[redacted]

**********[redacted] PRIVACY MARK UNDEFINED
****

Subject: EXECUTE ORDER TO INCORPORATE REALISTIC CYBERSPACE CONDITIONS INTO MAJOR DOD EXERCISES//
Originator: CJCS (SC)
DTG: 112040Z Feb 11
Precedence: ROUTINE
DAC: General
To: CDR USSTRATCOM(SC)
cc: CDR USCENTCOM(MC), CDR USPACOM HONOLULU HI(SC), CDR USSOUTHCOM(MC), CDR USJFCOM NORFOLK VA(MC), AFRICOM CDR(MC), CDR USSOCOM(MC), EUCOM CDR(MC), COMBATANT CDR USNORTHCOM(SC), CDR USTRANSCOM(SC), DIRNSA FT GEORGE G MEADE MD, DISA DIRECTOR(SC), DIA WASHINGTON DC, HQ USAF(SC), ARMY HQ, CNO WASHINGTON DC(SC), CMC WASHINGTON DC(SC), WHITE HOUSE SITUATION ROOM WASHINGTON DC, USD POLICY(SC), USD(INTEL)(SC), JOINT STAFF COMP(SC), JOINT STAFF DJ2(SC), JOINT STAFF DJ3(SC), JOINT STAFF DJ5(SC), JOINT STAFF DJ6(SC), JOINT STAFF DJ7(SC), JOINT STAFF J3 DEP-DIR GLOBAL OPS(SC), JOINT STAFF J3 NMCC OPS(SC), JOINT STAFF J3(SC)

[redacted]//DB
MSGID/GENADMIN,USMTF,2007/CJCS (SC)/F002//
SUBJ/EXECUTE ORDER TO INCORPORATE REALISTIC CYBERSPACE CONDITIONS INTO MAJOR DOD EXERCISES//
MSGID/ORDER/CJCS//
SUBJ/EXECUTE ORDER TO INCORPORATE REALISTIC CYBERSPACE CONDITIONS INTO MAJOR DOD EXERCISES(S//REL USA, FVEY)//
REF/A/DOC/CJCS MEMO TO SECDEF/MILITARY LARGE GROUP-PLUS FEEDBACK ON CYBER-WARFARE/27SEP2010//
REF/B/DOC/DEFENSE PLANNING AND PROGRAMMING GUIDANCE FY10//
REF/C/DOC/NATIONAL DEFENSE STRATEGY FOR CYBERSPACE OPERATIONS (DRAFT)//
REF/D/DOC/DODI 8530/COMPUTER NETWORK DEFENSE//9MAR2001//

(b)(1)

[redacted]

ORDTYP/EXORD/CJCS//
TIMEZONE/Z//

(b)(1)

