

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

**UNITED STATES CYBER COMMAND**



**USCYBERCOM**

**Operations Order (OPORD) 11-002**

**Operation Gladiator Shield (OGS)**

**19 May 2011**

~~Derived from: Multiple Sources~~  
~~Declassify on: 19 May, 2036~~

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

19 May 2011


SUBJECT: Operation Gladiator Shield (OGS)

SEE DISTRIBUTION: Annex Z

(U) References: Annex W

Subject: Letter of Transmittal

(U) CDRUSCYBERCOM OPORD 11-002, OGS, to secure, operate and defend the Department of Defense (DoD) Global Information Grid is approved and attached for widest possible implementation and dissemination within the DoD, and to appropriate mission partners.



KEITH B. ALEXANDER  
General, USA  
Commanding

## TABLE OF CONTENTS

|  |    |
|--|----|
| 1. (U// <del>FOUO</del> ) Situation.....                                   | 1  |
| a. (U// <del>FOUO</del> ) Threats and Vulnerabilities.....                 | 1  |
| b. (U// <del>FOUO</del> ) Friendly Forces.....                             | 4  |
| c. (U// <del>FOUO</del> ) Area of Concern.....                             | 5  |
| 2. <del>(S//REL TO USA, FVEY)</del> Mission.....                           | 6  |
| 3. (U) Execution.....  | 6  |
| a. (U// <del>FOUO</del> ) Concept of Operation.....                        | 6  |
| (1) (U// <del>FOUO</del> ) Intent.....                                     | 6  |
| (2) (U// <del>FOUO</del> ) Strategic Objectives.....                       | 10 |
| (3) (U// <del>FOUO</del> ) Operational Objectives.....                     | 11 |
| (4) (U// <del>FOUO</del> ) End States.....                                 | 12 |
| b. (U// <del>FOUO</del> ) Tasks.....                                       | 13 |
| (1) (U) Tasks to all DoD Components.....                                   | 13 |
| (2) (U) Tasks to HQ, USCYBERCOM.....                                       | 14 |
| (a) (U) J0.....  | 14 |
| (b) (U) J1.....  | 14 |
| (c) (U) J2.....  | 14 |
| (d) (U) J3.....  | 14 |
| (e) (U) J4.....  | 17 |
| (f) (U) J5.....  | 17 |
| (g) (U) J6.....  | 17 |
| (h) (U) J7.....  | 18 |
| (i) (U) J8.....  | 18 |
| (3) (U) Tasks to USCYBERCOM Service Components.....                        | 19 |
| (a) (U) Tasks to all USCYBERCOM Service Components.....                    | 19 |
| (b) (U) U.S. Air Force Cyber Command/24 <sup>th</sup> AF (AFCYBER).....    | 20 |
| (c) (U) U.S. Army Cyber Command /2d Army (ARCYBER).....                    | 20 |
| (d) (U) U.S. Fleet Cyber Command/10 <sup>th</sup> Fleet (FLTCYBERCOM)..... | 20 |
| (e) (U) U.S. Marine Forces Cyber Command (MARFORCYBER).....                | 20 |
| (4) (U) Tasks to Combatant Commands.....                                   | 20 |
| (5) (U) Tasks to Services.....   | 20 |
| (6) (U) Tasks to Agencies and Field Activities.....                        | 21 |
| (a) (U) Tasks to all Agencies and Field Activities.....                    | 21 |
| (b) (U) National Security Agency (NSA).....                                | 21 |
| (c) (U) Defense Information Systems Agency (DISA).....                     | 22 |
| (d) (U) Defense Intelligence Agency (DIA).....                             | 22 |
| (7) (U) Law Enforcement and Counterintelligence (LE/CI).....               | 22 |
| c. (U// <del>FOUO</del> ) Coordinating Instructions.....                   | 22 |
| 4. (U) Administration and Logistics.....                                   | 23 |
| 5. (U) Command and Control.....  | 25 |

HEADQUARTERS  
U.S. CYBER COMMAND  
FT. MEADE, MD 20755  
19 MAY 2011

UNITED STATES CYBER COMMAND (USCYBERCOM) OPERATION GLADIATOR  
SHIELD (OGS) OPERATIONS ORDER (OPORD) 11-002 (S//REL TO USA, FVEY)

(U//~~FOUO~~) NARRATIVE. This OPORD guides and directs the Department of Defense (DoD) and, as authorized, designated mission partners for cyberspace operations to secure, operate and defend the critical mission elements of the DoD Global Information Grid (DoD GIG) and represents a fundamental change in the way DoD will achieve unity of effort in cyberspace. CDRUSCYBERCOM is the supported commander for OGS and all other components are supporting unless otherwise specified or directed in this order. OGS is foundational in both scope and purpose and is a cornerstone for achieving the USCYBERCOM's overall mission to plan, coordinate, integrate, synchronize, and conduct activities to: direct the security, operations and defense of specified DoD information systems and networks; and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S. and allied freedom of action in cyberspace, and, when directed, deny the same to our adversaries. OGS leverages the full range of capabilities, capacity and authorities of the entire DoD and mission partners. It clarifies the command and control (C2) relationships and established authorities. OGS directs cyber responses that transcend a combatant command AOR, establishes and directs enforcement mechanisms and streamlines processes to enable rapid approval and timely execution of cyberspace operations.

1. (U//~~FOUO~~) Situation.

a. (U//~~FOUO~~) Threats and Vulnerabilities.

(1) (S//REL USA, FVEY) [redacted] (b)(1) USSC

[redacted] (b)(1) USSC

(2) (U//~~FOUO~~) [redacted] (b)(3) USSC

[redacted] (b)(3) USSC

(b)(3) USSC

(3) (U//FOUO) [redacted] (b)(3) USSC

(b)(3) USSC

(4) (U//FOUO) [redacted] (b)(3) USSC

(b)(3) USSC

(a) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC

(b)(1) USSC

(b) (U//FOUO) [redacted] (b)(3) USSC

(b)(3) USSC

(5) (U) Actors and associated threat vectors include:

(a) (U) Types of Actors. Adversaries are categorized into five broad types based on their respective cyberspace operations capabilities and tactics, techniques and procedures (TTP):

1. (U) Full Scope Actors. Actors possessing the full range of cyberspace access, expertise, capability, operational reach and espionage TTP.

2. (U) Developed Program Actors. Actors with extensive access to information technology (IT) through industry. They possess established cyberspace operations programs, to include programs for disruptive and destructive actions, and traditional espionage capabilities. This actor type has limited resources and may lack global reach.

3. (U) Capable Actors. Actors who possess traditional espionage capability and a developing cyberspace operations capability. They lack the resources or penetration of developed program actors. These actors focus on remote access, disruption of service and insider-enabled operations.

4. (U) Remote Access Capable Actors. These actors can access Internet connected systems using openly available hacker tools but lack a traditional espionage capability.

5. (U) Stand-alone Actors. Actors with access to hardware and software expertise who understand TTPs but exhibit little evidence of active cyberspace operations or traditional espionage activity.

(b) (U) Threat Vectors. Adversaries typically employ six (6) broad threat vectors, independently or in some combination, to affect the security of computer networks. These are general descriptions and any single threat may be a combination of several of these types:

1. (U) Insider. Self-motivated, co-opted or recruited individuals with legitimate access to targeted information systems using those systems in un-authorized manners.

2. (U) Remote Network. Intrusions or attacks through or on the Internet via other remotely available connections or access points.

3. (U) Outsourced Service. Access to information systems through individuals or companies contracted to provide services to the target.

4. (U) Supply Chain. Subversion of the design, manufacturing and production, distribution, installation, or maintenance of hardware or software, to include, access through outsourcing services, individuals, or companies contracted to provide services to the target.

5. (U) Close Access. Exploitation of information systems that requires the intruder to be in close proximity to the target because of security measures or isolation.

Close access includes the use of implanted devices as well as the collection of electronic emanations from the target or wireless access points.

6. (U) Foreign Ownership. Penetration of information systems and networks through foreign proxies, subsidiaries, or joint ventures. Closely associated with the insider, supply chain or outsourcing threat vectors.

b. (U//FOUO) Friendly Forces. In order to address risks to the DoD GIG effectively and to secure freedom of action in cyberspace, USCYBERCOM was established by DoD to integrate cyberspace operations and synchronize warfighting effects across the global security environment, as well as, to provide support to civil authorities and mission partners when directed. [redacted] (b)(3) USSC

[redacted] (b)(3) USSC

(1) (U//FOUO) Supporting Commands.

(a) (U//FOUO) Service Components. Those forces under the operational control (OPCON) of USCYBERCOM.

(b) (U//FOUO) Combatant Commands. Combatant commands build and maintain subordinate or supporting operational plans or associated named branch or sequel plans. They respond to direction from USCYBERCOM for DoD GIG Operations and Defensive Cyberspace Operations that transcend a given combatant command.

(2) (U//FOUO) Services. Each military service provides secure, assured, and interoperable information systems and networks and trained personnel for the effective execution of military cyberspace operations. The Services ensure that Service-managed portions of all DoD GIG programs are planned, resourced, acquired, and implemented IAW DoD policies and priorities. They provide USCYBERCOM Service Component forces required to execute OGS cyberspace operations.

(3) (U//FOUO) Agencies and Field Activities. All DoD agencies and field activities are subject to this order and USCYBERCOM direction for OGS cyberspace operations. Agencies and field activities ensure that agency managed portions of all DoD GIG programs are planned, resourced, acquired, and implemented IAW DoD priorities. The following agencies are specifically identified to support USCYBERCOM:

(a) (S//REL TO USA, FVEY) [redacted] (b)(1) / (b)(3) USSC

[redacted] (b)(1) / (b)(3) USSC

(b)(1) / (b)(3) USSC

(b) (U//~~FOUO~~) The Defense Information Systems Agency (DISA). DISA supports OGS by engineering and providing C2 capabilities and enterprise infrastructure to continuously operate and assure a global enterprise for the DISA elements of the DoD GIG providing direct support to joint warfighters, national-level leaders, and other mission partners across the full spectrum of operations.

(c)(U//~~FOUO~~)

(b)(3) USSC

(b)(3) USSC

(4) (U//~~FOUO~~) Law Enforcement/Counterintelligence (LE/CI). The LE/CI community, while not wholly within DoD, contributes to OGS by providing timely actionable intelligence in support of current operations. LE/CI identifies the linkages between insider and other threats to the DoD GIG. USCYBERCOM will share information and intelligence, and assist the LE/CI community as requested or directed.

(5) (U//~~FOUO~~) Other non-DoD agencies

(a) (U) Other U.S. Government Agencies. Other U.S. Government Agencies may have access to the DoD GIG and DoD GIG resources to include the DHS, DoJ, DoS, DoE, OMD, WHS, and FBI. USCYBERCOM, ICW DISA, will coordinate with non-DoD agencies for the security of those portions of the DoD GIG accessed or used by those.

(b) (S//REL TO USA, FVEY)

(b)(1) USSC

(b)(1) USSC

c. (U//~~FOUO~~) Area of Concern

(1) (U//~~FOUO~~) Area of Responsibility (AOR). The AOR for OGS is the DoD GIG.

(2) (U//~~FOUO~~) Area of Operations (AO). The AO for OGS is global with effects manifesting in the DoD GIG and with other portions of cyberspace accessed, as authorized, to achieve OGS objectives. The DoD GIG is the globally interconnected,



end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing on-demand information to warfighters, policy makers, and support personnel. The DoD GIG includes owned and leased communications and computing systems and services, software, data, security services, related services, and select networks of the National Security Systems (NSS).

(3) (U//FOUO) Area of Interest (AOI). For OGS, the AOI is global and is represented by the information environment comprised of physical, informational, spectral and cognitive dimensions and its cyberspace intersections with the air, land, maritime and space domains.

d. (S//REL TO USA, FVEY)

(b)(1) USSC

(b)(1) USSC

2. (S//REL TO USA, FVEY)

(b)(1) USSC

(b)(1) USSC

3. (U) Execution.

a. (U//FOUO) Concept of Operation.

(1) (U//FOUO)

(b)(7)(E) USSC

(b)(7)(E) USSC

(a) (S//REL TO USA, FVEY)

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(b) (S//REL TO USA, FVEY)

(b)(1) USSC

(b)(1) USSC

1. (S//REL USA, FVEY)

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

a. (S//REL USA, FVEY) (b)(1) USSC

(b)(1) USSC

b. (S//REL USA, FVEY) (b)(1) USSC

(b)(1) USSC

c. (S//REL USA, FVEY) (b)(1) USSC

(b)(1) USSC

2. (S//REL USA, FVEY) (b)(1) USSC

(b)(1) USSC

(b)(1) USSC

a. (S//REL USA, FVEY)

(b)(1) USSC

(b)(1) USSC

(1) (S//REL USA, FVEY).

(b)(1) USSC

(b)(1) USSC

(2) (S//REL USA, FVEY)

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

(3) (S//REL USA, FVEY)

(b)(1) USSC

(b)(1) USSC

(4) (S//REL USA, FVEY)

(b)(1) USSC

(b)(1) USSC

b. (S//REL USA, FVEY)

(b)(1) USSC

(b)(1) USSC

c. (S//REL USA, FVEY)

(b)(1) USSC

(b)(1) USSC

(2) (U//FOUO) Strategic Objectives.

