JFHQ-C Certification

Framework to Operationalize the JFHQ

(b)(3) 10 U.S.C. § 130b

The overall classification of this briefing is: ~~TOP SECRET// REL TO USA, FVEY~~

Agenda

- Section 1
  - Problem Statement
  - Purpose, Method, Endstate
  - Certification Criteria
- Section 2
  - JFHQ-C Mission Essential Task (MET) List
  - JFHQ-C METs and Mission Critical Functions (MCF)
- Section 3
  - USCYBERCOM Processes
- Section 4
  - Integrated MET, MCF, and USCYBERCOM processes
- Way Ahead

Section 1:
Problem Statement
Purpose, Method, Endstate
Certification Criteria

Problem Statement

- Conduct distributed, full spectrum cyberspace operations (CO) across 4x JFHQ-C that are responsive to planning and execution demands of the Combatant Command's while providing the overwatch and visibility needed for USCYBERCOM.

Purpose, Method, Endstate

- Purpose: To establish JFHQ-C criteria for initial and full operating capability (IOC/FOC).
- Method: This brief aligns JFHQ-C mission essential tasks (METs) and mission critical functions (MCF) with USCYBERCOM processes currently used to conduct full-spectrum cyberspace operations (CO). It integrates tactical actions contained in SOPs and daily battle rhythm into the JFHQ-C METs and MCFs. This integration forms the basis to conduct individual training to reach IOC. Collectively, the JFHQ-C and its sub-elements demonstrate proficiency in these processes as part of Tier I/II exercises to achieve FOC.
- Endstate: A METL-driven training program to baseline the individual and collective JFHQ-C readiness assessment criteria necessary to conduct full-spectrum, distributed CO.

Certification Criteria

- Certification occurs in two parts, individual and collective.
- Individual certification occurs upon mastery of individual training standards as defined by the Commander, JFHQ-C.
- Collective certification occurs upon successful participation by the JFHQ-C and its sub-elements in at least two major exercises. USCYBERCOM evaluates the JFHQ-C and its sub-elements.

  "For the purpose of certification, subordinate commands and USCYBERCOM Directorates may nominate their participation in any of the Command's required exercises. This exercise nomination must take place prior to the exercise and have a fully supported assessment plan, both during and after the exercise event. The exercise must clearly demonstrate the subordinate command and directorate abilities to perform assigned JMETs. Additionally, analysis of Learning Management System entries will be used to determine training readiness of individuals assigned to the directorate. At least two major exercises (Tier I or II) must be used to determine certification."

  (Joint Cyberspace Training and Certification Standards (JCT&CS) v1.2)

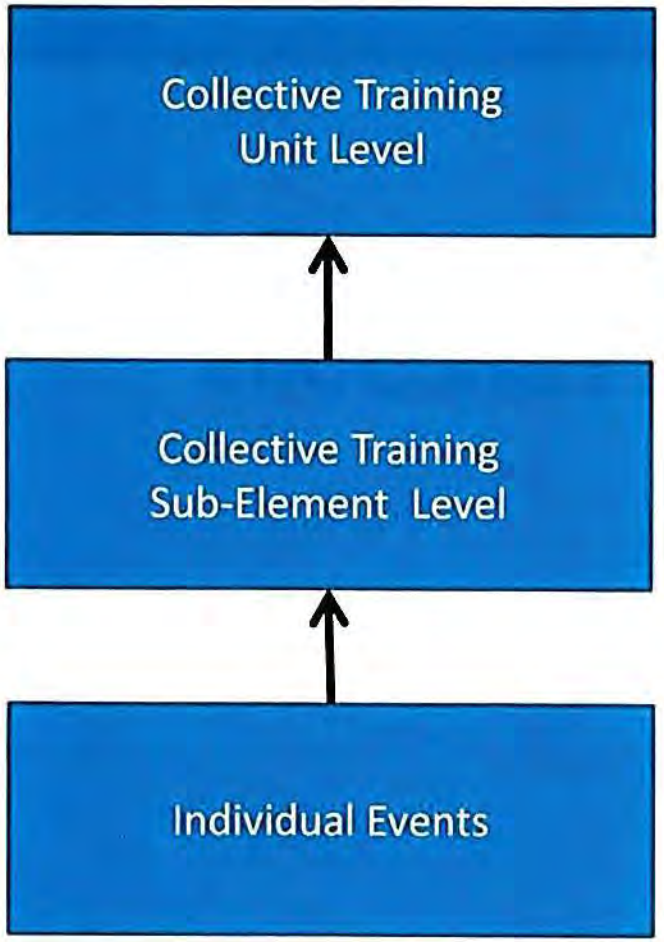
JFHQ-C IOC Criteria

	Administrative Criteria	Develops	Approves
1.	Mission, Tasks, Functions approved	USCC	USCC
2.	JFHQ-C CONOPs approved	SCC	USCC
2.1	Organization Design approved	SCC	USCC
3.	JFHQ-C METL approved	SCC	SCC
4.	Joint Staff C2 EXORD signed	USCC	USCC
5.	Key subject elements of MOA/ISSA are established with applicable Service Cyber Components, Services and NSA (MOA/ISSA not necessarily finalized).	SCC	SCC, CSS, Services and USCC
5.1	Team work-space allocation plan in place for IOC force	SCC	USCC
5.2	Operational process and relationship with NSA at Cryptologic Centers codified.	SCC	SCC and CSS
5.3	Logistics and Support processes and relationships with NSA, Services and Services Cyber Components are codified.	SCC	SCC, CSS, Services and USCC

JFHQ-C IOC Criteria

6.	JFHQ-C possesses manning and capability for C2 of attached forces	SCC	USCC
7.	Individual Job Qualification Requirements are Developed	USCC?SCC	USCC/SCC
8.	Individuals are trained in accordance with their JQR	SCC	SCC
9.	A functional Watch Element* (e.g. JOC) capable of supporting full spectrum cyber operations is in place	SCC	USCC
10.	A functional 24/7 IROC** capable of supporting full spectrum cyber operations is in place	SCC	USCC
11.	A functional intelligence oversight program is established incorporating JFHQ-C as required	SCC	USCC
12.	Continuity of Operations (COOP) Procedures established	SCC	SCC
13.	USCC and SCC J39 operational procedures integrated and codified	SCC	USCC
14.	Reporting procedures, to include operational and administrative missions	SCC	SCC