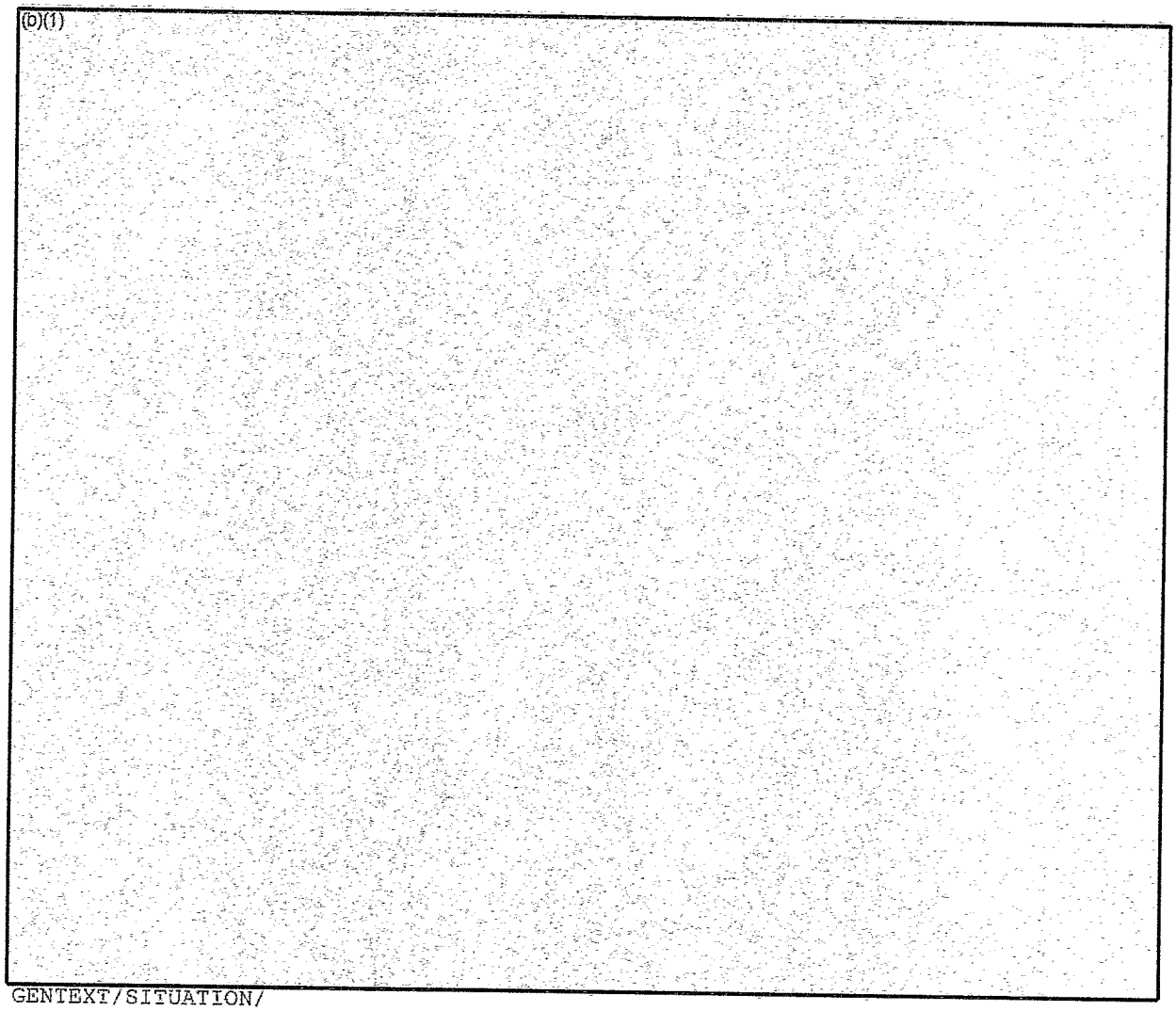
[redacted]

[redacted]

[redacted]

[redacted]

(b)(1)

