UNITED STATES CYBER COMMAND

(U) CYBER PROTECTION TEAM (CPT) CONCEPT OF OPERATIONS

The overall classification of this document is: UNCLASSIFIED//FOUO

26 May 2015

MICHAEL M. GILDAY
RADM, USN
Director, Operations

Table of Contents

1. (U) Introduction

1.A. (U//FOUO) General. Threats to the Department of Defense (DOD) Information Networks (DODIN) continue to present a significant risk to national security and global military operations. Reference (a) states that transformational changes to DOD's cyber culture, workforce, technology, policy, and processes are required to meet the challenges expected by the rapidly evolving cyber environment. In reference (a), the DOD identified four strategic focus areas: 1) Establish a Resilient Cyber Defense Posture; 2) Transform Cyber Defense Operations; 3) Enhance Cyber Situational Awareness; and 4) Assure Survivability against Highly-Sophisticated Cyber Attacks. Cyber Protection Teams (CPTs), an element of the new DOD cyber force model approved by the Joint Staff, are intended to address the first two focus areas. As one element of a layered, comprehensive and integrated cyber force they can adapt to meet DODIN defense requirements at the National, Service, Combatant Command (CCMD), and tactical levels.

1.B. (U//FOUO) Purpose. To provide an overarching framework pertaining to the intent, function, employment, and coordinating guidelines of the CCMD, Service, DODIN and National CPTs to conduct cyberspace defense activities in support of DOD missions.

1.C. (U//FOUO) Scope. This Concept of Operations (CONOPS) applies to Service, DODIN and National CPTs and coordinating guidelines for CCMD CPTs. It is intended to provide a joint force standardized guide for the construct and employment of CPTs for the execution of cyberspace defense activities, but does not establish specific operating procedures for mission execution.

1.D. (U//FOUO) Mission. To enable a supported commander's mission capabilities and supporting infrastructure, CPTs conduct Survey, Secure, and Protect missions to prepare local cyberspace defenders to sustain an advanced cyberspace defense posture and to defend the supported commander's critical assets and Cyberspace Key Terrain (C-KT).

1.E. (U//FOUO) Method. CPTs analyze supported commands' and organizations' missions and resources to support C-KT identification across the three layers of cyberspace (physical, logical, and persona). CPTs are deployed to assist supported commanders to evaluate and improve their mission assurance posture within and through cyberspace. CPTs will conduct this task primarily through deliberate, proactive, and systematic planning; the application of CPT forces across prioritized DOD missions; and, when applicable, support to crisis planning, incident response, and actions to mitigate high-risk situations to DOD priority missions. With specialized training and capabilities, CPTs enhance local mission assurance by conducting activities remotely and on site to create desired cyberspace effects in support of command requirements and ensure that local forces have the ability to sustain mission assurance.

1.F. (U//FOUO) End state. CPTs will re-deploy/enter recovery stage after the commander has assessed the risk of adversary exploitation and disruptive effects against a supported commander's C-KT are reduced to acceptable levels and the supported commander's ability to conduct missions through cyberspace is assured.

1.G. (U) Facts and Assumptions

1.G.1. (U) Facts

1.G.1.A. (U//FOUO) Reference (b) established the Cyber Protection Force (CPF) supporting four distinct mission areas. CPTs are identified by these mission areas and are referred to as Service, CCMD, DODIN, and National CPTs.

1.G.1.B. (U//FOUO) Reference (b) established that Service, CCMD, DODIN, and National CPTs shall conduct Defensive Cyber Operations – Internal Defensive Measures (DCO-IDM) in support of Service DODIN operations, CCMD network operations, Defense Information Systems Agency (DISA) DODIN enterprise services, and National missions, respectively.

1.G.1.C. (U//FOUO) References (b) and (c) established the command and control (C2) relationships for CPTs and the various DOD cyber component commands and units, authorizing the "Direct Support Model" for initial implementation.

1.G.2. (U) Assumptions

1.G.2.A. (U) Emerging cyberspace policy or doctrine will not significantly alter the Cyber Force Concept of Operations and Employment (CFCOE) with regards to CPT generation, assignment, or employment.

1.G.2.B. (U) Future changes to Computer Network Defense Service Providers (CNDSP) mission, capabilities, and/or employment will not directly conflict with CPT functions.

1.G.2.C. (U) Adequate personnel, training capacity, equipment, authorities, and clearance granting resources will be available to fill CPT requirements to achieve full operational capability.

1.G.2.D. (U) The CPT CONOPS will continue to be refined as real-world experiences are gained, best practices are developed, and tactics, techniques, and procedures (TTPs) are refined.

1.G.2.E. (U) CCMDs may develop CPT CONOPS and TTPs consistent with existing core concepts and synchronized with CYBERCOM guidance; CCMD CPT CONOPS should detail employment of teams during IOC through FOC.

2. (U) Organization and Employment

2.A. (U//FOUO) CPT Composition. A CPT is comprised of a staff element and five distinct, but interdependent squads. Each squad executes a specific cyberspace effect that, when combined with the others, enables the completion of a CPT mission. These squads are: 1) Mission Protection Squad; 2) Cyber Readiness Squad; 3) Cyber Support Squad; 4) Discovery and Counter-Infiltration (DCI) Squad; and 5) Cyber Threat Emulation (CTE) Squad. The team may be required to task organize and deploy based on the mission requirements.

2.B. (U) Core Tasks. To support the entire range of joint military operations, CPTs will accomplish two core tasks: 1) transform and rapidly improve cyberspace defenses; and 2) protect the supported commander's critical assets and C-KT.

2.C. (U) Force Integration. In order to provide support to a supported commander, CPTs will work with the following entities:

2.C.1. (U) The supported commander and his/her staff;
2.C.2. (U) Local cyberspace defenders;

2.C.3. (U) Intelligence entities (e.g., J2, G2) supporting the supported commander and the local cyberspace defenders;

2.C.4. (U) Other Cyber Mission Forces (CMF); and

2.C.5. (U) Other forces as dictated by the mission, and/or interagency support/partners.

2.D. (U//FOUO) CPT Area of Operations (AO) CPTs are employed to provide improved mission assurance enabled through advanced cyberspace capabilities, in support of USCYBERCOM, National, CCMD, JFHQ-DODIN or Service Cyber Component priorities. A CPTs area of operations (AO) is the friendly cyberspace (e.g., blue cyberspace) supporting a commander's mission, which may not be restricted to specific network enclaves; the CPTs AO may include or traverse multiple network enclaves with separate approval authorities.

2.E. (U) CPT Mission Areas

2.E.1. (U//FOUO) General. The basic structure and capabilities of the CPTs are standardized to enable them to operate interchangeably throughout the DODIN. There are four mission areas for CPT operations: 1) Service; 2) CCMD; 3) DODIN; and 4) National. While these mission areas only influence CPT force distribution across the DOD, they may require the development of dissimilar capabilities or effects. As the DOD further centralizes and standardizes supporting Cyberspace Operations (CO) and infrastructure (e.g., Unified Platform, Joint Information Environment, etc.), these mission areas may change to better align with the changing battle space environment and mission requirements.

(U//FOUO) Service CPTs operate primarily within Service controlled cyberspace environments to support Service priorities with the ability to support CCMD priorities as necessary and fulfill Service-unique challenges, priorities, and requirements.

2.E.2. (U//FOUO) CCMD CPTs operate primarily across CCMD controlled portion of DODIN cyberspace with the ability to coordinate across the DODIN, as needed, to support the protection of a CCMD mission. CCMD CPTs directly protect regional assets and C-KT, as well as portions of the DODIN outside of any specific Service or DISA area of control.

2.E.3. (U//FOUO) DODIN CPTs operate primarily across DISN controlled cyberspace with the ability to coordinate across the DODIN, as needed, to support the Protection of global CO or priority CCMD missions.

2.E.4. (U//FOUO) National CPTs operate across the entire DODIN and retain the capability, when directed, to support CCMD and U.S. Government priorities and activities outside the DODIN for the protection of Critical Infrastructure and Key Resources (CIKR). National CPTs directly Protect DOD global and/or strategic assets and cyberspace terrain, as well as portions of the DODIN outside of any specific Service, CCMD, or DISA area of control (e.g., support to other components of the DOD).

2.F. (U) CPT Mission Types

2.F.1. (U//FOUO) Within DCO-IDM, CPTs conduct three sub-missions: Survey, Secure, and Protect. Each sub-mission serves to support the end state specified by the supported commander.
2.F.2. (U//FOUO) CPT methodology follows two phases (Planning and Execution) and four supporting stages (Survey, Secure, Protect, and Recover) which are chosen based on the CPTs mission, as shown in

Table 1. CPT methodology is explained in greater detail in Annex C.

		Planning Phase	Execution Phase			
			Stage 1 Survey	Stage 2 Secure	Stage 3 Protect	Stage 4 Recover
MISSION	Survey	X	X			
	Secure	X	X	X		
	Protect	X	X	X	X	X

Table 1. CPT Missions and Associated Phases/Stages (U//FOUO)

2.F.2.A. (U//FOUO) Survey Mission. The Survey mission objective is to evaluate the supported commander's blue cyberspace through a mission impact analysis to identify risks and develop mitigation and countermeasure recommendations. The Survey mission requires the CPT to conduct a comprehensive baseline evaluation of the supporting cyberspace terrain and processes. This mission is optimally short in duration and used to provide recommendations to local cyberspace defenders and the supported commander or to support future mission planning for subsequent missions. Direct engagement to mitigate active risks to a supported commander's mission is not expected. If deployed to conduct a Survey mission, the CPTs ability to respond and conduct defensive actions may be very limited because of the limited scope of a Survey mission.

2.F.2.B. (U//FOUO) Secure Mission. The Secure mission objective is to improve and harden the defenses of a supported commander's C-KT and critical assets within cyberspace. This mission includes the specified tasks of the Survey mission as well as tasks to actively prepare and evaluate forces for conflict in cyberspace. The duration of this mission varies based on the level of integration and effort. Direct engagement to mitigate active risks to a supported commander's mission is not immediately expected. The CPT can respond and conduct limited defense action internal to the defended network in accordance with rules of engagement for the use of force. The Secure mission includes the Survey stage.

2.F.2.C. (U//FOUO) Protect Mission. The Protect mission objective is to respond, mitigate, and recover from threat effects to the supported commander's C-KT and critical assets and, if required, defend against an active adversarial threat. This mission includes the specified tasks of the Secure mission as well as a high level of mission assurance. This mission is conducted during times of high risk associated with threat activity to meet a specific need and for a limited duration. Direct engagement with active threats is both planned for and expected. Protect missions includes Survey, Secure, Protect, and Recover stages. Coordination with organic capabilities is necessary as the Protect Mission runs parallel with traditional functions and tasks of the CNDSP/Network Operations and Security Centers (NOSC).

2.G. (U//FOUO) Employment Models. The scale and scope of a supported mission and the time available to conduct preparations have a direct influence on the forces dedicated to mission assurance and the level of coordination and oversight required. Decomposing a supported mission to identify its specific dependencies across cyberspace can be a resource intensive task. CPTs can deploy in three models to support the level of effort required to meet the objectives: 1) Solo model; 2) Formation Model; and 3) Combined Model.

2.G.1. (U//FOUO) Proactive versus Reactive. The primary difference between the proactive and reactive CPT missions is the ability to prepare, synchronize, and improve the capabilities of local cyberspace defenders. The larger goal of DOD defensive CO is to provide mission assurance for operations within cyberspace against a persistent, dynamic, and aggressive threat. This goal is directly supported through training of and preparation by DOD forces. The preferred mission for a CPT is the proactive state of operations.

2.G.2. (U) Solo Model

2.G.2.A. (U//FOUO) Proactive. Lacking any global integrated operation or operational campaign, the solo model is the most common tactical employment of a CPT. This model focuses on a single support mission without integrating actions from other CPTs. Proactive solo employment is ideal for initial engagement with a supported command; it enables the reconnaissance and analysis of the mission owner's supporting cyberspace while providing immediate mission assurance improvements for the service providers supporting the mission owner. During a proactive solo employment, a CPT can prepare operational reporting to facilitate follow-on coordinated multi-CPT actions. A single team may also be employed to enhance the defensive cyber posture of a large mission through the conduct of Protect missions, sequentially maneuvering across a pre-established AO.

2.G.2.B. (U//FOUO) Reactive. The reactive solo model, also known as incident response, is the most common employment of CPT capabilities when a timely response is required to address specific and/or immediate threats. In this employment model, the CPT will complete defensive actions through coordination with organic incident response teams and local cyberspace defenders. Initial assessments may drive planning for additional alignment and positioning of other CPTs. CPTs conducting incident response focus on bounding the problem, determining lateral movement, identifying exfiltrated data, and fixing the vulnerabilities.

2.G.3. (U) Formation Model

2.G.3.A. (U//FOUO) Proactive. At the operational level, it may be necessary to deploy two or more CPTs in a coordinated effort from the same intermediate headquarters. Under this mission model, CPTs work together to mass force and capability against a specific high-risk area or conduct synchronized operations in non-contiguous cyberspace. The optimal employment for this construct would be to support and reinforce command-wide mission assurance across two or more cyberspace locations (i.e., securing cyberspace operations at both the local and distant ends of a supported mission).

2.G.3.B. (U//FOUO) Reactive. At the operational level, the ability to quickly respond with two or more CPTs to multiple locations from the same intermediate headquarters may be necessary. This model construct requires close coordination and information sharing between the aligned CPTs. Teams employed in a reactive formation will likely be responding to active threats or illuminated risks within the same mission space of their intermediate headquarters.

2.G.4. (U) Combined Model

2.G.4.A. (U//FOUO) Proactive. The aligning of two or more CPTs from multiple intermediate headquarters or using a CPT in a mission area where it does not routinely operate (i.e., Service CPT from one Service maneuvering to another Service's area) requires coordinated prioritization and support from USCYBERCOM, Joint Forces Headquarters DODIN (JFHQ-DODIN), and the CCMD in which operational activities will take place. This is the preferred operational model to support global and regional

integrated operations or strategic objectives. This mission model will be used to support operations that cross the AO of two or more intermediate headquarters or where aligned CPTs require direct JFHQ-DODIN support across disparate locations that are typically outside the supporting CPTs AO. Through proactive combined employment, two or more CPTs can be jointly aligned to protect a supported mission across the full breadth of the DODIN, and provide support to other areas in defense of national and CCMD objectives. The high level of coordination required for the combined mission model will enable the aligned CPTs to rapidly focus their efforts on increasing mission assurance across commands and identifying systemic issues that cross multiple AOs.

2.G.4.B. (U//FOUO) Reactive. Supporting large scale threats or significant risks to DOD operations that cross multiple AOs requires joint integrated efforts between multiple CPTs from multiple intermediate headquarters or using a CPT in a specified mission area in which it does not routinely operate. Under reactive combined employment, two or more CPTs respond to threats and risks that cross multiple AOs; this is the likely employment method in response to high-impact/high-priority operations, DOD-wide events, or significant national or regional issues.

2.H. (U//FOUO) Specialized CPT Capabilities. CPT capabilities are develop to provide transformational defensive effects in cyberspace from the tactical to strategic level. They serve a critical role in the joint development of TTPs and capabilities to best mitigate or respond to advanced threats against friendly forces in cyberspace. CPT Squads are tasked with improving cyberspace defense activities across the DOD while conducting specific tasks for a supported commander.

