SMO 3705/079 R 202244Z MAR 13
FM USCYBERCOM FT GEORGE G MEADE MD
TO 24AF LACKLAND AFB TX
CDRUSACYBER FT BELVOIR VA
COMFLTCYBERCOM FT GEORGE G MEADE MD
MARFORCYBERCOM FT MEADE MD
DIRNSA FT GEORGE G MEADE MD
INFO USCYBERCOM FT GEORGE G MEADE MD
HQ USSTRATCOM OFFUTT AFB NE
UNCLAS (~~FOR OFFICIAL USE ONLY~~)
QQQQ
SUBJECT: SUBJECT: (U) UNITED STATES CYBER COMMAND (USCYBERCOM) TASKING ORDER (TASKORD) 13-0289 - EXERCISE CYBER KNIGHT 13-1.

OPER/EXERCISE CYBER KNIGHT 13-1//

MSGID/ORDER/USCYBERCOM/J3/EXERCISE CYBER KNIGHT 13-1/
TASKORD 13-XX/(U//FOUO)//

REF/A/DOC/USCYBERCOM FY13-14 EXERCISE SUPPORT/USCYBERCOM /10 JUL 2012/-/-//.

AMPN/(U) REF A IS THE APPROVED FY13-14 USCYBERCOM EXERCISE SUPPORT PLAN//

ORDTYP/TASKORD/USCYBERCOM//

TIMEZONE/Z//

NARR/(U//~~FOUO~~) THIS ORDER NOTIFIES USCYBERCOM DIRECTORATES AND SERVICE COMPONENTS OF USCYBERCOM PARTICIPATION AND SUPPORT OF EXERCISE CYBER KNIGHT (CK) 13-1.//

GENTEXT/SITUATION/1. (U//~~FOUO~~) CYBER KNIGHT (CK) IS TACTICALLY FOCUSED ON VALIDATING SUB-ELEMENTS OF THE NEWLY FORMED CYBER NATIONAL MISSION FORCES (CNMF) VIA A DYNAMIC JOINT CYBER TRAINING ENVIRONMENT AGAINST A LIVE ADVERSARY EMULATOR. CK WILL LEVERAGE AND OPERATIONALIZE ONGOING PLANNING AND TRAINING EFFORTS, AND PROVIDE TACTICAL TRAINING OPPORTUNITIES FOR CYBER FORCES TO DETER, AND IF NECESSARY DEFEAT, A CYBER ATTACK AGAINST THE UNITED STATES AS DIRECTED BY THE PRESIDENT.//

GENTEXT/MISSION/2. U) USCYBERCOM CONDUCTS TACTICAL CYBERSPACE OPERATIONS IN A JOINT CYBERSPACE TRAINING ENVIRONMENT IN ORDER TO VALIDATE SUB-ELEMENTS OF THE CYBER NATIONAL MISSION FORCE EXECUTING 22-26 APR AT FORT MEADE, MD.//

GENTEXT/EXECUTION/3.

3.A. (U) CONCEPT OF OPERATIONS.

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

3.A.1.A. (U) PURPOSE. EXECUTE CK 13-1 IN ORDER TO VALIDATE SUB-ELEMENTS OF THE CYBER NATIONAL MISSION FORCE.

3.A.1.B. (U) METHOD. CK IS A 5 DAY, 24 HOUR, US ONLY CERTIFICATION EXERCISE FOR INTERNAL USCYBERCOM AND USCYBERCOM CYBER SERVICE COMPONENTS CONDUCTED ON A SECURE CLOSED-NETWORK VIRTUAL CONSTRUCTIVE RANGE ENVIRONMENT UTILIZING MULTIPLE EMULATION CAPABILITIES. THE VIRTUAL RANGE WILL SIMULATE INTERNET (GREY) SPACE AND ADVERSARY (RED) SPACE, DEPICTING IDENTIFIED KEY CYBER TERRAIN, ACTIONABLE ENDPOINTS WITHIN GREY SPACE, AND NETWORK TRAFFIC. OPPOSING FORCE (OPFOR)/ ADVERSARY EMULATORS WILL HAVE ON-SITE SUPPORT TEAMS LOCATED AT FT MEADE, MARYLAND.

3.A.1.C. (U) END STATE. IDENTIFY LESSONS LEARNED AND VALIDATES OPERATIONAL CONSTRUCT OF CNMF AND AIDS IN FURTHER PLANNING EFFORTS OF CNMF.

3.A.2. (U) GENERAL. USCYBERCOM DIRECTORATES AND COMPONENTS WILL PARTICIPATE IN ALL PHASES OF PLANNING AND EXECUTION OF FULL SPECTRUM CYBERSPACE OPERATIONS IN SUPPORT OF CYBER KNIGHT 13-1.

3.A.2.A. (U) REMAINING PLANNING CONFERENCES/EXECUTION DATES.

3.A.2.A.1. (U) SUB-ELEMENT VALIDATION EVENT #2: 25-29 MAR, FORT GEORGE G.
MEADE, MD.

3.A.2.A.2. (U) REHEARSAL/EXECUTION: 22-26 APR 13, FORT GEORGE G. MEADE, MD.

3.B. (U) TASKS.

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

3.B.1.A. (U) PUBLIC AFFAIRS OFFICE (PAO).

3.B.1.A.1. (U) DEVELOP/RELEASE APPROVED PUBLIC AFFAIRS GUIDANCE.

3.B.1.B. (U) STAFF JUDGE ADVOCATE (SJA).

3.B.1.B.1. (U) PROVIDE LEGAL REVIEW OF AUTHORITIES DURING EVENT EXECUTION.

3.B.1.C. (U) J0.

3.B.1.C.1. (U) PROVIDE AN OFFICER OF PRIMARY RESPONSIBILITY (OPR) FOR SECURITY CLEARANCE INFORMATION/REQUIREMENTS FOR PARTICIPANTS.

3.B.1.C.2. (U) PROVIDE PROTOCOL SUPPORT FOR EVENT TO INCLUDE, BUT NOT LIMITED TO THE FOLLOWING ACTIONS:

3.B.1.C.2.A. (U) PREPARE AND RELEASE DISTINGUISHED VISITOR INVITATIONS.

3.B.1.C.2.B. (U) TRACK RSVP, POC INFORMATION, TRAVEL ARRANGEMENTS.

3.B.1.C.2.C. (U) PREPARE AGENDAS, VISIT BOOKS, SEATING CHARTS, PARKING, CATERING, ETC.

3.B.1.C.2.D. (U) CREATE WELCOME PACKAGES.

3.B.1.D. (U) J1.

3.B.1.D.1. (U) ASSIGN ONE (1) MANPOWER SPECIALIST TO: CREATE, POPULATE, AND MAINTAIN JOINT MANPOWER DOCUMENT.