(a) (S//REL TO USA, FVEY)

(b)(1) USSC

(b)(1) USSC

(b) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(c) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(3) (U//~~F0U0~~) Operational Objectives.

(a) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(b) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(c) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(d) (U//~~F0U0~~) All DoD Components are in, and sustain, compliance with established DoD GIG standards.

(e) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(f) (U//~~F0U0~~) Key partner nations and organizations are enabled to coordinate, synchronize and, as required and authorized, execute DoD GIG Operations and Defensive Cyberspace Operations with USCYBERCOM to achieve OGS objectives and intent.

(g) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(h) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(i) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(j) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(k) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(l) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(m) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(n) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(o) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(p) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(q) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(r) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(s) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(t) (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

(4) (U//FOUO) End States.

(a) (U//FOUO) The DoD GIG is persistently secured, operated and defended with mission-critical elements given priority of effort.

(b) (U//FOUO) Freedom of action in cyberspace for DoD and mission partners is assured.

(c) (U//FOUO) Adversaries are deterred from attacking or exploiting the DoD GIG.

(d) (U//FOUO) DoD GIG Operations and Defensive Cyberspace Operations capabilities and capacity to secure, operate and defend the DoD GIG are fielded and available for employment.

(e) (U//~~FOUO~~) (U//~~FOUO~~) Defense Support to Civil Authorities (DSCA) is conducted when directed.

b. (U//~~FOUO~~) Tasks. Refer to Annexes for additional tasks.

(1) (U) Tasks to all DoD Components.

(a) (U//~~FOUO~~) Plan and execute DoD GIG Operations, Defensive Cyberspace Operations and related support activities to clear, hold and build a secure and defensible DoD GIG. Maintain and report compliance with USCYBERCOM orders and directives.

(b) (U//~~FOUO~~) Comply with all USCYBERCOM policies and orders. Respond to reporting requirements from USCYBERCOM J3.

(c) (U//~~FOUO~~) Provide situational awareness data to USCYBERCOM J3.

(d) (U//~~FOUO~~) Coordinate and collaborate on cyberspace equities.

(e) (U//~~FOUO~~) Collaborate to define and refine requirements that build a more secure and defensible DoD GIG.

(f) (U//~~FOUO~~) Comply with DoD IA standards.

(g) (U//~~FOUO~~) Comply with DoD equipment accountability standards and procedures.

(h) (U//~~FOUO~~) Develop and implement OPSEC plans ISO OGS.

(i) (U//~~FOUO~~) Provide USCYBERCOM J3 a list of mission-critical elements (systems, networks and nodes) on or connected to the DoD GIG.

(j) (U//~~FOUO~~) Implement Information Condition (INFOCON), or Cyber Condition (CYBERCON) when approved, and report compliance to the USCYBERCOM Joint Operations Center (JOC).

(k) (U//~~FOUO~~) ICW USCYBERCOM J3, develop and implement DoD GIG Operations and Defensive Cyberspace Operations assessment program.

(l) (U//~~FOUO~~) Implement USCYBERCOM-directed Cyber Security Inspection Program and provide reporting criteria to USCYBERCOM for DoD-wide assessments.

(m) (U//~~FOUO~~) Provide reporting as directed in the Annexes.

(n) (U//~~FOUO~~) ICW USCYBERCOM J8, program and budget for forces assigned or OPCON to USCYBERCOM. Provide USCYBERCOM J8 with Planning.



Programming, Budgeting and Execution (PPBES) documents, Service programs and PPBES issues impacting DoD GIG Operations and Defensive Cyberspace Operations.

(2) (U) Tasks to HQ, USCYBERCOM.

(a) (U) J0. Develop and maintain currency of Annex F (Public Affairs), Annex Y (Strategic Communications) and Appendix 9 (Legal) to Annex C (Operations).

(b) (U) J1

1. (U//~~FOUO~~) ICW USSTRATCOM J1, coordinate with the Services to ensure that qualified military and civilian personnel are assigned and recruited for DoD GIG Operations and Defensive Cyberspace Operations.

2. (U//~~FOUO~~) Provide plans, policies and guidance for personnel readiness issues that support execution of OGS.

3. (U//~~FOUO~~) ICW USSTRATCOM J1, identify skill sets, training and readiness metrics for forces in support of OGS.

4. (U//~~FOUO~~) Develop and maintain Annex E (Personnel). Coordinate input from J8 for Appendix 3 (Finance and Disbursing).

(c) (U) J2

1. (U//~~FOUO~~) Conduct Operational Preparation of the Environment (OPE) ISO OGS within the limits of USCYBERCOM's delegated authorities.

2. (U//~~FOUO~~) Conduct continuous intelligence operations, including post-event assessments, ISO OGS.

3. (U//~~FOUO~~) Through the Joint Intelligence Operations Center (JIOC), ensure the availability of all sources of intelligence information from Combatant Command and national intelligence resources.

4. (U//~~FOUO~~) Coordinate, synchronize and integrate intelligence into operational plans and DoD GIG Operations and Defensive Cyberspace Operations execution. Engage actively with the IC.

5. (U//~~FOUO~~) Provide a quarterly threat update to all DoD Components and authorized mission partners highlighting current and emerging threats.

6. (U//~~FOUO~~) ICW DIA and the IC, develop, implement and maintain an intelligence architecture to support USCYBERCOM operations.

7. (U//~~FOUO~~) Develop and maintain Annex B (Intelligence).

(d) (U) J3

1. (U//F0U0) Command and control DoD GIG Operations and Defensive Cyberspace Operations to achieve OGS objectives and desired end states.
2. (U//F0U0) Lead development and direct implementation of DoD GIG monitoring.
3. (U//F0U0) Direct, coordinate, synchronize and deconflict Defensive Cyberspace Operations in order to achieve unity of effort to clear adversary presence and vulnerabilities on the DoD GIG in priority of mission criticality.
4. (U//F0U0) Direct, coordinate and synchronize actions to hold secure the DoD GIG from adversary intrusion or attack with priority on the mission-critical elements.
5. (U//F0U0) ICW USSTRATCOM, define or update criteria and implement procedures for changes to INFOCON, or when approved, CYBERCON.
6. (U//F0U0) Lead development of, and issue, necessary orders to accomplish OGS objectives.
7. (U//F0U0) Lead development and direct the implementation of reporting and analysis processes for DoD GIG Operations and Defensive Cyberspace Operations.
8. (U//F0U0) Lead the development, coordination and synchronization of options to establish and maintain cyberspace superiority to hold secure the DoD GIG. Direct implementation as appropriate with priority to mission-critical elements.
9. (U//F0U0) Establish and implement procedures for the conduct of risk assessments related to DoD GIG Operations and Defensive Cyberspace Operations.
10. (U//F0U0) Establish and implement a process to assess Tactics, Techniques and Procedures (TTP) for DoD GIG Operations and Defensive Cyberspace Operations.
11. (U//F0U0) ICW USSTRATCOM and USNORTHCOM, establish a DoD process for responding to national-level cyber incidents.
12. (U//F0U0) Develop and implement a comprehensive program for assessing DoD components' DoD GIG Operations and Defensive Cyberspace Operations effectiveness and provide recurring feedback to DoD components on their status.
13. (U//F0U0) Establish and maintain an effective Cyber Security Inspection Program.

14. (U//FOUO) Establish and implement governance of the DoD GIG that specifies compliance requirements, establishes security standards, sets service delivery standards and enforcement processes and procedures.

15. (U//FOUO) Establish cyberspace SA information requirements, reporting procedures and technology baseline necessary to provide near real time SA. Implement and promulgate to all DoD Components and designated mission partners. Disseminate global DoD GIG Operations and Defensive Cyberspace Operations SA.

16. (U//FOUO) Establish a process to identify mission-critical elements of the DoD GIG. Maintain an active and current database.

17. (U//FOUO) Establish criteria and technology baseline and implement Indications and Warning (I&W) processes and procedures.

18. (U//FOUO) Establish and lead Joint Operational Planning Teams (OPT) in order to support future DoD GIG Operations and Defensive Cyberspace Operations.

19. (U//FOUO) Implement procedures and direct the operational configuration of DoD capabilities to achieve unity of effort ISO OGS.

20. (U//FOUO) Plan, implement and direct execution of DNDO, to include establishing Pre-approved Actions (PAA) through the use of deliberate orders processes, which enable rapid action to clear vulnerabilities and adversary presence on the DoD GIG. The priority for DNDO will be on mission-critical elements of the DoD GIG. Ensure deconfliction, coordination and synchronization across DoD and with mission partners having equities in any given action.

21. (U//FOUO) Develop and implement a more rapid and comprehensive early warning capability of adversary threat activities against the DoD GIG.

22. (U//FOUO) Provide geolocation and characterization of SATCOM interference; develop and promulgate TTP to resolve SATCOM interference.

23. (U//FOUO) ICW USSTRATCOM, NSA and DISA, develop and deploy shared or peer-to-peer sensors to monitor and detect adversary cyber capabilities and methods.

24. (U//FOUO) Plan, organize and deploy Cyber Support Elements (CSEs), to include Expeditionary Cyber Support Elements (ExCSEs), and other adaptive cyber organizations to the Combatant Commands to support planning and operations and improve SA.

25. (U//FOUO) On order of the SecDef and after completing the required inter-agency deconfliction, direct Defensive Cyberspace Operations beyond the boundary of the DoD GIG. Coordinate, synchronize and deconflict with other DoD and authorized mission partners, as appropriate.

26. (U//~~F~~OUQ) Develop and maintain the currency of the OGS Base Order and Annex A (Task Organization), Annex C (Operations), Annex J (Command Relationships), Annex R (Reports), Annex S (Special Technical Operations (STO)) and Annex Z (Distribution). Consolidate all Annexes with the Base Order. Disseminate to the DoD and authorized mission partners.

27. (U) Develop and implement a cyberspace synchronization process. Host a global synchronization conference at least annually and address coordination across DoD components and the U.S. Coast Guard.

(e) (U) J4

1. (U//~~F~~OUQ) Plan, coordinate, direct and execute logistics and sustainment functions ISO OGS.

2. (U//~~F~~OUQ) Develop and maintain Annex D (Logistics and Sustainment).

(f) (U) J5

1. (U//~~F~~OUQ) Develop, and update as required, a cyberspace campaign plan for cyberspace operations.

2. (U//~~F~~OUQ) Support current and future operations planning as subject matter experts for supported Combatant Command contingency plan execution.

3. (U//~~F~~OUQ) Lead development of future plans to accomplish OGS objectives.

4. (U//~~F~~OUQ) ICW USSTRATCOM and USCYBERCOM J8, advocate for future capabilities and capacity to achieve OGS objectives. Establish and maintain the Cyber Capabilities Registry (CCR) ICW DoD Components and mission partners.

5. (U//~~F~~OUQ) ICW USSTRATCOM, assess policy and doctrine related to OGS and recommend changes or new policy and doctrine supportive of full achievement of OGS intent and objectives.

6. (U//~~F~~OUQ) ICW USSTRATCOM, ensure future plans are supportive of OGS end states and objectives.

7. (U//~~F~~OUQ) Develop and maintain Annex O (Advocacy), Annex V (Mission Partner Coordination) and Annex W (Acronyms, Glossary, References).

(g) (U) J6

1. (U//~~F~~OUQ) Adjudicate security issues associated with connections on the DoD GIG. Coordinate adjudication with USCYBERCOM J3 and affected organization.

2. (U//~~FOUO~~) Advise and assist USCYBERCOM J3 with planning and execution of DoD GIG Operations and Defensive Cyberspace Operations.
3. (U//~~FOUO~~) Develop and implement network configurations to facilitate DoD GIG Operations and hold secure the DoD GIG.
4. (U//~~FOUO~~) ICW DISA and NSA, plan, develop, implement and integrate critical communications systems and services to support DoD GIG Operations and Defensive Cyberspace Operations.
5. (U//~~FOUO~~) ICW DISA and USCYBERCOM J1, J3 and J7, develop a user certification process and set of Information Assurance (IA) standards for baseline competency for authorized users on the DoD GIG.
6. (U//~~FOUO~~) Provide technical assistance and expertise to assure timely and accurate situational awareness and GIG monitoring capabilities to the USCYBERCOM J3 JOC.
7. (U//~~FOUO~~) Develop and maintain Annex K (Command, Control, Communications and Computing (C4)).

(h) (U) J7

1. (U//~~FOUO~~) ICW USJFCOM, develop, sponsor and conduct periodic joint training and exercises to assess DoD GIG Operations and Defensive Cyberspace Operations procedures, capabilities, effects, personnel training proficiency and TTP.
2. (U//~~FOUO~~) ICW J1, J3 and J6, develop a master training program to sustain and enhance the proficiency of personnel engaged in DoD GIG Operations and Defensive Cyberspace Operations.