2.H.1. (U//FOUO) Mission Protection Squad. The Mission Protection Squad analyzes the supported commander's identified cyberspace dependencies, essential and critical assets, and C-KT. The Mission Protection Squad conducts mission impact analysis to evaluate risk and develops recommendations for managing risk for mission assurance using CPT artifacts and collaborative team inputs. The Mission Protection Squad serves as the CPTs central link to build and sustain the CPTs understanding and awareness of the supported commander's mission; they provide the common operational picture of the mission to the staff element.

2.H.2. (U//FOUO) Cyber Readiness Squad. The Cyber Readiness Squad will focus on providing in-depth reviews of mission-supporting cyber assets based on DOD policies, regulations, and best practices. Through targeted evaluations, the squad will review the effectiveness of the current cyber security program, information security plan, and security policies; recommend or direct changes; and provide insight into the evaluated organization's readiness.

2.H.3. (U//FOUO) Cyber Support Squad. The primary mission of the Cyber Support Squad is to provide assistance in correcting security at the physical, logical, and persona layers; the intended end-state is an improved and self-sustaining security posture. This assistance can be procedural or technical in nature and is designed to cover gaps in training or capability to achieve or sustain proper security. The Cyber Support Squad will work closely with the organic network operators and defenders at an organization to plan, train, and deploy mitigations. Through the Cyber Support Squad, the CPT may recommend additional training for local cyberspace defenders to further enhance organic capabilities.

2.H.4. (U//FOUO) Discover and Counter Infiltration (DCI) Squad. The DCI Squad detects, illuminates, and defeats previously unknown adversary activity within a specified AO. Personnel are trained to detect, discover, and characterize advanced adversary tradecraft within friendly networks that evade routine security measures. The DCI Squad seeks to categorize threats and pass them to local cyberspace defenders for action; this procedure frees DCI Squad processing time for the deeper analysis needed to

illuminate advanced and often stealthy threats within cyberspace. The DCI Squad monitors networks for unusual activity that may indicate adversary presence and provides real-time Protection for critical systems during specific phases of the supported commander's mission. In contrast to the Mission Protection Squad, the DCI Squad identifies and responds to adversary presence already in friendly cyberspace vice seeking to prevent or deter that presence through enhanced defenses. Further, the DCI Squad uncovers risks that can be passed to the Mission Protection Squad for collaborative assessment and mitigation. The majority of the DCI Squad's operational time is focused on detecting and discovering persistent threats.

2.H.5. (U//FOUO) Cyber Threat Emulation (CTE) Squad. The CTE Squad provides the means to assess an organization's security posture with a focus on non-permissive network/information system access. The CTE Squad is the CPTs lead for the analysis and emulation of threats within cyberspace. This squad engages the supported commander's organic and CPT-employed defenses by emulating specific TTPs used by a known adversary to identify unmitigated vulnerabilities through simulated exploitation or attacks on DOD cyber resources. CTE squads differ from traditional penetration test teams or Red Teams as they work very closely and openly with local cyberspace defenders and closely resemble adversary offensive cyberspace activities in their processes and execution (e.g., target selection, strike packages, controlled weapon discharge, as well as other attributes). CTE squads will be certified to execute at specified tiers of operational capabilities (script hackers through nation state entities) in Operational Preparation of the Environment (OPE) and Intelligence, Surveillance, and Reconnaissance roles. The squads will also be certified to execute offensive cyberspace activities and roles most commonly used as opposing forces (OPFOR) during exercise events; primarily for use during the conduct of a CPT mission, not as a specified OPFOR role in an exercise.

2.H.5.1 (U//FOUO) CTE squads operate in two modes: Participative or Silent. Participative operations are controlled evaluations of a defenders ability to identify and respond to a specified adversary threat capability. CTE squads fire a specific capability in an unannounced and controlled process allowing defenders to refine both technological capabilities and response processes to the threat. Silent operations are executed without expressed awareness of the defensive capabilities against the threats being emulated. Silent operations are also used to validate that the refinements implemented during participative operations were effective and maintained. CTE squads are not constrained from performing additional dynamic out-of-the-box threat emulations to push the envelope of cyber security and cyber defense capabilities. Although CTE squads may be aligned to the emulation of specific threats, they must be capable of understanding and, as needed, executing advanced cutting-edge cyber threats. The CTE Squad must utilize capabilities that allow for positive attribution (i.e., identified as friendly forces vice adversary). Additionally, CTE squads must be able to dynamically create capabilities to shift and avoid (maneuver) in response to common signature-based security methodologies.

2.H.6. (U//FOUO) All-Source Intelligence Analyst. CPTs may integrate an intelligence analyst within each squad. The purpose is to support the development of information flow between the intelligence and operational communities and to support the development of each squad's area of specialization. Each all-source intelligence analyst will have a unique perspective on the problem set and a varied role based on his/her assigned squad; it is critical that the intelligence professionals from each squad work together to share their unique perspectives and knowledge. It is the responsibility of the team leader and each squad's Cyber Defense (CD) Manager (Squad Leader) to identify intelligence requirements that should be fulfilled through the intelligence professional.

2.H.7. U) Detailed descriptions of the CPT Squad methodologies are found in Tabs 1-6 to Annex C.

2.I. (U//FOUO) Force Positioning. CPTs can operate under several different force positioning models. There are three major constructs that CPTs will most commonly support: 1) Centralized; 2) Regionalized; and 3) Hybrid. Each model has benefits and detractors to operations and resources. With any force positioning model it is important to remember that transformation within CO, both near and long term, will continue to exert pressure to position forces close to or even integrate with other regional capabilities. The decision regarding the positioning of CPTs, both physically and logically, must be made with due consideration to the larger functional and operational objectives of the CPTs.

2.I.1. (U//FOUO) Centralized. Given a resource constrained environment, CPTs from one or more mission area (e.g., Service, CCMD, DODIN, and National) can be collocated in the same physical area. This model, referred to as centralization, provides a Service the greatest flexibility in supporting the operational readiness of all of their CPTs and enables the highest amount of inter-team collaboration and support. The centralized model immediately creates a dependency on remote and virtualized capabilities; an expected operational methodology with CO. Centralization puts specific emphasis on supporting infrastructure robustness and the ability to support world-wide CO, but also provides the Services the capability to focus resources to minimize acquisition impacts. Another resource consideration is the ability to support the physical deployment of support operations. CPTs need to work closely with the supported mission owners, local cyberspace defenders, and their intelligence support entities; they should also provide supplemental training to the local cyberspace defenders to support the mission owner's mission assurance objectives.

2.I.2. (U//FOUO) Regionalized. As a high-demand/low-density asset, there may not be enough CPTs available to a mission owner to fully evaluate and protect the breadth of the supported mission, requiring CPTs to be positioned regionally. This model provides the greatest flexibility to support CCMD priorities and rapidly project CPT effects world-wide. Regionalization minimizes the resource impacts of travel from a centralized location and provides for quick connection between CPTs and the support mission owner. However, regionalization requires a more deliberate effort to ensure CPTs are virtually connected, mutually supportive, and focused. Further, decentralization requires duplication of resources across regionalized areas which can create support redundancy. This redundancy is a direct benefit to localized mission assurance but at a potentially higher sustainment cost.

2.I.3. (U//FOUO) Hybrid. The hybrid force positioning model supports maximum flexibility mixing both aspects of centralization and regionalization. Under the hybrid model, Services can establish a CPT central operations center and, as needed, transition specified teams to regional areas in support of regional objectives or balanced global operations. It is reasonable to assume that a balanced approach would be the most desirable model to employ under ongoing build-assess-build methodologies for these advanced capabilities.

2.J. (U) Authorities and Rules of Engagement

2.J.1. (U//FOUO) Authorities. Authorities to conduct cyberspace defense activities are negotiated by the supported command, supporting command and the Authorizing Official (formerly the Designated Approving Authority (DAA)) on a per mission basis appropriate for the CPTs mission. SECDEF authorizes CDRSTRATCOM Directive Authority for Cyberspace Operations (DACO); DACO is delegated to CDRUSCYBERCOM with collateral authority delegated to CDRJFHQ-DODIN for broad application across the potential range of military operations in cyberspace; including coordination and deconfliction of CPT access across DODIN boundaries.

2.J.2. (U//FOUO) Rules of Engagement (ROE). CPTs, in their role of executing DCO-IDM, will routinely be

governed by the Standing ROE (SROE) authority and responsibility of commanders to protect their force, including cyberspace assets. Other ROE for a CPT are arranged and defined by the supported and supporting commander on a per mission basis and updated by leadership during execution. The CPT shall not assume the responsibility for generating defensive effects from local cyberspace defenders.

2.K. (U) Coordinating Instructions

2.K.1. (U) Intelligence Support

2.K.1.A. (U//FOUO) Each CPT will have organically assigned intelligence analysts. The intelligence analysts serve as the CPTs inject point into the intelligence community, both for requesting intelligence information in support of operations, and for feeding operational data and other information into the intelligence system for further processing and analysis.

2.K.1.B. (U//FOUO) For CPTs assigned to CCMDs, the CPT intelligence analyst's inject point into the intelligence community will be determined by the respective CCMD, this may include the CCMD intelligence resources, JFHQ-Cyber, or other intelligence resources, dependent on the intelligence requirements. The inject point for Service retained CPTs will be the component's respective intelligence directorate (e.g., AFCYBER/A2). All supporting intelligence functions provided by that directorate will be in accordance with normal intelligence support actions. JFHQ-DODIN/J2 is the intelligence supporting entity for DODIN CPTs and USCYBERCOM/J2 is the intelligence supporting entity for National CPTs. USCYBERCOM/J2 will also maintain supporting relationships with the CCMD and Service equivalents to assist in supporting assigned CPTs.

2.K.1.C. (U) Acquired data and information must be classified in accordance with the associated Security Classification Guide prior to dissemination. Access to Joint Worldwide Intelligence Communications System (JWICS) will be required for the intelligence analysts assigned to the CPTs to access and use operational intelligence to inform CPT missions.

2.K.2. (U//FOUO) CPT Request for Support (RFS) between Operational Commanders. In the event that adversarial cyber activity exceeds the ability of organic defenders and CPT elements aligned with a specific operational command to effectively respond, the supported commander may notify JFHQ-DODIN of the need for additional support. Any request for additional CPT support must be consistent with the proposed C2 relationships defined in references (b) and (c).

2.K.3. (U//FOUO) Reach Back. Mission reach back provides CPTs a way to communicate at a classified level with organic, non-deployed, team members, supporting HQ, USCYBERCOM, NSA, JFHQ-DODIN, and other off-site partners. CPT personnel conducting operations at a remote location (away from their home station) must be provided the means to communicate at the required classification levels for the supported mission. At a minimum, Secret level communications capability must be provided by the site or the supporting HQ, leveraging either Secure voice or Secure data. The headquarters deploying the CPT and supporting commands should either coordinate for, or assess the feasibility of deploying, higher level classified (TS) communications capabilities based on anticipated mission location, the time available, existing connectivity/infrastructure, and cost.

2.K.4. (U//FOUO) The initial supported and supporting reach back relationship, with respect to non-deployed team members, support teams and the supporting HQ, should be established prior to a deployment; the relationships may change as understanding of the incident evolves. The supporting

HQ provides 24/7 reach back for deployed CPTs and should manage all external communications to the NSTs and CSTs by directing requests for information (RFI), effects, and analysis via this 24/7 reach back capability.

2.K.5. (U//FOUO) Expanded support to the Cyber Protection Force (CPF) will involve National Security Agency (NSA) direct support personnel assigned to NSTs/CSTs. CPTs are authorized to coordinate with NSTs/CSTs, as appropriate, for DCO mission support. Further detail on the type of support that the NSTs/CSTs will provide to the CPT will be promulgated in the NST CONOPS and CST CONOPS (Annex X and Y of OGS).

3. (U) Administration and Logistics

3.A. (U//FOUO) Capability Development and Sustainment. CPTs must sustain their core functional capabilities as executed through their squads (i.e., Mission Protection, DCI, CTE, etc.), the equipment they use (i.e., hardware, software, tools, cyberspace capabilities, etc.), and the TTPs they execute. All of these are collectively referred to as CPT capabilities.

3.A.1. (U//FOUO) Capability Sponsorship. A capability sponsor establishes the venues to discuss, capture, and resolve capability requirements and challenges. Capability sponsors set the standards and guide the priorities to allow Services to properly organize, train, and equip CPTs. USCYBERCOM is the sponsor for the CPF as a unified capability. JFHQ-DODIN works closely with DISA, the National Security Agency (NSA), and/or other designated sponsors and partners to evaluate operational requirements and establish a standardized, synchronized, and integrated capability within and across the CPTs and acts as the final adjudication authority for changes to the CPF and its supporting capabilities. DISA, as the lead for readiness, network hygiene and associated training, is the capability sponsor for Cyber Readiness and Cyber Support capabilities. Additionally, it is envisioned that the DOD Director, Operational Test & Evaluation (DOT&E) will support the coordinated standardization of measures to support operational capability and readiness assessments in coordination with DISA. NSA is the intended capability sponsor for the Mission Protection, Discovery and Counter Infiltration, and CTE capabilities as the lead DOD component for similar activities.

3.A.2. (U//FOUO) Capability Development. Each of the CPTs squads has a specific set of capabilities to build, deploy, and maintain. It is the intent that each CPT capability is aligned for support in coordination with DISA, NSA, and other DOD components, as appropriate. It is envisioned that these agencies take on the direct role to assist in the development of the standards and requirements to execute specific CPT capabilities. Services and capability sponsors shall seek to achieve DOD-wide certification and accreditation reciprocity for CPT capabilities with the help of USCYBERCOM.

3.A.3. (U//FOUO) Capability Repository. USCYBERCOM and JFHQ-DODIN will maintain a repository for all cyberspace capabilities (e.g., software, automation, etc.) utilized by the CMF. All capabilities identified as "standard equipment" for the CPTs must be approved by USCYBERCOM and maintained within the repository; neither the repository nor a process for approval of the standard equipment list have been defined but will be promulgated when established. USCYBERCOM will further identify combat essential and support equipment from reported and maintained CPT capabilities.

3.B. (U//FOUO) CPT On-Site Support Requirements. Communications and Network Access. CPTs provide the supported commander cyberspace defense expertise and capabilities that may augment or exceed those of local cyberspace defenders. One key enabler of the CPTs' strength is the ability to

communicate with supporting organizations at the CNDSP and national levels. To support the ability to coordinate and synchronize DOD CO to facilitate a raised level of mission assurance for a supported mission owner, CPTs must work closely with local cyberspace defenders to identify and request external support for local activities, to include domain administration credentials to allow the use of toolkits on local networks. This means facilitating support between the supporting CNDSP, the Combat Support Agencies (e.g., DISA and NSA), JFHQ-DODIN, and USCYBERCOM. The primary channel for coordinating these support actions shall be through the local cyberspace defenders C2 and augmented by the CPTs alternate support channels when necessary. Another key enabler of the CPTs' strength and success is "the familiarization" of supported commanders' network architecture and environment.