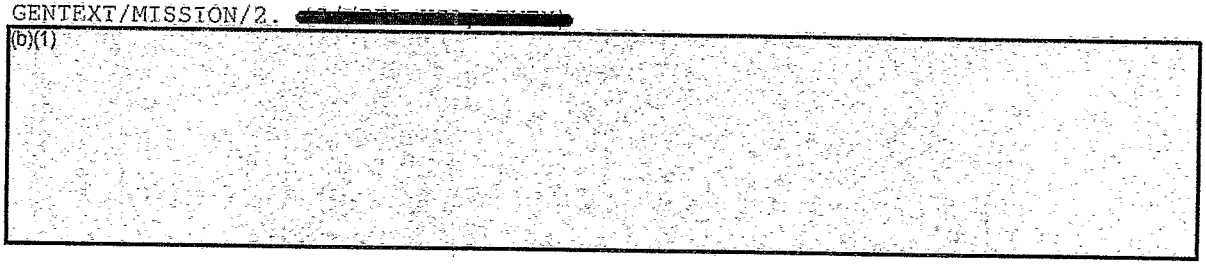


GENTEXT/SITUATION/

1. (U) CYBERSPACE IS A CONTESTED DOMAIN, AND WILL BECOME MORE HOTLY CONTESTED AS GLOBAL STATE AND NON-STATE ACTORS GAIN ACCESS TO SOPHISTICATED OFFENSIVE CYBER CAPABILITIES. DOD NETWORKS ARE SUBJECT TO CONSTANT ATTEMPTS AT INTRUSION, EXPLOITATION OR DATA COMPROMISE, AND ATTACK BY FOREIGN INTELLIGENCE AND MILITARY SERVICES, ORGANIZED CRIMINAL GROUPS, TERRORISTS, ACTIVISTS, HACKERS, AND INSIDERS. ALTHOUGH MANY SUCH EFFORTS ARE AIMED AT OBTAINING SENSITIVE INFORMATION, A POTENTIALLY GREATER OPERATIONAL CONCERN IS THAT A SOPHISTICATED ADVERSARY MIGHT HOLD DOD NET-CENTRIC WARFIGHTING OPERATIONS AT RISK. THE LOW COST OF ENTRY AND THE AVAILABILITY OF SOPHISTICATED CYBER ATTACK CAPABILITIES FOR HIRE, AS WELL AS THE IMPRACTICALITY OF PERFECT CYBER DEFENSE, MAKES A DEGRADED, COMPROMISED, OR LOCALLY/INTERMITTENTLY DENIED CYBER ENVIRONMENT A HIGH-PROBABILITY THREAT TO DOD NET-CENTRIC OPERATIONS IN ANY FUTURE CONFLICT.

GENTEXT/MISSION/2. [redacted]

(b)(1)



(b)(1)

GENTEXT/EXECUTION/3. (U) EXECUTION

3.A. (U) INTENT.