3. (S//REL TO USA, FVEY)

(b)(1) USSC

(b)(1) USSC

4. (U//~~FOUO~~) Establish and implement a lessons learned process to capture results, best practices and practices to avoid.
5. (U//~~FOUO~~) Develop and maintain Annex U (Exercises and Training).

(i) (U) J8

1. (U//~~FOUO~~) ICW USSTRATCOM, develop and implement a process to present OGS resource requirements in the POM cycle.
2. (U//~~FOUO~~) Perform resource management ISO OGS.

3. (U//FOUO) ICW J5 and J3, advocate for resources ISO OGS.
4. (U//FOUO) Publish and maintain Appendix 3 (Finance and Disbursing) to Annex E (Personnel) to OGS.

(3) (U) Tasks to USCYBERCOM Service Components.

(a) (U) Tasks to all USCYBERCOM Service Components.

1. (U//FOUO) Respond to direction from USCYBERCOM for planning and execution of DoD GIG Operations and Defensive Cyberspace Operations that secure, operate and defend the DoD GIG with priority of effort on mission-critical elements.
2. (U//FOUO) Coordinate with USCYBERCOM J3 for mission priorities, requirements and capabilities.
3. (U//FOUO) Develop and maintain subordinate or supporting operational plans and orders ISO USCYBERCOM OGS or associated branch or sequel plans and orders.
4. (U//FOUO) Maintain proficiency of, administer, support and report readiness of Service forces delegated as OPCON from USCYBERCOM.
5. (U//FOUO) If authorized to conduct such activities, conduct or support intelligence activities as directed.
6. (U//FOUO) ICW USCYBERCOM J1, coordinate with the Services to ensure that qualified military and civilian personnel are assigned and recruited for DoD GIG Operations and Defensive Cyberspace Operations.
7. (U//FOUO) ICW USCYBERCOM J3, facilitate the presentation of Service cyber forces for DoD GIG Operations and Defensive Cyberspace Operations and leverage Service capabilities and capacity.
8. (U//FOUO) Provide expeditionary forces as directed.
9. (U//FOUO) Assist USCYBERCOM, as requested, with operational planning, to include identifying forces, capabilities, logistics requirements and other related planning factors.
10. (U//FOUO) On order, assist in the establishment of a Joint Task Force (JTF) headquarters and, as available, deploy C2 systems to support the JTF.
11. (U//FOUO) ICW USCYBERCOM J33, provide SA and performance data of current cyber operations.
12. (U//FOUO) When supporting a Combatant Command, and ICW USCYBERCOM J3, coordinate for approval of Theatre-based cyber actions.

(b) (U) U.S. Air Force Cyber Command/24<sup>th</sup> AF (AFCYBER). Refer to Annexes for tasks specifically assigned and implied.

(c)(U) U.S. Army Cyber Command /2d Army (ARCYBER). Refer to Annexes for tasks specifically assigned and implied.

(d) (U) U.S. Fleet Cyber Command/10<sup>th</sup> Fleet (FLTCYBERCOM). Refer to Annexes for tasks specifically assigned and implied.

(e) (U) U.S. Marine Forces Cyber (MARFORCYBER). Refer to Annexes for tasks specifically assigned and implied.

(4) (U) Tasks to Combatant Commands.

(a) (U//~~F0U0~~) Respond to direction from USCYBERCOM for planning and execution of DoD GIG Operations and Defensive Cyberspace Operations that transcend a Combatant Command's AOR.

(b) (U//~~F0U0~~) Develop and maintain subordinate or supporting operational plans and orders ISO USCYBERCOM OGS or associated branch or sequel plans and orders.

(c) (U//~~F0U0~~) Collaborate with USCYBERCOM to facilitate coordination and deconfliction of DoD GIG Operations and Defensive Cyberspace Operations.

(d) (U//~~F0U0~~) Integrate DoD GIG Operations and Defensive Cyberspace Operations into contingency plans.

(e) (U//~~F0U0~~) Accept CSEs and LNOs and integrate into operational and intelligence flow.

(5) (U) Tasks to Services.

(a) (U//~~F0U0~~) Support OGS by providing secure, assured and interoperable information systems and networks and ensuring that pertinent information is shared with USCYBERCOM.

(b) (U//~~F0U0~~) Provide organized, trained and equipped forces to USCYBERCOM, through USSTRATCOM.

(c)(U//~~F0U0~~) ICW USCYBERCOM, ensure that Service-managed portions of all DoD GIG programs are planned, resourced, acquired and implemented to support attainment of OGS end states and objectives.

(d) (U//~~F0U0~~) As requested, support USCYBERCOM planning and execution of DoD GIG Operations and Defensive Cyberspace Operations.

(e) (U//~~FOUO~~) ICW USCYBERCOM, develop and maintain DoD GIG Operations and Defensive Cyberspace Operations capabilities for implementation ISO OGS.

(f) (U//~~FOUO~~) Support USCYBERCOM with assessment of DoD GIG standards compliance.

(g) (U//~~FOUO~~) Comply with standards to clear, hold and build a secure and defensible DoD GIG.

(h) (U//~~FOUO~~) Provide shared SA of Service-operated portions of the DoD GIG to USCYBERCOM to support DoD GIG Operations and Defensive Cyberspace Operations.

(i) (U//~~FOUO~~) ICW USSTRATCOM, provide Intelligence, Surveillance and Reconnaissance (ISR) forces and intelligence to USCYBERCOM J2.

(j) (U//~~FOUO~~) USSOCOM will comply with Service tasks with the exclusion of providing organized, trained, and equipped forces.

(6) (U) Tasks to DoD Agencies and Field Activities.

(a) (U) Tasks to all DoD Agencies and Field Activities.

1. (U//~~FOUO~~) ICW USCYBERCOM, ensure that agency-managed and field activity-managed portions of all DoD GIG programs are planned, resourced, acquired and implemented to support attainment of OGS end states and objectives.

2. (U//~~FOUO~~) As directed, support USCYBERCOM planning and execution of DoD GIG Operations and Defensive Cyberspace Operations.

3. (U//~~FOUO~~) Respond to direction from USCYBERCOM for planning and execution of DoD GIG Operations and Defensive Cyberspace Operations.

4. (U//~~FOUO~~) ICW USCYBERCOM J33, provide situational awareness and performance data of current and plan cyber operations for assigned portions of the GIG to support DoD GIG Operations and Defensive Cyberspace Operations.

(b) (U) National Security Agency (NSA).

1. (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC

2. (U//~~FOUO~~) [redacted] (b)(3) USSC  
[redacted] (b)(3) USSC

3. (S//REL TO USA, FVEY) [redacted] (b)(1) USSC  
[redacted] (b)(1) USSC



4. (S//REL USA, FVEY) [redacted] (b)(1) USSC

[redacted] (b)(1) USSC

(c) (U) Defense Information Systems Agency (DISA).

1. (U//F0U0) Provide engineering, C2 capabilities and enterprise infrastructure ISO OGS.

2. (U//F0U0) Provide direct support to USCYBERCOM for DoD GIG Operations and Defensive Cyberspace Operations.

(d) (U) Defense Intelligence Agency (DIA).

1. (U//FOUO) [redacted] (b)(3) USSC

(b)(3) USSC

2. (U//FOUO) [redacted] (b)(3) USSC

[redacted] (b)(3) USSC

3. (U//FOUO) [redacted] (b)(3) USSC

[redacted] (b)(3) USSC

(e) (U) Law Enforcement and Counterintelligence (LE/CI).

1. (U//F0U0) Provide timely actionable intelligence in support of DoD GIG Operations and Defensive Cyberspace Operations, to include identifying the linkages between insider and other threats.

2. (U//F0U0) Provide intelligence systems support, funding, personnel and training ISO OGS.

3. (U//F0U0) Synchronize investigative actions related to malicious activity against the DoD GIG among Department of Defense law enforcement and counterintelligence investigative organizations.

c. (U//F0U0) Coordinating Instructions.

(1) (U//F0U0) This OPORD is effective upon receipt for planning and execution.

(2) (U//F0U0) Direct Liaison Authorized (DIRLAUTH) as required to fulfill OGS mission requirements. Maintain close coordination with USCYBERCOM and supported commands. Coordination with partner nations must be accomplished through USCYBERCOM, ICW the supported command, USSTRATCOM and the Joint Staff (JS), and following appropriate foreign disclosure and information sharing regulations and policies, as well as, existing memorandums of agreement or understanding.

(3) (U//~~F0U0~~) For actions associated with OGS, the rules of engagement are per Ref d.

(4) (U//~~F0U0~~) To the maximum extent possible use the Joint Operations Planning and Execution System (JOPES) to facilitate planning.

(5) (U//~~F0U0~~) Routine rotation of forces is authorized, as coordinated with the supported command.

(6) (U//~~F0U0~~) Operational reporting will be in accordance with published annexes to this OPORD and occur via DoD component operational channels to the USCYBERCOM JOC while providing SA to the affected DoD component or mission partner.

(7) (U//~~F0U0~~) DoD components that desire to achieve effects that exceed authorities or capabilities, or are not otherwise addressed in existing plans or orders, will contact the USCYBERCOM J3 for direction and guidance.

(8) (U//~~F0U0~~) DoD GIG Operations and Defensive Cyberspace Operations affecting IC networks under authority of the Director of National Intelligence (DNI) and all networks that process sensitive compartmented information (SCI) will be executed in accordance with joint procedures defined by the Secretary of Defense (SecDef) and the DNI or their designees.

(9) (U//~~F0U0~~) Submit any recommended updates to this OPORD, its annexes, or appendixes to USCYBERCOM J3.

(10) (U//~~F0U0~~) USCYBERCOM OPORD 05-01 (formerly Joint Task Force-Global Network Operations (JTF-GNO)) is superseded by this order.

(11) (U//~~F0U0~~) A standard set of metrics and measurements, developed and promulgated by USCYBERCOM, will be used to assess DoD GIG operating performance, determine the mission impact of service degradations or outages, and assess the effectiveness of Defensive Cyberspace Operations capabilities, to include, sensors and systems to counter threats and vulnerabilities.

#### 4. (U) Administration and Logistics.

a. (U//~~F0U0~~) Funding. DoD components will fund all costs of operations required or incurred as a result of OGS, including deployment and redeployment of personnel or units. USCYBERCOM Service Components will track and report all incremental costs incurred ISO this order to USCYBERCOM J8. Refer to Annex O for further guidance, tasks and requirements.

b. (U//~~F0U0~~) Logistics and Sustainment. Refer to Annex D for further guidance, tasks and requirements.

(1) (U//~~F0U0~~) All DoD components and supporting mission partners will conduct sustainment activities to ensure uninterrupted conduct of OGS.

(2) (U//~~F0U0~~) While it is anticipated that the majority of cyberspace operations forces would not physically deploy to accomplish OGS tasks, if deployment is necessary all USCYBERCOM Service Components will coordinate with the USCYBERCOM J4.

c. Personnel. Refer to Annex E for further guidance, tasks and requirements.

(1) (U//~~F0U0~~) Concept of Personnel Support. Prior to and during OGS, components will receive the majority of routine personnel support through their home station and parent unit. J1 monitors component personnel operations and provides assistance, as required.

(2) (U//~~F0U0~~) Strength Reporting. USCYBERCOM J1 provides the Joint Personnel Status (JPERSTAT) to Joint Staff J1, USSTRATCOM J1 and USCYBERCOM leadership as directed. All components that are under the Operational Control (OPCON) of CDRUSCYBERCOM will submit the JPERSTAT to USCYBERCOM J1 daily by 1600Z. The JPERSTAT Report is to be classified SECRET and the primary transmission method shall be via secure email. Reports shall be formatted in accordance with CJCSM 3150.13C.

d. (U//~~F0U0~~) Public Affairs (PA). Refer to Annex F for further guidance, tasks and requirements.

(1) (U//~~F0U0~~) The PA posture for OGS is passive, respond to query only. USCYBERCOM Service Components will coordinate and synchronize PA products with USCYBERCOM PAO prior to release.

(2) (U//~~F0U0~~) In the event that information regarding a specific defensive cyberspace operation is disclosed, the following statement is authorized after proper notification to USCYBERCOM PAO: "The Department of Defense depends on cyberspace for critical military capabilities and must be able to secure, operate and defend DoD networks. The Department has more than 15,000 networks and 7 million computing devices that are vital to our operations. The Department's strategy requires the full range of capabilities to defend against a variety of threats and to protect our networks."

e. (U//~~F0U0~~) Strategic Communication (SC). USCYBERCOM Service Components will coordinate and synchronize OGS-related SC themes and messages with USCYBERCOM SC prior to release. Refer to Annex Y for further guidance, tasks and requirements.

