```
R 092250Z MAR 15
FM USCYBERCOM FT GEORGE G MEADE MD
TO COMFLTCYBERCOM FT GEORGE G MEADE MD
COMNAVIDFOR SUFFOLK VA
NAVNETWARCOM SUFFOLK VA
NAVCYBERDEFOPSCOM SUFFOLK VA
CDRUSACYBER FT BELVOIR VA
CDRUSACYBER G3 FT BELVOIR VA
CDRUSACYBER G33 FT BELVOIR VA
ARMY FORCES CYBER CMD PETERSON AFB CO
ARMY GNOSC FT BELVOIR VA
MARFORCYBERCOM FT MEADE MD
MCNOSC QUANTICO VA
24AF LACKLAND AFB TX
DISA FT GEORGE G MEADE MD
DIRNSA FT GEORGE G MEADE MD
NSA FT GEORGE G MEADE MD
NSACSS FT GEORGE G MEADE MD
JFHQ DODIN FT GEORGE G MEADE MD
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
BT
```

S E C R E T   (REL US/GBR/CAN/AUS/NZ)

SUBJECT: (U//FOUO) FRAGORD 06 TO USCYBERCOM TASKORD 13-0747
         ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF)
         TEAMS IN FISCAL YEAR (FY) 2014

OPER/OPERATION GLADIATOR SHIELD//

MSGID/ORDER/USCYBERCOM/FRAGORD 06 TO USCYBERCOM TASKORD 13-0747
ESTABLISHMENT AND PRESENTATION OF CYBER MISSION FORCE (CMF) TEAMS
IN FISCAL YEAR (FY) 2014/FRAGORD/(S//REL TO USA,FVEY)//

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

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

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

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

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

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

REF/G/MTG/CYBER COMPONENTS COMMANDER CONFERENCE (TS//REL
TO USA, FVEY)/USCYBERCOM/22OCT13/-//

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

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

REF/N/FRAGORD/(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/O/DOC/(U//FOUO) USSTRATCOM READINESS REPORTING AND ASSESSMENTS
(UNCLASSIFIED)/USSTRATCOM/19 MARCH 2012/-//

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

REF/Q/DOC/(U//FOUO) CMF TEAM FULL OPERATIONAL CAPABILITY (FOC)
APPROVAL AND CERTIFICATION PROCESS DECLARATION SOP
(U//FOUO)/USCYBERCOM/30JANUARY15/-//

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

ORDTYPE/FRAGORD/USCYBERCOM//

TIMEZONE/Z//

NARR/(U//FOUO) THIS ORDER REFINES GUIDANCE TO SERVICE COMPONENTS IN
THE BUILDING OF CMF TEAMS. ADDITIONALLY, IT CLARIFIES SERVICE CYBER
COMPONENT AND OPERATIONAL COMMANDER (CDR) ROLES IN THE INITIAL
OPERATING CAPABILITY (IOC) AND FULL OPERATION CAPABILITY (FOC)
DECLARATION PROCESSES. THIS ORDER ALSO ENUMERATES IOC AND FOC
APPROVAL AUTHORITIES, SUPPORTING STAFFING PROCESSES AND READINESS

REPORTING REQUIREMENTS.//

GENTEXT/SITUATION/1.

1.A. (U) NO CHANGE.

1.B. (U) ADVERSARY FORCES. NO CHANGE.

1.C. (U) FRIENDLY FORCES. NO CHANGE.

1.C.1. (U) NO CHANGE.

1.C.2. (U) NO CHANGE.

1.C.3. (U) NO CHANGE.//

GENTEXT/MISSION/2.

2.A. (U) NO CHANGE.//

GENTEXT/EXECUTION/3.

3.A. (U) CONCEPT OF OPERATIONS.

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

3.A.1.A. (U) PURPOSE. NO CHANGE.

3.A.1.B. (U) METHOD. NO CHANGE.

3.A.1.C. (U) END STATE. NO CHANGE.

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

3.A.2.A. (U) NO CHANGE.

3.A.2.A.1. (U) NO CHANGE.

3.A.2.A.2. (U) NO CHANGE.

3.A.2.A.3. (U) DELETE.

3.A.2.B. (U) NO CHANGE.

3.A.2.C. (U) NO CHANGE.

3.B. (U) TASKS.

3.B.1. (U) USCYBERCOM.

3.B.1.A. (U) NO CHANGE.

3.B.1.B. (U) NO CHANGE.

3.B.1.C. (U) DELETE.

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

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

3.B.1.F. (U) DELETE.

3.B.2. (U) ALL SERVICE COMPONENTS.

3.B.2.A. (U) NO CHANGE.