3.B.1.D.2. (U) CONDUCT IN/OUTPROCESSING AT EVENT

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

3.B.1.E.1. (U) ASSIGN AT A MINIMUM ONE (1) INTELLIGENCE/ SCENARIO PLANNERS TO:

3.B.1.E.1.A. (U)ATTEND APPROPRIATE EXERCISE PLANNING CONFERENCES AND LEAD THE INTEL/SCENARIO WORKING GROUP.

3.B.1.E.1.B. (U)ASSIST WITH SCENARIO/OBJECTIVE DEVELOPMENT, EXERCISE INJECTS, AND PREPARATION OF INTEL PORTION OF THE ROAD TO CRISIS.

3.B.1.E.2. (U) PROVIDE RECOGNIZED EXPERTS TO THE J37 LED STANDARDS AND EVALUATIONS TEAM IN THE FIELDS OF ALL SOURCE ANALYSIS AND TARGETING.

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

3.B.1.F.1. (U) ASSIGN ONE (1) EXERCISE PLANNER TO:

3.B.1.F.1.A. (U) PREPARE AND RELEASE DEPLOYMENT ORDER (DEPORD).

3.B.1.F.2. (U) ASSIGN THREE (3) DYNAMIC NETWORK DEFENSE OPERATIONS DIVISION PERSONNEL TO WORK IN THE WHITE CELL.
3.B.1.F.3. (U) ASSIGN ONE (1) CURRENT OPERATIONS POSITION TO WORK IN THE WHITE CELL AS A JOINT OPERATIONS CENTER (JOC) ROLE PLAYER.

3.B.1.F.4. (U) ASSIGN THREE (3) OFFENSIVE CYBERSPACE OPERATIONS DIVISION PERSONNEL TO WORK IN THE WHITE CELL.

3.B.1.F.5. (U) PROVIDE ONE (1) SUBJECT MATTER EXPERT (SME) TO LEAD STANDARDS AND EVALUATIONS TEAM IN FIRES PLANNING.
3.B.1.G. (U) J4.

3.B.1.G.1. (U) COORDINATE EXERCISE SPACE REQUIREMENTS WITH NSA'S INSTALLATIONS AND LOGISITICS (I&L), BASED ON INPUTS RECEIVED FROM J7 EXERCISE PLANNERS.

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

3.B.1.H.1. (U) ASSIGN ONE (1) OFFENSIVE CYBERSPACE OPERATIONS PLANNER TO WORK IN THE WHITE CELL

3.B.1.H.1.A. (U) PROVIDE TECHNICAL EVALUATION AND RISK ASSESSMENT OF OFFENSIVE CYBER CAPABILITIES SUPPORTING EXERCISE OBJECTIVES.

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

3.B.1.I.1. (U) ASSIGN FIVE (5) SYSTEM ENGINEERS TO:

3.B.1.I.1.A. (U) PROVIDE TECHNICAL ASSISTANCE DURING PLANNING/EXECUTION.

3.B.1.I.1.B. (U) PREPARE WORKSTATION NETWORK FOR EXERCISE.

3.B.1.I.1.C. (U) COORDINATE/DIRECT EXERCISE FLOOR SETUP/TEAR DOWN.

3.B.1.I.2. (U) ASSIGN ONE (1) INFORMATION ASSURANCE SUBJECT MATTER EXPERT (SME) TO:

3.B.1.I.2.A. (U) PROVIDE INFORMATION ASSURANCE/INFORMATION TECHNOLOGY (IA/IT) SUPPORT.

3.B.1.I.2.B. (U) IF APPLICABLE, PROVIDE TECHNICAL ASSISTANCE FOR JOINT INFORMATION OPERATIONS RANGE (JIOR) INTERCONNECTION SECURITY AGREEMENT (ISA) COORDINATION/SIGNATURE.

3.B.1.J. (U) J7.

3.B.1.J.1. (U) ASSIGN TWELVE (12) EXERCISE PLANNERS TO:

3.B.1.J.1.A. (U) HOST/COORDINATE PLANNING CONFERENCES.

3.B.1.J.1.B. (U) LEAD FOR SCENARIO DEVELOPMENT.

3.B.1.J.1.C. (U) DEVELOP/COORDINATE/EXECUTE EXERCISE REQUIREMENTS.

3.B.1.J.1.D. (U) COORDINATE SIGNIFICANT MILITARY EXERCISE BRIEF (SMEB) PROCESS.

3.B.1.J.1.E. (U) PREPARE/BRIEF IN-PROGRESS REVIEWS (IPR).

3.B.1.J.1.F. (U) PREPARE DAILY SITREPS DURING EXECUTION.

3.B.1.J.1.G. (U) COORDINATE ALL PLANNING/EXECUTION REQUIREMENTS WITHIN USCYBERCOM.

3.B.1.J.1.H. (U) DIRECT EVENT EXECUTION.

3.B.1.K. (U) J8.

3.B.1.K.1. (U) PROVIDE FUNDING EXECUTION SUPPORT.

3.B.1.K.2. (U) PROVIDE CONTRACT DEVELOPMENT SUPPORT.

3.B.1.K.3. (U) PROVIDE DEFENSE TRAVEL SYSTEM (DTS)/COMMERCIAL TICKET

PROGRAM (CTP) PROCESSING FOR JOINT MANNING DOCUMENT (JMD) BILLETS.

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

3.B.2.A. (U) ARCYBER.

3.B.2.A.1. (U) PROVIDE ONE (1) CYBER NATIONAL MISSION TEAM (CNMT) SUB-ELEMENT STAFFED IAW CNMT CONOP FOR THE PURPOSE OF DEVELOPING, TESTING AND EVALUATING THE CNMT CERTIFICATION PROCESS DURING SUB-ELEMENT VALIDATION ELEMENTS IN MARCH.

3.B.2.A.2. (U) WITHIN 24 HOURS OF THIS ORDER BEING RELEASED, PROVIDE POC AT PARA 5.B.1, A "BY NAME" LIST OF ARCYBER CNMT SUB-ELEMENT TEAM REPRESENTATIVES TO SUPPORT THE STANDARDS AND EVALUATION PROCESS. THE TEAM SHALL CONSIST OF REPRESENTATIVES FOR THE FOLLOWING WORK ROLES: ONE (1) MISSION COMMANDER WITH 6 MONTHS EXPERIENCE, ONE (1) SENIOR WATCH OFFICER WITH 6 MONTHS OF EXPERIENCE, (1) INTERACTIVE ON-NET OPERATOR (ION), E-6 OR ABOVE, AND ONE (1) ENDPOINT EXPLOITATION ANALYST (EEA), E-6 OR ABOVE.