3.C. (U//FOUO) Situational Awareness. In addition to supporting the operational integration of external resources with local cyberspace defenders, the CPTs are required to ensure complete synchronization of their activities with aligned forces; a mechanism to enable synchronization will be developed by USCYBERCOM. Supplementing the established C2 is the shared situational awareness that CPTs have with each other. This situational awareness has several types: 1) general operational awareness of other CPT missions; 2) direct operational awareness of other CPT missions in adjoining cyberspace or areas of threat interest; 3) direct operational awareness of other CPT missions in common or shared areas of threat interest; and 4) direct operational synchronization between CPTs in common or shared areas of cyberspace or areas of threat interest. CCMDs and Services must have oversight and situational awareness of all CPTs conducting missions (physically and logically) within their area of responsibility.

3.C.1. (U//FOUO) General. General operating awareness is the understanding of where and why another CPT is conducting maneuvers. This awareness provides other CPTs insight into the priorities, efforts, and challenges that CPTs are working. Due to the nature of cyberspace and the threats that operate within it, this level of situational awareness is a minimum requirement for all CPTs. Through this awareness, CPTs can be informed of other CPTs operating in adjoining or common areas, despite the fact that the CPTs may be geographically dispersed or that the operations may be planned and executed independently.

3.C.2. (U//FOUO) Adjoining. Direct operational awareness between adjoining CPTs is the visibility that a CPT maintains about the actions and issues related to a CPT that is either operating in virtual proximity to another CPT or the similarity in the areas of threat (i.e., same threat area but not the same specific threat). This awareness enables CPTs to quickly and collaboratively work together to develop or conduct risk mitigations for a similar threat and potentially provide the ability to outmaneuver similar threats across one or more mission areas.

3.C.3. (U//FOUO) Common. Direct operational awareness between common CPTs is the visibility that a CPT maintains about the actions and issues related to a CPT that is operating within the same threat area (i.e., same threat area and cover of the same specific threat). This awareness enables CPTs to quickly and collaboratively work together to develop or conduct risk mitigations for a specific threat and provide the ability to outmaneuver the threat across one or more mission areas.

3.C.4. (U//FOUO) Synchronized. Direct operational synchronization between CPTs is the deliberate coordination between two or more CPTs operating either in the same cyberspace terrain, in protection of the same mission, or with respect to the same threat. Direct synchronization requires deliberate C2 to enable prioritization, deconfliction, and economy of force.

3.D. (U//FOUO) Training and Certification. USCYBERCOM is teamed with JFHQ-DODIN, NSA's

Associate Directorate for Education and Training (ADET), and DISA to establish certification and training standards for cyber forces. These standards are documented in the Joint Cyberspace Training and Certification Standard (JCT&CS). All CPTs must demonstrate that all personnel are fully trained IAW USCC TASKORD 13-0244 to be considered certified as Full Operational Capability (FOC). Certification of personnel is conducted individually and collectively. The Services will build their training programs to meet these objectives. Annex (C) of reference (d) provides additional details regarding training, certification, and readiness.

3.D.1. (U//FOUO) Individual. In accordance with the Joint Training System, individual training will prepare CPT personnel to perform mission unique duties. Training events will focus on individual core competencies, proficiencies, skills and knowledge necessary to accomplish assigned joint tasks. Mission commanders and individual work centers will oversee each team member's individual training and qualification status.

3.D.2. (U//FOUO) Collective/Team. Collective or team training builds upon individual skills and squad events. This critical part of the readiness evolution can include a combination of academic or practical events that culminate in an exercise that includes the entire team. Based on all aspects of the team's responsibilities, the exercise is designed to ensure that, at the operational and tactical level, DOD cyber units and cyber-relevant combat support agencies are prepared to execute their assigned missions, functions, and tasks. The CPTs operational headquarters, in coordination with the providing Service Cyber Component, will establish and execute collective training and readiness evaluations on an annual basis to certify teams for operations. Standards for collective training will be published by USCYBERCOM and JFHQ-DODIN.

3.D.3. (U//FOUO) Specialized Systems. Frequently, CPTs will be called upon to assist with the defense of mission systems that provide extremely specialized capabilities to DOD forces. These unique and non- commercial systems and applications will need to be understood by CPT members to enable effective defensive measures. Specialized training on such systems will be coordinated as needed in order for a CPT to operate effectively in support of discrete missions. The supported commander is responsible for the coordination of CPT member training from program manager or local sources but the CPTs sourcing Service will be responsible for the cost of CPT training.

4. (U) Command and Control

4.A. (U//FOUO) Command and Control Structures. All CPT operations will be coordinated, conducted, and synchronized with appropriate network owners and the operational commander in accordance with references (b), (c) and (d). The Operational Control (OPCON) relationships are depicted in appendix A of the Execution Order (EXORD); due to the classification, the figure is not included in this document. Figure 1 displays the approved CPT C2 relationship. For further guidance, refer to annex (G) of reference (e).

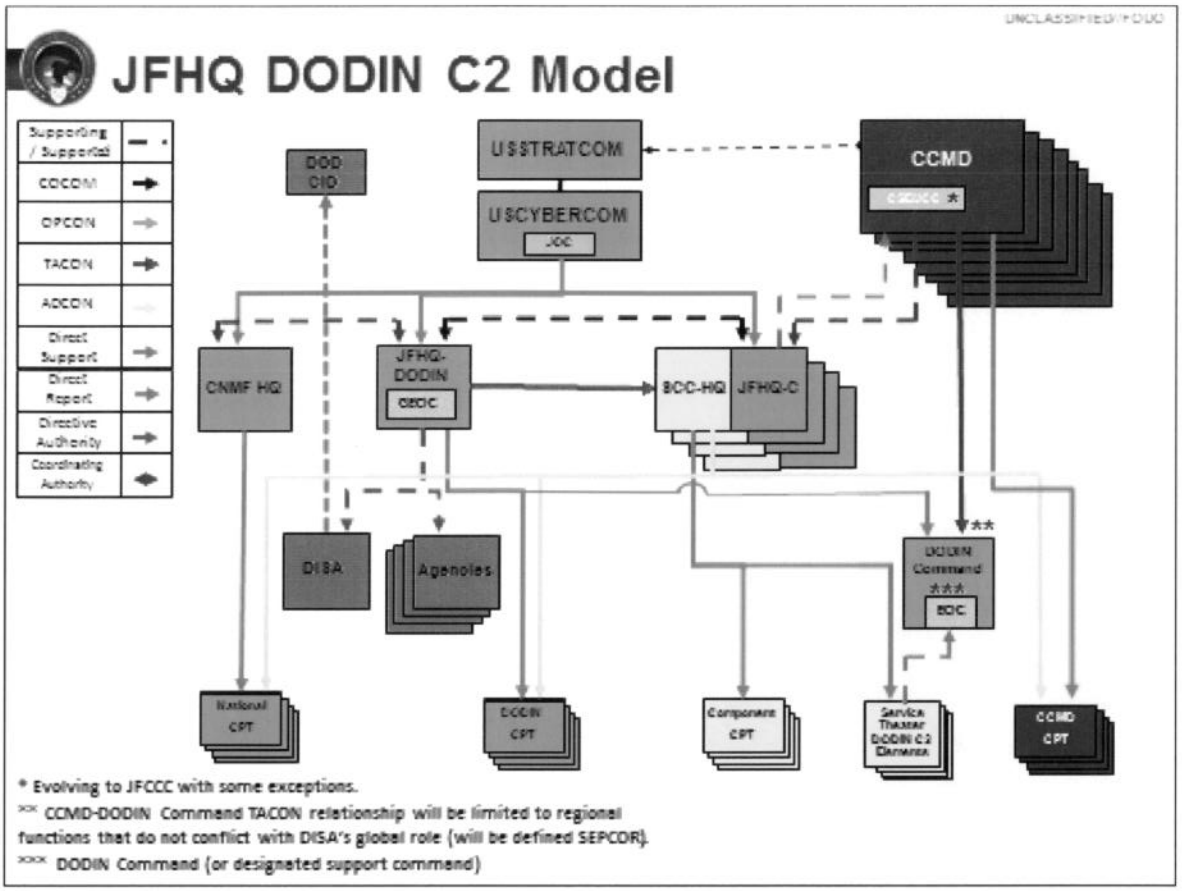

Figure 1. (U//FOUO) CPT C2 Relationships

4.A.1. (U//FOUO) General. Each of the four CPT forces (Service, CCMD, DODIN, and National) has a specified command and control structure. USCYBERCOM, as delegated by USSTRATCOM, exercises operational control of assigned DOD cyberspace forces. At the intermediate level, JFHQ-DODIN, Services and Cyber National Mission Forces (CNMF) receive guidance and direction from USCYBERCOM, evaluate and balance internal and external priorities, source capabilities to best meet the desired effects, and task tactical units - in this case CPTs - to support those effects. Consequently, it is the responsibility of each headquarters to maintain situational awareness of its tactically employed forces, support deconfliction and attribution, and submit requests for support (RFS) as required.

4.A.2. (U//FOUO) Service CPTs operate primarily across Service controlled cyberspace. Focused on Service unique environments and challenges, these teams address priorities in support of Service requirements. Service CPTs may be considered the force to directly support the Protection of CO within Service controlled areas of operations. Service CPTs will operate under the OPCON of the Service Cyber Component.

4.A.3. (U//FOUO) CCMD CPTs operate primarily across CCMD controlled cyberspace with the ability to coordinate across the DODIN as needed to support the Protection of a CCMD mission. These CPTs will operate under the OPCON of the CCMD Commander.

4.A.4. (U//FOUO) DODIN CPTs operate primarily across DISA controlled cyberspace with the ability to coordinate across the DODIN as needed to support the Protection of global CO or priority CCMD missions. These CPTs will operate under the OPCON of the JFHQ-DODIN.

4.A.5. (U//FOUO) National CPTs operate across the entire DODIN and retain the capability to support, when directed, U.S. Government priorities and activities outside the DODIN. National CPTs directly Protect DOD global and/or strategic assets and terrain, and directly cover areas of the DODIN outside of any specific Service, CCMD, or DISA areas of control (i.e., support to other DOD components). These CPTs operate under OPCON of the CNMF Commander.

4.A.6. (U//FOUO) Administrative Control. Services are responsible to organize, train and equip their sourced CPTs IAW mission owner requirements.

4.B. (U//FOUO) Prioritization and Force Allocation. Due to their low-density/high-demand nature, prioritization and allocation of CPTs requires deliberate coordination between all DOD components; USCYBERCOM's role is to synchronize operations and provide strategic guidance to intermediate headquarters. Intermediate headquarters are responsible to prioritize requirements within their AO, position their CPTs accordingly, and communicate their priorities and actions to USCYBERCOM and the supported CCMD. The capabilities of CPTs are best utilized when focused on larger strategic objectives and employed rapidly throughout friendly cyberspace as opposed to focusing on smaller tactical priority objectives. Misalignment or inappropriate pairing of CPTs to objectives can hinder team maneuverability, drain valuable resources, and delay the needed transformation of DOD cyberspace activities.

4.B.1. (U//FOUO) CPTs assigned to support national missions will be assigned mission sets based on USCYBERCOM identified priorities. DODIN CPTs will receive mission prioritization from the Director DISA. CCMD CPTs will receive mission prioritization from CCMD Commanders. Service CPTs will receive mission prioritization from associated Service Cyber Components.

4.B.2. (U//FOUO) The CCMD is responsible to synchronize operations and provide theater guidance to intermediate headquarters for prioritization and allocation of CPTs.

4.B.3. (U//FOUO) CCMDs/Services/Agencies, acting on indications and warnings, national command directives, or global need, may request the assistance of CPTs that are OPCON to other organizations. Disputes shall be resolved in accordance with the deconfliction provisions set forth in section 3.C of reference (b).

4.C. (U//FOUO) Mission Area and Required Support (MARS) Process. While CCMDs and Services retain the ability to task CPTs as desired, the need to provide strategic level deconfliction of CPT capabilities requires a high-level coordination and synchronization process. The MARS process has been established to deconflict mission areas among Service, CCMD, DODIN, and National CPTs, to identify how to achieve mission objectives seamlessly across enclaves, and to provide a mechanism to ensure that CPTs across the DOD are not duplicating efforts. A regularly scheduled CPT working group has been established by USCYBERCOM to ensure strategic level mission assignment issues are addressed.

4.D. (U//FOUO) CPT Mission Assignment. CPT mission assignments are dynamic and are subject to the employer's mission priorities. CPT employers do not have the authority to assign or task CPTs outside of their OPCON. If a CPT employer requires support from a Service, CCMD, DODIN or National CPT, he/she shall submit a RFS/RFF as discussed in paragraph 2.K.2 of this document.

4.D.1. (U//FOUO) CPT Mission Changes. Mission changes must be shared with USCYBERCOM and the CPT community to ensure that CPTs across the DOD are not duplicating efforts. USCYBERCOM has implemented and manages a mechanism to provide employers with the flexibility to change CPT

missions and provide the CPT community with the information required for deconfliction efforts. USCYBERCOM hosts a regularly scheduled CPT working group to ensure strategic level mission assignment issues are addressed expeditiously.

4.E. (U//FOUO) Primacy and Supported/Supporting. The diverse authorities, cyberspace terrain, and areas of operations that exist in DOD CO present a challenge to CPT operations. While all teams are designed to be tightly integrated, mutually supportive, and interchangeable across the domain, there remain inherent differences within cyberspace terrain as managed by the different Service components; these differences must be accounted for and managed. To address these issues, commanders must consider C2 and the supported/supporting relationship carefully. For CO involving multiple CPTs, a lead team should be identified for coordination and situational awareness of all teams involved, especially for teams that are operating across the same mission areas. For example, a mission supported within Air Force cyber terrain should have a Service CPT provided by the Air Force as the lead to facilitate Service dialog and operational risk mitigation. The intermediate headquarters will be responsible for the operational area within each defined mission area (Service, CCMD, DODIN or National). For example, a CCMD CPT that is focused on supporting CCMD priorities and missions should act as the lead CPT for all CPTs protecting a singular mission in support of the CCMD's objectives, as the CCMD CPT will be most aware of the specific issues. In the event of conflict between CPT employers, such that a lead CPT cannot be agreed upon, JFHQ-DODIN will adjudicate the lead CPT based on its assessment of mission priorities and requirements.

4.F. (U) Reporting and Situational Awareness

4.F.1. (U//FOUO) Reporting. USCYBERCOM and JFHQ-DODIN will maintain situational awareness of all DODIN cyberspace defense activities. Cyberspace defense units are responsible for reporting ongoing, planned, and completed activities to USCYBERCOM, JFHQ-DODIN (for DODIN activities), and the respective CCMD and Service, through the operational chain of command. CPTs are required to submit initial, interim, and post-mission reports, via the operational chain of command, to USCYBERCOM, JFHQ-DODIN (for DODIN activities); respective CCMDs and Services should receive reports for situational awareness purposes if they are not a part of the operational chain of command. Report formats will utilize DOD standardized reporting (e.g., TACREP, OPREP, SITREP, MISREP, etc.) and be tailored in accordance with Annex (R) to support C2 of CPF missions and cyberspace data and information sharing across the DOD. All reporting, at a minimum, will include the root cause of issues, actions being taken to address the issue, and the overall impact to the supported mission.