3.B.2.B. (U) NO CHANGE.

3.B.2.C. (U) NO CHANGE.

3.B.2.D. (U) NO CHANGE.

3.B.2.E. (U) NO CHANGE.

3.B.2.F. (U) CHANGE. Provide updates to team mission alignment, build status, and readiness assessment data (personnel, training, facilities, equipment and CYBERCOM directed CMF team mission essential tasks) to USCYBERCOM by close of business each Wednesday. Report on the USCYBERCOM Cyber Mission Force SIPRNET Intelink SharePoint portal (AKA: BATTLE ROSTER): (https://intelshare.intelink.sgov.gov/sites/uscybercom/nmf/nmf/cmf/sitepages/home.aspx).

3.B.2.F.1. (U) ADD. USCYBERCOM expanded battle roster readiness reporting requirements to support additional C2 and higher headquarters CMF readiness requirements. Battle roster reporting is required for all current FY and prior FY CMF teams. Battle roster entries will be made by team leads and validated by the next higher headquarters in the operational chain of command. Service components are responsible for completing battle roster entries for CMF teams without an assigned team lead.

3.B.2.F.2. (U) ADD. PERSONNEL. Team leads or Service component POCs will continue to report the name, rank and source of each person assigned to the team.

3.B.2.F.3. (U) ADD. EQUIPMENT AND SUPPLIES ON HAND. Team leads or Service component POCs report whether each team member on hand has been assigned equipment necessary to conduct assigned work role. Unit custodian will report on equipment assigned for team mission requirements, where individual assignment is not applicable.

3.B.2.F.4. (U) ADD. EQUIPMENT CONDITION. Team leads or Service component POCs report whether the equipment assigned to each team member on hand is adequate to conduct assigned work role. Unit custodian will report on equipment adequacy where individual assignment is not applicable.

3.B.2.F.5. (U) ADD. TRAINING. Team leads or Service component POCs will continue to report whether personnel on hand are fully trained or in training.

3.B.2.F.6. (U//FOUO) ADD. CAPACITY AND CAPABILITY. If team FOC requirements are no longer met (e.g. due to personnel rotation or new

equipment requirements), parent unit will report the change in status in the current reporting week. Services will report projected team degrades from FOC to less than FOC status upon projection. Attainment of FOC is a milestone. If a team drops below FOC criteria standards, notification to USCC is informational only and does not alter previously approved FOC designation.

3.B.2.G. (U//FOUO) CHANGE. 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 (as revised).

3.B.2.H. (U) NO CHANGE.

3.B.2.I. (U) NO CHANGE.

3.B.2.I.1. (U) NO CHANGE.

3.B.2.J. (U) NO CHANGE.

3.B.2.K. (U) NO CHANGE.

3.B.2.K.1. (U//FOUO) CHANGE. CMF TEAM IOC DECLARATION PROCESS. Establishing service component CDR certifies their CMF team has achieved all IOC criteria, and then initiates the IOC declaration process. Service component CDR coordinates with the gaining Operational CDR to accept OPCON transfer. Upon acceptance of OPCON, Service component CDR declares team IOC.

3.B.2.K.1.A. (U//FOUO) ADD. IOC WAIVERS. The gaining Operational CDR has the authority to designate approval authority for IOC waivers in order to 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 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.

3.B.2.K.1.B. (U//FOUO) ADD. CMF TEAM FOC DECLARATION PROCESS IAW REF M. Operational CDR, in coordination with the establishing Service component commander, verifies their CMF team (NMT, NST, CMT, CST, N-CPT, C-CPT, and D-CPT) has achieved all FOC criteria, and then routes the FOC request to DCDR USCYBERCOM. For service CPTs, the Service cyber component CDR routes the FOC request to DCDR USCYBERCOM. DCDR USCYBERCOM declares all CMF teams FOC IAW ref M.

3.B.2.K.2. (U//FOUO) CHANGE. REPORTING OF FORCES. Service components maintain reporting responsibility over teams tasked via ref D and ref H until they are transferred to the gaining operational CDR.

3.B.2.L. (U//FOUO) CHANGE. JFHQ-C FOC is achieved when the following criteria is met. FOC will be achieved NLT 30 JUNE 2015.

3.B.2.L.1. (U) NO CHANGE.

3.B.2.L.2. (U) NO CHANGE.

3.B.3. (U) ARMY CYBER COMMAND (ARCYBER).

3.B.3.A. (U) NO CHANGE.

3.B.3.A.1. (U) NO CHANGE.

3.B.3.A.2. (U) NO CHANGE.

3.B.3.B. (U) NO CHANGE.

3.B.3.B.1. (U) NO CHANGE.