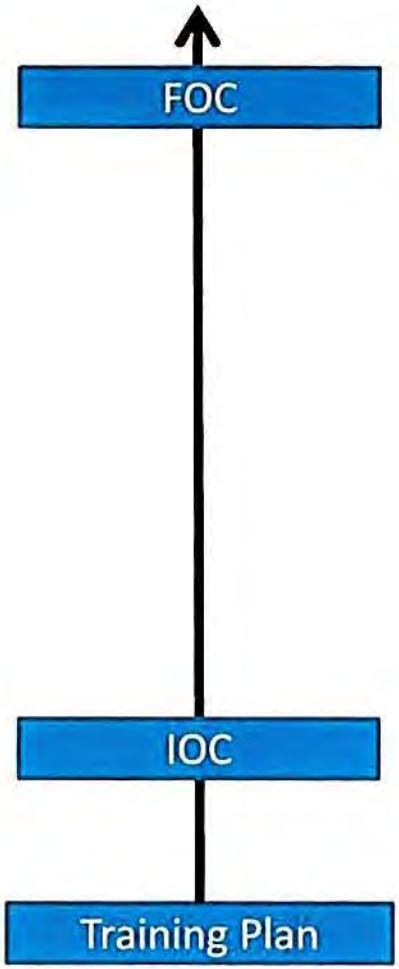
A Building Block Approach to IOC/FOC



- Tier I/II Exercises
  - (b)(1) Sec. 1.7(e)
- Mission Rehearsal Exercise
- JFHQ-C training

- Sub-Element Validation Events (SEV)
  - Cyber Flag
  - (b)(1) Sec. 1.7(e)
- Branch/Division training
- Team/Section training

- Individual qualification
- OJT
- Individual training pipeline
- Formal initial training



Section 2:
JFHQ-C Mission Essential Tasks & Mission Critical Functions

JFHQ-C MET and MCF Background Information

- In March, 2013, USCYBERCOM established a working group to develop the Mission Essential Tasks and subsequent Mission Critical Functions for the JFHQ-C. The WG performed a detailed scrub of the Universal Joint Task List (UJTL) identifying all UJTL entries that were listed under "Joint Task Force" and debated within the WG on which JTF UJTLs were most relevant to the JFHQ-C. The following METs and MCFs were reviewed and approved by USCYBERCOM J3 in June, 2013.

JFHQ-C Mission Essential Task List (METL)

1. Exercise C2 of all attached CMF ISO CCMD mission.
2. Exercise SIGINT Authority, Mission Delegation and Intelligence Oversight (to include SIGINT IO and auditing) of all attached CMF ISO CCMD mission.
3. Plan and direct Cyber ISR, Cyber OPE, Cyber Attack and – when directed – Cyber Defense actions to accomplish CCMD specified missions, and BPT conduct crisis action planning and CO in response to global threats.
4. Coordinate, integrate, synchronize and de-conflict CO of attached CMF with other JFHQ-C, NMF-HQ and USCC, operating in the same networks, at the tactical level, to maximize operational effectiveness. Coordinate as required with NSA Cryptologic Center Commanders.
5. Conduct intelligence operations; including managing CMF intelligence requirements and the collection, production and dissemination of intelligence.
6. Coordinate JFHQ-C support functions for attached and for co-located CMF with USCC, NSA, service and functional components; direct CMF training, exercises, and readiness requirements.

JFHQ-C Mission Essential Tasks and Functions Brief dtd 21JUN13

JFHQ-C MET 1 and MCFs

- MET 1: Exercise C2 of all attached CMF ISO CCMD mission. Command and Control Joint Force Headquarters – Cyber
- Mission Critical Functions (MCF)
  - 1.1 Exercise Command and Control of CMF maneuver teams
  - 1.2 Report Readiness
  - 1.3 Provide for Legal Services ISO planning & operations, except that all operational SIGINT legal advice will be provided by NSA OGC
  - 1.4 Maintain Operational Information and Force Status (Also supports Tasks 2-5)
  - 1.5 Conduct Joint Force Staff Operations
  - 1.6 Conduct operational synchronization and integration with JCC/JFCCC
  - 1.7 Conduct Knowledge Management and Information Management

JFHQ-C MET 2 and MCFs

- MET 2: Exercise SIGINT Authority, Mission Delegation and Intelligence Oversight (to include SIGINT IO and auditing) of all attached CMF ISO CCMD mission.
- Mission Critical Functions (MCF)
  - 2.1 Manage the SIGINT collection process
  - 2.2 Conduct asset management
  - 2.3 Manage mission delegation
  - 2.4 Oversee CMF Cryptologic Intelligence Oversight (CIO) program
  - 2.5 Provide advice and guidance on SIGINT policy and procedures
  - 2.6 Provide Operations & Intelligence system support

JFHQ-C MET 3 and MCFs

- MET 3: Plan and direct Cyber ISR, Cyber OPE, Cyber Attack and – when directed – Cyber Defense actions to accomplish CCMD specified missions, and BPT conduct crisis action planning and CO in response to global threats.
- Mission Critical Functions (MCF)
  - 3.1 Prepare Plans and Orders
  - 3.2 Conduct Mission Analysis
  - 3.3 Issue Planning Guidance
  - 3.4 Develop COA/Prepare staff estimates
  - 3.5 Issue Commander's Estimate
  - 3.6 Issue Plans and Orders
  - 3.7 Coordinate battlespace maneuver & integrate with firepower
  - 3.8 Support Target System Analysis, Electronic Target Folders and Target List Production/Management

JFHQ-C MET 3 and MCFs (Cont.)