3.B.2.A.3. (U) PROVIDE ONE (1) REPRESENTATIVE FOR EACH ROLE TO BE EVALUATED TO SERVE ON A TIGER TEAM TO FURTHER DEVELOP THE CNMT STANDARDS. REPRESENTATIVE(S) MUST BE ABLE TO SPEAK AS A SUBJECT-MATTER EXPERT (SME) FOR EACH ROLE OF THE CNMT SUB-ELEMENT TEAM.

3.B.2.A.4. (U) PROVIDE CNMT PERSONNEL TO FILL MANNING GAPS ON EXERCISE TEAM FOR APRIL CK 13-1. REQUIREMENTS WILL NOT EXCEED ONE SUB ELEMENT AS DESCRIBED PREVIOUSLY IN THIS MESSAGE. OFFICIAL NUMBER AND TYPE WILL BE COORDINATED AND PROVIDED SEPARATE CORRESPONDENCE (SEPCOR).

3.B.2.B. (U) FLTCYBER

3.B.2.B.1. (U) PROVIDE (1) ONE CYBER NATIONAL MISSION TEAM (CNMT) SUB-ELEMENT STAFFED IAW CNMT CONOP FOR THE PURPOSE OF DEVELOPING, TESTING AND EVALUATING THE CNMT CERTIFICATION PROCESS DURING SUB-ELEMENT VALIDATION ELEMENTS IN MARCH.

3.B.2.B.2. (U) WITHIN 24 HOURS OF THIS ORDER BEING RELEASED, PROVIDE POC AT PARA 5.B.1, A "BY NAME" LIST OF FLTCYBER CNMT SUB-ELEMENT TEAM REPRESENTATIVES TO SUPPORT THE STANDARDS AND EVALUATION PROCESS. THE TEAM SHALL CONSIST OF REPRESENTATIVES FOR THE FOLLOWING WORK ROLES: ONE (1) MISSION COMMANDER WITH 6 MONTHS EXPERIENCE, ONE (1) SENIOR WATCH OFFICER WITH 6 MONTHS OF EXPERIENCE, ONE (1) INTERACTIVE ON-NET OPERATOR (ION), E-6 OR ABOVE, AND ONE (1) TARGET DEVELOPMENT NETWORK ANALYST (TDNA), E-6 OR ABOVE.

3.B.2.B.3. (U) PROVIDE ONE REPRESENTATIVE FOR EACH ROLE TO BE EVALUATED TO SERVE ON A TIGER TEAM TO FURTHER DEVELOP THE CNMT STANDARDS. REPRESENTATIVE(S) MUST BE ABLE TO SPEAK AS A SUBJECT-MATTER EXPERT (SME) FOR EACH ROLE OF THE CNMT SUB-ELEMENT TEAM.

3.B.2.B.4. (U) PROVIDE CNMT PERSONNEL TO FILL MANNING GAPS ON EXERCISE TEAM FOR APRIL CK 13-1. REQUIREMENTS WILL NOT EXCEED ONE SUB ELEMENT AS DESCRIBED PREVIOUSLY IN THIS MESSAGE. OFFICIAL NUMBER AND TYPE WILL BE COORDINATED AND PROVIDED SEPCOR.

3.B.2.C. (U) MARFORCYBER

3.B.2.C.1 (U) WITHIN 24 HOURS OF THIS ORDER BEING RELEASED, PROVIDE POC AT PARA 5.B.1, A "BY NAME" REPRESENTATIVE TO SUPPORT THE STANDARDS AND EVALUATION PROCESS. THE NAMED INDIVIDUAL MUST BE ABLE TO REPRESENT ONE OF THE FOLLOWING WORK ROLES: ONE (1) INTERACTIVE ON-NET OPERATOR (ION) OR ENDPOINT EXPLOITATION ANALYST (EEA), E-6 OR ABOVE.

3.B.2.D. (U) AFCYBER.

3.B.2.D.1. (U) PROVIDE THREE (3) CNMT(S) SUB-ELEMENTS FOR EVALUATION AND CERTIFICATION DURING FOR CK 13-1 APRIL EVENT EXECUTION. SUB-ELEMENTS SHOULD BE STAFFED IAW CNMT CONOP. COORDINATE WITH USCYBERCOM J73 AND CNMF STAFF WHERE THERE ARE MANNING AND TRAINING GAPS.

3.B.2.D.2. (U) WITHIN 24 HOURS OF THIS ORDER BEING RELEASED, PROVIDE POC AT PARA 5.B.1, A "BY NAME" LIST OF AFCYBER CNMT SUB-ELEMENT TEAM REPRESENTATIVES TO SUPPORT THE STANDARDS AND EVALUATION PROCESS. THE TEAM SHALL CONSIST OF REPRESENTATIVES FOR THE FOLLOWING WORK ROLES: ONE (1) STANDARDS AND EVALUATION TEAM LEADER, ONE (1) INTERACTIVE ON-NET OPERATOR (ION), E-6 OR ABOVE, AND ONE (1) TARGET DEVELOPMENT NETWORK ANALYST (TDNA), E-6 OR ABOVE.

3.B.2.D.3. (U) PROVIDE ONE (1) REPRESENTATIVE FOR EACH ROLE TO BE EVALUATED TO SERVE ON A TIGER TEAM TO FURTHER DEVELOP THE CNMT STANDARDS. REPRESENTATIVE(S) MUST BE ABLE TO SPEAK AS A SUBJECT-MATTER EXPERT (SME) FOR EACH ROLE OF THE CNMT SUB-ELEMENT TEAM.

3.B.3. (U) EXTERNAL AGENCIES/OTHER COMMANDS.

3.B.3.A. (U) NATIONAL SECURITY AGENCY. (U) REQUEST SUPPORT TO ACT AS NSA RED LEAD OPFOR FOR PLANNING/EVENT EXECUTION AND SUPPORT FOR TOOL DEVELOPMENT.

3.B.3.B. (U) AIR WARFARE CENTER. (U) REQUEST SUPPORT TO, ASSIGN FIVE (5) PERSONNEL FROM THE 57TH INFORMATION AGGRESSOR SQUADRON TO ACT AS THE AGGRESSORS FOR PLANNING/EVENT EXECUTION.

GENTEXT/ADMIN AND LOGISTICS/4.

4.A. (U) SPECIFIC DETAILS CONCERNING ADMIN, LOGISTICS, SECURITY WILL BE COVERED IN EXERCISE DIRECTIVE SCHEDULED TO BE RELEASED AFTER THE FINAL PLANNING CONFERENCE.

4.B. (U) FUNDING WILL COMPLY WITH FISCAL AUTHORITIES FOR THE

APPLICABLE MISSION AND FORCES.

4.C. (U) BE PREPARED TO SUPPORT AND COMPLY WITH FURTHER LOGISTICS REQUIREMENTS AS OUTLINED BY USCYBERCOM IN SUBSEQUENT DIRECTIVES/ORDERS.//

GENTEXT/COMMAND AND CONTROL/5.