5. (U) Command and Control.

a. (U//FOUO) CDRUSCYBERCOM is the supported commander for OGS and all other DoD components are supporting. USCYBERCOM provides the C2 that ensures synchronization, coordination, deconfliction and direction of DoD GIG Operations and Defensive Cyberspace Operations that transcend a Combatant Command AOR or that have effects of a global nature. CDRUSSTRATCOM delegated authority to CDRUSCYBERCOM in USSTRATCOM OGP OPORD to direct the security, operation and defense of the DoD GIG. USCYBERCOM was designated the main effort in the USSTRATCOM OGP OPORD with all other DoD components supporting. Previously, CDRUSSTRATCOM was designated the supported commander in the DoD by the SecDef.

b. (U//FOUO) For DSCA operations, USCYBERCOM and USCYBERCOM Service Components are supporting to USPACOM and USNORTHCOM.

c. (U//FOUO) For Combatant Command AOR-specific and functional mission networks and systems, the relevant Combatant Command is the supported commander for DoD GIG Operations and Defensive Cyberspace Operations requirements and USCYBERCOM and its components are supporting. The supported Combatant Command is responsible for the timing, sequencing and operational effects within its AOR.

d. (C//REL TO USA, FVEY)

(b)(1) USSC

(b)(1) USSC

e. (C//REL TO USA, FVEY)

(b)(1) USSC

(b)(1) USSC

f. (U//FOUO) All communications regarding OGS will be by appropriately secured means, and with full adherence to OPSEC requirements.

g. (U//FOUO) DoD GIG Operations and Defensive Cyberspace Operations data will be shared and exchanged through common interoperable standards in accordance with DoD data sharing policies and guidance.

h. (U//FOUO) (U//FOUO) Standard orders formats (OPORD, Fragmentary Order (FRAGO), Warning Order (WARNORD) and Plan Order (PLANORD)) will be used to issue operational direction to secure, operate and defend the DoD GIG and for any other cyberspace operation when directed. Information dissemination formats will be limited to Cyber Daily Reports, Situation Awareness Bulletins, J2 Cyber Alerts and Intelligence Summaries. Methods of dissemination will remain unchanged. Refer to Appendix 23 (Orders and Reports) to Annex C for further guidance and direction.

i. (U//FOUO) In the event USCYBERCOM is unable to operate from its facilities at Fort George G. Meade, C2 will be executed per USCYBERCOM Continuity of Operations (COOP) Plan.



KEITH B. ALEXANDER  
General, USA  
Commanding

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

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

Annexes

- A – Task Organization
- B – Intelligence
- C – Operations
- D – Logistics and Sustainment
- E – Personnel
- F – Public Affairs
- G – Civil Affairs (omitted)
- H – Meteorological and Oceanographic (omitted)
- I – Not Used
- J – Command Relationships
- K – Command, Control, Communications, and Computer (C4) Systems
- L – Environmental Considerations (omitted)
- M – Geospatial Information and Services (omitted)
- N – Space Operations (omitted)
- O – Advocacy
- P – Host Nation Support (omitted)
- Q – Medical Services (omitted)
- R – Reports
- S – Special Technical Operations (STO)
- T – Consequence Management (omitted)
- U – Exercises and Training
- V – Mission Partner Coordination
- W – Acronyms, Glossary, References
- X – Execution Checklist (omitted)
- Y – Strategic Communications
- Z - Distribution

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL~~

Subject: (U//~~FOUO~~) OPORD 12-1016 (HOST BASED SECURITY SYSTEM (HBSS)  
DEPLOYMENT AND OPERATIONS)

Originator: USCYBERCOM(SC)

DTG: 212131Z Aug 12

Precedence: ROUTINE

DAC: General

To: AFOG AFWATCH(SC), AFRICOM CDR(MC), AFRICOM JOC CHIEF(MC), CDR NORAD(SC),  
CDR USCENTCOM(MC), CDR USPACOM HONOLULU HI(SC), CDR USSOCOM(MC), CDR  
USSOUTHCOM(MC), CDR USSTRATCOM(SC), CMD CTR USSTRATCOM(SC), CMC WASHINGTON  
DC(SC), CNO WASHINGTON DC(SC), COMDT COGARD WASHINGTON DC, DA HODA  
SECRETARIAT(SC), EUCOM EPOC JOC(MC), EUCOM CDR(MC), HQ AFRICOM(MC), HQ USAF  
CC(SC), HQ USPACOM JOC(SC), HQ USPACOM(SC), HQ USSOUTHCOM(MC), HQ  
USSTRATCOM(SC), N-NC CMD CENTER(SC), USCENCOM COMMAND CENTER(MC), BTA  
ARLINGTON VA(SC), DARPA ARLINGTON VA(MC), DECA HQ(SC), DFAS CLEVELAND OH(SC),  
DISA DCC(SC), DISA DIRECTOR(SC), DSCA OPS(SC), DNI WATCH, DSS WASHINGTON DC,  
DTRA OPSCENTER WASHINGTON DC, HQ DCMA(SC), HQ DLA FORT BELVOIR VA(SC), MDA  
OPERATIONS CENTER(MOC)(SC), NRO WASHINGTON DC, TMA FALLS CHURCH VA, USUHS  
BETHESDA MD(SC), DIA WASHINGTON DC, DISA WASHINGTON DC(SC), DNI WASHINGTON  
DC, DNI WATCH WASHINGTON DC, NSACSS FT GEORGE G MEADE MD, NSACSS SAN ANTONIO  
TX, OSD CIO-PENTAGON CIO(SC), 24AF A3(SC), 24AF CC(SC), 6240C CC(SC), ARCYBER  
WATCH OFFICER(MC), ARCYBER CDR(SC), ARCYBER G3(SC), ARCYBER G33(MC),  
COMLTCYBERCOM FT GEORGE G MEADE MD(SC), COMNAVCYBERFOR VIRGINIA BEACH  
VA(SC), MARFORCYBERCOM FT MEADE MD(SC), COGARD CTRT ALEXANDRIA VA, COGARD  
CYBERCOM WASHINGTON DC

cc: OSD WASHINGTON DC, DEPT OF COMMERCE WASHINGTON DC, DEPT OF ENERGY  
WASHINGTON DC, DEPT OF HOMELAND SECURITY WASHINGTON DC, DEPT OF JUSTICE  
WASHINGTON DC, DEPT OF STATE WASHINGTON DC, NAVCYBERDEFOPSCOM VIRGINIA BEACH  
VA(SC), FEMA HQ WASHINGTON DC, NMCC WASHINGTON DC, SECDEF WASHINGTON DC,  
USCYBERCOM FT GEORGE G MEADE MD

-----  
~~SECRET//REL TO USA, AUS, CAN, GBR, NZL/25X1~~

REF/A/OPORD/USCYBERCOM/19MAY11/(U//~~FOUO~~) OPERATION GLADIATOR SHIELD (OGS)  
OPERATIONS ORDER (OPORD) 11-002 (S//REL TO USA, FVEY)//  
REF/B/DOC (U) FRAGO 13 TO JTF-GNO OPORD 05-01 REQUIREMENTS FOR RAPID  
DEPLOYMENT OF HBSS ON SIPRNET AND UNCLASSIFIED NETWORKS/26 NOV 08//(S//REL TO  
USA, FVEY)// REF/C/DOC (U) USCYBERCOM CTO 10-080 HOST BASED SECURITY SYSTEM  
BASELINE UPDATES FOR MAINTENANCE RELEASE 5 (MR5)/(U//~~FOUO~~)//  
REF/D/SIPRNET URL(S) ~~HTTPS://WWW.TYPER.COM.MIL/MIL/US/HBSS/DEFAULT1.ASPX//~~  
REF/E/SIPRNET URL(U) ~~HTTPS://PATCHES.MONT.DISA.MIL//~~  
REF/E/SIPRNET URL(U) ~~HTTPS://PATCHES.MONT.DISA.MIL//~~  
REF/G/DOC(U)CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL 6510.01A INFORMATION  
ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND) VOLUME 1 (INCIDENT HANDLING  
PROGRAM)/24 JUN 09//  
REF/H/DOC(U)CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION 6510.01E  
INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND)/09 FEB 11//  
REF/I/DOC(U)DOD DIRECTIVE 0-8530.1 COMPUTER NETWORK DEFENSE(CND)/08 JAN  
01//(U//~~FOUO~~)//  
REF/J/DOC (U) USCYBERCOM CTO 10-133 COMMUNICATIONS TASKING ORDER (CTO) 10-133  
PROTECTION OF CLASSIFIED INFORMATION ON DEPARTMENT OF DEFENSE (DOD) SECRET  
INTERNET PROTOCOL ROUTER NETWORK (SIPRNET)

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL~~



3.A. (U//~~FOUO~~) COMMANDER'S INTENT.//

3.A.1. (U//~~FOUO~~) PURPOSE. THE DEPLOYMENT, EMPLOYMENT, REPORTING, ANALYSIS, AND OPERATIONAL USE OF HBSS FOR DEFENSE OF THE DOD GIG.//

3.A.2. (U//~~FOUO~~) METHOD. USCYBERCOM WILL DIRECT DEFENSIVE ACTIONS AND MANEUVER TO DENY THE ADVERSARY A Foothold ON THE DOD GIG. THE DOD REQUIRES ROBUST, ADAPTIVE, AND AGILE PROTECTION OF ITS INFORMATION SYSTEMS. HBSS PROVIDES A CRITICAL LAYER OF THE DEFENSE-IN-DEPTH OF THE GIG, AND IS ABLE TO DETECT, PREVENT, AND/OR MITIGATE CYBER ATTACKS AT THE HOST LEVEL.//

3.A.3. (U) END STATE//

3.A.3.A. (U//~~FOUO~~) HBSS CAPABILITY IS FIELDed AND FULLY MISSION READY.

3.A.3.B. (U//~~FOUO~~) ADVERSARIES ARE DETERRED FROM ATTACKING OR EXPLOITING THE DOD GIG.

3.A.3.C. (U//~~FOUO~~) THE DOD GIG IS PERSISTENTLY SECURED AND DEFENDED USING HBSS AS A KEY ELEMENT OF LAYERED, INTEGRATED DEFENSIVE CYBER OPERATIONS.

3.B. (U) CONCEPT OF OPERATIONS. SEE ANNEX C FOR DETAILED DESCRIPTION.

3.C. (U) TASKS

3.C.1. (U) TASKS TO CC/S/A/FA

3.C.1.A. (U//~~FOUO~~) DEPLOY HBSS AGENT AND MODULES TO ALL COMPATIBLE SYSTEMS AND NETWORKS IAW ANNEX C, APPENDIX 1 AND 2, IN ORDER TO DENY AND DETER ADVERSARIAL ACTION ON THE DOD GIG. SYSTEM COMPATIBILITY IS DETERMINED BY THE OPERATING SYSTEM. A LINK TO THE "HBSS COMPATIBILITY MATRIX" IS PROVIDED AT (REF D) UNDER THE TTP SUBPAGE.

3.C.1.B. (U//~~FOUO~~) REPORT ASSFT DATA TO THE TIER ONE (ENTERPRISE) SERVER IAW ANNEX C, APPENDIX 1 IN ORDER TO PROVIDE INDICATIONS AND WARNING DATA FOR FURTHER ANALYSIS FROM TIER THREE (LOCAL) TO TIER ONE (ENTERPRISE).

3.C.1.C. (U//~~FOUO~~) PROVIDE AND MAINTAIN EVENT DATA FEEDS TO THE TIER ONE (ENTERPRISE) SECURITY INFORMATION AND EVENT MANAGER (SIEM) IAW ANNEX C, APPENDIX 1 AND 2, IN ORDER TO PROVIDE I&W FOR DEFENSIVE CYBER OPERATIONS AND SITUATIONAL AWARENESS FROM TIER THREE (LOCAL) TO TIER ONE (ENTERPRISE).

3.C.1.D. (U//~~FOUO~~) REPORT EVENTS INDICATING AN IMMINENT THREAT TO THE GIG OR SIGNIFICANT DEGRADATION OF THE DEFENSIVE POSTURE OF THE GIG IAW ANNEX C, APPENDIX 3, IN ORDER TO MAINTAIN SITUATIONAL AWARENESS FROM TIER THREE (LOCAL) TO TIER ONE (ENTERPRISE).

3.C.1.E. (U//~~FOUO~~) REPORT DEPLOYMENT AND COMPLIANCE IAW ANNEX C, APPENDIX 1, IN ORDER TO PROVIDE SITUATIONAL AWARENESS ON THE DEFENSIVE POSTURE OF THE DOD GIG.

3.C.1.F. (U//~~FOUO~~) PROVIDE CONTACT INFORMATION FOR ALL TIER TWO (CC/S/A/FA) PERSONNEL RESPONSIBLE FOR ALL ASPECTS OF HBSS ON A QUARTERLY BASIS IAW FORMATS SPECIFIED AT (REF D) IN ORDER TO ENHANCE EFFECTIVE COMMAND AND CONTROL OF HBSS.