- MET 3: Plan and direct Cyber ISR, Cyber OPE, Cyber Attack and – when directed – Cyber Defense actions to accomplish CCMD specified missions, and BPT conduct crisis action planning and CO in response to global threats.
- Mission Critical Functions (MCF)
  - 3.9 Support HPT/HVT development
  - 3.10 Conduct operational rehearsals
  - 3.11 Conduct operational maneuver
  - 3.12 Conduct effects and tactical assessments
  - 3.13 Prioritize OPE and ISR efforts
  - 3.14 Conduct dynamic targeting
  - 3.15 Participate in Task Forces (Joint/interagency/international)
  - 3.16 Conduct Computer Network Exploitation (CNE) enabling operations (Cyberspace ISR and Cyberspace OPE)

JFHQ-C MET 4 and MCFs

- MET 4: Coordinate, integrate, synchronize and de-conflict CO of attached CMF with other JFHQ-C, NMF-HQ and USCC, operating in the same networks, at the tactical level, to maximize operational effectiveness. Coordinate as required with NSA Cryptologic Center Commanders.
- Mission Critical Functions (MCF)
  - 4.1 Synchronize, deconflict, and integrate operations/fires
  - 4.2 Coordinate employment of CO
  - 4.3 Manage use and assignment of terrain
  - 4.4 Synchronize and integrate operations
  - 4.5 Conduct Operational Assessment
  - 4.6 Employ tactical cyberspace firepower
  - 4.7 Coordinate and integrate joint/multinational and IA support
  - 4.8 Coordinate with cryptologic enterprise elements (NSA)

JFHQ-C MET 5 and MCFs

- MET 5: Conduct intelligence operations; including managing CMF intelligence requirements and the collection, production and dissemination of intelligence.
- Mission Critical Functions (MCF):
  - 5.1 Process and exploit collected operational information
  - 5.2 Direct Joint Intelligence Support Element (JISE) operations
  - 5.3 Perform Collection Management (Planning & Prioritization, Requirements Management, & Tasking Cyber ISR Assets)
  - 5.4 Conduct Intelligence Preparation of the Battlespace (IPB)
  - 5.5 Gain & Maintain Situational Understanding
  - 5.6 Provide Intelligence Support to Plans, Operations, and Fires
  - 5.7 Develop Operational Targets
  - 5.8 Conduct Cyberspace ISR
  - 5.9 Conduct Single Source Exploitation
  - 5.10 Provide SIGINT on Specified Targets
  - 5.11 Produce Operational Intelligence
  - 5.12 Conduct Intelligence Staff Operations

JFHQ-C MET 6 and MCFs

- Coordinate JFHQ-C support functions for attached or co-located CMF with USCC, NSA, service and functional components; direct CMF training, exercises, and readiness requirements.

- Mission Critical Functions (MCF):
  - 6.1 Plan, Direct, and Execute Exercises
  - 6.2 Provide Resource Management
  - 6.3 Serve as the USCC Coordinating Authority facilitating as required, Service Component ADCON through local coordination of admin, logistics & support requirements for all co-located (attached and unattached) CMF
  - 6.4 Serve as the USCC Coordinating Authority to coordinate and deconflict deliberate mission scheduling for unattached, co-located CMF
  - 6.5 Serve as the USCC Coordinating Authority to coordinate and deconflict time sensitive operations for unattached, co-located CMF
  - 6.6 Prioritize Architecture and Capabilities Development and Requirements (ISO Task 4)
  - 6.7 Coordinate Logistic Services
  - 6.8 Manage Personnel Accountability & Strength Reporting
  - 6.9 Provide Security (ACCM) Management & oversee STO/SAP operations
  - 6.10 Conduct Joint Force Staff Operations
  - 6.11 Conduct command designated coordination operations
  - 6.12 Coordinate and direct weapon capability development

Section 3:
USCYBERCOM Processes

USCYBERCOM Processes

- The following are the processes, B2C2WG and tactical actions that USCYBERCOM uses to conduct full spectrum CO.

- Processes

P1 Cyberspace Tasking Cycle (Modified Air Tasking Cycle)
  - Cyberspace Operations Directive (CyOD)
  - Master Cyber Operations Plan (MCOP)
  - Integrated Tasking Order (ITO)
  - Special Instructions (SPINs)
  - Joint Tactical Cyber Request (JTCR)
  - Assessment (MISREPs, BDA/MEA/Re-strike/Re-target)

P2 Cyberspace Effects Request Form (CERF)

P3 (b)(3) 10 U.S.C. § 130e

P4 Planning Teams

P5 Operational Priorities and Intelligence Collection Priorities

P6 Joint Targeting Cycle
  - Target Development: TDWG/JTWG
  - Strike Package Coordination: JTCM
  - Target Validation/Approval: JTCB