4.F.2. (U//FOUO) Cyber Identification Friend or Foe (C-IFF). As part of the maintenance of global cyber force situational awareness, JFHQ-DODIN Operations Center is the central hub for all activities governing C-IFF in accordance with procedures outlined in reference (e). Suspicious activity discovered on the DODIN will be subject to a C-IFF review to determine if friendly forces are responsible for the activity. If C-IFF is unable to determine friendly force involvement at the operational level, USCYBERCOM will enable global C-IFF review to ensure local commanders have the most timely and accurate information available when making defensive decisions. USCYBERCOM will issue specific guidance and establish supporting procedures to direct and enable timely, accurate, and efficient C-IFF.

4.G. (U//FOUO) Battle Hand-over. CPTs will likely encounter situations that require a hand-off of cyberspace defense activities to another CPT or organization, or a transition of cyberspace defense activities external to their AO. Once the CPT has minimized the threat and trained the staff, a battle handover brief will be conducted. This brief will provide information, direction and guidance relative to

the mission that facilitates situational awareness. Additionally, it provides an understanding of the rationale for key decisions necessary to ensure there is a coherent transfer from CPT to CPT/CNDSP. These factors coupled together are intended to maintain the intent of the concept of operations, promote unity of effort, and generate tempo.

4.G.1. (U//FOUO) Battle Handover Brief. This is an informal transition brief to subordinate or adjacent commanders and to the staff supervising execution of the mission. It is given to ensure all actions necessary to implement the mission are known and understood by those executing the mission. The brief should be an overview and include items such as: commanders intent, CCIRs, responsible headquarters mission (tasks and intent), subordinate/adjacent mission, task organization, situation (enemy and friendly), concept of operations, execution (including branches and sequels), and planning support tools (synchronization matrix, JIPOE products, etc).

4.H. (U//FOUO) Deconfliction Process. During mission execution, CPTs must balance and support no less than three chains of command: 1) the C2 of the CPT unit and their intermediate headquarters; 2) the C2 of the supported mission owner; and 3) the C2 of the local cyberspace defenders. This complexity requires CPTs to identify, clarify, and streamline the required authorities and reporting for the conduct of their mission. Deconfliction of CPT activities at the local level is handled through the local cyberspace defenders chain of command to the greatest extent possible. In instances where local deconfliction is ineffective, deconfliction will be passed to JFHQ-DODIN, the CCMD/JCC, Service, or CNMF as applicable. In instances where deconfliction between Service, CCMD, DODIN and/or National CPT activity is necessary, USCYBERCOM will perform deconfliction. During routine operations, as stated in paragraph 4.C. of this document, USCYBERCOM will host a regularly scheduled CPT working group to ensure strategic level mission assignment issues are addressed.

(U) Acronyms

AO - Area of Operations
ADET - Associate Directorate for Education and Training
CCMD - Combatant Command
CERT - Computer Emergency Response Team
CFCOE - Cyber Force Concept of Operations and Employment
C-IFF - Cyber Identification Friend or Foe
CIKR - Critical Infrastructure and Key Resources CJCS
– Chairman of the Joint Chiefs of Staff
C-KT - Cyber Key Terrain
CNDSP - Computer Network Defense Service Provider
CNMF - Cyber National Mission Force
CO - Cyberspace Operations COA
- Courses of Action CONOPS -
Concept of Operations CD – Cyber
Defense CPF - Cyber
Protection Force
CPT - Cyber Protection Team
CSSP – Cyber Security Service Provider (replacing CNDSP)
CTE - Cyber Threat Emulation
DCI - Discovery and Counter-Infiltration
DCO-IDM - Defensive Cyber Operations – Internal Defensive Measures
DCO-RA - Defensive Cyber Operations Response Actions
DISA - Defense Information Systems Agency
DODIN - Department of Defense Information Networks
DOT&E - Director, Operational Test & Evaluation EXORD
- Execution Order
FCDF - Friendly Cyberspace Defense Force
FOC - Fully Operational Capability
IOC - Initial Operational Capability ION
- Interactive Operator
IPB - Intelligence Preparation of the Battlefield
JIPOE – Joint Intelligence Preparation of the Operational Environment JTIMS
- Joint Training Information Management System
MARS - Mission Area and Required Support Process MDP
- Mission Defense Plan
MOE - Measures of Effectiveness
MOP - Measures of Performance
NCOIC - Non-Commissioned Officer in Charge NOSC
- Network Operations and Security Centers NSA -
National Security Agency
OPE - Operational Preparation of the Environment
OPCON - Operational Control
OPFOR - Opposing Forces
OPTEMPO - Operations Tempo
OPSO - Operations Officer

POA&M - Plan of Action and Milestone RFF
- Request for Forces
RFS - Request for Support RMP
- Risk Mitigation Plan SECDEF -
Secretary of Defense
TTP - Tactics, Techniques, and Procedures

(U) Glossary

(U) Cyberspace Key Terrain (C-KT). Any locality or area in cyberspace (logical, physical, or persona) whose seizure, retention, or disruption affords a marked advantage to any combatant. C-KT is driven by the commander's mission.

(U//FOUO) Local Cyberspace Defenders. The existing cyberspace defenders responsible to conduct cyberspace defense activities with a specified area of operations. Local cyberspace defenders include the cyberspace defense chain of command and support (e.g., the local commander, Information Assurance Manager (IAM), Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), Program Management Office (PMO) for a Program of Record (POR), Authorizing Official, Chief Information Officer (CIO), and/or Computer Network Defense Service Provider (CNDSP)

(U) References

(a) (U) DOD Strategy for Defending Networks, Systems, and Data, 13 November 2013
(b) (U) Execution Order to Implement Cyberspace Operations Command and Control, 21 June 2013
(c) (U) MOD to EXORD to Implement Cyberspace Operations C2 Framework 14 Nov 2014
(d) (U) MOD 01 to EXORD 13-13: Implement Cyberspace Operations Command and Control Framework, 19 Nov 2014
(e) (U) USCYBERCOM CFCOE, 22 July 2014
(f) (U) FRAGO 21 to OPORD 05-01, 31 Mar 2011
(g) (U) DOD Strategy for Operating in Cyberspace, April 2011
(h) (U) 2011 International Strategy for Cyberspace, May 2011

Annex B to Concept of Operations (CONOPS) for Cyber Protection Teams (U)
Intelligence (U)

(U//FOUO) To be published in OPERATION Gladiator Shield rewrite

Annex C to Concept of Operations (CONOPS) for Cyber Protection Teams (U)
Operations: CPT Methodology (U)

(U//FOUO) General. CPT methodology follows two phases (Planning and Execution) and four supporting stages (Survey, Secure, Protect, and Recover) which are chosen based on the CPTs mission. CPTs will task organize based on support requirements; in some situations, the entire CPT may not be required. Throughout these phases and stages no CPT Squad operates in isolation. Each squad draws from and supports the other squads to conduct each phase and stage of the CPT operational methodology. Through the conduct of these phases, CPTs deliberately integrate with the supported commander's staff, local cyberspace defenders, and supporting intelligence elements. The intent of this approach is to rapidly build and transform cyberspace defensive activities through direct training and support to local cyberspace defenders and all vested parties.

1. (U//FOUO) Time. Each phase of CPT operations has a notional timeline required for completion. The timeline is highly dependent on the scope of the mission and the time required for mission execution. Through their interconnected relationship, all CPTs work deliberately to improve the tools, tactics, techniques, and procedures they utilize to conduct their operations. As CPT operations mature, the time required to complete these actions may be adjusted. In situations where time is limited, leadership must decide how to best tailor the actions and effects to meet the mission objectives.

Mission Phase		*Core Actions*
Planning Phase		• *Mission Analysis / Problem Framing* • *Identification of, and Coordination with, Local Defense Personnel* • *Establishment of Authority to Conduct Mission* • *Area of Operations Definition* • *Orders*
Execution Phase	***Survey***	• *Refined Definition of Supported Mission* • *Mission/Terrain Mapping, Key Terrain /Critical Asset Identification* • *Participative Evaluation of Existing Defensive Capabilities* • *Development of Risk Mitigation Plan*

	Secure	• *Implementation of Risk Mitigation Plan*
		  ○ *Technical and procedural mitigations*
		  ○ *Provision of Education and Training*
		• *Non-Participative Defensive Evaluation*
		  ○ *Validation of Deployed Mitigations*
		• *Development of Mission Defense Plan*

	Protect	• *Active Risk Mitigation* • *Active Surveillance / Detection Efforts* • *Threat Response / Risk Mitigation Actions*
	Recover	• *Recovery & Rebaselining* • *Transition of Stay-Behind Capabilities* • *POA&M Development for Outstanding Risks* • *Final Reporting*

Table 1. Summary of CPT Mission Phases, Stages, and Associated Core Actions

2. (U) Mission Planning Phase

2.A. (U//FOUO) The purpose of the planning phase is to: 1) establish and execute normal planning for tactical CPT operations; 2) identify key leadership and authorities; 3) establish command, control, and communications (C3); and 4) build actionable requirements and orders to conduct CPT operations and achieve the desired results.

2.B. (U//FOUO) Through the mission planning phase, CPT capabilities are tailored to meet the unique requirements of the assigned mission. The mission planning phase requires the CPT to identify and link with the local cyberspace defenders and their supporting intelligence entities, elicit essential information, establish the CPT forward deployment area, and identify resource requirements. Further, identifying preapproved actions and approval authorities will improve the time efficiency during the execution phase.

2.C. (U//FOUO) Due to the low density and high demand nature of CPTs, mission planning takes into consideration all levels of military operations. Strategic mission planning occurs when CCMDs seek to align CPT operations directly to strategic objectives under their purview. However, not all CPT missions will be directly or easily tied to the immediate needs of the CCMDs. The CPTs higher headquarters will receive and prioritize requests for support from within their AO (e.g., Service support to Service operations). Due diligence by the operational-level headquarters should be conducted to ensure CPT missions have the best strategic alignment and highest level of impact.

(U//FOUO) Tactical mission planning occurs between the CPT, the supported commander, and the associated local cyberspace defenders. CPT mission planners must work to properly scope the terrain for CPT operations. Should mission planning identify the requirement for additional resources; the CPT will make recommendations to address the deficiency to its next higher headquarters.

3. (U) Execution Phase: Survey

3.A. (U//FOUO) General. The Survey stage serves to set the baseline understanding of a supported commander's mission, the supporting cyberspace terrain, risks to the terrain, and develops the Risk Mitigation Plan (RMP). During this stage the CPT will focus on the following objectives: 1) reconnaissance of the friendly cyberspace AO; 2) identifying and clearing the area of active threats; and 3) the development of a RMP. The Survey stage is subdivided into five supporting objectives: 1) Mission Survey; 2) Terrain Mapping; 3) Essential and Critical Elements analysis; 4) C-KT analysis; and 5) Risk Assessment/COA development. A supported commander's mission and its cyberspace terrain are dynamic; consequently, all objectives of the Survey stages must be continuously reassessed after any changes to the underlying terrain occur to maintain situational awareness. All objectives of the Survey stage are critical to the development of a qualified RMP and the integration and support of advanced cyberspace defense.

3.B. (U//FOUO) Mission Survey. During and throughout Mission Survey, a CPT works to understand the execution, timing, and the broad utilization of cyberspace terrain and assets of a supported commander's mission. Largely executed and synchronized through the Mission Protection Squad and led by CPT leadership, this objective: 1) determines the cyberspace needs of the supported commander's mission; 2) initiates and builds communication between the supported commander and the CPT; and 3) refines the CPTs tasked mission and AO. All CPT Squads work to develop their understanding of the supported commander's mission, elements supporting the mission, and the

supported commander's associated mission objectives. Understanding the supported commander's mission and objectives are central to the ability of the CPT to build an effective RMP and, if required, the ability to Protect. Mission Survey is not comprised solely of static cyberspace analysis. Through Mission Survey, the CPT must understand how the supported commander's priorities shift through the operational phases and how these changes affect the cyberspace terrain. Mission Survey maps the conduct of operations and the cyberspace persona layer and links them to mission generated cyberspace terrain maps.

3.C. (U//FOUO) Terrain Mapping in Cyberspace. Building upon the information obtained during the planning phase, terrain mapping provides an aggregated view and understanding of the cyberspace terrain supporting the assets and effects of a supported commander's mission. Terrain Mapping builds the physical and logical elements of the cyberspace terrain enabling the commander's mission. Largely conducted and led by the Cyber Support Squad, this objective lays the foundational reference point for all other CPT capabilities. The terrain mapping objective is initially agnostic of unique mission systems or the inferred importance of elements of the cyberspace terrain. The foundational map provides each squad the ability to establish reference points for their operations, generate squad specific overlays that enable and consolidate CPTs effects, and establish a reference for communication with local cyberspace defenders and the mission owner. Terrain mapping directly supports the interconnections between the physical, logical, and persona layers of cyberspace.

3.D. (U//FOUO) Essential and Critical Elements Analysis. Refining the efforts conducted during the planning phase and evaluating the cyberspace terrain enabling a supported commander's mission further narrows the focus areas for CPT operations. During this process, the CPT evaluates the cyberspace terrain, developed through Terrain Mapping, by overlaying the objectives of the supported commander's mission, learned through Mission Survey. This effort, largely synchronized through the Mission Protection Squad, seeks to identify terrain and assets as either essential or critical to the supported commander's mission without regard to risk. This objective works to both identify and illustrate a supported commander's cyberspace terrain requirements and grade their importance to the supported commander's mission. This objective can be mutually supportive of the identification of DOD CIKR. Of note, the determination of C-KT is the responsibility of the system owner; however, the CPT will assist in analyzing and refining the C-KT as discussed in paragraph 4.E of annex C.

3.E. (U//FOUO) Cyber Key Terrain (C-KT) Analysis. The CPT evaluates mission-supporting C-KT with specific regard to identifying and prioritizing the following: 1) critical elements of mission essential functions; 2) adversary capabilities; 3) adversary's will and intent; and 4) the adversary's likely courses of action. The C-KT analysis, led and synchronized by the Mission Protection Squad, leverages Joint Intelligence Preparation of the Operational Environment (JIPOE) products and threat templates to identify key terrain in cyberspace. This phase requires extensive knowledge of threat capability, intent, and TTPs which are leveraged through the CPTs access, fusion, and integration of operational and intelligence reporting. The objective, supported by the squad's intelligence analysts, is to directly link operations with supporting intelligence entities to enable self-sustainable, dynamic analysis, and identification of C-KT. C-KT analysis strives to identify areas of supporting cyberspace terrain where contest for control of terrain or assets within that terrain may directly impact the supported commander's or the CPTs ability to conduct its mission.

3.F. (U//FOUO) Risk Assessment/Course of Action (COA) Development. Risks are a function of: 1) the criticality of a mission's cyberspace terrain or assets; 2) the characteristics of the terrain or assets (e.g. vulnerabilities, routes, etc.); 3) the characteristics of the threat (e.g., capability, intent, and targeting/will); and 4) the likelihood of attack. The risk functions are summed to provide an evaluation of

risk across the AO; the risk evaluation enables the CPTs to prioritize their risk mitigation efforts accordingly.