3.B.3.B.2. (U) NO CHANGE.

3.B.3.B.3. (U) NO CHANGE.

3.B.3.B.4. (U) NO CHANGE.

3.B.3.B.5. (U) NO CHANGE.

3.B.3.B.6. (U) NO CHANGE.

3.B.4. (U) FLEET CYBER COMMAND (FLTCYBER).

3.B.4.A. (U) NO CHANGE.

3.B.4.B. (U) NO CHANGE.

3.B.4.B.1. (U) NO CHANGE.

3.B.4.B.2. (U) NO CHANGE.

3.B.4.C. (U) NO CHANGE.

3.B.4.C.1. (U) NO CHANGE.

3.B.4.C.2. (U) NO CHANGE.

3.B.4.C.3. (U) NO CHANGE.

3.B.5. (U) AIR FORCES CYBER COMMAND (AFCYBER).

3.B.5.A. (U) NO CHANGE.

3.B.5.A.1. (U) NO CHANGE.

3.B.5.A.2. (U) NO CHANGE.

3.B.5.B. (U) NO CHANGE.

3.B.5.B.1. (U) NO CHANGE.

3.B.5.B.2. (U) NO CHANGE.

3.B.5.B.3. (U) NO CHANGE.

3.B.5.C. (U) NO CHANGE.

3.B.5.C.1. (U) NO CHANGE.

3.B.5.C.2. (U) NO CHANGE.

3.B.5.C.3. (U) NO CHANGE.

3.B.5.C.4. (U) NO CHANGE.

3.B.5.C.5. (U) NO CHANGE.

3.B.6. (U) MARINE FORCES CYBER COMMAND (MARFORCYBER).

3.B.6.A. (U) NO CHANGE.

3.B.6.A.1. (U) NO CHANGE.

3.B.6.A.2. (U) NO CHANGE.

3.B.6.A.3. (U) NO CHANGE.

3.B.6.B. (U) NO CHANGE.

3.B.6.B.1. (U) NO CHANGE.

3.B.6.B.2. (U) NO CHANGE.

3.B.7. (U) NATIONAL SECURITY AGENCY (NSA).

3.B.7.A. (U) NO CHANGE.

3.B.7.B. (U) NO CHANGE.

3.B.7.C. (U) NO CHANGE.

3.B.8. (U) DEFENSE INFORMATION SYSTEMS AGENCY (DISA).

3.B.8.A. (U) DELETE.

3.B.8.B. (U) DELETE.

3.B.8.C. (U) DELETE.

3.B.8.D. (U) DELETE.

3.B.8.E. (U) DELETE.

3.B.8.F. (U) DELETE.

3.B.8.G. (U) DELETE.

3.C. (U) COORDINATING INSTRUCTIONS.

3.C.1. (U//FOUO) CHANGE. DIRLAUTH for service components, CNMF HQ, JFHQ-C and JFHQ-DODIN with supported commands to coordinate the location and positioning of CPTS for planning purposes.

3.C.2. (U//FOUO) CHANGE. DIRLAUTH for service components, CNMF HQ, JFHQ-C and JFHQ-DODIN with NSA/CSS ADET for coordination of NSA-provided training. Keep USCYBERCOM J7 informed IAW 3.B.2.G.

3.C.3. (U//FOUO) CHANGE. All responses and change requests, including inability to reach IOC, should be in memo message format with supporting documentation attached as required. Send to USCC_CMF_READINESS@NSA.IC.GOV.

3.C.4. (U) NO CHANGE.

3.C.5. (U) NO CHANGE.

3.C.6. (U) NO CHANGE.

3.C.7. (U) NO CHANGE.

3.C.8. (U) NO CHANGE.

3.C.9. (U) ADD. JFHQ-C, CNMF-HQ and JFHQ-DODIN coordinate with CYBERCOM service components via the weekly CMF O-6 synchronization meetings and supporting working groups to develop, refine and report readiness metrics, standards and performance measures IAW 3.B.2.F.//

GENTEXT/ADMIN AND LOGISTICS/4.

4.A. (U//FOUO) CHANGE. USCYBERCOM J4 is the single point of coordination for CMF facilities based on the NSA cryptologic infrastructure. Team leads ICW associated headquarters (CNMF HQ, JFHQ-Cs, DISA/JFHQ-DODIN) are responsible to notify J4 of space and NSA co-location requirements. J4 will aggregate initial space; NSA co-location requirements based on rosters, and provide team requirements to NSA for space requests.