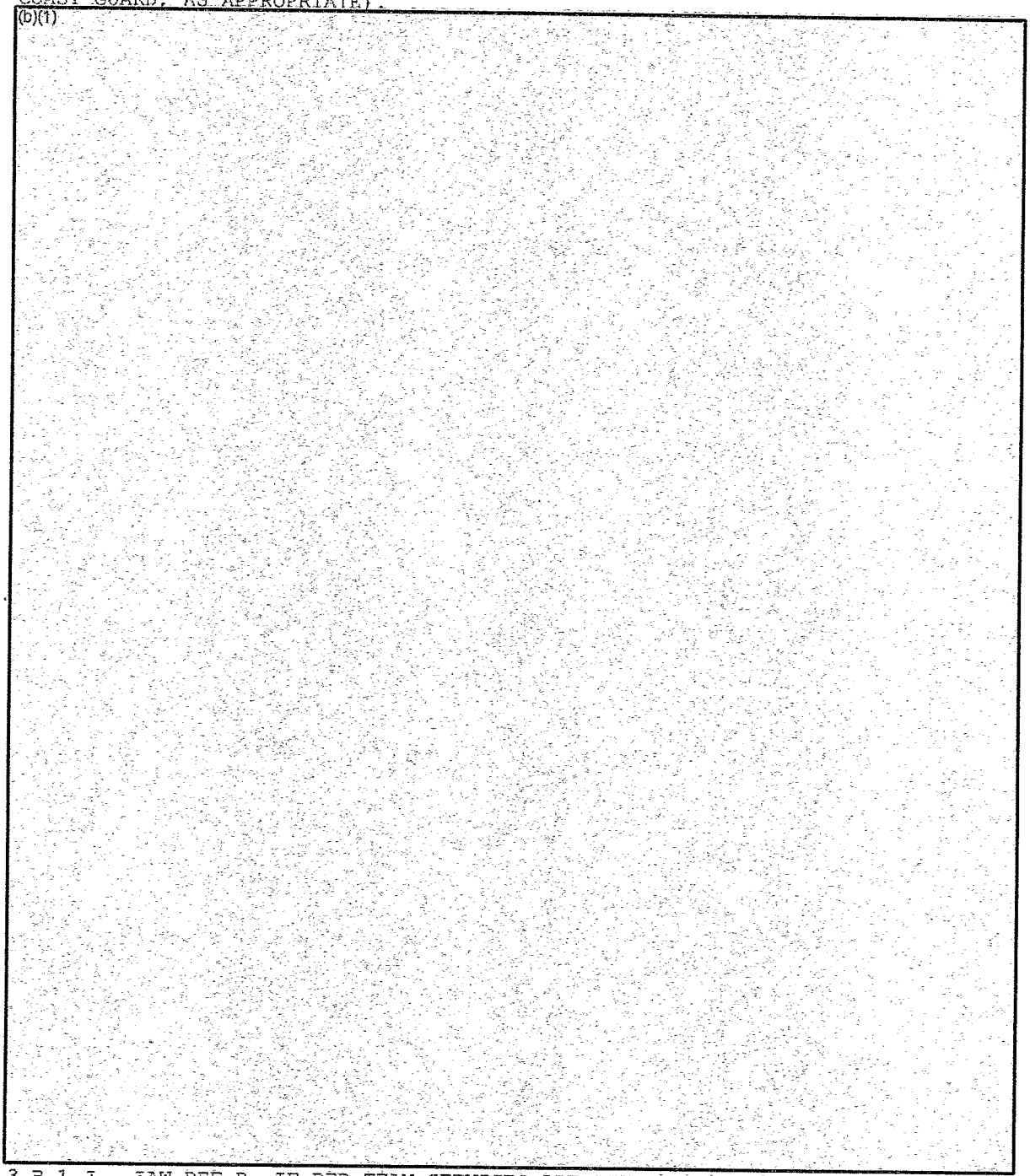
3.A.1. (U) COMBATANT COMMANDERS, SERVICE CHIEFS, AND SUBORDINATE ELEMENTS INCORPORATE REALISTIC CYBERSPACE CONDITIONS, TO INCLUDE ROBUST RED TEAM OPERATIONS, INTO MAJOR EXERCISES IN ORDER TO DEVELOP CAPABILITIES AND TTP'S TO SUSTAIN COMBAT AND OTHER ESSENTIAL OPERATIONS IN A DEGRADED OR DENIED CYBER ENVIRONMENT. THIS EXORD SUPPORTS BUT DOES NOT REQUIRE THE DEVELOPMENT OF COMPONENT CYBER AGGRESSOR TEAMS-IN INITIAL PHASES, RED TEAM OPERATIONS MAY NOT BE REQUIRED TO GENERATE DESIRED EXERISE EFFECTS-BUT DOES REQUIRE NSA CERTIFICATION AND STRATCOM ACCREDITATION OF ANY COMPONENT CYBER AGGRESSOR TEAMS PRIOR TO LIVE PLAY ON DOD NETWORKS, STARTING 180 DAYS AFTER RELEASE OF THIS ORDER. CERTIFICATION REQUIREMENT DOES NOT AFFECT RED TEAM PLAY THAT HAS ALREADY BEEN SCHEDULED FOR COMBATANT COMMAND EXERCISES PRIOR TO THAT DATE. TEAMS THAT HAVE ALREADY BEEN CERTIFIED TO OPERATE BY NSA DO NOT HAVE TO GET RECERTIFIED BY CYBERCOM, BUT WILL NEED TO KEEP THEIR CERTIFICATION CURRENT IAW CRITERIA TO BE ESTABLISHED BY CYBERCOM ICW NSA.

(b)(1)

3.B. (U) TASKS

3.B.1. (U) DOD COMPONENTS (FOR THE PURPOSES OF THIS ORDER, INCLUDES THE MILITARY DEPARTMENTS, THE COMBATANT COMMANDS, DEFENSE AGENCIES, AND THE US COAST GUARD, AS APPROPRIATE).

(b)(1)



3.B.1.J. IAW REF D, IF RED TEAM SERVICES ARE ACCOMPLISHED BY YOUR CERTIFIED TIER 2 CNDSP, ENSURE YOUR CND/SUBSCRIBER AGREEMENTS CAPTURE THE REQUIREMENT IDENTIFIED IN THIS EXORD.