3.F.1. (U//FOUO) During the Survey stage the CPT evaluates the supported commander's mission, the supporting cyberspace terrain, C-KT within the AO, and mitigation techniques employed to identify risks. An evaluation of current defenses/mitigation techniques is essential to understanding how local cyberspace defenders and defenses are employed and provide the CPTs the insight required to make effective recommendations to improve defense methodologies. Risk mitigation options are developed by all CPT Squads; each squad provides a different perspective on the feasibility and suitability to support the objective of the mitigation.

4.F.2. (U//FOUO) Teams collectively works with the supported commander, local cyberspace defenders, and reach back support through its higher headquarters, to facilitate the rapid development of appropriate COAs. Within the COA development process, the team works to build the supported commander and local cyberspace defenders ability to conduct COA development and the ability to request external support. Once appropriate COAs are developed, the CPT, led by the Mission Protection Squad, develops the RMP. The RMP is the culmination of the Survey stage. It prioritizes and outlines the options and actions available, both technical and procedural, to provide a greater level of mission assurance for the supported commander's mission through the consolidation of all squad recommendations. The team's specific mission and the authorities outlined under the mission dictate the level of direct action that the team can take to implement mitigations. The plan must reflect both action entities and tasking mechanisms to achieve the desired effects.

4. (U) Execution Phase: Secure.

4.A. (U//FOUO) General. The Secure stage focuses on the implementation of the RMP, as adjudicated and approved by the supported commander and local cyberspace defenders. This stage can be implemented by local cyberspace defenders with CPT oversight or implemented by the CPT with local cyberspace defender oversight. The authority given to a CPT to directly implement mitigations and capabilities may vary depending on the mission. During this stage, a CPT will be focused on three objectives: 1) deployment of risk mitigations; 2) validation of deployed mitigations; and, if anticipating transition into the Protect stage, 3) the development of the Mission Defense Plan (MDP). The Secure stage is subdivided into four supporting objectives: 1) Education and Training; 2) COA Implementation; 3) Risk Mitigation Validation; and 4) Summary Reporting. A supported commander's mission and his/her cyberspace terrain are dynamic and should be adaptive; a feature of cyberspace that CPTs look to leverage for a tactical advantage. Since terrain in cyberspace can be easily changed, CPTs must establish and integrate flexible and dynamic processes for defensive operations that account for these environmental modifications. Ongoing defensive improvements are directly enabled through the repeated conduct of objectives from both the Survey and Secure stages. All objectives of the Secure stage are critical to both the development of a qualified MDP and the integration and preparation of advanced cyberspace defense actions to defend a supported commander's mission.

4.B. (U//FOUO) Improving Local Defensive Posture. Improving Local Defensive Posture is focused on conducting the training necessary to educate local cyberspace defenders on the technical and procedural mitigations employed. This objective, largely led by the Cyber Support Squad, seeks to establish a baseline skill level for the conduct of advanced cyberspace defense actions to include best practices for system configuration and maintenance as well as operational methodologies. During this objective, the CPT provides training in each of the five squad methodologies for the local cyberspace defenders. The purpose of this objective is to build the baseline training to strengthen local cyberspace

defenders ability to Protect the supported commander's mission and enable CPT redeployment.

4.C. (U//FOUO) COA Implementation. The COA Implementation objective serves to complete COA selection and deploy approved risk mitigations as outlined in the RMP. The CPT works with the supported commander, local cyberspace defenders, and other specified authorities, to review the RMP, war game proposed options, and seek approval to execute specific COAs. Working with local cyberspace defenders and guided by the Mission Protection and Cyber Support Squads, the CPT systematically implements approved risk mitigations to support a higher state of mission assurance for a supported commander's mission. COA implementation is one of the most challenging objectives of the Secure stage as it requires considerable synchronization and approval to deploy specific risk mitigations. Efforts to identify preapproved actions and approval authorities during the Mission Planning phase and close coordination with local cyberspace defenders may improve the speed of execution.

4.D. (U//FOUO) Risk Mitigation Validation. The Risk Mitigation Validation objective provides the final evaluation of deployed risk mitigations. This objective goes beyond the validation implemented in the Survey stage. The core differences are: 1) the evaluation of CPT capabilities that are deployed through the RMP; 2) the non-participative evaluation of CPT and local cyberspace defenders capabilities led by the CTE Squad; and 3) the Cyber Readiness Squad's evaluation of the defenders operational preparedness to defend the mission. The Risk Mitigation Validation objective provides the final opportunity for defensive tuning prior to the conduct of defensive activities by the local cyberspace defenders and CPT, if tasked to assist in mission defense.

4.E. (U//FOUO) Summary Reporting. The Summary Reporting objective provides the final report to capture all of the lessons learned from the Survey and Secure stages.

4.F. (U//FOUO) Development of the MDP. If a mission requires execution of the Protect stage, then the Secure stage will also require development of the MDP, led by the Mission Protection Squad. The MDP outlines the residual mission risks and illustrates how CPT capabilities will be integrated into and coordinated with the local cyberspace defenders to enhance the cyberspace defense of a supported commander's mission. Once the MDP is completed it serves as both the guide for the conduct of cyberspace defense activities and as a reference point for successive evaluations and conduct of ongoing defensive improvements.

5. (U) Execution Phase: Protect

5.A. (U//FOUO) General. The Protect stage is the execution of the CPTs combat role. The execution of this stage is optimally conducted with strong interconnection between the CPT, the supported commander's assets, and local cyberspace defenders. Working closely with local cyberspace defenders, the CPT executes cyberspace security and defense tasks as outlined in the MDP. This stage is the most dynamic of all CPT operations and requires the continuous reassessment of objectives from the Survey and Secure stages to sustain situational awareness and COA development. The objective of this stage is to sustain the execution of a supported commander's mission on and through its supporting cyberspace terrain. The Protect stage is subdivided into five supporting objectives: 1) Ongoing Hardening; 2) Detection; 3) Response; 4) Coordinated Situational Awareness; and 5) Record. Mission defense is the CPTs second core task. The direct tactical defense of a supported commander's mission is highly dynamic and is focused on implementing risk mitigation measures. A notable difference in the Protect stage is the transition of the CTE Squad from an active threat emulation capability to an active support capability, guiding the DCI and Mission Protection Squad activities. The Protect stage continues until mission success criteria are

achieved.

5.B. (U//FOUO) Ongoing Hardening. The Ongoing Hardening objective encapsulates the continual implementation of risk mitigations. This objective contains foundational processes established in the Survey and Secure stage. This objective, led through the Mission Protection Squad, is focused on proactively sustaining defensive improvement efforts and effects until direct response is required to defend supporting cyberspace terrain against active threats.

5.C. (U//FOUO) Detection. The Detection objective of the Protect stage leverages integrated operational and intelligence reporting to enable deliberate reconnaissance and surveillance operations as outlined in the MDP. This objective, led by the DCI Squad and directly supported through active patrolling by the Cyber Readiness and Cyber Support Squads, monitors the established AO for changes in security posture; changes in security posture could result from purposeful or inadvertent changes to protected cyberspace terrain or from the identification of anomalous activity or overt threat actions. During the conduct of the Protect stage, a CPT is actively searching for threats but does not solely rely on detection as a precursor to risk mitigation. As mentioned previously, the CTE Squad is a critical link, enhancing the detection and defeat of threats by actively maintaining adversary situational awareness. This is achieved through multiple avenues including the collection and fusion of operational and intelligence reporting, to include appropriate indications and warnings. Armed with an understanding of the adversary, the CTE squad works with the other squads and local cyberspace defenders to guide detection activities and inform preventative risk mitigations.

5.D. (U//FOUO) Response. The Mission Protection Squad develops the appropriate mixture of Protect, detect, characterize, counter, and mitigate to respond to and defeat threats to defended cyber terrain. The Response objective is initiated through the identification of emerging significant risks, indications and warnings of adversary maneuver and effects or direct contact with an adversary in the defended space. This objective works to rapidly evaluate, respond, adapt to, and mitigate the immediate risk to sustained mission assurance. Response is not limited to the CPT; to support successful response, a CPT must evaluate, enable, and conduct integrated risk mitigation measures with local cyberspace defenders and external defensive CO forces to address advanced persistent threats to the defended mission within cyberspace.

5.E. (U//FOUO) Coordinated Situational Awareness. The CPT must directly support the situational awareness for all parties involved in preparation for or in response to threats. The CPT must maintain awareness of the maneuvers and risk mitigation efforts of local cyberspace defenders, other CPTs, and the DOD's larger CO and cyberspace defense actions. The effort to sustain situational awareness is foundational to rapid adaptation, synchronization and execution of desired cyberspace effects. The Mission Protection Squad is central to this effort and is directly supported by the DCI and CTE Squads. The Coordinated Situational Awareness objective contains the CPTs operational and the intelligence fusion requirements for a CPT mission.

5.F. (U//FOUO) Record. The Record objective, executed by all CPT Squads, conducts the necessary actions to document and annotate dynamic CPT risk mitigation measures deployed during the Protect stage. The Record objective is conducted concurrently throughout the Protect stage and is essential for capturing lessons learned and the required actions for the Recover stage. All Record objectives are conducted by each CPT Squad; the Mission Protection Squad will consolidate records for final reporting through the team leadership to the supported commander, JFHQ-DODIN, and USCYBERCOM. Recording also enables an orderly withdrawal of CPT capability and transition to local cyberspace defenders by ensuring all actions are documented.

6. (U) Execution Phase:

6.A. (U//FOUO) Recover. The Recover stage covers all actions taken by the CPT to complete the mission and conduct a battle hand-off with the local cyberspace defenders. During this stage, the CPT is focused on three main objectives: 1) transition of defensive responsibilities; 2) strengthening intelligence support to local cyberspace defenders; and 3) the development of the CPTs final report. The Recover stage is subdivided into four general supporting activities: 1) Recover and Re-baseline; 2) Train and Equip; 3) Plan of Action and Milestone (POA&M) Development; and 4) Final Reporting. The focus of this stage is to ensure local cyberspace defenders can sustain advanced cyberspace defense methodologies for a supported commander's mission. CPTs work with local cyberspace defenders to reinforce Survey-Secure-Protect concepts and phases. This Recover stage is the culmination of the CPTs efforts to work with and enable the local cyberspace defenders to protect the cyberspace terrain. When a CPT is tasked to return to conduct a new mission, every effort is made in this stage to enable a higher level of mission assurance for a supported commander as provided by local cyberspace defenders.

6.B. (U//FOUO) Recover and Re-baseline. The Recover and Re-baseline objectives focus on activities required to recover from active defensive actions. It is assumed that tactical decisions will be made to adjust cyberspace terrain or processes to best address significant risks that may not be practical over the long term. It may also be necessary to return defended cyberspace terrain to a known-good state after contest with an adversary. These objectives enables CPTs to evaluate cyberspace defense actions and affects that were executed, determine what actions need to be taken to sustain a higher level of mission assurance post activity, and execute those actions. The Recover and Re-baseline objective, largely led by the Cyber Support Squad, requires significant coordination with local cyberspace defenders and the other CPT Squads. This allows the CPT to safely communicate, coordinate, and transition tools and capabilities to local cyberspace defenders, effectively executing a relief-in-place for the defensive operations of a supported commander.

6.C. (U//FOUO) Train and Equip. The Train and Equip objective, led by the Cyber Support Squad, provides the necessary actions to conduct any final training for the conduct of advanced cyberspace defense actions. During the execution of this objective the CPT evaluates what CPT-deployed equipment and processes will be provided to local cyberspace defenders for use and identifies training required for local cyberspace defenders to incorporate these capabilities. This objective directly addresses the sustainment of intelligence support to local cyberspace defenders allowing the conduct of necessary cyberspace defense actions for the supported commander's mission.

6.D. (U//FOUO) POA&M Development. CPTs and local cyberspace defenders must develop feasible, suitable, and acceptable POA&Ms for the transition of CPT activities to local cyberspace defenders or actions to sustain long-term defensive improvements. It is assumed that risk mitigation actions may have a longer implementation plan than the duration of a tactical CPT operation. The Cyber Readiness Squad works with local cyberspace defenders to build POA&Ms through the Recover stage. POA&Ms may include additional training requirements as identified by the Cyber Support Squad to address deficiencies that could be mitigated with additional Service/commercial training. POA&Ms may include supplemental CPT actions and support to local cyberspace defenders beyond the previously planned termination of a CPT operation.

6.E. (U//FOUO) Final Reporting. A core deliverable from the Recover stage is the annotation, consolidation, and distribution of reporting from the conduct of a CPT operation. Led by the team's leadership, conducted by the Mission Protection Squad, and supported by all other squads, this objective builds a comprehensive master final report. The master final report includes but is not limited to the following: 1) information from the RMP; 2) information from the MDP; 3) information from the completion of Protect stage; and 4) information, analysis, and POA&Ms resulting from the Recover stage. Follow-up or close-out of POA&M will be conducted in accordance with the supported commander's guidance. The purpose of this objective is to ensure that all necessary actions to address operational reporting and intelligence fusion are completed. This objective directly feeds local cyberspace defenders, other forces conducting CO, and the intelligence community.

Tab 1 to Annex C to Concept of Operations (CONOPS) for Cyber Protection Teams (U)
Staff Element Methodology (U)

1. (U//FOUO) Staff Summary. The Staff element is the primary link between a supported commander's mission and the CPTs capabilities. Their principle focus is to understand the supported commander's mission priorities and leverage this information to guide CPT capabilities in prioritization, risk mitigation, and Protection of the supported cyberspace assets and terrain. This element establishes coordination efforts with the supported mission owner, local cyberspace defenders, supporting intelligence forces, and other Cyber Mission Forces (CMF). The Staff element is the central planning, coordination, synchronization, and execution authority for the CPT. The Staff element conducts this coordination to: 1) establish C2 and authorities; 2) effectively integrate the CPT within and through the AO; and 3) plan and execute cyberspace security and defense activities for the supported commander. The Staff element works to primarily enable two direct actions: 1) improve mission assurance for the supported commander; and 2) synchronize the execution of CPT capabilities with larger DOD CO.

2. (U) Team Leadership Positions

2.A. (U//FOUO) Team Leader. The CPT Leader has direct responsibility for the execution of the team's mission. The Team Leader is the primary advocate for the CPTs capabilities; the lead identifies requirements to improve assurance and effectiveness and educates senior leadership about the CPTs capabilities to support vital decisions for the Protection of DOD cyberspace. The Team Leader oversees mission planning and serves as the lead coordination point with the higher headquarters, the supported commander, local cyberspace defenders, adjacent units, and other DOD defensive cyberspace forces at the senior leadership level. The Team Leader establishes and oversees the integration and coordination of the CPTs capabilities with the supported commander and local cyberspace defenders. The Team Leader acts as the central voice of the team and facilitates coordination and actions with the supported commander and local cyberspace defenders.

2.B. (U//FOUO) NCOIC. The NCOIC directly supports the team's objectives and direction, as outlined by the Team Leader and overall management of team personnel. The NCOIC manages the overall health and safety of the team and its individuals. The NCOIC advises the Team Leader and Operations Officer on personnel needs and training issues, technical capability development and readiness, and supports the leadership team as required.