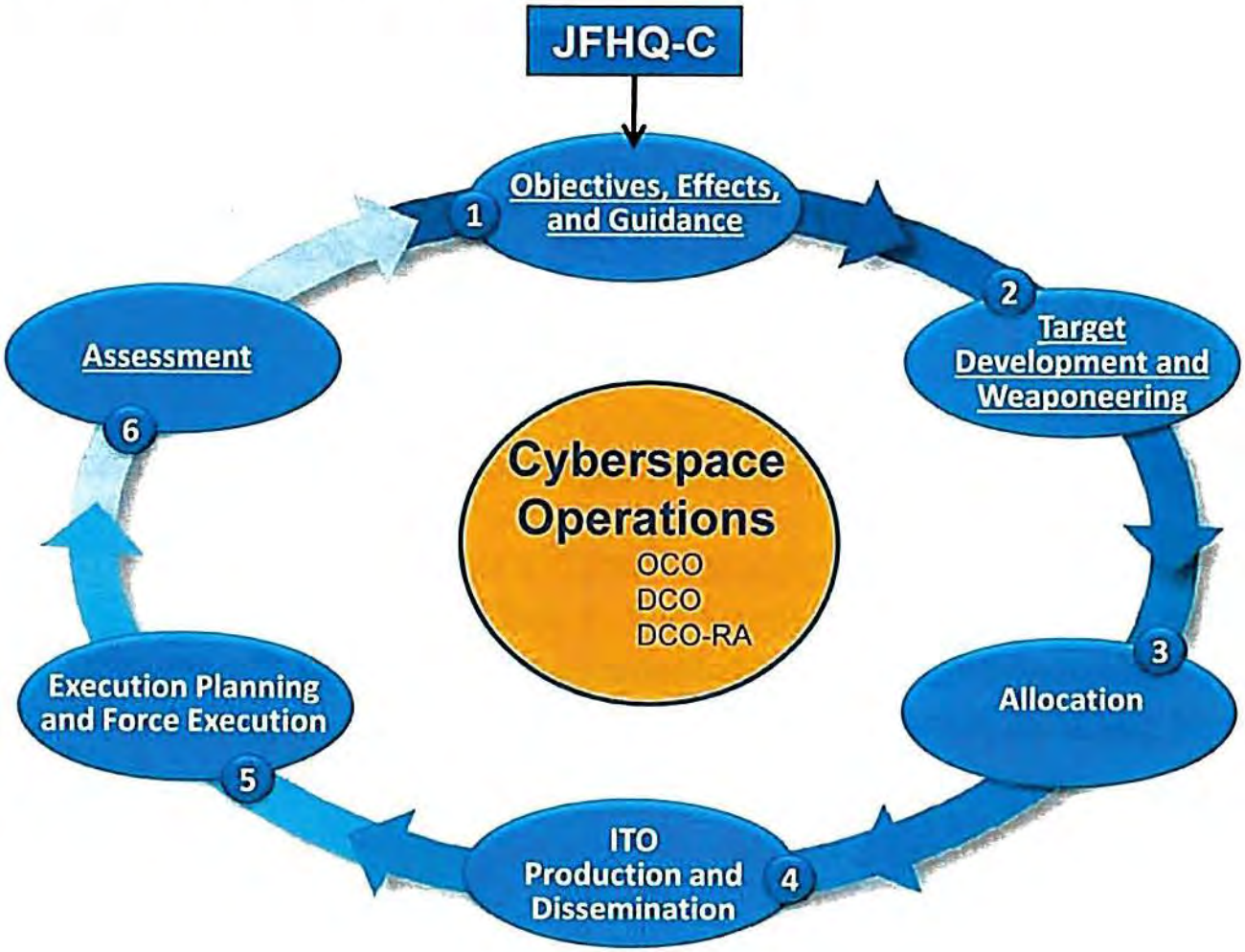
P7 Operations Synchronization

USCYBERCOM Process 1 and ITs

- P1: Cyberspace Tasking Cycle
  - The Cyberspace Tasking Cycle is a modified air tasking cycle. It provides for effective and efficient employment of Joint forces and capabilities. It is an iterative, cyclic is a six step process to plan, schedule, execute, and assess full-spectrum cyberspace operations.

- Individual Tasks (ITs)
  1.1 Objectives, Effects, and Guidance (CyOD)
  1.2 Target Development and Weaponeering (Joint Targeting Process)
  1.3 Allocation (MCOP, JTCR)
  1.4 ITO Production and Dissemination (b)(3) 10 U.S.C. § 130e
  1.5 Execution Planning and Force Execution (SPINs)
  1.6 Assessment
    - MISREP
    - MOP/MOE
    - Combat Assessment Process (BDA, MEA, and Re-strike/Re-target)