5.A. (U) CDRUSCYBERCOM IS THE SUPPORTED COMMANDER.

5.B. (U) POINTS OF CONTACT (POC).

5.B.1. (U)

5.B.2. (U) AFTER HOURS POC: USCYBERCOM JOC CBC:

5.B.3. (U//~~FOUO~~) J3 POC:

5.C. (U) ALL ADDRESSES WILL ACKNOWLEDGE RECEIPT OF THIS ORDER TO THE POC IDENTIFIED IN PARAGRAPH 5.B.1. WITHIN 72 HOURS OF THE RECEIPT OF RELEASE OF THIS ORDER.

GENTEXT/AUTHENTICATION/FOR //

BT
#3705

(b)(3) 10 U.S.C. §130b
(b)(6)

CONCEPT OF OPERATIONS

FOR EMPLOYMENT OF

COLLATERAL NETWORK ATTACK CAPABILITIES

IN SUPPORT OF UNITED STATES CYBER COMMAND

EXERCISE CYBER KNIGHT

MARCH 2013

(b) (6)

[redacted]

SIGNED: 8 March 2013

[redacted]

Chief, HQ USSTRATCOM Non-kinetic Division

(U) References:

- (U) Ref A: Unified Command Plan 2011, 8 Apr 11
- (U) Ref B: SECDEF Delegation of Approval Authority for use of Computer Network Attack (CNA) Capabilities and Designated Special Access Programs (SAP) Capabilities in Support of Combatant Command (COCOM) Sponsored Exercises, DTG 101416Z Nov 11
- ~~(S)~~ Ref C: HQ USSTRATCOM OPORD, Operation Gladiator Phoenix, 18 Feb 2011
- (U) Ref D: CONPLAN 8039-08, Cyberspace Operations, 22 Apr 08, (S//NF)
- (U) Ref E: HQ USCYBERCOM Concept of Operations, 10 Aug 10
- (U) Ref F: Execute Order to Incorporate Realistic Cyberspace Conditions into Major DOD Exercises, 11 Feb 11 (S//REL to USA, FVEY)

(U) **Introduction:** The nature of the cyber environment is rapidly evolving and unconstrained by global boundaries thereby creating unparalleled challenges in the development of dedicated, consistently trained, and ready cyber force with the capacity to adapt to and meet the totality of DOD cyberspace operations requirements. The Secretary of Defense (SecDef) approved a Chairman of the Joint Chiefs of Staff (CJCS) recommendation to grow and reorganize elements of the cyber force structure as described in the Cyber Force Presentation Model presented to the 30 November 2012 Joint Chiefs of Staff (JCS) Tank and 11 December 2012 Deputy's Management Action Group (DMAG). There were three types of forces that encompass the new cyber force presentation model:

- (U) Cyber Mission Forces (CMF) are organized into Cyber National Mission Teams (CNMT), Cyber Combat Mission Teams (CCMT) and Cyber Protection Platoons (CPP).

- (U) The CNMT's purpose is strategic defense against offensive cyber attack. They are focused on adversary cyber actors (Iran, China, Russia, Non-State) and are supported by associated Direct Support Teams (DST). Their mission is to See, Block, Maneuver in Red and Grey space to deny adversary objectives and, if authorized, strike to destroy adversary capability.

- (U) Cyber Combat Mission Teams (CCMT). Their purpose is to deliver effects in support of combatant command planning and operations. They are supported by associated Direct Support Teams (DST). They focus on developing target accesses and capabilities necessary to deliver cyber effects. Their mission is target discovery and development in support of CCMD plans and operations and, when authorized they deliver and assess cyber effects against CCMD targets.

- (U) Cyber Protection Platoons (CPP). Their purpose is to further enable the operation and defense of DoD information networks (DODIN). Platoons are organized to provide support in conjunction with CNMTs defend the nation objectives, global DODIN support in conjunction with DISA, Combatant Command support, and Service network defense requirements. Cyber Protection Platoons do not replace existing network operations and defense elements, but instead provide additional expertise and complementary capabilities to improve network defense. Although their primary mission is defense of the DODIN, some teams may be employed to assist outside the DODIN, when required and authorized.

(U) The goal of Exercise Cyber Knight is to ensure newly formed CMFs, under the new Cyber Force Presentation Model, are able to: provide effective cyber defense of the Nation, to include critical infrastructure and key resources (CIKR), and DoD networks in a manner consistent with the organization of forces in the other operational domains; deliver effects in support of the combatant commands; and capable of seamless execution during joint and combined operations.

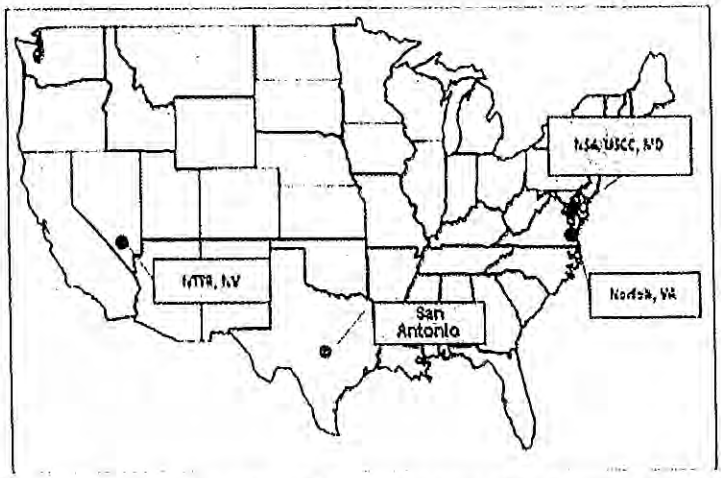
(b)(1) Sec. 1.4(a)(g)
(b)(3) 50 U.S.C. §3605

1. (~~S//REL~~) **Situation:** Exercise Cyber Knight is a Headquarters (HQ) United States Strategic Command (USSTRATCOM) sponsored and HQ United States Cyber Command (USCYBERCOM) planned and executed joint cyberspace training exercise focused on ensuring constituted cyber forces are prepared to defend the nation against foreign hostile actions and imminent threats in cyberspace.

1.a. (~~S~~) Exercise Cyber Knight will be executed 12 hours a day from 22 – 26 April 2013 utilizing the Joint Information Operations (IO) Range (JIOR) closed loop network and U.S. Government owned and controlled range equipment and networks.

1.b. (U) **Location and Participants**. The physical location of the Joint training event will be at Fort Meade, MD, with virtual private network (VPN) connections in Norfolk, VA, and Nellis Test and Training Range (NTTR), Nellis AFB, NV. Cyber Knight will provide a training environment to integrate the CMF that will plan and "fight through" realistic adversary threats. The environment is designed to replicate real-world operational network configurations, and incorporate critical mission systems and key cyber terrain. The exercise will occur in two phases:

Exercise Locations



1.b.1. (~~S~~) Phase 1 - Recce Period: This serves as a familiarization and initial preparation of the operating environment by Red/Blue forces from 15 – 19 Apr. It is expected that systems and personnel will be available for 8 hours each work day during RECCE for support from 1000 hrs to 1800 hrs (EST). Live-fire of cyber capabilities are not authorized during this period.

