mbx.foia-liaison@mail.mil

Office of Government Information Services:

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

Administrative Appeal:

Ms. Joo Chung
ODCMO Director of Oversight and
Compliance
4800 Mark Center Drive
ATTN: DPCLTD, FOIA Appeals
Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

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

From: 87401-05380923@requests.muckrock.com on behalf of '87401-05380923@requests.muckrock.com' <87401-05380923@requests.muckrock.com>
Sent: Saturday, February 8, 2020 9:48 AM
To: CYBERCOM_FOIA
Subject: [Non-DoD Source] RE: Freedom of Information Act Request: FBI Metasploit release of EternalBlue (U.s. Cyber Command)

Follow Up Flag: Follow up
Flag Status: Completed

U.s. Cyber Command
FOIA Office
Suite 6171 Fort George G.
9800 Savage Road
Meade, MD 20755

February 8, 2020

This is a follow up to a previous request:

Good afternoon,

Thanks for checking back and sorry for the vague wording.

I think for now your suggestion will do.

Please continue with: "Assessments or investigations resulting from security vulnerabilities and exploits shared via Metasploit Project."

Best,
Jurre

Filed via MuckRock.com
E-mail (Preferred): 87401-05380923@requests.muckrock.com
Upload documents directly:
https://accounts.muckrock.com/accounts/login/?next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fus-cyber-command-17349%252Ffbi-metasploit-release-of-eternalblue-us-cyber-command-87401%252F%253Femail%253DCYBERCOM_FOIA%252540cybercom.mil&url_auth_token=AABT4M_V2Y0PK7_s83DY-xf01gc%3A1j0RP6%3AzIPZMktPOO3A-WSqpt6cnBF1HXg
Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):
MuckRock News
DEPT MR 87401

411A Highland Ave
Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.

On Feb. 6, 2020:

Subject: RE: [Non-DoD Source] Freedom of Information Act Request: FBI Metasploit release of EternalBlue (U.s. Cyber Command)

Good morning Mr. Van Bergen,

Thanks for your request. Before we initiate this action, we want to be sure that you concur with our interpretation, which we think may be the gist of what you're looking for:

"Assessments or investigations resulting from security vulnerabilities and exploits shared via Metasploit Project."

As worded in your email, the "any records" caveat associated with multiple keywords is problematic for us, as it does not enable an organized, non-random search.

Are you satisfied with our interpretation of your request, or would you like to provide a different description of the desired records that will help us locate them with a reasonable amount of effort?

v/r

Garth

Garth C.
USCYBERCOM FOIA
(301) 688-3585

On Feb. 4, 2020:

Subject: Freedom of Information Act Request: FBI Metasploit release of EternalBlue (U.s. Cyber Command)

To Whom It May Concern:

Pursuant to the Freedom of Information Act, 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.

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7.

EternalBlue is a cyberattack exploit developed by the U.S. National Security Agency. It was leaked by the Shadow Brokers hacker group on April 14, 2017, one month after Microsoft released patches for the vulnerability. On May 12, 2017, the worldwide WannaCry ransomware used this exploit to attack unpatched computers.

EmeraldThread, EternalChampion, EskimoRoll, EternalRomance, EducatedScholar, EternalSynergy, EclipsedWing are all cyber attacks tool developed by the U.S National Security Agency. It was leaked by the Shadow Brokers hackers group in 2017.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 20 business days, as the statute requires.

Sincerely,

Jurre van Bergen

Filed via MuckRock.com

E-mail (Preferred): 87401-05380923@requests.muckrock.com

Upload documents directly:

https://accounts.muckrock.com/accounts/login/?next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fus-cyber-command-17349%252Ffbi-metasploit-release-of-eternalblue-us-cyber-command-87401%252F%253Femail%253DCYBERCOM_FOIA%252540cybercom.mil&url_auth_token=AABT4M_V2Y0PK7_s83DY-xf01gc%3A1j0RP6%3AzIPZMktPOO3A-WSqpt6cnBF1HXg

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News

DEPT MR 87401

411A Highland Ave

Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.



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

OCT 26 2021

Cristin Monahan
The National Security Archive
Gelman Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037


Re: 19-R070

Dear Ms. Monahan,

Thank you for your July 1, 2019, Freedom of Information Act (FOIA) request for U.S. Cyber Command concepts of operations to support U.S. European Command, or requests for support from U.S. European Command to U.S. Cyber Command between the years 2012 and 2018.

We have located and reviewed 62 pages of material responsive to your request. As the Initial Denial Authority, I have determined that 55 pages are exempt from disclosure under the FOIA, title 5, United States Code, section 552(b)(1), (b)(3), and (b)(5). We referred 7 pages to U.S. European Command for review and direct response to you.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information about these services is enclosed.