4.A. (U//~~FOUO~~) HBSS OPERATIONS SECURITY (OPSEC). HBSS HAS BEEN DEPLOYED ACROSS THE GIG IAW THE COMMERCIAL VENDOR INSTALLATION INSTRUCTIONS. HBSS PROVIDES A VALUABLE SECURITY AND ANALYSIS TOOL CRITICAL BOTH TO THE OPERATIONAL COMMANDER AND THE PROTECTION OF INFORMATION ACROSS THE GIG. WHILE INITIAL COMMERCIAL CONFIGURATIONS AND CAPABILITIES OF HBSS ARE AVAILABLE ON THE INTERNET, DOD SPECIFIC CONFIGURATIONS, POLICIES, REQUIREMENTS, AND CAPABILITIES MUST BE PROTECTED. ALL DOD SPECIFIC UNCLASSIFIED HBSS MITIGATIONS, CONFIGURATIONS, MODULES AND REQUIREMENTS WILL BE PROTECTED FROM INADVERTENT DISCLOSURE OUTSIDE THE DOD AND ENCRYPTED WHEN TRANSFERRED OVER ANY UNCLASSIFIED NETWORK. ALL DOD SPECIFIC HBSS THRESHOLDS ARE CLASSIFIED SECRET REL FVY IAW (REF K) AND MUST BE PROTECTED AS SUCH. CLASSIFIED INFORMATION MUST BE TRANSMITTED ON THE APPROPRIATE NETWORKS OR COMMUNICATION DEVICES.//

GENTEXT/COMMAND AND SIGNAL/5.

5. (U) COMMAND AND SIGNAL

5.A. (U//~~FOUO~~) DIRECT ALL TECHNICAL IMPLEMENTATION QUESTIONS TO YOUR LOCAL INFORMATION ASSURANCE MANAGER (IAM) OR CNDSP. FOR QUESTIONS NOT ADDRESSED BY YOUR LOCAL IAM OR CNDSP, TECHNICAL REFERENCES ARE AVAILABLE AT (REF D), AND FURTHER ASSISTANCE CAN BE OBTAINED FROM THE DISA CUSTOMER SUPPORT DESK.

5.B. (U//~~FOUO~~) DIRECT ALL HBSS OPERATIONAL QUESTIONS TO:  
JOINT OPERATIONS CENTER (JOC) HBSS ANALYST  
COMM: 443-654-3977  
NSTS: 969-1473  
NIPR: J34 EPTMPO@DEFENSE.MIL  
SIPR: J34 EPTMPO@DEFENSE.MIL.MIL

5.C. (U//~~FOUO~~) ACKNOWLEDGEMENT. ALL DOD CC/S/A/FA WILL ACKNOWLEDGE RECEIPT OF THIS ORDER WITHIN 48 HOURS BY SENDING E-MAILS TO BOTH:  
JOC DYNAMIC NETWORK DEFENSE OFFICER (DNDO)  
COMM: 443-654-3972  
NSTS: 969-1494  
NIPR: DNDO WATCH@CYBER.COM.SMIL.MIL  
SIPR: DNDO WATCH@CYBER.COM.SMIL.MIL

JOC DUTY OFFICER (JDO)  
COMM: 443-654-3951  
NSTS: 966-8730  
NIPR: JOCDO@DEFENSE.MIL  
SIPR: JOCDO@DEFENSE.MIL.MIL

GENTEXT/AUTHORIZATION/FOR THE COMMANDER, BRETT T. WILLIAMS, MAJOR GENERAL, US AIR FORCE, UNITED STATES CYBER COMMAND DIRECTOR OF OPERATIONS, J3.//

(b)(1) USSC

(b)(1) USSC

(b)(1) USSC

- (U) Limited Scope DDoS EXORD

- (S//REL USA, FVEY) (b)(1) USSC

- (b)(1) USSC

- (TS//SI//REL USA, FVEY) (b)(1) USSC

- (b)(1) USSC

- (b)(1) USSC

- (U) Draft EXORD currently in staffing with the Joint Staff. Awaiting brief to CJCS and SecDef.

- (TS//REL USA, FVEY) (b)(1) USSC

- (b)(1) USSC

- (TS//REL USA, FVEY) (b)(1) USSC

- (U) Iranian Cyber Actors

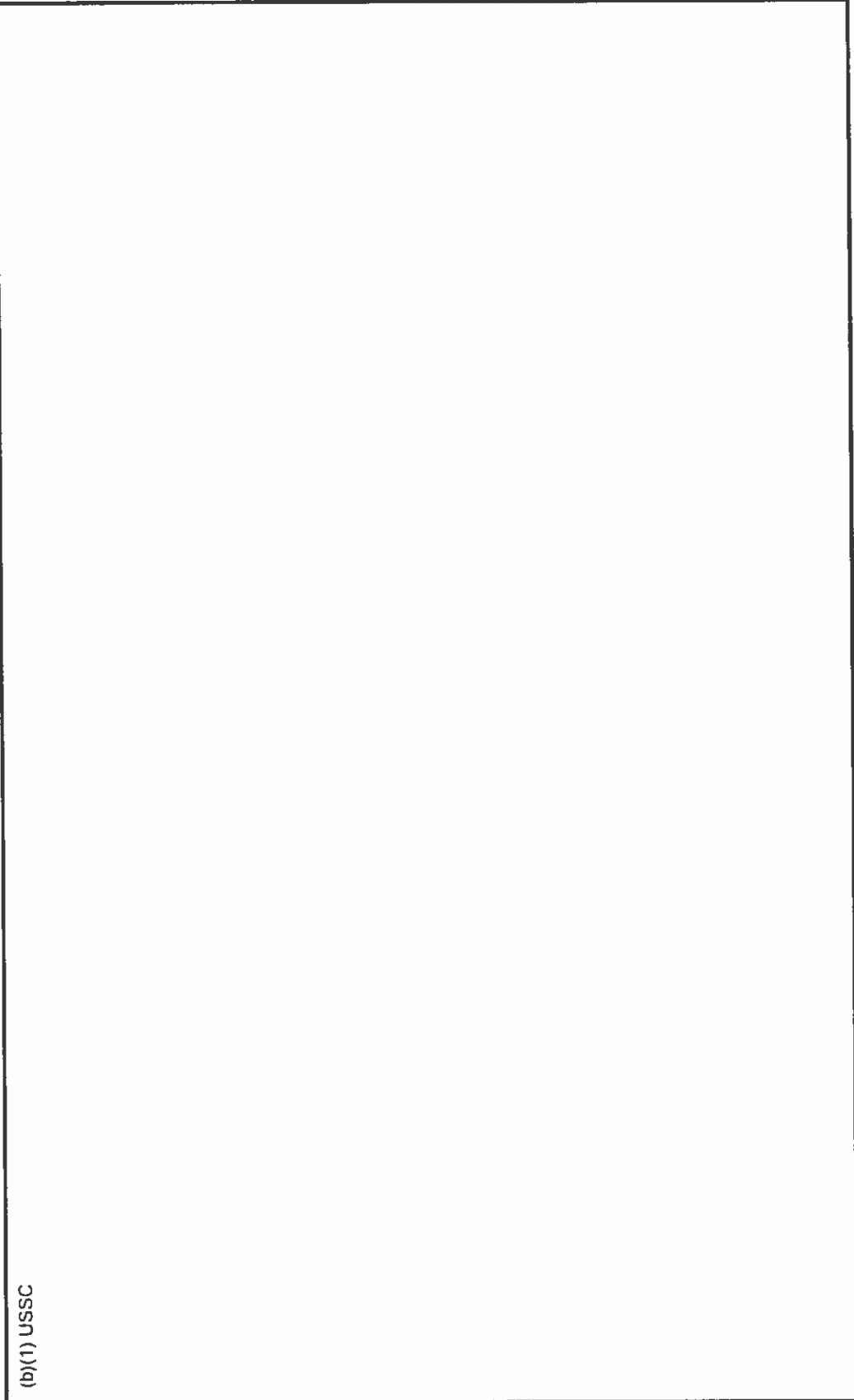
- (TS//SI//REL USA, FVEY) (b)(1) USSC

- (b)(1) USSC

- (S//REL USA, FVEY) (b)(1) USSC

- (b)(1) USSC

(b)(1) USSC



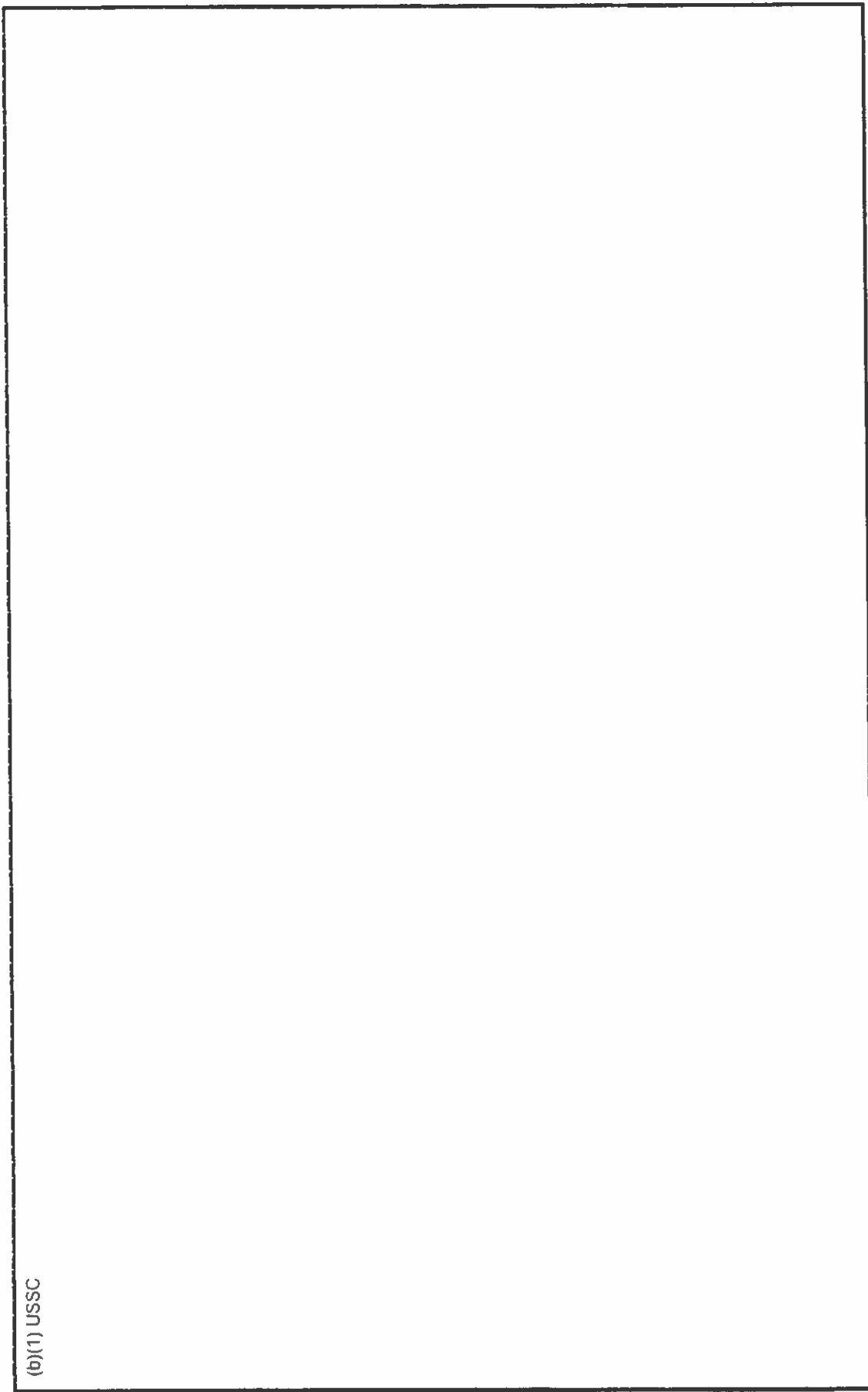
(b)(1) USSC

(b)(1) USSC



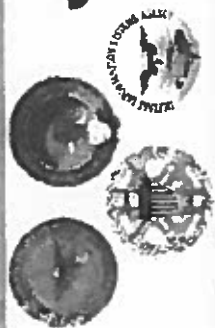
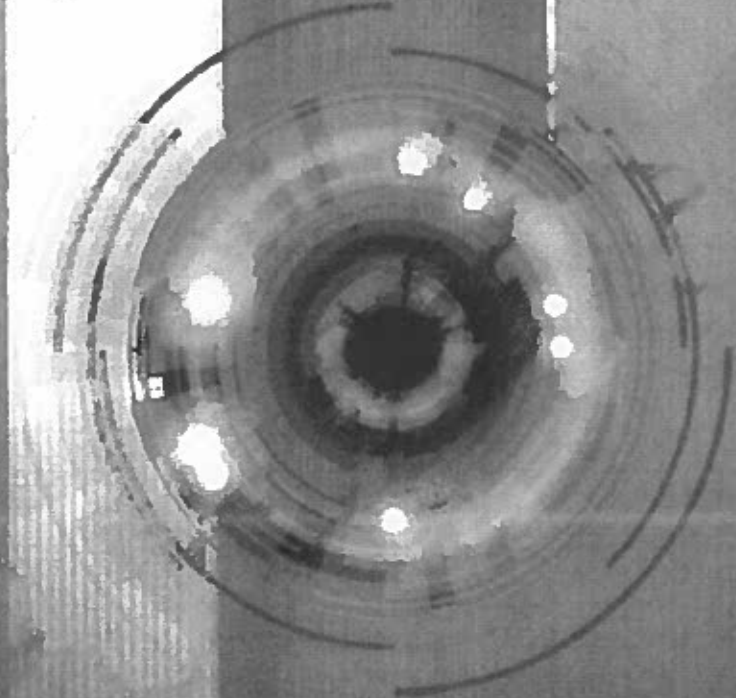
(b)(1) USSC