Cyberspace Tasking Cycle

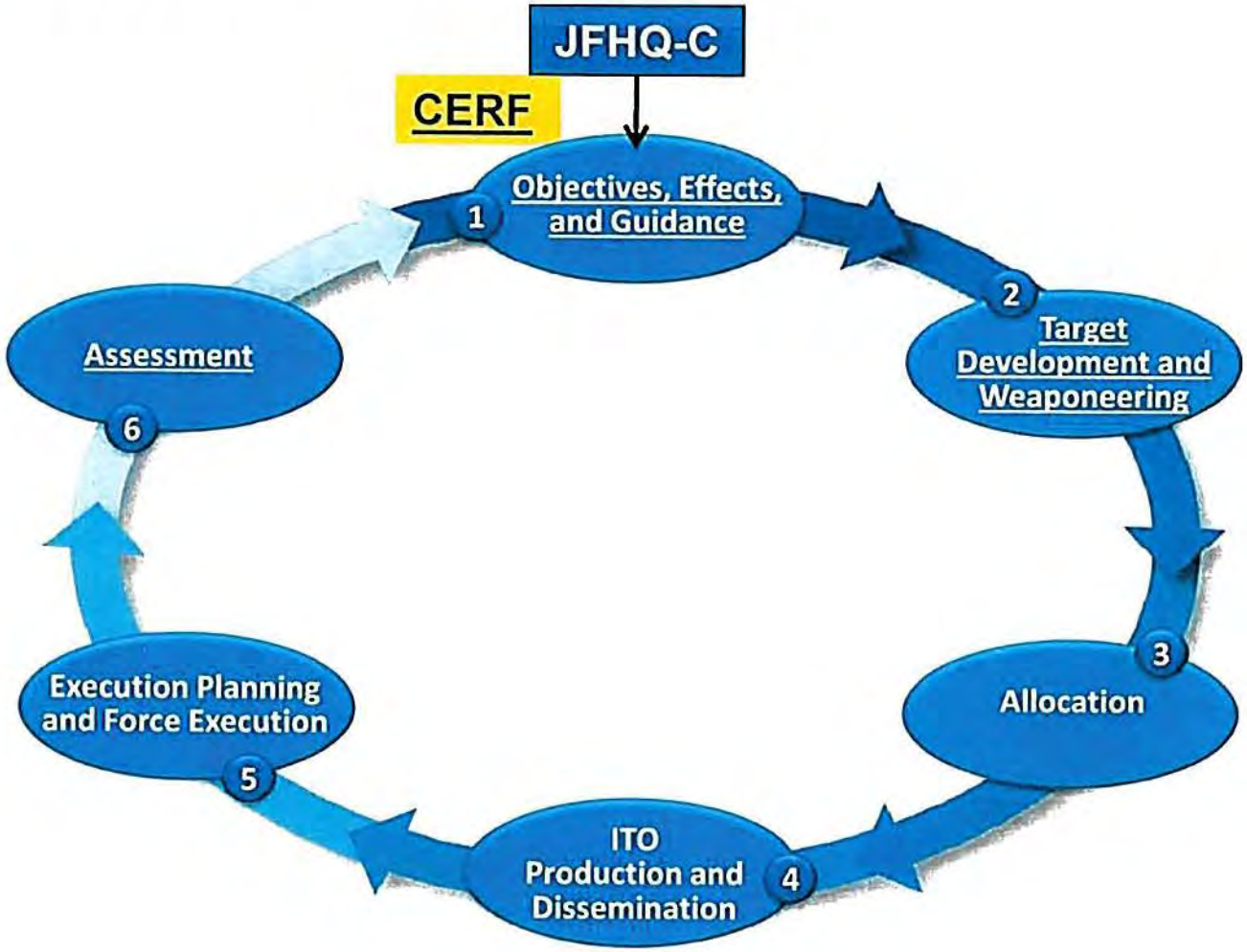


USCYBERCOM Process 2 and ITs

- P2: Cyberspace Effects Request Form (CERF):
  - A CERF is a formal request for USCYBERCOM *operational* support. It is the form USCYBERCOM uses to receive, track, and provide operational effects in support of planning and execution across all lines of operations: offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DOD global information grid operations (DGO).

- Individual Tasks (ITs):
  - 2.1 Links the desired effects with the tactical objective, operational goal and strategic endstate
  - 2.2 Records, tracks, and manages requests from the supported JFC
  - 2.3 Assigned to planning team IAW time horizon and function
  - 2.4 Facilitates dialogue/DIRLAUTH and transparency throughout the process
  - 2.5 Automated status of planning tracker

Cyberspace Tasking Cycle



USCYBERCOM Process 3 and ITs

- P3: (b)(3) 10 U.S.C. § 130e
  -
- Individual Tasks (ITs):
  - 3.1 (b)(3) 10 U.S.C. § 130e
  - 3.2

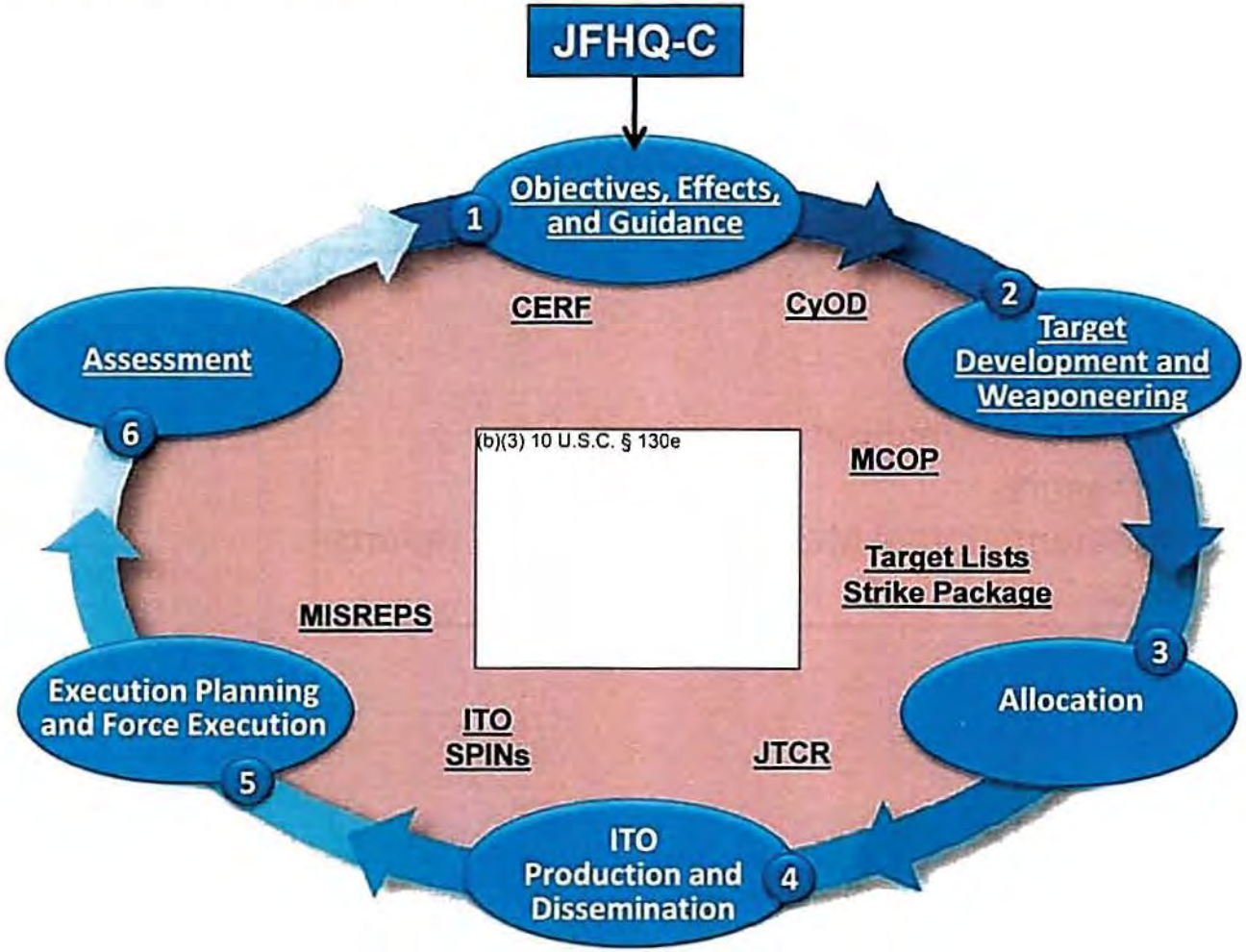
USCYBERCOM Process 3 and ITs (Cont.)