1.b.2. (~~S~~) Phase 2 - Exercise Event: The operational check is set to start on 22 April and continue through 26 April. This is the start of 12-hour a day operations and live-fire of cyber capabilities.

1.c. (~~S~~) **Exercise Scenario:** Cyber Knight evaluates CMF's ability to rapidly respond to escalating threats against the United States involving aggression by foreign adversaries. The exercise will commence with unambiguous warning of impending adversary attack against U.S. national security systems and U.S. CIKR. Upon order by POTUS/SECDEF, CDRUSCYBERCOM will direct CMF to conduct Cyberspace ISR, Cyberspace OPE, and Cyberspace Attack, against adversary computer network infrastructure and actors in order to mitigate adversary actions.

2. (~~S~~) **Mission:** CDRUSSTRATCOM executes Exercise Cyber Knight from 22 – 26 April 2013 and employs collateral offensive cyberspace capabilities on the JIOR in order to validate that Cyber Mission Forces are prepared to defend the nation against foreign hostile actions and imminent threats in cyberspace.

3. (~~S~~) **Execution:**

3.a. (~~S//NF~~) **Concept of Operations (CONOP)**: Exercise Cyber Knight leverages and operationalizes ongoing planning and training efforts, and provides tactical training opportunities for cyber forces to deter, and if necessary defeat, a cyber attack directed against the United States, as directed by the President. Overall exercises objectives:

3.a.1. (U) Provide Commanders a means to validate mission readiness and the effectiveness of unit cyberspace performance.

3.a.2. (U) Provide an event to assess and document unit cyberspace proficiency and capability to accomplish assigned cyberspace duties.

3.a.3. (U) Develop and ensure standardization of operational procedures for weapon system employment.

3.a.4. (U) Ensure compliance with appropriate operational, training, and administrative directives.

3.a.5. (U) Evaluate and revise operational directives, tactics, techniques and procedures, as required.

3.a.6. (U) Recognize trends and recommend/initiate changes to training programs and directives.

3.b. (U) This CONOP provides general guidance for the employment of collateral cyber capabilities on the JIOR during Exercise Cyber Knight. Authorization to employ offensive cyberspace capabilities will be approved upon full compliance with established criteria set by the Secretary of Defense in Ref B and the National Security Agency. At a minimum, Exercise Cyber Knight meets the following specified requirements:

3.b.1. (U) Offensive cyberspace capabilities will be employed over the JIOR, a certified closed-loop network.

3.b.2. (U) Exercise events will only affect computer systems located at U.S. military and government facilities in the continental U.S.

3.b.3. (U) A certified VPN has been established between all involved networks.

3.b.4. (U) All communications and data traffic will be encrypted when data leaves secure areas.

3.b.5. (U) Open air, radio frequencies, or wireless devices will not be used.

3.b.6.(U) All personnel with access to exercise networks have appropriate security clearances.

3.b.7 ~~(S/NF)~~ Specialized NSA capabilities will only be employed by NSA-certified operators.

3.c. (U) **Commander's Intent:** CDRUSSTRATCOM executes Exercise Cyber Knight in order to strengthen joint military readiness to perform integrated cyberspace operations supporting Combatant Command (CCMD), Components, and Service's cyber objectives to:

3.c.1. (U) Integrate offensive and defensive cyberspace operations.

3.c.2. (U) Leverage and operationalize ongoing planning efforts.

3.c.3. (U) Exercise USCYBERCOM global lines of operation while supporting Geographic Combatant Command (GCC) kinetic operations.

3.c.4. (U) Exercise Response Actions against adversary cyber attacks on DoD networks and U.S. critical infrastructure.

3.c.5. (U) Identify and defend cyber operational key terrain with mission assurance focus.

3.c.6. Conduct dynamic Joint and Coalition cyberspace operations in a contested environment.

3.d. (U) **Tasks to USSTRATCOM and Components.**

3.d.1. (U) Commander USSTRATCOM:

3.d.1.a. ~~(S)~~ IAW Ref B, issue EXORD for the employment of collateral offensive cyberspace capabilities in support of Exercise Cyber Knight.

3.d.1.b. (U) Designate USCYBERCOM as the Cyber Knight Exercise Executive Agent.

3.d.1.c. (U) Conduct legal review of the Cyber Knight CONOP.

3.d.2 (U) Commander USCYBERCOM:

3.d.2.a. (U) Identify an Exercise Director who will provide Cyber Knight exercise control and over-arching command and control coordinating cyber effects. The Exercise Director will compile an after-action report

and brief USSTRATCOM leadership and the Joint Staff NLT 30 days following exercise completion.

3.d.2.b. (U) Be prepared to respond to media queries.

3.e. (U) **Tasks to Supporting Agencies.**

3.e.1. ~~(S)~~

3.e.1.a. ~~(S)~~

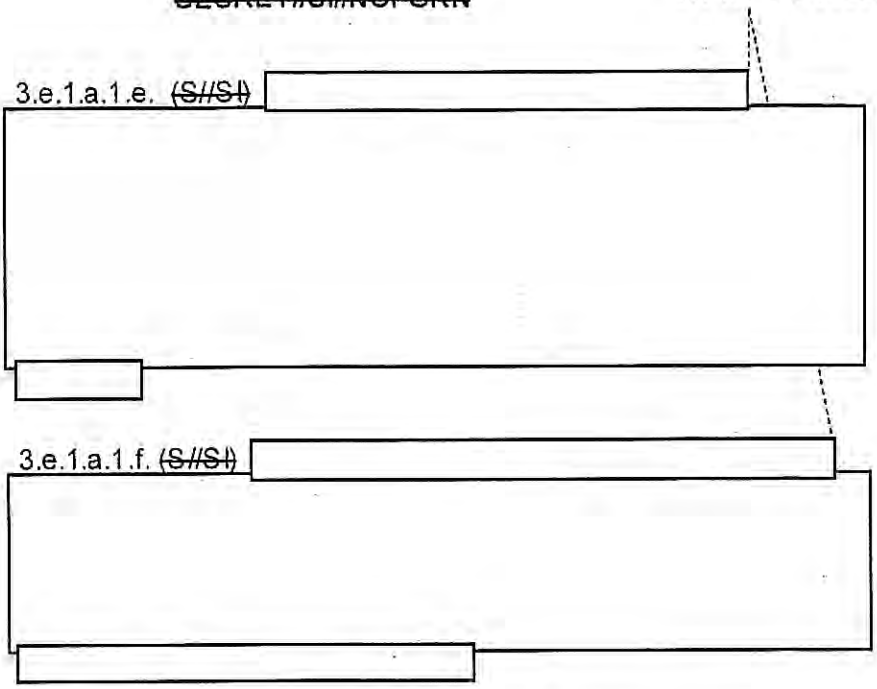
3.e.1.a.1. (U) Operations:

3.e.1.a.1.a. ~~(S)~~

3.e.1.a.1.b. ~~(S//SI)~~

3.e.1.a.1.c. ~~(S//SI)~~

3.e.1.a.1.d. ~~(S//SI)~~



3.e.2. (S) Director, DIA: Provide any updates to the Political-Military Assessment (PMA) in accordance with (IAW) Ref B.