3.B.1.K. SERVICES INCORPORATE OPERATIONAL TTP'S DEVELOPED TO MITIGATE EFFECTS OF ADVERSARY DISRUPTION OF NET-CENTRIC CAPABILTIES INTO OPERATIONS

[redacted]

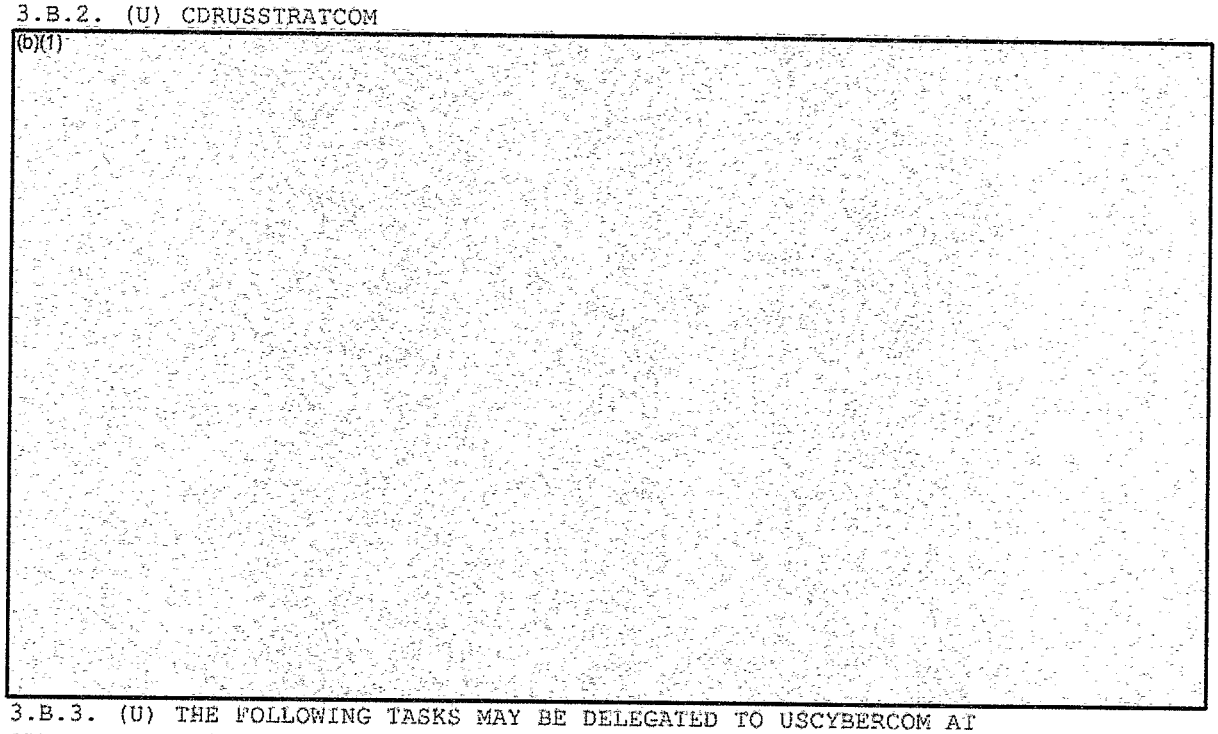
SCHOOLHOUSES, INCLUDING WEAPONS SCHOOLS. INTEGRATE NETOPS TTP'S INTO SERVICE NETWORK OPERATIONS TRAINING VENUES.

3.B.1.L. COORDINATE WITH USSTRATCOM ON ALL TIER 1 RED TEAM OPERATIONS EMPLOYED UNDER DOD COMPONENT CONTROL AS PART OF THIS EXORD, IN ORDER TO FACILITATE STRATCOM'S GIG-WIDE SITUATIONAL AWARENESS, EVENT CHARACTERIZATION, AND DECONFLICTION OF ON-NET OPERATIONS.