- P3: (b)(3) 10 U.S.C. § 130e
  -

- Individual Tasks (ITs):

3.3 (b)(3) 10 U.S.C. § 130e

Cyberspace Tasking Cycle



LEGEND	
CERF – Cyber Effects Request Form	MCOP – Master Cyber Operations Plan
CYOD – Cyber Operations Directive	ITO – Integrated Tasking Order
JTCR – Joint Tactical Cyber Request	CCO – Cyber Control Order

USCYBERCOM Process 4 and ITs

- P4: Planning Teams
  - *"Planning translates strategic guidance and direction into campaign plans, contingency plans, and operations orders (OPORDs). Joint operation planning may be based on defined tasks identified in the Guidance for Employment of the Force (GEF) and the Joint Strategic Capabilities Plan (JSCP). Alternatively, joint operation planning may be based on the need for a military response to an unforeseen current event, emergency, or time-sensitive crisis."* (JP 5-0)

- Individual Tasks (ITs)

  4.1 Strategy Division/Future Operations Team (J35)
    - Base OPORD/EXORD
    - Branches and sequel planning
    - Propose changes to ROE and Rules for Use Of Force (ROF)
    - Develop and coordinate the CyOD
    - Operational assessment reports and plans

USCYBERCOM Process 4 and ITs (Cont.)

- P4: Planning Teams
  - *"Planning translates strategic guidance and direction into campaign plans, contingency plans, and operations orders (OPORDs). Joint operation planning may be based on defined tasks identified in the Guidance for Employment of the Force (GEF) and the Joint Strategic Capabilities Plan (JSCP). Alternatively, joint operation planning may be based on the need for a military response to an unforeseen current event, emergency, or time-sensitive crisis."* (JP 5-0)

- Individual Tasks (ITs)

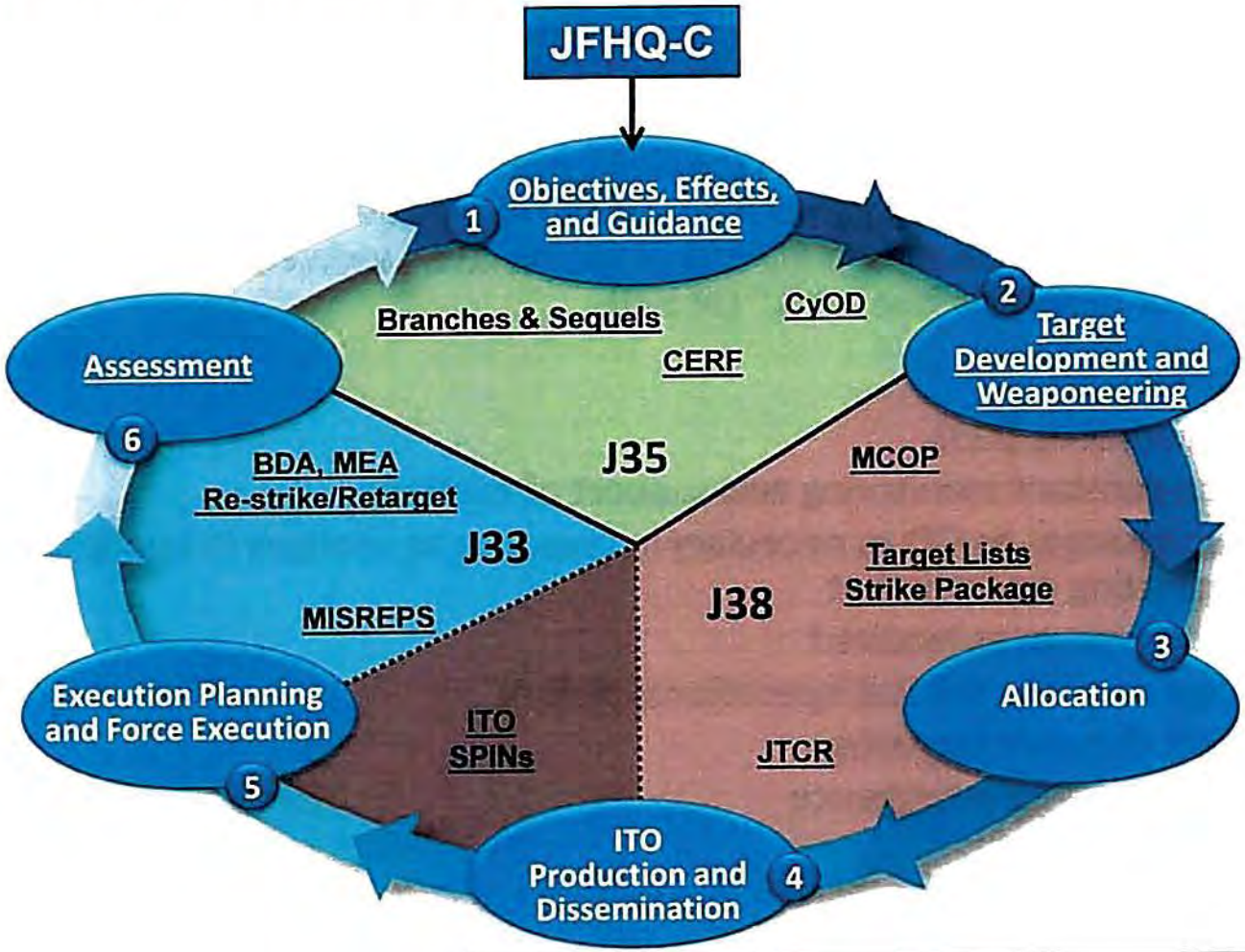
  4.2 Combat Plans/Joint Fires Element (J38)
    - Conduct Crisis Action Planning
    - Produce MCOP
    - Process/generate JTCRs
    - Produce ITO
    - Generate SPINs
    - Conduct combat assessments
    - Conduct advanced target development (Weaponeering)
    - Produce the draft JIPTL
    - Build and coordinate Strike Package
    - Manage Target Lists

USCYBERCOM Process 4 and ITs (Cont.)