3.f. (U) **Consequence Management**:

3.f.1. (U) Risk Mitigation Measures:

3.f.1.a (U) Closed loop network minimizes risk of unintended effects.

3.f.1.b. (U) All targets reside on government-controlled installations and equipment.

3.f.1.c. (U) All live fires will be conducted over the JIOR and certified closed loop network architecture.

3.f.1.d. (U) All data will be encrypted in VPN tunnels and separated to prevent unauthorized disclosure.

3.f.1.e. (U) All electronic exercise related CNA information is communicated via Secret Internet Protocol Router Network (SIPRNET) / Joint Worldwide Intelligence Communications System (JWICS). All cyberspace attack related conversations will be conducted via DOD-

approved secure communications (ie. Secure Terminal Equipment (STE)/ National Secure Telephone System (NSTS)/JIOR event phones.

3.f.1.f. (U) All exercise related materials are controlled in a TOP SECRET SCI environment

3.f.1.g. ~~(S//NF)~~ Specialized NSA capabilities will only be employed by NSA-certified operators.

3.f.2. (U) Incident Handling and Reporting

3.f.2.a. (U) The Exercise Director is responsible for establishing incident handling and reporting procedures.

3.f.2.b. (U) At a minimum, an incident can be one of the following:

3.f.2.b.1. (U) Any compromise or threat to confidentiality of the data being carried across the exercise network.

3.f.2.b.2. (U) Any compromise or threat to the integrity of the closed-loop nature of network ranges.

3.f.2.b.3. (U) Any unscheduled or unanticipated outages.

3.f.2.b.4. (U) Event participants are responsible for incident reporting within established procedures. Should an event participant detect an anomalous security incident within their environment, they will follow local reporting requirements and notify the Exercise Director immediately.

3.f.3. ~~(S)~~ Defense Intelligence Agency (DIA) Political-Military Assessment. Recommended assessment: No adverse political impact is anticipated. All exercise-related cyberspace operations will take place on the JIOR closed-loop network. No adverse military effects are expected. No real-world military operations will be affected during Cyber Knight, as all cyberspace operation actions will take place on the JOIR closed loop network.

3.f.4. ~~(S)~~ [redacted]

4. (U) **Administration and logistics:** Refer to Ref B

4.a. (U) **Basic Security Classification Requirements:** Reference specific Service offensive cyber capabilities chart and NSA and specific capabilities security classification guidance.

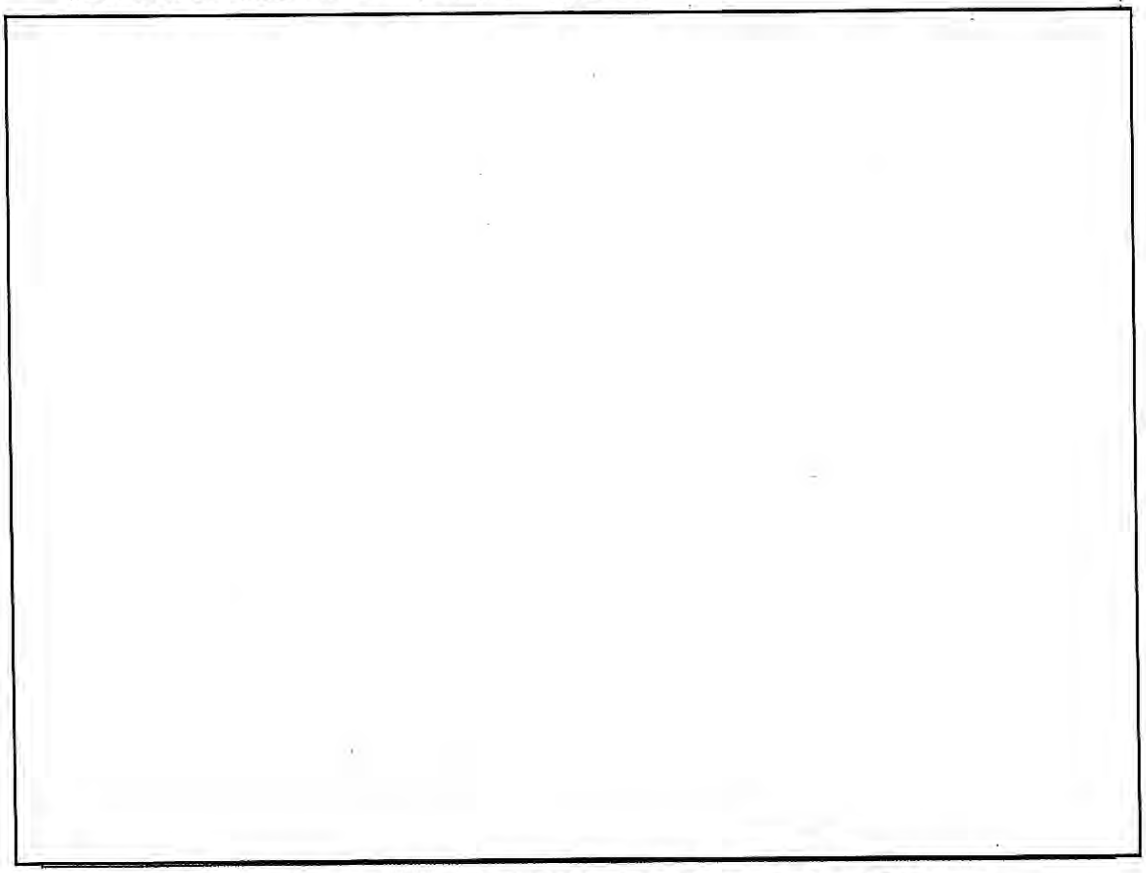
4.b. (U) **Public Affairs (PA):** Overarching PA stance is response to query only.

4.b.1. (U) Authorized contingency statement: "Cyber Knight" is a U.S. Cyber Command (USCYBERCOM) tactical level exercise designed to exercise command, control and communications between USCYBERCOM, and its assigned cyber components. Cyber Knight provides realistic training opportunities for the command and its cyber components to exercise its primary mission which is to operate and defend the Department of Defense information networks and when directed by the President of the United States – to conduct full spectrum operations. The objectives of Cyber Knight are to exercise the command's C2 relationship with its cyber components and to exercise its cyber capabilities." Any media queries should be directed to HQ United States Cyber Command, Public Affairs Office.