3.B.1.M. IDENTIFY RESOURCE CONSTRAINTS ASSOCIATED WITH THIS EXORD TO USSTRATCOM FOR ADVOCACY.

3.B.2. (U) CDRUSSTRATCOM

(b)(1)



3.B.3. (U) THE FOLLOWING TASKS MAY BE DELEGATED TO USCYBERCOM AT CDRUSSTRATCOM'S DISCRETION.

(b)(1)

[redacted]

[redacted]

(b)(1)

3.B.3.E. (U) DEVELOP A STANDARD REPORTING TOOL TO CAPTURE LESSONS LEARNED, INCLUDING EFFECTIVE RESPONSES TO RED TEAM ACTIONS, IN THE JLLIS DATABASE, AND DISSEMINATE UPDATES ANNUALLY IN THE GLOBAL CYBER-SYNCHRONIZATION CONFERENCE, OR MORE FREQUENTLY AS NEEDED. SHARE LESSONS LEARNED FROM RED TEAM OPERATIONS WITH COMPONENTS, CND-SP'S, AND DOT&E IN ORDER TO IMPROVE GLOBAL CYBER DEFENSES.

(b)(1)

3.B.3.G. (U) ASSIST SERVICES IN INCORPORATING INDICATIONS AND WARNING OF ADVERSARY CYBER ATTACKS, AND CYBER DEFENSE-RELATED MITIGATING TTP'S INTO DOD CYBER DEFENSE AND NETWORK OPERATIONS TRAINING VENUES.

(b)(1)

3.B.3.J. (U) SUBJECT TO FOREIGN DISCLOSURE REGULATIONS, SHARE EFFECTIVE CYBER-DEFENSE TTP'S, TO INCLUDE I&W, WITH APPROPRIATE MISSION PARTNERS TO IMPROVE ALLIED AND COALITION CYBER DEFENSE AND SECURITY EFFORTS.

3.B.4 (U) DIRECTOR, NATIONAL SECURITY AGENCY (DIRNSA)

(b)(1)

3.B.5. (U) DEFENSE INTELLIGENCE AGENCY (DIA). IN ADDITION TO APPLICABLE "COMPONENT" TASKS (PARA 3.B.1):

(b)(1)

[redacted]

(b)(1)

3.B.6. (U) DEFENSE INFORMATION SYSTEMS AGENCY (DISA). IN ADDITION TO APPLICABLE "COMPONENT" TASKS (PARA 3.B.1), BPT PROVIDE INFORMATION ASSURANCE AND NETOPS SUPPORT TO DOD COMPONENTS IN DEVELOPING AND IMPLEMENTING CAPABILITY TO FIGHT THROUGH A DEGRADED OR COMPROMISED CYBER ENVIRONMENT. WHERE ADDITIONAL RESOURCES ARE REQUIRED ISO THIS EFFORT, IDENTIFY THEM THROUH NORMAL RESOURCING PROCESSES AND CHANNELS.

3.B.7. (U) OFFICE OF THE SECRETARY OF DEFENSE / DOD CHIEF INFORMATION OFFICER (DOD CIO). PROVIDE POLICY DIRECTION AND GUIDANCE FOR THE DEVELOPMENT AND IMPLEMENTATION OF CYBER DEFENSE REQUIREMENTS IDENTIFIED IN THE COURSE OF RED-TEAM OPPOSED EXERCISES AND WARGAMES.

3.B.8. (U) OFFICE OF THE SECRETARY OF DEFENSE / DIRECTOR, OPERATIONAL TEST AND EVALUATION (DOT&E).

3.B.8.A. (U) IAW STATUTORY GUIDANCE, AND ICW DOD COMPONENTS, PERFORM OPERATIONAL ASSESSMENTS OF CYBER DEFENSE AND INFORMATION ASSURANCE ACTIVITIES ISO MAJOR WARFIGHTING EXERCISES.