- P4: Planning Teams
  - *"Planning translates strategic guidance and direction into campaign plans, contingency plans, and operations orders (OPORDs). Joint operation planning may be based on defined tasks identified in the Guidance for Employment of the Force (GEF) and the Joint Strategic Capabilities Plan (JSCP). Alternatively, joint operation planning may be based on the need for a military response to an unforeseen current event, emergency, or time-sensitive crisis."* (JP 5-0)
- Individual Tasks (ITs)

  4.3 Current Operations (J33)
    - Provide constant monitoring and support of missions
    - Publish changes to ITO as necessary in response to changes in operations and/or the operating environment
    - Develop reports as required
    - Manage common tactical/operational picture
    - Conduct dynamic targeting
    - Provide real time intelligence

Cyberspace Tasking Cycle



LEGEND	
CERF – Cyber Effects Request Form	MCOP – Master Cyber Operations Plan
CYOD – Cyber Operations Directive	ITO – Integrated Tasking Order
JTCR – Joint Tactical Cyber Request	CCO – Cyber Control Order

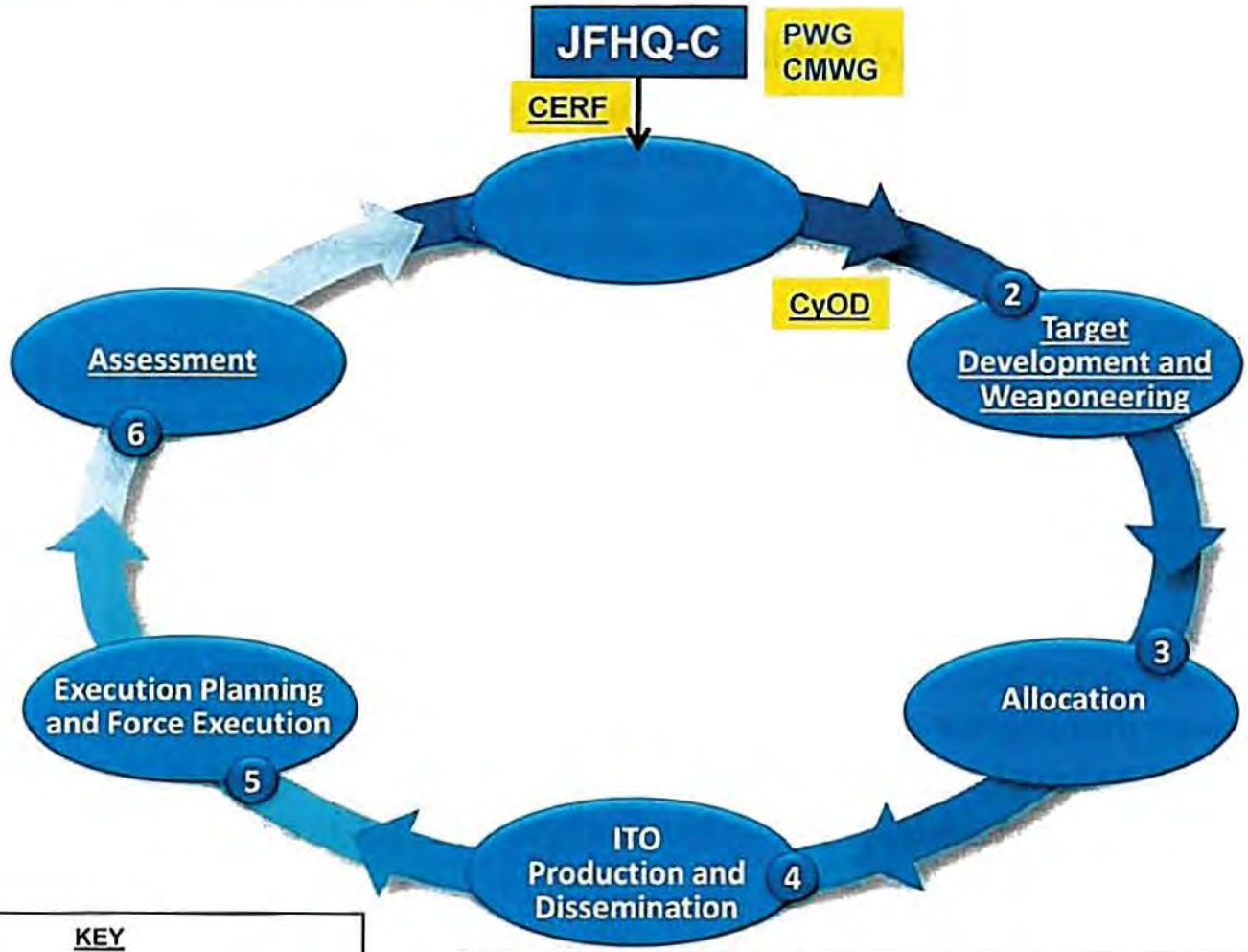
USCYBERCOM Process 5 and ITs

- P5: Operational Priorities and Intelligence Collection Priorities
  - The priorities process allows the Commander to shift his main and supporting efforts by periodically assessing operational priorities within three mission areas (Defend the Nation, Operate and Defend the DODIN, and Support to Combatant Commanders). The process aligns intelligence collection efforts with operational priorities.
- Individual Tasks (ITs):

  5.1 Priorities Working Group (PWG) - Analyzes demand signal from CERFs and command guidance against current operational and planning priorities. Creates proposed operational planning priorities for approval by DCDR via J2/J3/J5 review.