4.c. (U) **JIOR:** The JIOR is an Internet Protocol (IP) based network of testing ranges used by Combatant Commands, Services and Agencies and other organizations as required, to test, train, exercise and demonstrate tactics, techniques and procedures (TTP) of emerging IO capabilities. The JIOR is an integrated environment composed of processes and structures configured to establish a realistic test, training, exercise and demonstration environment for developing and operationalizing IO capabilities and weapon systems and their associated TTPs. The JIOR provides an environment that is representative of actual combat targets, systems and situations to conduct technical assurance and performance testing for weapon

systems certification. It is supported by an infrastructure that includes distributed, interconnected facilities, targets and instrumentation capable of supporting live-fire employment of capabilities and weapons.

4.c.1. (U) Interconnection Security Agreement (ISA). A certified ISA for Exercise Cyber Knight is currently in coordination. The JIOR uses this ISA to formally document the reasons, methodology, and approvals for interconnecting information technology systems and to discuss potential security risks associated with the interconnections. The approved Closed Loop Determination memo will be added at Attachment B upon final approval.



(U) Figure 1 – Cyber Knight JIOR Logical Range Network Diagram

4.c.2 (U) JIOR Network Security Configuration: For this event, the JIOR will be comprised of 2 "logical ranges" (LR) which include one Event VoIP LR and one IP Data TGT LR. The complete network utilized for this event is illustrated in Figure 1.

(b) (3) 10 U.S.C. §130e

4.c.2.a. (U//~~FOUO~~)

4.c.2.b. (~~S//NF~~)

4.c.2.c. (U) DoD was used to configure the security of the JIOR equipment. In addition, the following mitigations are used:

4.c.2.c.1. (U//~~FOUO~~) JIOR

4.c.2.c.2. (U//~~FOUO~~) JIOR utilizes

4.c.2.c.3. (U//~~FOUO~~) JIOR utilizes

4.c.2.c.4. (U//~~FOUO~~) JIOR utilizes

4.c.2.c.5. (U//~~FOUO~~) JIOR utilizes

4.c.2.c.6. (U//~~FOUO~~) JIOR provides

4.c.2.c.7. (U//~~FOUO~~) JIOR provides

4.c.2.c.8. (U//~~FOUO~~) JIOR

4.c.2.c.9. (U) The JIOR is a closed-loop environment and does not provide these types of connectivity outside of the closed loop.

4.c.2.c.10. (U) Data logging or data capture is not authorized.

4.c.2.d. (U)

(b) (3) 50 U.S.C. §3605

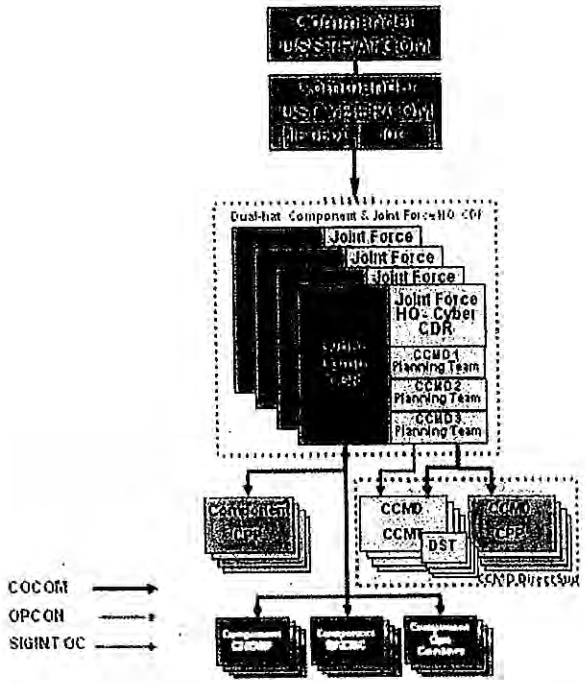
4.d. (~~S/NF~~) **Capabilities**: Service collateral cyber capabilities will be approved for employment via the Joint Staff RAP process outlined in Ref B. A consolidated list of capabilities is shown at the Attachment A.

5. (U) **Command and Control:**

5.a. (U) **HQ USSTRATCOM.** IAW Ref B, CDRUSSTRATCOM is the supported Commander for Exercise Cyber Knight. CDRUSSTRATCOM exercises COCOM of all cyber forces and delegates operational control (OPCON) of forces and cyber capabilities to CDRUSCYBERCOM.

5.b. (U) **Exercise Scenario C2:** Cyber Knight is a tactically focused event validating CMF's ability to conduct Cyberspace OPE and Cyberspace Attack. The CMF is a Joint USCYBERCOM and NSA/CSS force that is constituted and designated by the Commander, USCYBERCOM. The CMF is operationally controlled by USCYBERCOM via the Joint Operations Center (JOC), see figure 2.5.c.

5.c. (U) **Exercise C2 Relationship**: Figure 2, below, provides an overview of the exercise C2 relationships between HQ USSTRATCOM, HQ USCYBERCOM, Service Cyber Components/JFHQs and the Cyber Mission Forces.



(U) Figure 2 – Exercise Command and Control (C2)

5.c. (U) **Organizations participating in Cyber Knight include:**

USCYBERCOM (J3/J7)	NIOC Maryland
NSA [redacted]	315th Network Warfare Sq
780th MI BDE	175th Network Warfare Sq (Maryland ANG)
FLTCYBER	Joint Staff (Joint IO Range)

(b) (3) 50 U.S.C. §3605

(b) (6)

5.d. (U) **Points of contact:**

5.d.1. (U) HQ USSTRATCOM

5.d.2. (U) USCYBERCOM

5.d.3. (U) USCYBERCOM

5.d.4. (U) National Security Agency

5.d.5. (U) HQ USCYBERCOM Public Affairs:

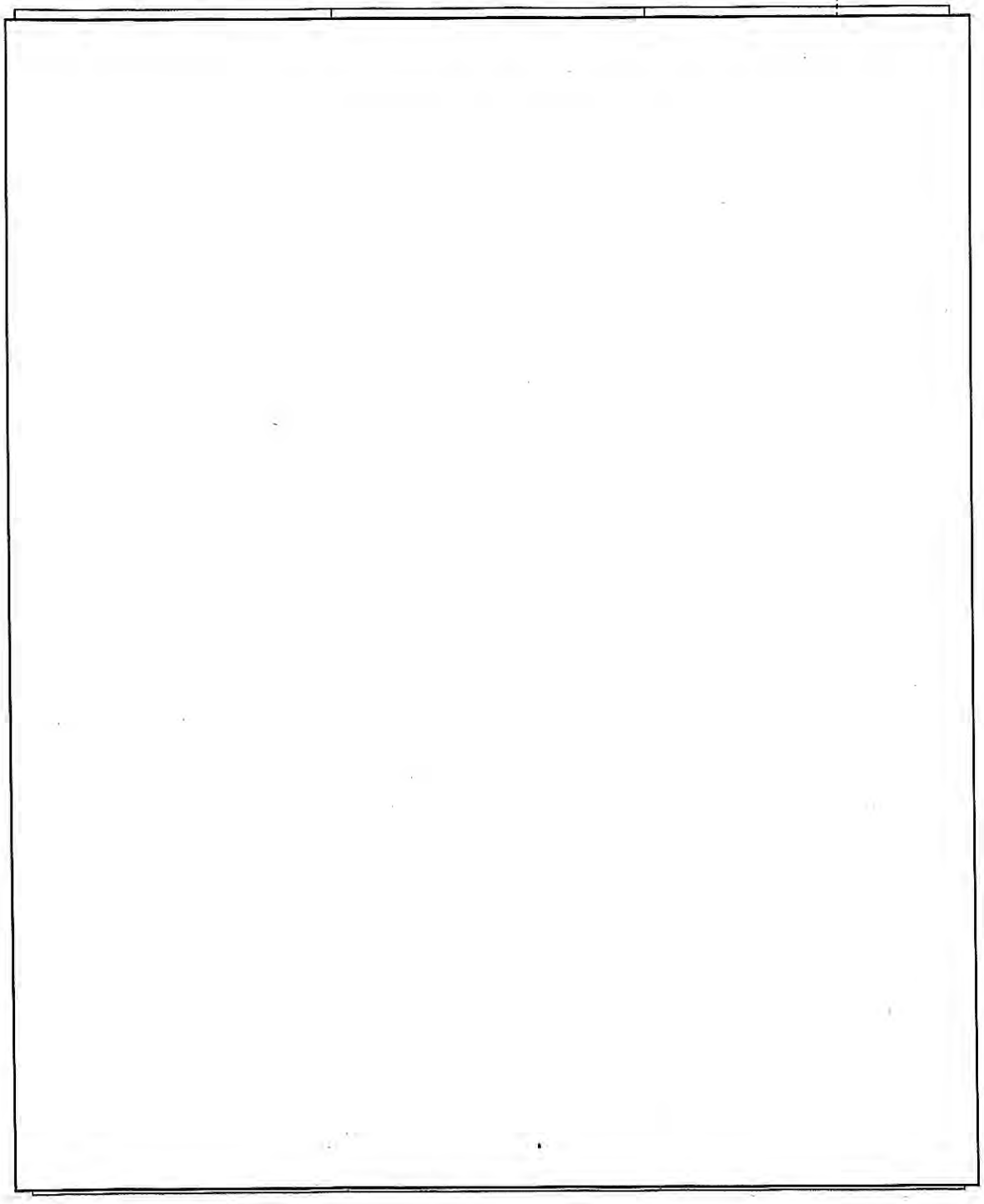
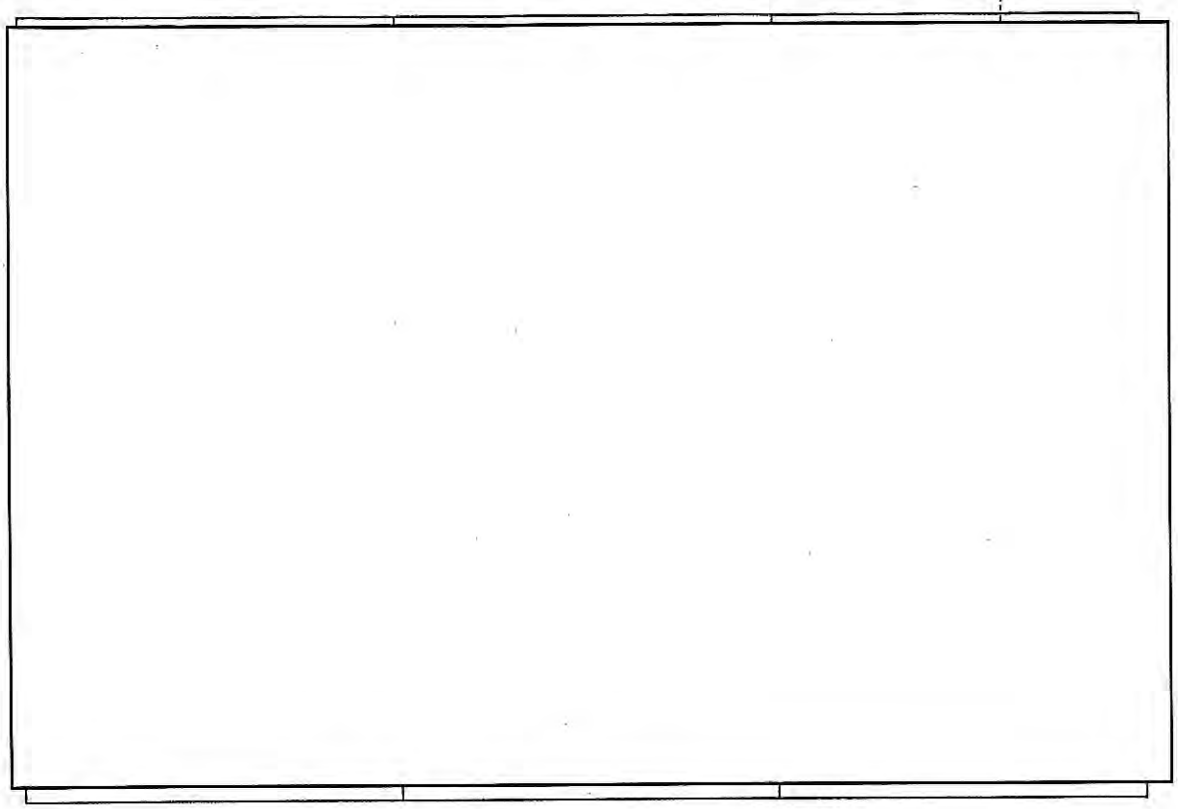
5.d.6. (U) HQ USSTRATCOM GOC BWC : Coml 402-294-1800, DSN 271-1800, battlewc@stratcom.smil.mil (After duty hours only)

(b) (3) 50 U.S.C. §3605

(b) (3) 10 U.S.C. §130b
(b) (6)

(b) (1) Sec. 1.4(a) (c)
(b) (3) 50 U.S.C. §3024(i)
(b) (3) 50 U.S.C. §3605

(U) Attachment A – List of CNA Capabilities in Support of Cyber Knight



(b) (1) Sec. 1.4(a)(c)
(b) (3) 50 U.S.C. §3024(i)
(b) (3) 50 U.S.C. §3605