2.C. (U//FOUO) Operations Officer (OPSO). The OPSO is the keystone to the successful conduct of the team's mission. The OPSO works with the Team Leader, Cyberspace Operations, and Cyber Planner to support senior leadership requests for effects and properly plans tasks to support these objectives. The Team OPSO serves as the central position for coordination between all Squad Leaders to synchronize their effects in support of the team's objectives. The Team OPSO directly controls the conduct, timing, and tempo of the team's mission execution, as guided by the Team Leader's direction. The OPSO provides the critical operational link between other CPTs, other defensive cyberspace forces, and the supported commander for coordination and synchronization of operations. The Team OPSO must understand the specific capabilities of the team and how to execute these capabilities for maximum effect at the minimal acceptable cost and risk to the DOD.

2.D. (U//FOUO) Cyberspace Operations Cyber Planner (Cyberspace Operations Planner). The Cyberspace Operations Cyber Planner coordinates with senior leadership, the supported commander, and local cyberspace defenders to build a feasible, suitable, and acceptable plan of action to support the required mission objectives. The Cyberspace Operations Cyber Planner works closely with the Team Leader and OPSO to ensure the team is best prepared and aligned to meet the mission objectives and that foundational information is collected, coordinated, and approved prior to hand-off for execution. The Cyberspace Operations Cyber Planner is key to the development of the required relationships and support between the CPT, other cyberspace defense forces, and the intelligence community. The Cyberspace Operations Cyber Planner facilitates and builds the team's support to integrated operations and coordinates support from other DOD cyberspace capabilities to meet mission objectives. The planner translates objectives to team courses of action and provides options.

Tab 2 to Annex C to Concept of Operations (CONOPS) for Cyber Protection Teams (U)
Mission Protection Squad Methodology (U)

1. (U//FOUO) Squad Summary. The Mission Protection Squad's principal focus is to understand the supported commander's mission priorities and leverage this information to guide CPT capabilities in prioritization, risk mitigation and defense of the associated cyberspace assets and terrain. This squad supports the mission owner in: 1) identification of tasks and mission objectives to be supported by CPT effects; 2) identification of essential and critical C-KT; and 3) the development and execution of the mission RMP and MDP. Mission Protection capabilities work to enable two direct actions: 1) to improve embedded cyberspace defenders ability to conduct mission, cyberspace terrain, and risk analysis and employ risk mitigation effects; and 2) to direct the execution of risk mitigation efforts through the CPT in synch with the larger DOD CO.

2. (U//FOUO) Execution Stages

Stage	*Core Mission Protection Squad Actions*

Survey	• *Lead Refinement of Critical Assets / Key Terrain to Focus CPT*
	  ○ *Build Increased Understanding of Supported Mission*
	  ○ *Consolidate all Squads' Cyber Terrain Awareness Efforts*
	  ○ *Develop/Refine Awareness of Threats to Mission*
	• *Lead Development of Risk Mitigation Plan*
	  ○ *Consolidate all Squad's Recommendations Resulting from the Participative Defensive Evaluation*
	  ○ *Assess and Prioritize Risks to Supported Mission*
	  ○ *Propose COAs to Address Identified Risks*

Secure	• *Assist in Implementation of the Risk Mitigation Plan*
	• *Lead the Development of the Mission Defense Plan*
	  ○ *Consolidate Recommendations from all CPT Squads*
	  ○ *Develop COAs to Mitigate Residual Risk*

Protect	• *Coordinate CPT Activities to Sync with Supported Mission* • *Coordinate Active Risk Mitigation Efforts* • *Lead Threat Response Actions* • *Conduct Operational Reporting*
Recover	• *Lead the Development of Final Report/Lessons Learned*

Table 1. (U//FOUO) Summary of Mission Protection Squad's Actions in the Execution Phase

2.A. (U) Execution Phase: Survey

2.A.1. (U//FOUO) The Survey stage sets the commencement of efforts to identify and propose risk mitigation measures for the sustainment of a supported commander's mission by the Mission Protection Squad. During the Survey stage, the Mission Protection Squad has four key objectives: 1) mission analysis; 2) develop risk analysis data; 3) evaluate current risk mitigation measures; and 4) develop recommendations to modify or add risk mitigations.

2.A.2. (U//FOUO) The Mission Protection Squad works to refine their understanding of the supported commander's objectives, timeline, and cyberspace requirements; this is a primary and enduring task for a Mission Protection Squad throughout all phases of CPT operations. Through team leadership, the Mission Protection Squad will establish the communication and information necessary to act as the intermediary between the supported commander and the CPT to maintain operational synchronization and facilitate the development of risk mitigation measures. The Mission Protection Squad works directly with the other squads to support the analysis and sustained awareness of the dynamic cyber AO.

2.A.3. (U//FOUO) Initial evaluations by the Mission Protection Squad will consist of a comprehensive review of cyber-based risk to the supported commander's mission. The risk analysis is based on a clear understanding of the supporting cyberspace terrain. The risk analysis is evaluated by assessing: 1) mission criticality (based on phase of operation); 2) vulnerabilities within the cyber terrain or assets (C-KT and interconnected external terrain); 3) the will, intent, and capabilities of known threats; and 4) the likelihood of attack. The Mission Protection Squad refines and confirms the terrain and assets as either essential or critical to the execution of the supported commander's mission. Once the foundational cyberspace terrain is understood with supporting analysis from the other squads, the Mission Protection Squad will identify any gaps in coverage of the terrain or assets. The Mission Protection Squad works with the CTE Squad and local cyberspace defenders to identify and sustain a real-time awareness of threats to the supported commander's mission. This analysis is the core for the RMP which serves as the reference point for all future risk mitigation efforts.

2.A.4. (U//FOUO) The Mission Protection Squad will review and strengthen the local intelligence support provided to the local cyberspace defenders. Through these channels the Mission Protection Squad conducts a comprehensive risk analysis by evaluating available JIPOE and Intelligence Preparation of the Battlefield (IPB) products. Supported by the other squads, the Mission Protection Squad will work closely with the supported commander and local cyberspace defenders to evaluate and improve supporting information and intelligence requirements for the development of the RMP. In coordination with the Cyber Readiness Squad, the Mission Protection Squad identifies intelligence gaps and augments the local cyberspace defenders ability to integrate intelligence support to local cyberspace defense.

2.A.5. (U//FOUO) The Mission Protection Squad conducts a comprehensive baseline evaluation of the cyberspace terrain and processes that enable the supported commander's mission. During the participative evaluation, effects are announced and executed by the CTE Squad. While adversary effects are generated, the Mission Protection Squad works closely with the other CPT Squads to deliberately and systematically validate existing cyberspace defense capabilities. The evaluation combined with further risk analysis enables the squad to quantify the residual risk to the supported commander's mission. With the support of the other squads, the Mission Protection Squad deploys processes and capabilities to establish sustainable risk monitoring, necessary for comprehensive evaluation and required for the initiation of the Protect stage.

2.A.6. (U//FOUO) Throughout the Survey stage, the Mission Protection Squad reports their risk analyses, evaluations, and follow-on actions in a CPT standardized format. This format should be compatible so that it can be overlaid upon the foundational cyberspace terrain mapping generated by the Cyber Support Squad. The Mission Protection Squad's overlay identifies the essential and critical supporting cyberspace terrain and assets for the supported commander's mission and the conduct of a CPT Protect mission. The overlay also identifies and outlines C-KT and risk mitigation capabilities to include the effects of dynamic terrain shaping.

2.A.7. (U//FOUO) At the completion of the participative evaluation, the Mission Protection Squad documents findings and leads a collaborative effort to build the RMP. The Mission Protection Squad receives reporting from each squad in its area of specialty to identify and prioritize mission risks. It consolidates and evaluates the reports and develops a prioritized assessment of risks to the supported commander's mission. The Mission Protection Squad then leads the effort to develop risk mitigations with the other squads and the local cyberspace defenders. As the technical leaders, the Mission Protection Squad identifies the technical risk mitigation options available in the development of the RMP. When complete, the RMP is shared and coordinated with the supported commander and local cyberspace defenders to facilitate understanding and approval for the implementation of mitigations proposed in the RMP.

2.B. (U) Execution Phase: Secure

2.B.1. (U//FOUO) During the Secure stage, the Mission Protection Squad works with the Cyber Support Squad to implement security control (e.g., Safeguards/Countermeasures), or DCO-IDM methodology as identified in the RMP. The Mission Protection Squad works closely with local cyberspace defenders to deploy or adapt needed capabilities. The Mission Protection Squad leads the effort to enhance intelligence support and integration between the local cyberspace defenders and their supporting intelligence elements. While fully capable of conducting independent risk mitigations, the Mission Protection Squad is specifically focused to enable and validate the local cyberspace defenders ability to conduct and support the required adjustments.

2.B.2. (U//FOUO) Once all required risk mitigations are in place, the Mission Protection Squad works with the Cyber Readiness and CTE Squads to conduct a non-participative evaluation of the employed risk mitigations. During this process the Mission Protection Squad conducts a second round of risk analyses. These analyses support the Cyber Readiness Squad's evaluation of the local cyberspace defenders mission readiness and the CPTs ability to conduct cyberspace defense actions for the supported commander's mission. The Mission Protection Squad reevaluates and prioritizes residual risk for the supported commander's mission based on foundational efforts to build the RMP and supplemental findings.

2.B.3. (U//FOUO) The Mission Protection Squad uses the results from the non-participative evaluation along with inputs from the other squads and local cyberspace defenders to identify and seek approval for supplemental risk mitigations required. The Mission Protection Squad must be careful to limit supplemental adjustments to those that can be implemented feasibly within the time constraints and are necessary to achieve mission objectives.

2.B.4. (U//FOUO) If the team has been tasked directly, or via an on-order mission, to execute the Protect stage, then the Mission Protection Squad leads the development of the MDP in coordination with the other squads, CNDSP, and local cyberspace defenders. The MDP is generated to enable a Protect action by local cyberspace defenders and/or the CPT. Throughout its development, the MDP is coordinated with the supported commander and local cyberspace defenders. This collaboration is conducted to harness local expertise, expedite any required approvals, and ensure a viable plan is developed.

2.C. (U) Execution Phase: Protect.

2.C.1 (U//FOUO) In the Protect stage, the Mission Protection Squad sustains CPT synchronization with the supported commander's mission objectives and facilitates the flow of operational reporting.

Throughout the Protect stage, the Mission Protection Squad continues to support responsive risk assessments through enduring relationships between the other squads, local cyberspace defenders, the supported commander's mission, and supporting intelligence elements. These risk assessments guide and prioritize tactical risk mitigations to support defensive activities. The Mission Protection Squad directs tactical risk mitigation actions both in support of ongoing risk reduction and in response to threats. During the Protect stage the Mission Protection Squad leads counter-threat actions and the development of ad-hoc countermeasures.

2.D. (U) Execution Phase: Recover.

2.D.1 (U//FOUO) Upon initiation of the Recover stage, the Mission Protection Squad works closely with the Cyber Support Squad to evaluate risks and support the return of defended cyberspace terrain to a known-good state, either post-attack from cyberspace threats or for the removal of unsustainable tactical mitigation measures. The squad works to ensure that Mission Protection methodologies are successfully transferred to the local cyberspace defenders and properly integrated with the supported commander and supporting intelligence elements. To support these efforts the Mission Protection Squad identifies and shares the Mission Protection POA&M with the Cyber Readiness Squad and local cyberspace defenders. The Mission Protection Squad reviews and advises on the local cyberspace defenders ability to assume and execute Mission Protection methodologies to successfully defend a supported commander's mission. Finally, the Mission Protection Squad, under the direction of team leadership, coordinates and facilitates the collaborative effort with the other squads, to build a comprehensive final master report which includes lessons learned and a close-out of all final operational reports and, if required, intelligence fusion.

3. (U//FOUO) Mission Protection Positions. The Mission Protection Squad is comprised of the following: 1) one CD (JCT&CS, 09 October 2014 now refers to this function as Cyber Defense) Manager (Squad Leader); 2) one Systems Architect (Windows); 3) one Systems Architect (UNIX); 4) one Cyber Security Analyst/Information Security Professional; 5) one Network Infrastructure Specialist; 6) one Access Network Operator; and 7) one all source Intelligence Analyst. Detailed description of these positions/work roles can be found in Appendix 1 to Annex F of reference (d).

Tab 3 to Annex C to Concept of Operations (CONOPS) for Cyber Protection Teams (U)
Cyber Readiness Squad Methodology (U)

1. (U//FOUO) Squad Summary. The Cyber Readiness Squad evaluates and helps sustain the compliance and readiness of cyberspace capabilities in support of a specified mission. The Cyber Readiness Squad primarily enables four direct actions: 1) evaluate components of CO and defense for compliance with DOD policy and standards; 2) assess readiness and resiliency of a mission to survive and sustain capability under threat; 3) improve embedded cyberspace defenders abilities to conduct self-evaluation and enhancement; 4) support the defense of a specified mission within a defined cyberspace AO.

2. (U//FOUO) Execution Stages

Stage	*Core Cyber Readiness Squad Actions*
Survey	• *Develops Initial MOEs/MOPs for Assessments* • *Conduct Compliance Analysis* • *Coordinate/Conduct Participative Readiness Evaluation* ○ *Assess Existing Defenses and Defender's Ability to Operate in a Contested Environment* • *Provide Recommendations to Risk Mitigation Plan*

Secure	• *Assist in Implementation of Risk Mitigation Plan*
	• *Coordinate/Conduct Non-Participative Readiness Evaluation*
	  ○ *Evaluate Deployed Risk Mitigations*
	  ○ *Evaluate Local cyberspace defenders, and CPT if Planned to Conduct a Protect mission, Ability to Operate in a Contested Environment*
	• *Provide Readiness Recommendations to Mission Defense Plan*

Protect	• *Conduct Ongoing Monitoring/Evaluation of Baseline Compliance* • *Assist in Conduct of Ongoing Risk Mitigation Efforts* • *Assist in Implementing Technical Threat Response Actions*
Recover	• *Provide Recommendations to Improve Local cyberspace defenders Self-Assessment Capabilities* • *Consolidate/Manage Plans of Action and Milestones (POA&M)* • *Provide Readiness Recommendations for Inclusion in Final Report*

Table 1. (U//FOUO) Summary of Cyber Readiness Squad's Actions in the Execution Phase

2.A. (U) Execution Phase: Survey

2.A.1. (U//FOUO) During the Survey stage, the Cyber Readiness Squad evaluates three major areas: 1) baseline compliance of the supporting cyberspace terrain, 2) the effectiveness of deployed risk mitigation measures; and 3) the ability for local cyberspace defenders to apply risk mitigation methods.

2.A.2. (U//FOUO) Early in the Survey stage, the Cyber Readiness Squad will work directly with the Mission Protection Squad to understand the supported commander's mission and develop an understanding of the

supporting cyberspace terrain through the Cyber Support Squad. The Cyber Readiness Squad will work directly with Mission Protection and Cyber Support Squads to scope and sustain awareness of the dynamic AO. As the lead auditing capability of the CPT, the Cyber Readiness Squad develops the initial measures of effectiveness (MOE) and measures of performance (MOP) for the conduct of their assessments and, if required, assists the other squads in developing measures to support their actions.