(b)(1) USSC



(b)(1) USSC





# Joint Information Environment

November 19, 2012

The Overall Classification of this Brief is

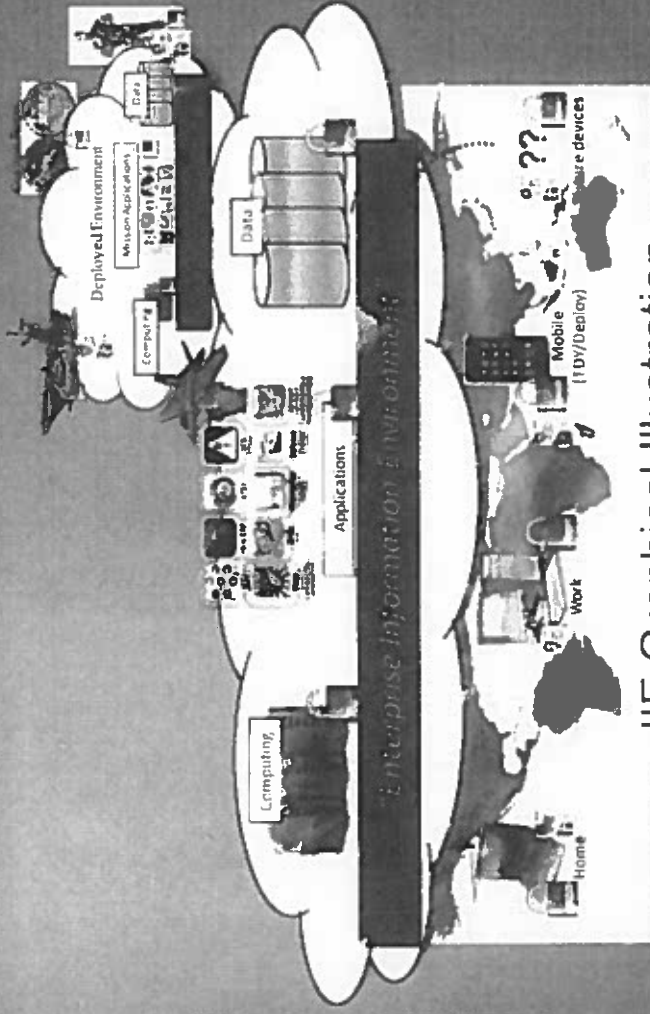
# Joint Information Environment (JIE)

TEAMCYBER

*A secure joint information environment, comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. JIE is operated and managed per Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs).*

## JIE is not:

- Program of Record /Joint Program Office
- Turn key solutions
- Independent way of doing things



JIE Graphical Illustration

## Joint Information Environment - Benefits

TEAMCYBER ↑

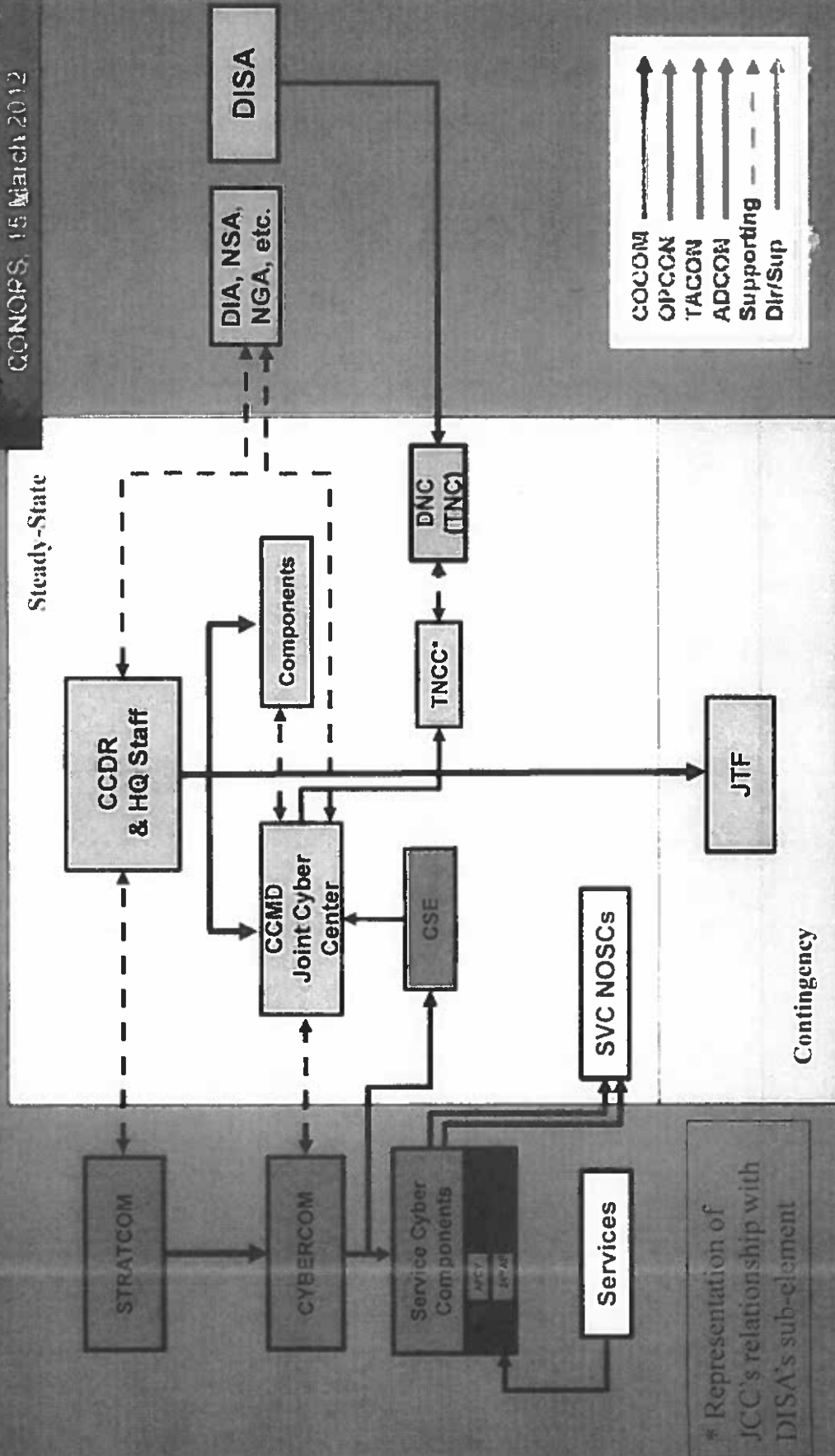
- Mission Effectiveness
  - Rapidly and dynamically respond to and support changing mission information needs for all operational scenarios
  - Users and systems will have timely and secure access to the data and services needed to accomplish their assigned missions, regardless of their location
  - Users and systems can trust their connection from end to end with the assurance that their activity will not be compromised
  - Capabilities are still available during an event, even if they are degraded
- Increased Security
  - Can operate, monitor and defend the DoD's IT assets to attain and maintain information dominance
  - We'll know who's on the network, what they're doing, and we can prove it
- IT Efficiencies
  - Information assets are joint assets to be leveraged for all Department missions
  - A consistent IT architecture supports effective fielding of Department capabilities
  - The DoD has renewed visibility about its IT expenditures through increased budget transparency

**JIE: Enhancing the Nation's Strategic Flexibility**

# Transitional Cyber C2 Concept

TEAMCYBER

Joint Staff Transition Cyber C2  
Operations Command & Control  
CONOPS, 15 March 2012

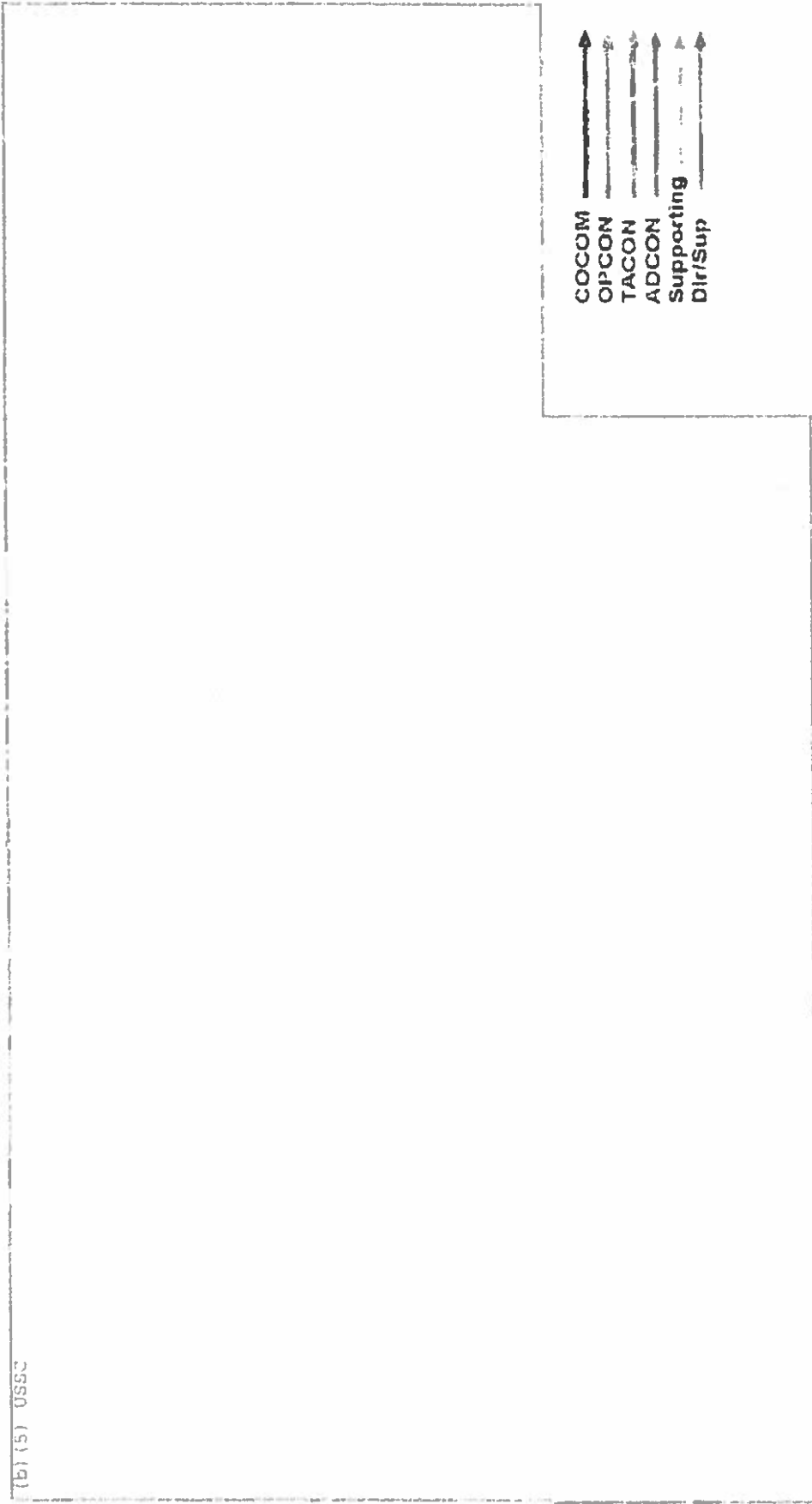


## JIE C2 Based on Transition Model Current

(Service-Led EOC)

PRE-DECISIONAL FOR DISCUSSION PURPOSES ONLY...