DAVID T. ISAACSON
Major General, U.S. Army
Chief of Staff

Attachments:
Enclosure a/s

OCT 26 2021

Re: 19-R070

FOIA Exemptions Cited:

(b)(1) – information properly and currently classified in the interest of national defense or foreign policy, pursuant to Executive Order 13526, Classified National Security Information:

Section 1.4(a) – military plans, weapons systems, or operations

Section 1.4(c) – intelligence activities (including covert action), intelligence sources or methods, or cryptology

Section 1.4(d) – foreign relations or foreign activities of the U.S., including confidential sources

Section 1.4(e) – scientific, technological, or economic matters relating to the national security

Section 1.4(g) – vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security

Section 1.7(e) – individually unclassified items of information that reveal an additional association or relationship that (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information

(b)(3) – information specifically exempted from disclosure by statute:

10 U.S.C. § 130b, personally identifying information of DoD personnel in sensitive units

10 U.S.C. § 130e, defense critical infrastructure security information

50 U.S.C. § 3024(i)(1), information pertaining to intelligence sources and methods pursuant to the National Security Act of 1947

(b)(5) – inter- or intra-agency documents containing information that qualifies for the deliberative process privilege

(b)(6) – information in personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy

DoD FOIA Public Liaison:

Ms. Tonya Fuentes
Phone: (571) 371-0462
Email: osd.mc-alex.ocmo.mbx.foia-liaison@mail.mil

Office of Government Information Services:

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

Administrative Appeal:

Ms. Joo Chung
ODCMO Director of Oversight and Compliance
4800 Mark Center Drive
ATTN: DPCLTD, FOIA Appeals
Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

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

19-R070

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

Monday, July 1, 2019

9800 Savage Road, Suite 6171
Fort George G. Meade, MD 20755

Re: Request under the FOIA, in reply refer to Archive# 20190840CYB020

Dear :

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

Any requests for CYBERCOM support by EUCOM, or CONOPS for CYBERCOM support to EUCOM, between 2012 and 2018.

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,



Michael Martelle



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

OCT 28 2021

Adam Janofsky
The Record
adam.janofsky@recordedfuture.com

Re: 22-R001

Dear Mr. Janofsky,

Thank you for your Freedom of Information Act (FOIA) request dated September 24, 2021, received in our office on October 1, 2021. We attempted to clarify the scope of your request with you on October 7, 2021, via email.

As previously explained, the FOIA requires that a requester provide a reasonable description of the records sought, to enable the DoD Component to locate the records with a reasonable amount of effort. Your request remains overly broad and inadequate to describe specific records sought, and we are therefore unable to process the request as submitted.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information about these services is enclosed.

Sincerely,

A handwritten signature in black ink, reading "Paul R. Guevin III", is positioned above the typed name.

PAUL R. GUEVIN III, GG15, DAF
Chief Knowledge Officer

Attachments:
Enclosure a/s

OCT 28 2021

Re: 22-R001

DoD FOIA Public Liaison:

Ms. Tonya Fuentes
Phone: (571) 371-0462
Email: osd.mc-alex.ocmo.mbx.foia-liaison@mail.mil

Office of Government Information Services:

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

Administrative Appeal:

Ms. Joo Chung
ODCMO Director of Oversight and
Compliance
4800 Mark Center Drive
ATTN: DPCLTD, FOIA Appeals
Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

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

From: Adam Janofsky <adam.janofsky@recordedfuture.com>
Sent: Friday, October 1, 2021 11:19 AM
To: CYBERCOM_FOIA
Subject: [Non-DoD Source] US Cyber Cyber Command — FOIA Request
Attachments: USCC-2021-01_20210924_Request.pdf

Follow Up Flag: Follow up
Flag Status: Completed

VIA EMAIL

Dear FOIA Officers,

Pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552 The Record makes the following request for records:

Emails, memos, powerpoint presentations, and other documents sent to or held by US Cyber Command that reference the word "BlackMatter" between the years 2016 and 2021 (most recent date available). Such documents may include mention of "ransomware".

Fee Waiver Request

In accordance with 5 U.S.C. § 552(a)(4)(A)(iii) and your agency's regulations, The Record requests a waiver of fees associated with processing this request for records. The subject of this request concerns the operations of the federal government, and the disclosures will likely contribute to a better understanding of relevant government procedures by the general public in a significant way. Moreover, the request is primarily and fundamentally for journalistic purposes.