3.B.8.B.(U) CAPTURE CYBER DEFENSE AND OTHER APPLICABLE LESSONS LEARNED IN JLLIS.

3.B.8.C. (U) SHARE METRICS DEVELOPED AS PART OF ASSESSMENT PROCESS WITH USCYBERCOM AND NSA TO SUPPORT DEVELOPMENT OF STANDARDIZED, REPLICABLE PROCESSES ISO AGGRESSOR TEAM TRAINING AND CERTIFICATION.

3.B.8.D. (U) LEVERAGE PARTICIPATION IN DIA ADVERSARY TACTICS ANALYSIS TO ASSIST CYBERCOM IN DEVELOPING AN ADVERSARY TACTICS PLAYBOOK ISO COMPONENT TRAINING (SEE PARA 3.B.3.F).

4. (U) COORDINATING INSTRUCTIONS

(b)(1)

4.B. (U) DIRLAUTH WITHIN DOD. ACTIVE COORDINATION WITH COUNTERPARTS ABOVE AND BEYOND JULLS AND GLOBAL CYBER SYNCHRONIZATION CONF REQUIREMENTS TO DISSEMINATE AND IMPROVE UPON LESSONS LEARNED IS HIGHLY DESIRED.

4.C. (U) USSTRATCOM WILL ESTABLISH C2 CHANNELS FOR EXERCISE PLAY. ONCE A LETTER OR REQUEST FOR RED TEAM SUPPORT/AUGMENTATION IS RECEIVED FROM A COMMANDER, USCYBERCOM WILL COORDINATE WITH THE COMPONENTS FOR RED TEAM SUPPORT. COORDINATION WILL INCLUDE EXERCISE-SPECIFIC GROUND RULES AS NEEDED TO ASSURE REAL-WORLD MISSION ASSURANCE/CONTINUITY.

5. (U) GROUND RULES.

(b)(1)

(b)(1)

6. (U) DEFINITIONS:

6.A (U) DOD COMPONENTS. FOR THE PURPOSES OF THIS ORDER, INCLUDES THE MILITARY DEPARTMENTS, THE COMBATANT COMMANDS, DEFENSE AGENCIES, AND DOD FIELD ACTIVITIES. ALSO INCLUDES THE US COAST GUARD, AS APPROPRIATE.

6.B (U) DEGRADED CYBERSPACE ENVIRONMENT. FOR THE PURPOSES OF THIS EXORD, AN OPERATING ENVIRONMENT IN WHICH THE AVAILABILITY OR RELIABILITY OF MISSION ESSENTIAL NETWORKS OR SYSTEMS IS NOT ASSURED, WHETHER AS A RESULT OF ADVERSARY ACTION, DEFENSIVE MITIGATION MEASURES (SUCH AS IMPLEMENTATION OF "MINIMIZE", USE OF ALTERNATIVE BANDWIDTH-CONSTRAINED SYSTEMS, OR ADDITIONAL SECURITY MEASURES), INADVERTENT FRIENDLY ACTION, OR NATURAL EVENT. MAY INCLUDE TEMPORARY, INTERMITTENT, OR LOCALIZED NON-AVAILABILITY (DENIAL) OF NETWORK OR SYSTEM ACCESS DUE TO ADVERSARY ACTIVITY, NATURAL EVENT, OR FRIENDLY DEFENSIVE ACTIONS SUCH AS SYSTEM ISOLATION IN THE EVENT OF KNOWN OR SUSPECTED COMPROMISE.