(b) (5) USSC



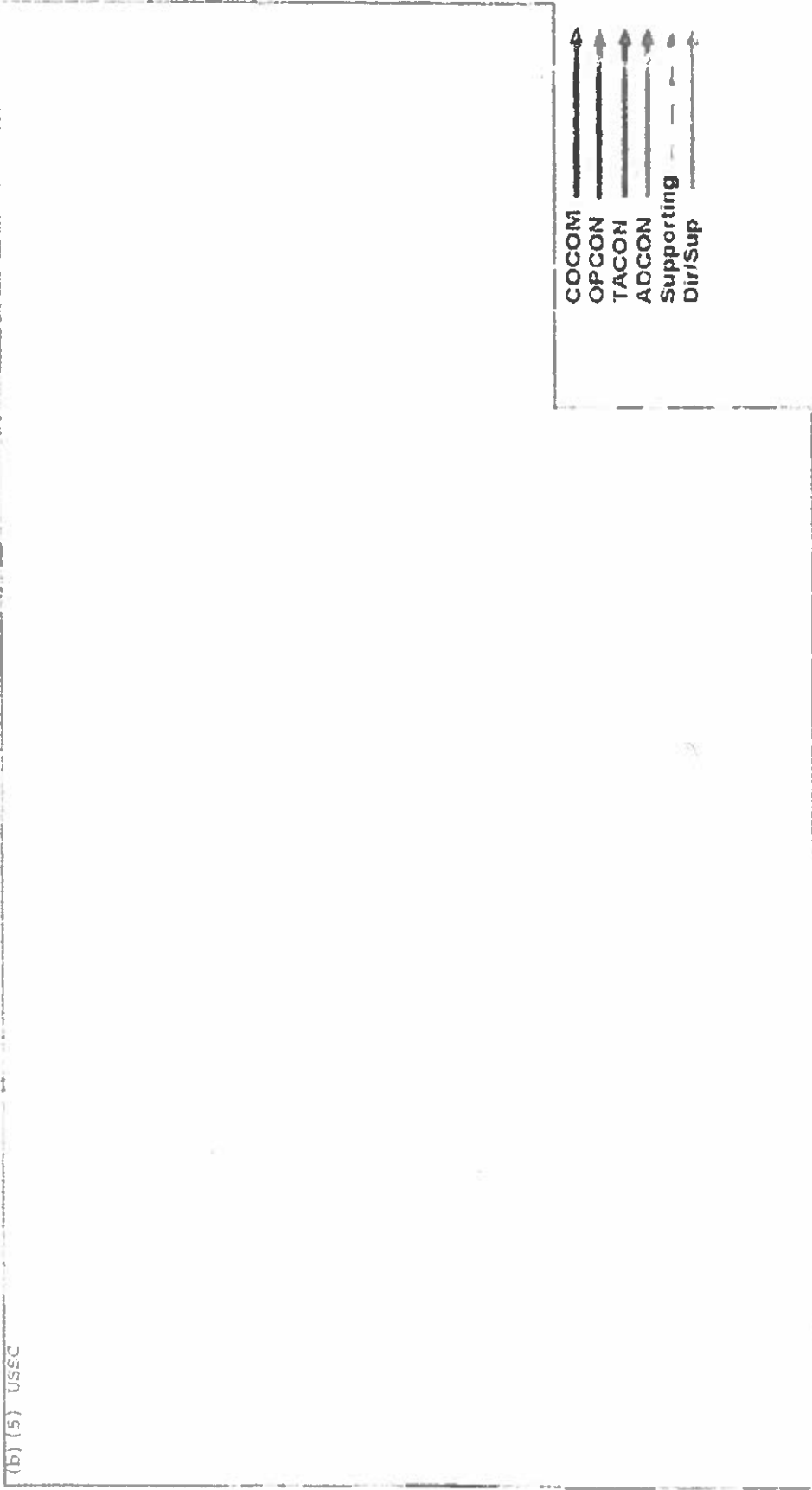
- COCOM
- OPCON
- TACON
- ADCON
- Supporting
- Dir/Sup



## JIE C2 Based on Transition Model Current (DISA-Led EOC)

PRE-DECISIONAL FOR DISCUSSION PURPOSES ONLY...

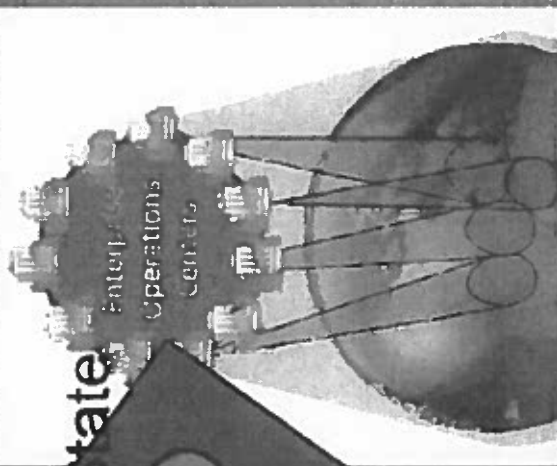
(b) (5) USEC



- COCOM ———>
- OPCON ———>
- TACON ———>
- ADCON ———>
- Supporting - - ->
- Dir/Sup - - ->

# Operational Concept

TEAMCYBER

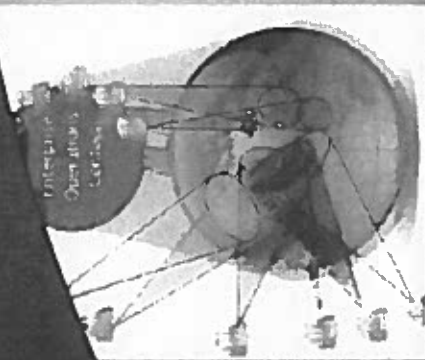
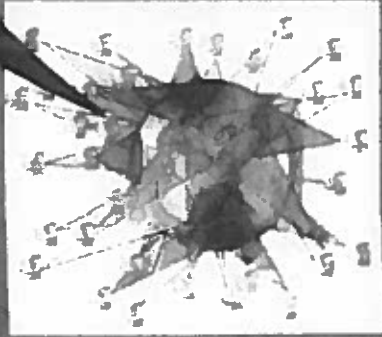


End-State

3-5  
Year

- Service Center non-standard operations centers
- Non-standard TTPs architectures & applications
- No standard ops architecture

No

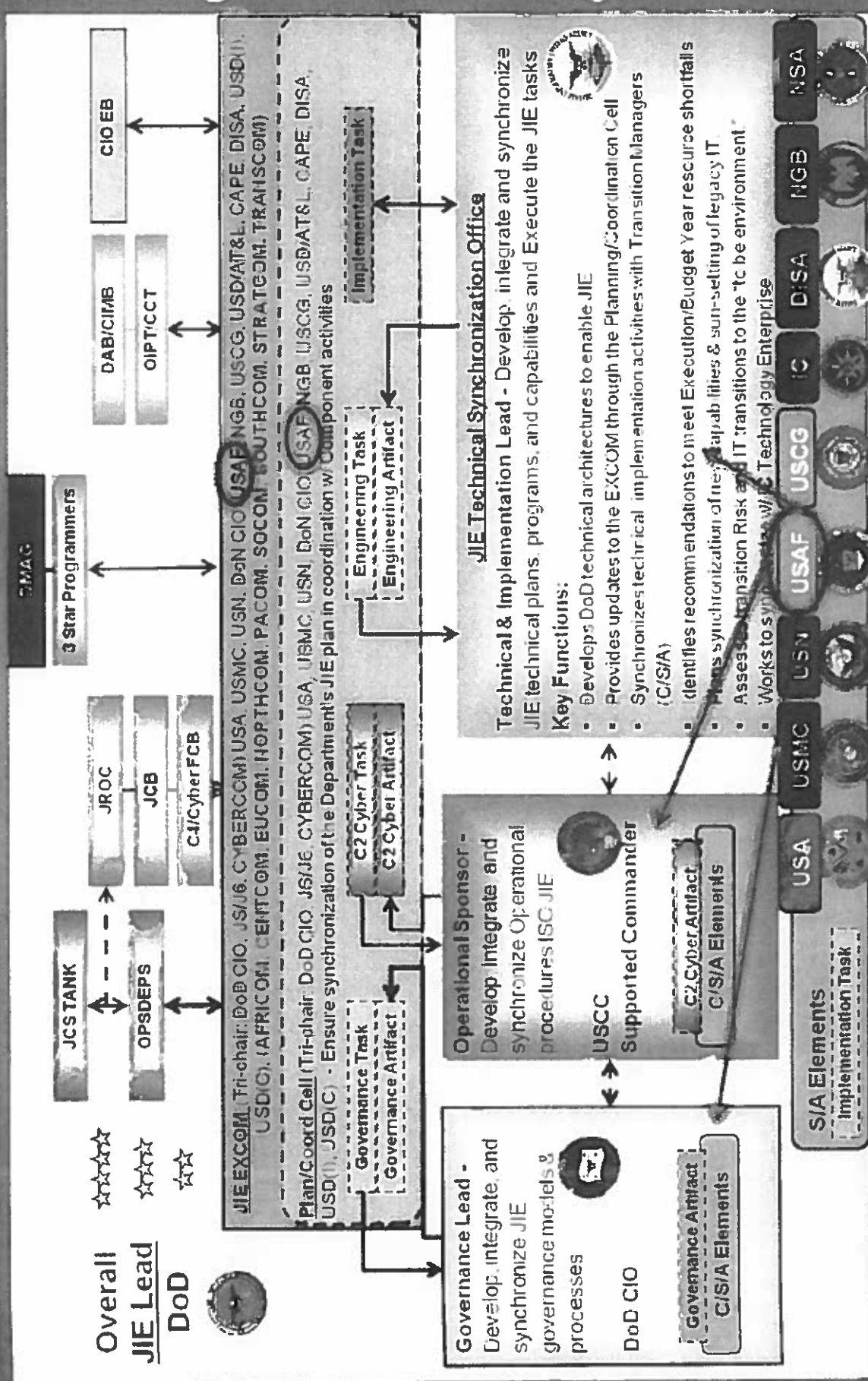


- CCEOC established
- Standardized TTPs
- JIE ops architecture & Initial COP capability
- Mixture of JIE EOCs and Service centers
- Reduced number of CNDSPs

- Fully meshed EOCs provide seamless control and failover
- EOCs in place for all non-Service unique missions
- JIE COP in place
- Automated capabilities in place, e.g. compliance verification and reporting
- Standard TTPs, Architectures & Applications

# JIE Management Construct

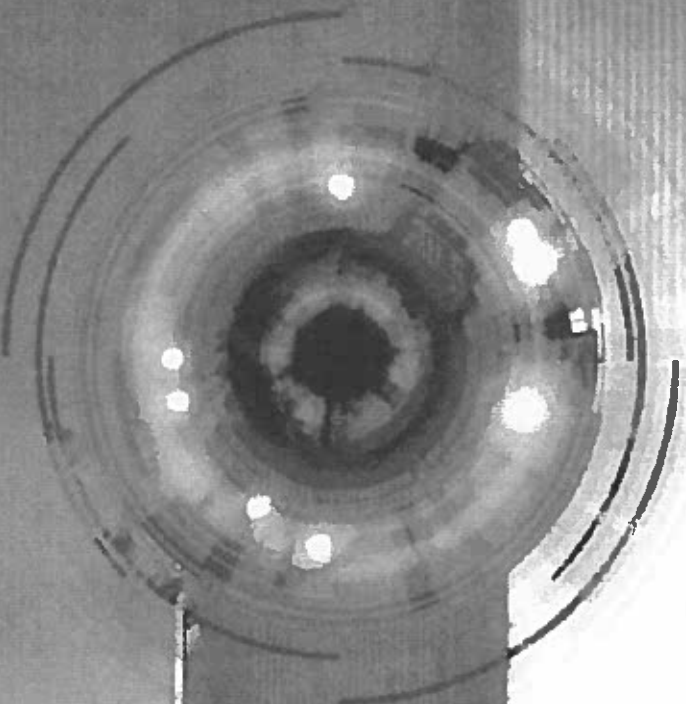
TEAMCYBER







# Joint Information Environment



# QUESTIONS

*The relevance of space and cyberspace to national security will grow exponentially in magnitude or importance. Our reliance on technological superiority is a potential vulnerability that our adversaries will seek to exploit.*

General Martin E. Dempsey, U.S. Army

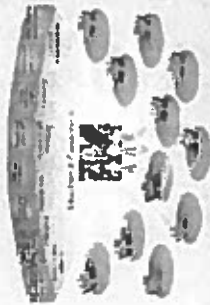
UNCLASSIFIED//FOR OFFICIAL USE ONLY

# Operational Concept

TEAMMEMBER 3

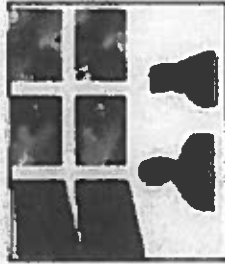
## Global Enterprise Operations Center (Manages JIE Enterprise)

- Directs full spectrum operations
- Works global cyber challenges
- Prioritizes global cyber missions (IAW COCOM priorities)
- Manage JIE global external interfaces (ex. Internet Access Points, etc.)
- JIE global focal point for external partners (Law Enforcement, etc.)
- Maintains global situational awareness



## Enterprise Operations Centers

- Directs DCO/DGO activities within assigned area
- Works regional cyber challenges (as needed/directed)
- Prioritizes regional cyber missions (IAW COCOM priorities)
- JIE focal point for regional external partners (multinational, etc.)
- Operate, maintain, and manage security & aggregation points within assigned area
- Maintains regional situational awareness
- Computer Network Defense Service Provider (CNDSP) functions



## Base/Camp/Post/Station

### Air Force



- Host Service maintains local infrastructure
- Host Service provides touch labor
- Host Service provides local DGO/DCO incident response
- Services maintain support to tactical units
- Maintain "unique" support labor and mission

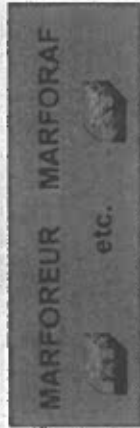
### Army



### Navy



### Marines



## Guiding Principles

TERMCYBER

- All stakeholders are committed to achieving the end state
- DoD IT will operate in an enterprise model with enforced governance
- Mission success is the first priority
- Common technical standards and processes are the default; uniqueness may be allowed when essential for mission success
- We will maximize utilization of existing efforts to include the IC and Coast Guard
- We must and will enhance security
- We will operate within the existing statutory framework
- Requirements, PPBE, and Acquisition processes will be aligned to achieve the end state









# JIE Increment 1 Authority

TEAMCYBER

- 6 Jul 12 – DMAG approved JIE Increment 1 Way Ahead
  - Directed development of metrics with periodic updates back to DMAG
- 6 Aug 12 – JCS endorsed JIE Increment 1 implementation

3. Recommend the JCS endorse the attached DoD Information Technology Effectiveness brief, which approves JIE increment 1 implementation with a focus in Europe as the first JIE area.