The Record requests a waiver of fees because disclosure of the requested information is "in the public interest because it is likely to contribute significantly to public understanding of operations or activities of the government." The public has a significant interest in understanding ransomware threats. Records with the potential to shed light on this matter would contribute significantly to public understanding of operations of the federal government. The Record is committed to transparency and intends to make newsworthy responses agencies provide to FOIA requests publicly available in the course of reporting, and the public's understanding of the government's activities would be enhanced through The Record's analysis and publication of these records.

The Record is a media outlet staffed by professional journalists which regularly reports news related to cybersecurity issues and is frequently cited by other outlets, including The Washington Post. The Record is also ranked competitively on relevant news aggregators such as Techmeme's Leaderboard. As a news outlet, we frequently publish materials gathered through reporting on our public website and promote their availability on social media platforms, including Twitter.

Accordingly, The Record qualifies for a fee waiver.

Guidance Regarding the Search & Processing of Requested Records

In connection with its request for records, The Record provides the following guidance regarding the scope of the records sought and the search and processing of records:

- Please search all locations and systems likely to have responsive records, regardless of format, medium, or physical characteristics. For instance, if the request seeks "communications," please search all locations likely to contain communications, including relevant hard-copy files, correspondence files, appropriate locations on hard drives and shared drives, emails, text messages or other direct messaging systems (such as iMessage, WhatsApp, Signal, or Twitter direct messages), voicemail messages, instant messaging systems such as Lync or ICQ, and shared messages systems such as Slack.
- In conducting your search, please understand the terms "record," "document," and "information" in their broadest sense, to include any written, typed, recorded, graphic, printed, or audio material of any kind. We seek records of any kind, including electronic records, audiotapes, videotapes, and photographs, as well as letters, emails, facsimiles, telephone messages, voice mail messages, and transcripts, notes, or minutes of any meetings, telephone conversations, or discussions.
- Our request for records includes any attachments to those records or other materials enclosed with those records when they were previously transmitted. To the extent that an email is responsive to our request, our request includes all prior messages sent or received in that email chain, as well as any attachments to the email.
- Please search all relevant records or systems containing records regarding agency business. Do not exclude records regarding agency business contained in files, email accounts, or devices in the personal custody of your officials, such as personal email accounts or text messages. Records of official business conducted using unofficial systems or stored outside of official files are subject to the Federal Records Act and FOIA. It is not adequate to rely on policies and procedures that require officials to move such information to official systems within a certain period of time; The Record has a right to records contained in those files even if material has not yet been moved to official systems or if officials have, by intent or through negligence, failed to meet their obligations.
- Please use all tools available to your agency to conduct a complete and efficient search for potentially responsive records. Agencies are subject to government-wide requirements to manage agency information electronically, and many agencies have adopted the National Archives and Records Administration (NARA) Capstone program, or similar policies. These systems provide options for searching emails and other electronic records in a manner that is reasonably likely to be more complete than just searching individual custodian files. For example, a custodian may have deleted a responsive email from his or her email program, but your agency's archiving tools may capture that email under Capstone. At the same time, custodian searches are still necessary; agencies may not have direct access to files stored in .PST files, outside of network drives, in paper format, or in personal email accounts.
- In the event some portions of the requested records are properly exempt from disclosure, please disclose any reasonably segregable non-exempt portions of the requested records. If a request is denied in whole, please state specifically why it is not reasonable to segregate portions of the record for release.
- Please take appropriate steps to ensure that records responsive to this request are not deleted by the agency before the completion of processing for this request. If records potentially responsive to this request are likely to be located on systems where they are subject to potential deletion, including on a scheduled basis, please take steps to prevent that deletion, including, as appropriate, by instituting a litigation hold on those records.

Conclusion

If you have any questions regarding how to construe this request for records or believe that further discussions regarding search and processing would facilitate a more efficient production of records of interest to The Record, please do not hesitate to contact us to discuss this request. We welcome an opportunity to discuss its request with you before you undertake your search or incur search or duplication costs. By working together at the outset, The Record and your agency can decrease the likelihood of costly and time-consuming litigation in the future.

Where possible, please provide responsive material in an electronic format by email. Alternatively, please provide responsive material in native format or in PDF format on a USB drive. Please send any responsive

material being sent by mail to 8200 Greensboro Dr. Ste 1100 McLean VA, 22102. If it will accelerate release of responsive records to The Record, please also provide responsive material on a rolling basis.

We share a common mission to promote public understanding of the federal government and its policies. The Record looks forward to working with your agency on this request.

If you do not understand any part of this request, please contact adam.janofsky@recordedfuture.com. Also, if The Record's request for a fee waiver is not granted in full, please contact us immediately upon making such a determination.