2.A.3. (U//FOUO) The Cyber Readiness Squad will conduct a comprehensive baseline evaluation of the cyberspace terrain and processes to validate the local cyberspace defenders compliance with the current published system technical implementation and vulnerability mitigation guidance. The Cyber Readiness Squad also works with the local cyberspace defenders to employ processes and capabilities to establish sustainable compliance monitoring, necessary for comprehensive evaluations and required for the conduct of the Protect stage. The Cyber Readiness Squad evaluates the ability for local cyberspace defenders to perform compliance practices. This evaluation serves as a reference point for supplemental training requirements and additional readiness evaluations to ensure local cyberspace defenders can sustain compliance practices or identify gaps requiring additional support. Baseline compliance evaluations ensure employed risk mitigation measures meet minimum DOD and organizational policies. Compliance evaluations highlight where gaps exist in risk mitigation and the conduct of routine cyberspace security practices. The Cyber Readiness Squad also incorporates findings of operational practices for cyberspace assets from thee Cyber Support Squad to evaluate with compliance evaluations and serve as a reference point for readiness evaluations in the Secure stage. The Cyber Readiness Squad submits reporting from this evaluation and following actions in a CPT standardized format. This format should allow the squad's findings to easily be overlaid with the cyberspace terrain mapping.

2.A.4. (U//FOUO) The second evaluation by the Cyber Readiness Squad is the deliberate assessment of technical and procedural risk mitigation measures currently deployed; this evaluation should be coordinated with the CTE Squad to directly illuminate mitigation shortfalls. To complete an evaluation of deployed risk mitigation measures, the Cyber Readiness Squad must develop measures for the risks to the supported commander's mission. This assessment also evaluates the ability of local cyberspace defenders to request, integrate, and utilize intelligence from supporting intelligence elements (e.g., J2, G2 shop). This evaluation serves as a baseline for the readiness evaluation in the Secure stage.

2.A.5. (U//FOUO) At the completion of the compliance and current risk mitigation evaluations, the Cyber Readiness Squad documents findings and supports the collaborative effort to build an RMP for the supported commander's mission as led by the Mission Protection Squad. The Cyber Readiness Squad actively supports risk mitigation development for the defense of a supported commander's mission. While primarily focused on how to audit and measure effects in cyberspace, the Cyber Readiness Squad directly supports the technical development of risk mitigation options.

2.B. (U) Execution Phase: Secure

2.B.1. (U//FOUO) At the start of the Secure stage, the Cyber Readiness Squad supports the CPT and local cyberspace defenders to implement technical and procedural risk mitigation measures from within the RMP as guided by the Mission Protection Squad and implemented by the Cyber Support Squad. The Cyber Readiness Squad provides technical support, to include supplemental tactical coding in the field, as needed to implement risk mitigation effects. The Cyber Readiness Squad's actions during the Secure stage accentuates that all CPT members are foremost active cyberspace defenders, not purely assessment capabilities.

2.B.2. (U//FOUO) During the Secure stage the Cyber Readiness Squad also prepares to and conducts the formal evaluation of the readiness of defensive CO, conducted by local cyberspace defenders and, if required, the CPT, to Protect a supported commander's mission within cyberspace. This evaluation is directly supported through non-participative threat replication by the CTE squad. The Cyber Readiness Squad works collaboratively with the CTE squad to determine appropriate evaluation methodologies for CTE actions and to identify measurement opportunities for CTE effects and cyberspace defense action response to those effects. In addition, the Cyber Readiness Squad coordinates with Mission Protection Squad to evaluate and address residual risk issues as a result of Cyber Readiness evaluation.

2.B.3. (U//FOUO) The Cyber Readiness Squad is a crucial element to providing team leadership and the Mission Protection Squad with the mission's readiness posture and identification of any capability or performance gaps. The Cyber Readiness Squad provides recommendations to support the Mission Protection Squad's final risk evaluations and mitigation adjustments. The Cyber Readiness Squad works closely with the other squads to develop the MDP led by the Mission Protection Squad.

2.C. (U) Execution Phase: Protect.

2.C.1. (U//FOUO) In the Protect stage, the Cyber Readiness Squad takes an active role in the continued monitoring and reporting of mission-supporting cyberspace terrain compliance with policies and the MDP. The Cyber Readiness Squad conducts tactical, on-demand technical support to adapt or restore cyberspace terrain or supplemental mitigation measures led by the Mission Protection Squad. During the Protect stage the Cyber Readiness Squad actively works to support counter threat actions for the defended cyberspace terrain. In addition, the Cyber Readiness Squad supports active operational reporting and intelligence support needs for the CPT.

2.D. (U) Execution Phase: Recover.

2.D.1. (U//FOUO) The Cyber Readiness Squad is the CPT lead for the collection, coordination, and validation of the POA&M. The Cyber Readiness Squad establishes appropriate measures for the completion of milestones to meet the planned objectives. During the Recover stage, the Cyber Readiness Squad removes or transfers, as appropriate, Cyber Readiness capabilities to local cyberspace defenders. In planning for POA&Ms, the Cyber Readiness Squad develops periodic self-evaluation milestones or, if required, external evaluations support milestones to validate the local cyberspace defenders ability to sustain the advanced cyberspace defense actions necessary for the supported commander's mission. The Cyber Readiness Squad will work with the other CPT Squads to provide a final review to ensure intelligence support and integration is implemented by and sustainable for local cyberspace defenders. The CPTs intent is to ensure that the local cyberspace defenders have the ability to successfully defend the supported commander's mission; this objective is guided by the actions of the Cyber Readiness Squad to project an actionable path for local cyberspace defenders once the CPT redeploys. Finally, the Cyber Readiness Squad works collaboratively with the other CPT Squads as led by the Mission Protection Squad to build a comprehensive final report.

3. (U//FOUO) Cyber Readiness Positions. The Cyber Readiness Squad is comprised of the following: 1) one CD (JCT&CS, 09 October 2014 now refers to this function as Cyber Defense) Manager (Squad Leader); 2) one Systems Architect (Windows); 3) one Systems Architect (UNIX); 4) one Cyber Security Analyst/Information Security Professional; 5) one Network Infrastructure Specialist; 6) one Access Network Operator; and 7) one all source Intelligence Analyst. Detailed description of these positions/work roles can be found in Appendix 1 to Annex F of reference (d).

Tab 4 to Annex C to Concept of Operations (CONOPS) for Cyber Protection Teams (U)
Cyber Support Squad Methodology (U)

1. (U//FOUO) Squad Summary. The Cyber Support Squad provides procedural and technical support to embedded cyberspace operators and defenders to enhance the cyberspace security posture for a specified mission and directly enables the effects of the CPT. The Cyber Support Squad primarily enables two direct actions: 1) to identify and correct deficiencies in defensive operations, policies, and procedures to implement an improved and self-sustaining security posture; and 2) to provide training and CO support to sustain a specified mission within a defined cyberspace AO.

2. (U//FOUO) Execution Stages

Stage	*Core Cyber Support Squad Actions*
Survey	• *Develops Initial MOEs/MOPs for Assessments* • *Conduct Compliance Analysis* • *Coordinate/Conduct Participative Readiness Evaluation* ○ *Assess Existing Defenses and Defender's Ability to Operate in a Contested Environment* • *Provide Recommendations to Risk Mitigation Plan*

Secure	• *Assist in Implementation of Risk Mitigation Plan*
	• *Coordinate/Conduct Non-Participative Readiness Evaluation*
	  ○ *Evaluate Deployed Risk Mitigations*
	  ○ *Evaluate Local cyberspace defenders, and CPT if Planned to Conduct a Protect mission, Ability to Operate in a Contested Environment*
	• *Provide Readiness Recommendations to Mission Defense Plan*

Protect	• *Conduct Ongoing Monitoring/Evaluation of Baseline Compliance* • *Assist in Conduct of Ongoing Risk Mitigation Efforts* • *Assist in Implementing Technical Threat Response Actions*
Recover	• *Provide Recommendations to Improve Local cyberspace defenders Self-Assessment Capabilities* • *Consolidate/Manage Plans of Action and Milestones (POA&M)* • *Provide Readiness Recommendations for Inclusion in Final Report*

Table 1. (U//FOUO) Summary of Cyber Support Squad's Actions in the Execution Phase

2.A. (U) Execution Phase: Survey

2.A.1. (U//FOUO) The Cyber Support Squad has three main objectives in the Survey stage: 1) to conduct the foundational cyberspace terrain mapping; 2) to evaluate the configuration and maintenance of cyberspace assets; and 3) to identify and plan for supplemental training of local cyberspace defenders. During the Survey stage, the Cyber Support Squad works to build direct and close operational relationships with local cyberspace defenders.

2.A.2. (U//FOUO) The Cyber Support Squad executes the base mapping of the supporting cyberspace

terrain in the AO, a foundational role of the CPT mission. Cyberspace terrain mapping is initially agnostic of role and purpose of assets to a supported commander's mission; it is the closest cyberspace analogy to a terrain map in the physical domain. As the lead network engineers and cyberspace cartographers of a CPT, the Cyber Support Squad builds a standardized cyberspace terrain map upon which data gathered by the other squads is overlaid. Mapping is provided for both physical and logical perspectives. Through the conduct of the Survey stage the Cyber Support Squad works closely with the Mission Protection Squad to understand the cyberspace needs of the supported commander's mission. Over time, the squads' overlays to the foundational map will highlight the cyberspace terrain and assets that directly enable the supported commander's mission. The Cyber Support Squad works with all squads to build an understanding of the cyberspace AO, enabling the ability to conduct synchronized actions within it.

2.A.3. (U//FOUO) During the Survey stage, the Cyber Support Squad evaluates cyberspace assets from a DODIN operations or engineering perspective. This evaluation is focused on the operational configuration and performance of cyberspace assets. The Cyber Support Squad directly evaluates assets under stress from CTE effects during the participative risk mitigation evaluation effort. From this evaluation the Cyber Support Squad builds recommendations to mitigate operational impact from degradation or loss of cyberspace terrain, the assets that generate it, or the assets that provide other mission supporting capabilities or effects. During the Survey stage, the Cyber Support Squad actively plans risk mitigation measures that allow for the rapid adaptation and transformation of cyberspace to enable the conduct of a supported commander's mission and, if required, directly hinder or halt advanced cyberspace threats.

2.A.4. (U//FOUO) As the lead CPT trainers, the Cyber Support Squad evaluates the training needs of the local cyberspace defenders and is supported by the observations and needs expressed by the other CPT Squads. From these evaluations, the Cyber Support Squad develops a training plan to address skill gaps identified from the Survey stage and requirements that result from risk mitigation actions to be executed in the Secure stage. The training plan could consist of immediate or onsite training as well as formal training to occur at a later date.

2.A.5. (U//FOUO) Concurrent to the evaluation of training needs is the evaluation of necessary actions to improve the supported commander's mission and the local cyberspace defenders ability to integrate and operationalize intelligence support. The Cyber Support Squad assesses findings from the Cyber Readiness Squad's evaluation and prepares options to enhance support or address shortfalls in intelligence integration.

2.A.6. (U//FOUO) At the completion of terrain mapping, the terrain and asset evaluations, and identification of training needs, the Cyber Support Squad documents findings and supports the collaborative effort to build an RMP for the supported commander's mission as led by the Mission Protection Squad. The Cyber Support Squad directly supports the technical development of risk mitigation options and prepares to implement risk mitigation measures called for in the RMP.

2.B. (U) Execution Phase: Secure

2.B.1. (U//FOUO) During the Secure stage, the Cyber Support Squad leads all efforts to implement technical capabilities to support risk mitigations and conduct required training of personnel as identified in the RMP. The Cyber Support Squad works closely with local cyberspace defenders to deploy or adapt needed capabilities. While capable of conducting independent risk mitigation efforts, the Cyber Support Squad provides the focused insight necessary to enable and validate the local cyberspace defenders

ability to conduct and support the required adjustments. The Cyber Support Squad provides all supplemental training during the Secure stage prior to conducting the non-participative and final evaluations of the adjusted risk mitigation measures.

2.B.2. (U//FOUO) During this final evaluation of deployed risk mitigations, the Cyber Support Squad conducts a final evaluation of the operational readiness and resiliency of the supported cyberspace terrain and assets, and those charged to operate and defend it. The Cyber Support Squad identifies and provides final adjustments to risk mitigations and training to required personnel to support the readiness of the supported commander's mission. The Cyber Support Squad works closely with the other squads to develop the MDP led by Mission Protection.

2.C. (U) Execution Phase: Protect.

2.C.1. (U//FOUO) In the Protect stage, the Cyber Support Squad is the lead for implementing ad-hoc countermeasure deployments and the sustainment and adaptation of cyberspace terrain. The Cyber Support Squad has an active role in the continued operational monitoring and support to the mission assets generating foundational cyberspace terrain and effects and for compliance with the MDP. The Cyber Support Squad conducts tactical on-demand technical support to adapt or restore cyberspace terrain or supplemental mitigation measures in concert with the other CPT Squads and the local cyberspace defenders. During the Protect stage, the Cyber Support Squad actively works to support counter threat actions for the defended cyberspace terrain. In addition, the Cyber Support Squad contributes to operational reporting and intelligence needs for the CPT.

2.D. (U) Execution Phase: Recover.

2.D.1. (U//FOUO) The Cyber Support Squad is the CPT lead to re-baseline, restore, and coordinate activities to return defended cyberspace terrain to a known-good state, either post attack from cyberspace threats or for the removal of unsustainable tactical mitigation measures. Working closely with local cyberspace defenders, the Cyber Support Squad builds or transfers, as appropriate, CPT capabilities to local cyberspace defenders. In concert with these efforts, the Cyber Support Squad will work with the other squads to provide a final review to ensure intelligence support and integration are implemented by and sustainable for local cyberspace defenders. To support these efforts, the Cyber Support Squad identifies and shares Cyber Support POA&M with the Cyber Readiness Squad. The Cyber Support Squad reviews and advises on local cyberspace defenders ability to assume and execute the Cyber Support Squad methodologies to successfully defend a supported commander's mission. Finally, the Cyber Support Squad works with the other squads, as led by the Mission Protection Squad, to build a comprehensive final master report and close out all operational reporting and, if required, intelligence fusion.

3. (U//FOUO) Cyber Support Positions. The Cyber Support Squad is comprised of the following: 1) one CD (JCT&CS, 09 October 2014 now refers to this function as Cyber Defense) Manager (Squad Leader); 2) one Systems Architect (Windows); 3) one Systems Architect (UNIX); 4) one Cyber Security Analyst/Information Security Professional; 5) one Network Infrastructure Specialist; 6) one Access Network Operator; and 7) one all source Intelligence Analyst. Detailed description of these positions/work roles can be found in Appendix 1 to Annex F of reference (d).

Tab 5 to Annex C to Concept of Operations (CONOPS) for Cyber Protection Teams (U)
Discover and Counter-Infiltration (DCI) Squad Methodology (U)

1. (U//FOUO) Squad Summary. The DCI Squad detects, illuminates, and, as authorized, responds directly to threats to a mission owner's C-KT and critical assets. The squad is configured to detect, discover, and characterize advanced adversary tradecraft within friendly networks that evade routine security measures. The DCI Squad primarily enables two direct actions: 1) improve existing local cyberspace defenders ability to conduct DCI effects; and 2) apply advanced DCI effects.