4.A.1. (U//FOUO) CHANGE. After initial requirements are provided to NSA by J4; USCYBERCOM J4 will submit the consolidated space requirements throughout the cryptologic centers through a NSA staff processing form (SPF) to affected NSA mission areas. The request will include detailed breakdowns of expected CMF, including any specific space requirements to include how many personnel are required to co-locate with each NSA mission area.

4.A.2. (U) NO CHANGE.

4.A.3. (U) NO CHANGE.

4.B. (U//FOUO) CHANGE. IOC AND FOC REQUIREMENTS. Service CDRS and operational CDRS coordinate to build and employ CMF teams. Upon build

milestone achievement, service component CDRs or Operational CDRs
initiate the applicable declaration process IAW ref M and 3.B.2.K.1
of this order.

4.B.1. (U//FOUO) CHANGE. Service components retain all service-unique
organizational, training, equipment and sustainment responsibilities
for all CMF teams, regardless of OPCON relationship.

4.B.1.A. (S//REL TO USA, FVEY) CHANGE. A minimum of [(b)(1) Sec. 1.4(a)]
[(b)(1) Sec. 1.4(a)]
[(b)(1) Sec. 1.4(a)] 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 J,
4.B.1.A.3 (CPT IOC core work roles).

4.B.1.A.1. (U) NO CHANGE.

4.B.1.A.2. (U) NO CHANGE.

4.B.1.A.3. (S//REL TO USA, FVEY) CHANGE. CPT IOC Core Position
Titles:

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

4.B.1.A.4. (U) NO CHANGE.

4.B.1.A.5. (U) NO CHANGE.

4.B.1.B. (U//FOUO) TEAM MISSIONS IDENTIFIED.

4.B.1.B.1. (U//FOUO) ADD. Team leader is in receipt of mission.

4.B.1.C. (U//FOUO) CHANGE. All Available personnel have been placed
in work-roles as specified in para 4.B.1.A. and mission alignment
process is complete ICW USCYBERCOM J3F.

4.B.1.D. (U) NO CHANGE.

4.B.1.E. (U//FOUO) CHANGE. NST or CST is identified and aligned or identified for build (not applicable to CPT).

4.B.1.F. (U) NO CHANGE.

4.B.2. (U//FOUO) CHANGE. FOC. CMF teams will be declared FOC by DCDR USCYBERCOM, IAW ref M, based on the DOTMLPFP model, using the following criteria:

4.B.2.A. (U) NO CHANGE.

4.B.2.B. (U) NO CHANGE.

4.B.2.C. (U) NO CHANGE.

4.B.2.D. (U) NO CHANGE.

4.B.2.E. (U) NO CHANGE.

4.B.2.F. (U) NO CHANGE.

4.B.2.G. (U) NO CHANGE.

4.B.3. (U) POLICY.

4.B.3.A. (U) NO CHANGE.

4.B.3.B. (U) NO CHANGE.

4.C. (U) DELETE.//

GENTEXT/COMMAND AND CONTROL/5.

5.A. (U) NO CHANGE.

5.B. (U) NO CHANGE.

5.C. (U) POINTS OF CONTACT (POC):

5.C.1. (U) PRIMARY POC: [(b)(3) 130b], CYBERCOM Readiness and Assessments Branch, J338
NSTS: 966-6589/6591
COMM: [(b)(3) 130b]
SIPR: USCC_CMF_READINESS@NSA.SMIL.MIL
JWICS: USCC_CMF_READINESS@NSA.IC.GOV

5.C.2. (U) CHANGE. SECONDARY POC: [(b)(3) 130b], CYBERCOM Lessons Learned Division, J74
NSTS: 969-4183
COMM: [(b)(3) 130b]
SIPR: USCC_CMF_READINESS@NSA.SMIL.MIL
JWICS: USCC_CMF_READINESS@NSA.IC.GOV

5.C.3. (U) All DoD components will acknowledge receipt and

understanding of this FRAGORD within 24 hours at the following
website: (https://intelshare.intelink.sgov.gov/sites/uscybercom/joc/

orders/lists/orders%20acknowledgement/allitems.aspx).//

5.C.4. (U)After Hours POC: USCYBERCOM JOC JDO
NSTS: 969-1645
COMM: [(b)(3) 130b]
NIPR: jocops@CYBERCOM.MIL
SIPR: jocops@CYBERCOM.SMIL.MIL.

5.C.5. (U//FOUO) Request for information regarding execution of this
order, amplifying guidance, and/or additional details are to be
submitted at this link:
(https://intelshare.intelink.sgov.gov/sites/uscybercom/pages/
rfi.aspx).

GENTEXT/AUTHENTICATION/FOR THE COMMANDER, [(b)(3) 130b],
[(b)(3) 130b].//

AKNLDG/YES//
BT
#6072
NNNN