JCS Meeting, DoD IT Effectiveness, 13 July 2012

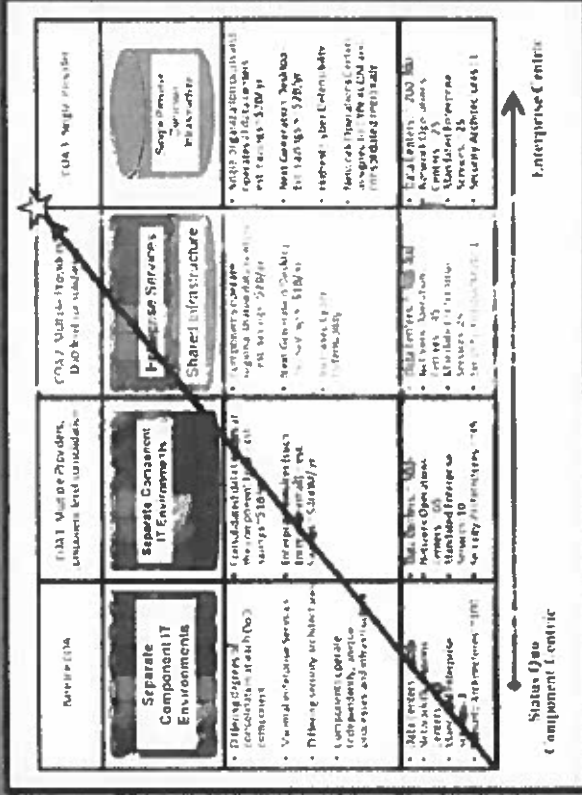
|          |  |                     |
|----------|--|---------------------|
| • CJCS:  |    | DATE: 6 Aug 12      |
| • VCJCS: |   | DATE: 7/31/12       |
| • USAF:  |  | DATE: 23 JUL 12     |
| • USN:   |  | DATE: 23 JUL 12     |
| • USMC:  |  | DATE: 7/25/12       |
| • USA:   |  | DATE: 7/25/12       |
| • NGR:   |  | DATE: 19 JUL 12     |
| • USCG:  |  | DATE: 8/1 JULY 2012 |



# Background: Key Decisions on Why JIE



- Secretary of Defense's Efficiencies
  - 9 Aug 10: IT community tasked to address organization optimization, and sustainable processes
  - 6 Oct 10: Secretary of Defense provided direction to consolidate the IT infrastructure to optimize for the joint environment (COA 2)
  - 5 Oct 11: DepSecDef signed DoD IT Enterprise Strategy & Roadmap (ITESR)
- Joint Chiefs of Staff Decision Forum Direction
  - 14 Nov 11: JCS meeting directed Components to build the DoD Plan to achieve IT Efficiencies as a result of USCYBERCOM presentation
  - Joint Information Environment Task Force established. 6 month effort to develop:
    - Architectural definitions for Joint Information Environment
    - Plan of Action and Milestones
    - Use Cases
- DoD Senior Leadership Direction
  - 6 Jul 12: Implement and develop JIE Business Case Analysis



## Keep Initial Focus on Big Rocks

TEAMCYBER

- **Network Normalization**
  - Common network standards and TTPs
  - Single Security Architecture
- **Data Center Consolidation**
  - Core Enterprise Data Center Standards
  - Service Data Center consolidation plans move to a Department focused plan
- **Identity and Access Management**
  - Access the Network from anywhere
  - Attributes access to data
- **Enterprise Services**
  - Common capabilities across the Department
  - Mission specific applications remain
- **Governance**
  - Move Service IT efforts into optimized DoD plan

# Focus work on Key Nodes

TEAMCYBER

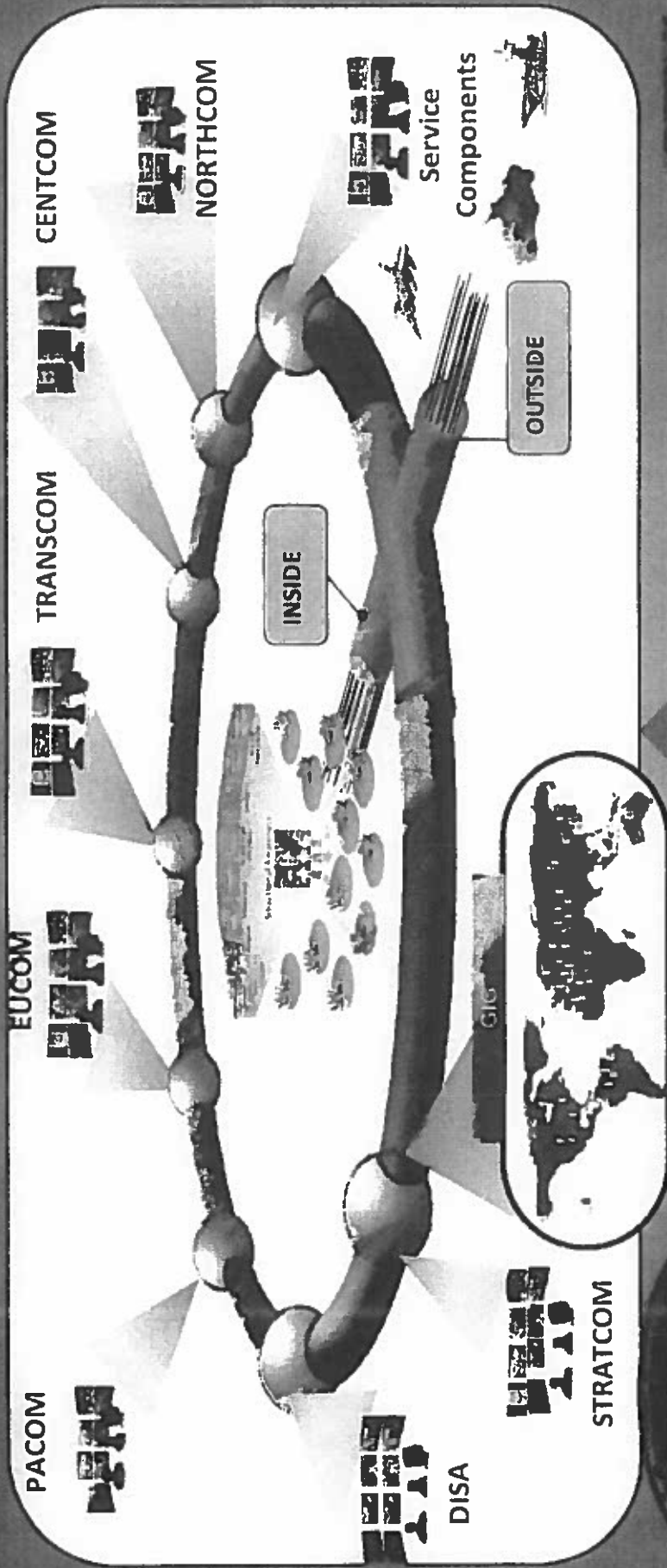
Enterprise Operations Centers

Core Data Centers

12/15/13

# End State Architecture: Operate & Defend

TEAMCYBER



Management, Monitoring & Reporting

Secure Share

Secure Access

Secure Connect

Policy

Process

Architecture

Standards

Technology

Secure Resilient Global Mission Enablement

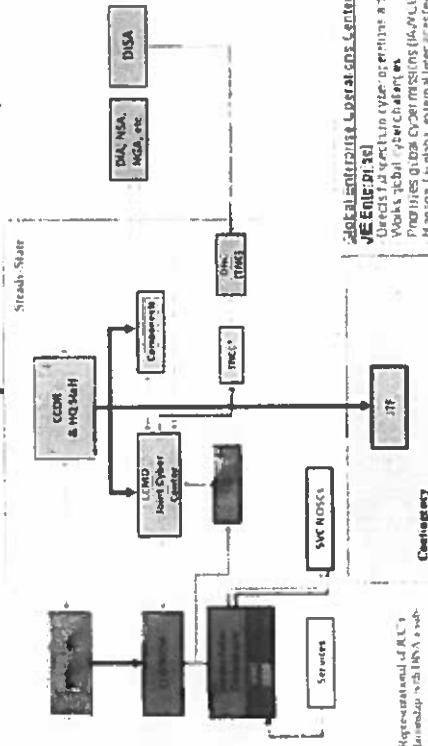


# JIE Concepts support and enable Cyber C2

TECHCYBER

## Transitional Cyber C2 Concept

Unclassified For Official Use Only



Representation of RLC's relationship with INVA is subject to demand

Joint Staff Transitional Cyberspace Operations Command and Control

Unclassified For Official Use Only

## JIE Operations

Now

JIE Interim

JIE End State

- Service-specific multi-standard operations centers
- Non-standard TTPs, architectures & applications
- No standard ops.

- Standardized TTPs
- JIE ops architecture
- GECC established
- Initial JIE COP capability
- Maturity of JIE, EOCs and the centers
- Set of

- Fully meshed EOCs provide seamless control and follow
- EOCs in place for all ops
- Service unique missions
- JIE COP in place
- Automated capabilities in place, e.g. compliance verification and reporting

### Enterprise Operations Centers

- Treats DC/OSO titles with respect to:
  - Workflows
  - Challenges (as requested)
  - Priority regional cyber missions (AW-COC/CI/CD)
  - JIE focal task or regional task (AW-COC/CI/CD)
  - Operate in tandem with the security & aggregation for its own
  - Aggressiveness
  - Highly visible & shared awareness
  - Combat school Defense
  - Service specific



### Joint Staff Transitional Cyberspace Operations Center - Managers

- Needs to structure operations & times
- Works global cyber mission
- Provides global cyber missions (AW-COC/CI/CD)
- Manages global external inter-agency in direct
- Access/Force etc.
- Global focus point for all cyber (ILW, Enforcement, etc.)
- MS - has global electronic warfare



**Air Force**

**Post/Command Stations**

- Not a separate unit, it is a capability
- Not a separate unit, it is a capability
- Not a separate unit, it is a capability
- Not a separate unit, it is a capability
- Not a separate unit, it is a capability

**Marine**

**Joint**

# JIE Capability - POA&M

TEAM CYBER

FY2012    FY2013    FY2014    FY2015    FY2016    FY2017    FY2018

**SHAPE**

**NORMALIZE**

**OPTIMIZE**

**SUSTAIN**

**JIE - Inc. 1**

- Conduct BCA and site survey
- Develop implementation plan
- Publish data center standards
- Close 69 data centers
- Design 5 core data centers
- Network Normalization
- Implement security architecture
- Consolidate services desks
- Define Single Security Architecture
- Enterprise Services
- Initial Standard Headers Management process
- Enterprise Portal subsystems
- DKOAKO
- Cross Domain ICC
- Identity and Access Mngt
- Initial Data Tagging & enhanced personal ID Service

**JIE - Inc. 2**

- Conduct BCA and site survey
- Develop implementation plan
- Regional or global focus to be defined by BCA
- Data Center Consolidation
- Establish 5 more core data centers
- Initial Technical Data Centers
- Network Normalization
- Continue Inc 1 initiatives
- Enterprise Services
- Continue Inc 1 initiatives
- Start phase out of point-to-point cross domain solutions
- Identity and Access Mngt
- Continue Inc 1 initiatives

**JIE - Inc. 3**

- Data Centers Consolidation
- 10 more core data centers
- Final Technical Data Centers
- Network Normalization
- Continue Inc 2 initiatives
- Enterprise Services
- Review Core E Mail Content
- Complete Enterprise Portal
- Initial Unified Capabilities
- Identity and Access Mngt
- Credentialing and authentication services

**Data Center Consolidation**

- Fully franchised DOD
- Close 50% services (data enabled)
- Network Normalization
- Continue Inc 2 initiatives
- Enterprise Services
- Unified Capabilities - Phase out legacy switches
- Complete Enterprise Email
- Complete point-to-point Cross Domain solutions
- Identity and Access Mngt
- Continue Inc 3 initiative

**Data Center Consolidation**

- Sustain
- Network Normalization
- Sustain
- Enterprise Services
- Unified Capabilities
- Services that enabled
- Identity and Access Mngt
- Sustain

**Initial Focus on Big Rocks**

- Network Normalization
- Data Center Consolidation
- Identity and Access Management
- Enterprise Services
- Governance

Note: Level of Programmatic, Execution and Operational Risks are captured and mitigated as implementation occurs



**Limited**

**Operational Flexibility**

**Cyber Security**

**Service Work**

**Maximized**

**Defendable**

**Mission Effectiveness**

**Increased Security**

**IT Efficiencies**

# Operational Concept – Service Desks

TEAMCYBER

(b)(5) USSC