2. (U//FOUO) Execution Stages

Stage	*Core DCI Squad Actions*
Survey	• *Develops Initial MOEs/MOPs for Assessments* • *Conduct Compliance Analysis* • *Coordinate/Conduct Participative Readiness Evaluation* ○ *Assess Existing Defenses and Defender's Ability to Operate in a Contested Environment* • *Provide Recommendations to Risk Mitigation Plan*

Secure	• *Assist in Implementation of Risk Mitigation Plan*
	• *Coordinate/Conduct Non-Participative Readiness Evaluation*
	  ○ *Evaluate Deployed Risk Mitigations*
	  ○ *Evaluate Local cyberspace defenders, and CPT if Planned to Conduct a Protect mission, Ability to Operate in a Contested Environment*
	• *Provide Readiness Recommendations to Mission Defense Plan*

Protect	• *Conduct Ongoing Monitoring/Evaluation of Baseline Compliance* • *Assist in Conduct of Ongoing Risk Mitigation Efforts* • *Assist in Implementing Technical Threat Response Actions*
Recover	• *Provide Recommendations to Improve Local cyberspace defenders Self-Assessment Capabilities* • *Consolidate/Manage Plans of Action and Milestones (POA&M)* • *Provide Readiness Recommendations for Inclusion in Final Report*

Table 1. (//FOUO) Summary of DCI Squad's Actions in the Execution Phase

2.A. . (U//FOUO) Execution Phase: Survey

2.A.1. (U//FOUO) The DCI Squad has two main objectives in the Survey stage: 1) to identify and clear the area of active threats; and 2) to evaluate currently deployed capabilities and processes to illuminate threats.

2.A.2. (U//FOUO) The DCI Squad seeks to scope and initiate a rapid patrol of supporting cyberspace terrain based on direct dialogue with the Mission Protection and Cyber Support Squads. The Cyber Support Squad provides generic insight to the cyberspace terrain of the AO and Mission Protection provides the understanding of the supported commander's mission to allow for initial correlation and

analysis of their activities. A key action enabling DCI detection capabilities is the coordinated development of a baseline to enable change detection. The DCI Squad uses this baseline and learned information to develop their overlay to the foundational terrain developed by the Cyber Support Squad.

2.A.3. (U//FOUO) The DCI Squad has the responsibility to identify preexisting threats in the cyberspace terrain. The DCI Squad maintains an active role in finding threats throughout all phases to enable safe conduct of the supported commander's mission. Upon detection of a threat, the DCI Squad works with the Mission Protection Squad and local cyberspace defenders to properly address the threat. The DCI Squad works closely with the local cyberspace defenders to clear threats in the cyberspace terrain.

2.A.4. (U//FOUO) The formal evaluation, performed by the DCI Squad, is separated into three main areas: 1) the evaluation of current defenses; 2) planning for threat detection enhancements within the supporting terrain; and 3) intelligence support to enable DCI effects. During the CPTs evaluation of current risk mitigations the DCI squad reviews and assesses the capabilities and processes used by local cyberspace defenders to illuminate threats to the supported commander's mission. The DCI Squad acts as the lead for detecting the participative effects generated by the CTE squad and evaluating local cyberspace defenders needs to support DCI effects. The squad also identifies and evaluates terrain for use to enable DCI effects and supports the Mission Protection Squad's evaluation of mission risk. This evaluation guides the development and deployment of DCI capabilities, either by the local cyberspace defenders or the CPT. Finally, the DCI Squad evaluates supporting intelligence available to support DCI operations and develops recommendations to address gaps.

2.A.5. (U//FOUO) At the completion of the compliance and current risk mitigation evaluations the DCI Squad documents findings and supports the collaborative effort to build a RMP for the supported commander's mission as led by the Mission Protection Squad. While primarily focused on hunting for threats in cyberspace, the DCI Squad also directly supports the technical development of risk mitigation options.

2.B. (U) Execution Phase: Secure

2.B.1. (U//FOUO) Within the Secure stage, the DCI Squad works with the Cyber Support Squad and local cyberspace defenders to deploy DCI capabilities as identified in the RMP. The DCI Squad builds a cohesive DCI process, creating and enabling necessary linkages between local cyberspace defenders, the larger DOD CO, and the CPT for the synchronization of cyber effects. Concurrently, the DCI Squad actively builds intelligence integration for the conduct of DCI operations.

2.B.2. (U//FOUO) During this final evaluation of deployed risk mitigations, the DCI Squad conducts a final evaluation of the local cyberspace defenders detection capabilities executed by the local cyberspace defenders and/or the DCI Squad, to execute a Protect action. The DCI squad identifies and provides final adjustments to risk mitigations and training to required personnel to support the DCI operations of the supported commander's mission. The DCI Squad works closely with the other squads to develop the MDP led by the Mission Protection Squad.

2.C. (U) Execution Phase: Protect.

2.C.1. (U//FOUO) The DCI Squad actively hunts for threats to a supported commander's mission during the Protect stage. DCI receives direct guidance on mission objectives from the Mission Protection Squad and threat guidance from the CTE Squad. During the Protect stage, the DCI Squad works closely with the Mission Protection Squad and CPT leadership to communicate and synchronize with external cyberspace

defense capabilities at the operational and strategic levels to enable combined arms effects appropriate to sustaining operational security.

2.D. (U) Execution Phase: Recover.

2.D.1. **(U//FOUO)** Upon initiation of the Recover stage the DCI Squad works with the Cyber Support Squad to enable the return of cyberspace terrain to a known-good state, either post attack from cyberspace threats or for the removal of unsustainable tactical mitigation measures. The squad works to transfer DCI capabilities, as appropriate, to local cyberspace defenders for a supported commander's mission and ensures that methodologies are successfully transferred to the local cyberspace defenders and properly integrated with the supported commander and supporting intelligence elements. To support these efforts the DCI Squad identifies and shares the DCI Squad POA&M with the Cyber Readiness Squad and local cyberspace defenders. The DCI Squad reviews and advises on local cyberspace defenders ability assume and execute DCI methodologies to successfully defend a supported commander's mission. Finally, the DCI Squad supports the Mission Protection Squad to build a comprehensive final master report and close out all operational reports and, if required, intelligence fusion.

3. (U//FOUO) DCI Positions. The DCI Squad is comprised of the following: 1) one CD (JCT&CS, 09 October 2014 now refers to this function as Cyber Defense) Manager (Squad Leader); 2) one Systems Architect (Windows); 3) one Systems Architect (UNIX); 4) two Interactive Operators (ION); 5) one Network Infrastructure Specialist; and 6) one all source Intelligence Analyst. Detailed description of these positions/work roles can be found in Appendix 1 to Annex F of reference (d).

Tab 6 to Annex C to Concept of Operations (CONOPS) for Cyber Protection Teams (U)
Cyber Threat Emulation (CTE) Squad Methodology (U)

1. (U//FOUO) Squad Summary. The CTE Squad generates the effects necessary to evaluate a mission's cyberspace security posture with a focus on non-permissive network access through the realistic replication of representative threats to the mission owner's C-KT and critical assets. The CTE Squad primarily enables three direct actions: 1) the education and improvement of local cyberspace defenders' understanding of cyber threat tactics, techniques, and procedures (TTP); 2) replication of representative threats to support risk mitigation efforts; and 3) the provision of advice on the conduct of cyber defense from a "red cell" perspective.

2. (U//FOUO) Execution Stages

Stage	*Core CTE Squad Actions*
Survey	• *Develops Initial MOEs/MOPs for Assessments* • *Conduct Compliance Analysis* • *Coordinate/Conduct Participative Readiness Evaluation* ○ *Assess Existing Defenses and Defender's Ability to Operate in a Contested Environment* • *Provide Recommendations to Risk Mitigation Plan*

Secure	• *Assist in Implementation of Risk Mitigation Plan*
	• *Coordinate/Conduct Non-Participative Readiness Evaluation*
	  ○ *Evaluate Deployed Risk Mitigations*
	  ○ *Evaluate Local cyberspace defenders, and CPT if Planned to Conduct a Protect mission, Ability to Operate in a Contested Environment*
	• *Provide Readiness Recommendations to Mission Defense Plan*

Protect	• *Conduct Ongoing Monitoring/Evaluation of Baseline Compliance* • *Assist in Conduct of Ongoing Risk Mitigation Efforts* • *Assist in Implementing Technical Threat Response Actions*
Recover	• *Provide Recommendations to Improve Local cyberspace defenders Self-Assessment Capabilities* • *Consolidate/Manage Plans of Action and Milestones (POA&M)* • *Provide Readiness Recommendations for Inclusion in Final Report*

Table 1. (U//FOUO) Summary of CTE Squad's Actions in the Execution Phase

2.A. . (U//FOUO) Execution Phase: Survey

2.A.1. (U//FOUO) The CTE Squad has two main objectives in the Survey stage: 1) to understand the threats levied against the supported commander's mission; and 2) to replicate those threats for cooperative analysis of currently deployed risk mitigations.

2.A.2. (U//FOUO) At the start of the Survey stage the CTE Squad coordinates with the Mission Protection Squad to gain an understanding of the supported commander's mission and objectives. The

CTE squad maintains awareness of adversary threats as a part of their routine operations. This awareness is focused and refined through the mission planning phase and further developed during deployment. Working with the intelligence elements supporting the local cyberspace defenders, the supported commander's assets and utilizing threat information developed from other DOD CPT operations, the CTE Squad builds understanding of the threats to guide DCI operations through fusion of relevant intelligence and operational information; otherwise referred to as data and information across Red, Gray and Blue space within the cyberspace domain. This action serves as the foundation to the CTE Squad's enduring role to maintain awareness of the threat and the ability to guide risk mitigation efforts against them. The CTE Squad also provides threat information for the development of the Mission Protection Squad's risk analysis processes initiated in the Survey stage and carried throughout the CPT mission.

2.A.3. (U//FOUO) A core objective of the Survey stage is the evaluation of currently deployed risk mitigations which are enabled through the CTE Squad's effects. The CTE Squad works closely with the Mission Protection Squad to identify C-KT and replicate threats to contest it. The CTE Squad coordinates primarily with the Mission Protection Squad for specific targeting of cyberspace terrain to support mission objectives. The CPT, the supported commander's assets, and local cyberspace defenders all provide input to the perceived and reported threats to shape the threats replicated by the CTE squad. This effort is a critical enabler for the rest of the CPT to conduct and develop meaningful risk analysis for the supported commander's mission and prioritize risk mitigation efforts.

2.A.4. (U//FOUO) Once the desired threat replication is understood and built, the CTE Squad executes those effects in a specific, controlled, and expected manner. This approach enables both a learning opportunity and an assessment measure. The CTE Squad utilizes replicated threat capabilities as developed and shared through all CPT CTE Squads or dynamically develops capabilities to support evaluation objectives. During the Survey stage, the CTE Squad coordinates with the other squads, primarily directed by the Cyber Readiness and Mission Protection Squads, for the execution of replicated threat in a participative method, evaluating the risk mitigation capabilities and processes for each threat action.

2.A.5. (U//FOUO) During the Survey stage, the CTE Squad may be requested to conduct Disrupt, Degrade, Deny, Destroy or Manipulate effects. Prior to these effects being conducted, the squad coordinates with local cyberspace defenders and the Mission Protection Squad, supplemented by the other squads, to minimize collateral risk and validate authorities and approvals for the effects.

2.A.6. (U//FOUO) At the completion of the compliance and current risk mitigation evaluations the CTE Squad documents findings and supports the collaborative effort to build an RMP for the supported commander's mission as led by the Mission Protection Squad. The CTE Squad actively supports risk mitigation development for the defense of a supported commander's mission as well as replicating threat and sustaining threat awareness.

2.B. (U) Execution Phase: Secure

2.B.1. (U//FOUO) In the Secure stage, the CTE Squad becomes more dynamic and adversarial. The CTE Squad builds and executes a non-participative replication of threats to the supported commander's mission. Working only with the Cyber Readiness Squad, the CTE Squad generates appropriate replicated threats as seen in the Survey stage with the addition of dynamic or modified replicated threats to stress the risk mitigation capabilities and processes implemented under the RMP.

2.B.2. (U//FOUO) At the conclusion of the non-participative evaluation, the CTE Squad works with the other squads and local cyberspace defenders to evaluate risk mitigations and assists with identifying and providing both final adjustments to risk mitigations and training to required personnel. To conclude the Secure stage, the CTE Squad reviews effects and findings and works closely with the other squads to develop the MDP led by the Mission Protection Squad.

2.C. (U) Execution Phase: Protect

2.C.1. (U//FOUO) The Protect stage is a transition point for the CTE Squad, moving from active threat replication to active threat tracking. The CTE Squad supports the DCI and Mission Protection Squad, to plan for, anticipate, and proactively counter threat actions. During the Protect stage the CTE Squad continues to ingest DOD and local operational and intelligence reporting to sustain awareness of threats to the supported commander's mission. The CTE Squad also conducts one of the most essential aspects of CPT operations - the insight and provision of feedback to CPT risk mitigation efforts specific to threat. The CTE Squad guides defenders to anticipate and counter threats to the supported commander's mission objectives.

2.C.2. (U//FOUO) The CTE Squad also supports reporting of operationally relevant data and internal fusion analysis of that data with regard to threats to the supported commander's mission. The squad reviews the needs and observations of the CPT in a Protect action in order to provide reporting supportive of larger DOD intelligence reporting and production efforts. While the CTE Squad remains sharply focused on building its understanding of threats to the supported commander's mission, it ties threat information to vulnerabilities in the systems and pushes this information to the local cyberspace defenders, other CPTs, and the larger DOD cyberspace community.

2.C.3. (U//FOUO) In addition, the CTE Squad supports counter threat actions and the development of ad-hoc countermeasures as needed.

2.D. (U) Execution Phase: Recover.

2.D.1. (U//FOUO) Upon initiation of the Recover stage the CTE Squad works to support the return of defended cyberspace terrain to a known-good state, either post attack from cyberspace threats or for the removal of unsustainable tactical mitigation measures. The squad transfers CTE capabilities, as appropriate, to local cyberspace defenders for a supported commander's mission and ensures methodologies are successfully transferred to the local cyberspace defenders and properly integrated with the supported commander and supporting intelligence elements. To support these efforts, the CTE Squad identifies and shares CTE Squad POA&M with the Cyber Readiness Squad. The CTE Squad reviews and advises on local cyberspace defenders ability to assume and execute approved and appropriate CTE methodologies to successfully defend a supported commander's mission. Finally, the CTE Squad supports the collaborative effort with the other CPT Squads, as led by the Mission Protection Squad, to build a comprehensive final master report and close out all final operational and, if required, intelligence fusion.

3. (U//FOUO) CTE Positions. The CTE Squad is comprised of the following: 1) one CD (JCT&CS, 09 October 2014 now refers to this function as Cyber Defense) Manager (Squad Leader); 2) one Systems Architect (Windows); 3) one Systems Architect (UNIX); 4) one ION (Systems Testing and Evaluation); 5) one ION (Exploitation Analyst); 6) one Network Infrastructure Specialist; and 7) one all source Intelligence Analyst. Detailed description of these positions/work roles can be found in Appendix 1 to Annex F of reference (d).

Annex R to Concept of Operations (CONOPS) for Cyber Protection Teams (U) Reports (U)

(U//FOUO) To be published following further analysis of real-world operations.