6.C. (U) COMPROMISE. FOR THE PURPOSES OF THIS EXORD, A COMPROMISED OPERATING ENVIRONMENT IS ONE IN WHICH THE CONFIDENTIALITY, INTEGRITY, OR NON-REPUDIATION OF MISSION ESSENTIAL NETWORKS, SYSTEMS, OR DATA IS ASSESSED AS QUESTIONABLE, DUE TO INSIDER THREAT, INADVERTENT ACTION, OR ADVERSARY EXPLOITATION. IN A COMPROMISED CYBER ENVIRONMENT, NETWORKS AND SYSTEMS MAY APPEAR TO BE OPERATING NORMALLY EVEN WHILE BEING ALTERED OR EXPLOITED BY A CRIMINAL OR HOSTILE ENTITY. A COMPROMISED CYBERSPACE ENVIRONMENT IS INHERENTLY HARDER TO DETECT THAN A DEGRADED CYBERSPACE ENVIRONMENT, AND CONSEQUENCES MAY BE MORE FAR-REACHING. FOR INSTANCE, IF C2 OR LOGISTICAL DATA IS INTERCEPTED, CORRUPTED, OR ALTERED, CRITICAL SUPPLIES AND COMPONENTS, SUCH AS AERIAL REFUELERS, AMMUNITION, OR MEDICAL SUPPORT, MAY BE MISROUTED OR INTERCEPTED, OR BLUE FORCE/IFF TRACKING MAY BE ALTERED SO AS TO CREATE FRIENDLY FIRE INCIDENTS OR MASK ADVERSARY ACTIVITIES.

6.D. (U) DENIED CYBERSPACE ENVIRONMENT: FOR THE PURPOSES OF THIS EXORD, AN OPERATING ENVIRONMENT IN WHICH ACCESS TO, OR NORMAL FUNCTIONS OF, A MISSION-ESSENTIAL NETWORK OR SYSTEM ARE PREVENTED BY ADVERSARY ACTIVITY, UNINTENDED EVENT, OR COMMANDER-DIRECTED RESTRICTION IN RESPONSE TO SUCH CONDITIONS.

6.E. (U) DEFENSE CRITICAL INFRASTRUCTURE (DCI). FOR THE PURPOSES OF THIS EXORD AND PER DODD 3020.40, DOD AND NON-DOD NETWORKED ASSETS ESSENTIAL TO PROJECT, SUPPORT AND SUSTAIN MILITARY FORCES AND OPERATIONS WORLDWIDE.

(b)(1)

[redacted]

(b)(1)

10. (U) PUBLIC AFFAIRS (PA) GUIDANCE.
10.A. (U) POSTURE. THE PA POSTURE FOR ALL DEFENSIVE CYBER OPERATIONS IS PASSIVE, RESPONSE TO QUERY ONLY.
10.B. (U) DISCLOSURE. IN THE EVENT THAT INFORMATION REGARDING A SPECIFIC EXERCISE OR CYBER DEFENSIVE ACTION IS DISCLOSED, THE FOLLOWING CONTINGENCY STATEMENT IS AUTHORIZED FOR OASD/PA USE AFTER NOTIFICATION OF AND APPROVAL BY PROPER RELEASING AUTHORITIES. ALL AGENCIES WILL DEFER TO OASD/PA.
10.C. (U) APPROVED STATEMENT. "MAINTAINING THE DOD'S ABILITY TO SUSTAIN GLOBAL OPERATIONS IN A CONTESTED CYBER ENVIRONMENT IS VITAL TO U.S. NATIONAL INTERESTS. THE DOD PLANS AND CONDUCTS EXERCISES TO BUILD AND SUSTAIN ITS NET-CENTRIC OPERATIONAL CAPABILITIES ACROSS AN ARRAY OF FORESEEABLE CONDITIONS, TO INCLUDE CYBER ATTACK AGAINST ITS NETWORKS AND VITAL SYSTEMS AND DATA. BECAUSE IT WOULD AID THOSE WHO WOULD THREATEN U.S. INTERESTS IN CYBERSPACE, IT WOULD BE IRRESPONSIBLE TO DISCUSS THE NATURE OF ANY SPECIFIC OPERATIONS, ACTUAL OR ALLEGED."
11. (U) POC IS JCS/DJ3 CYBER DIVISION (CNOD), DSN 671-1991. THIS ORDER WILL REMAIN IN EFFECT UNTIL RESCINDED.//

[redacted]

[redacted]