Sincerely,
Adam Janofsky



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

NOV 10 2021

Stefan Soesanto
Center for Security Studies
Haldeneggsteig 4, IFW C 47.1
Zurich, Switzerland 8092

Re: 22-R007

Dear Mr. Soesanto,

Thank you for your October 29, 2021, Freedom of Information Act (FOIA) request for records regarding North Atlantic Treaty Organization (NATO) cyber rapid reaction teams.

After a thorough search of our files, we did not locate records responsive to your request.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information about these services is enclosed.

Sincerely,

A handwritten signature in black ink, reading "Paul R. Guevin III", is positioned above the typed name.

PAUL R. GUEVIN III, GG15, DAF
Chief Knowledge Officer

Attachments:
Enclosure a/s

NOV 10 2021

Re: 22-R007

DoD FOIA Public Liaison:

Ms. Tonya Fuentes
Phone: (571) 371-0462
Email: osd.mc-alex.ocmo.mbx.foia-liaison@mail.mil

Office of Government Information Services:

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

Administrative Appeal:

Ms. Joo Chung
ODCMO Director of Oversight and
Compliance
4800 Mark Center Drive
ATTN: DPCLTD, FOIA Appeals
Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

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

The following list contains the entire submission submitted October 29, 2021 12:10:13pm ET, and is formatted for ease of viewing and printing.

Contact information

| | |
|-----------------------------|---|
| First name | Stefan |
| Last name | Soesanto |
| Mailing Address | Center for Security Studies, Haldeneggsteig 4, IFW C 47.1 |
| City | Zurich |
| State/Province | Zurich |
| Postal Code | 8092 |
| Country | Switzerland |
| Phone | +41 446320837 |
| Company/Organization | Center for Security Studies (CSS), ETH Zurich |
| Email | stefan.soesanto@sipo.gess.ethz.ch |

Request

| | |
|----------------------------|--|
| Request ID | 278666 |
| Confirmation ID | 278141 |
| Request description | Information on the deployment of NATO's Cyber Rapid Reaction Teams (RRTs): (1) Number of cyber incidents or cyber attacks that led to the activation of a NATO RRT (2012-2021) (2) Country or location where these cyber incidents or cyber attacks took place / RRT missions were carried out (3) Duration of the RRT missions (average of all and/or duration of the individual RRT missions) (3) Descriptions of the information and communication systems affected (4) Information on any attribution assessments made ("who done it?") (5) After-action reports / NATO RRT performance evaluations |

Supporting documentation

Fees

| | |
|----------------------------|-------------|
| Request category ID | educational |
| Fee waiver | no |

Expedited processing

Expedited Processing

no



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

NOV 18 2021



Re: 22-R010

(b) (6)

Dear 

This letter responds to your November 16, 2021, Freedom of Information Act (FOIA) request for contact information of a U.S. Cyber Command employee.

To be subject to the FOIA, a record must exist and be in Command possession and control when the Command conducts its search. We are not obligated to create, compile, or answer questions to satisfy a FOIA request. Moreover, we do not disclose the names and duty information of Command personnel.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information about these services is enclosed.

Sincerely,

PAUL R. GUEVIN III, GG15, DAF
Chief Knowledge Officer

Attachments:
Enclosure a/s

NOV 18 2021

Re: 22-R010

DoD FOIA Public Liaison:

Ms. Tonya Fuentes
Phone: (571) 371-0462
Email: osd.mc-alex.ocmo.mbx.foia-liaison@mail.mil

Office of Government Information Services:

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

Administrative Appeal:

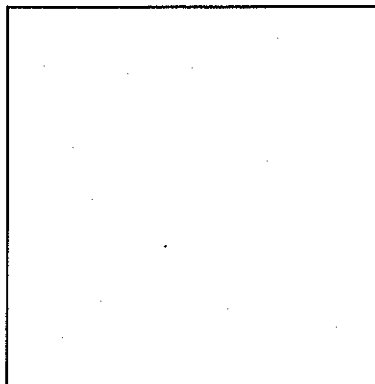
Ms. Joo Chung
ODCMO Director of Oversight and
Compliance
4800 Mark Center Drive
ATTN: DPCLTD, FOIA Appeals
Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

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

The following list contains the entire submission submitted November 16, 2021 11:42:02am ET, and is formatted for ease of viewing and printing.

Contact information

First name
Last name
Mailing Address
City
State/Province
Postal Code
Country
Phone
Email




Request

Request ID 284391

Confirmation ID 283866

Request
description

Contact information for the Joint Exercise Planner USCYBERCOM J-7 Security Manager. I would like the contact information for the security office/officer in charge in order to contact them regarding  admission of misconduct.

(b) (6)

Supporting documentation

Additional Information

Birth cert.jpg

Fees

Request category ID

other

Fee waiver

no

Explanation

N/A

Willing to pay

100.00

Expedited processing

Expedited Processing

no