  5.2 Collection Management Working Group (CMWG)
  - Reviews and prioritizes Joint Integrated Prioritized Collection List (JIPCL) – intelligence, access, capability, and interagency requirements
  - Develops intelligence collection guidance and priorities for ISR forces
  - Provides status of collection actions and evaluates effectiveness of collection
  - Deconflicts Command/Service Cyber Component (SCC) requirements

Cyberspace Tasking Cycle



KEY

SOPs

Battle Rhythm (B2C2WG)

LEGEND

CERF – Cyber Effects Request Form
CYOD – Cyber Operations Directive
JTCR – Joint Tactical Cyber Request
MCOP – Master Cyber Operations Plan
ITO – Integrated Tasking Order
CCO – Cyber Control Order

USCYBERCOM Process 6 and ITs

- P6: Joint Targeting Cycle
  - *"Targeting is the process of selecting and prioritizing targets, matching the appropriate response to them, and considering operational requirements and capabilities."* (JP 3-60) Integrating and synchronizing planning, execution, and assessment is pivotal to the success of targeting.

- Individual Tasks (ITs)

  6.1 Target Development Working Group (TDWG) – Responsible developing targets through the basic through intermediate development process and produces a vetted target ready for advanced development. The focus of the TDWG is target status to properly vet the target.

  6.2 Joint Targeting Working Group (JTWG) – Responsible for approving entities for target development and providing the status of advanced targets; ultimately producing a target strike package to the JTCM for coordination. The focus of the JTWG is to ensure fires and effects delivered in and through cyberspace support the objective(s).

USCYBERCOM Process 6 and ITs (Cont.)

- P6: Joint Targeting Cycle
  - *"Targeting is the process of selecting and prioritizing targets, matching the appropriate response to them, and considering operational requirements and capabilities."* (JP 3-60) Integrating and synchronizing planning, execution, and assessment is pivotal to the success of targeting.

- Individual Tasks (ITs)

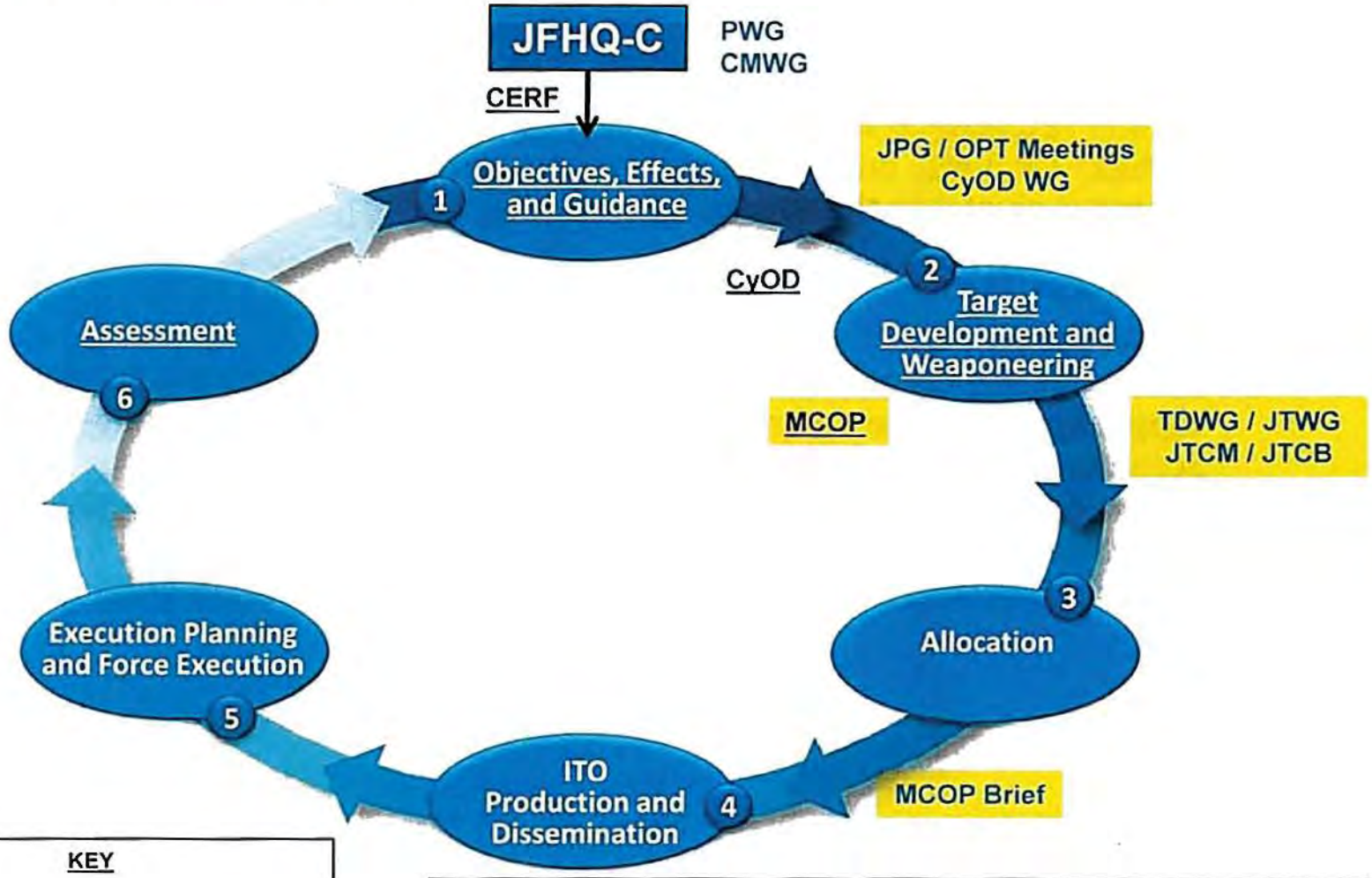
  6.3 Cyberspace Strike Package - The primary product presented to the chairman of the JTCB for the purpose of informing the Commander's decision regarding the execution of an operation. The Cyberspace Strike Package includes:
  - Concept of Fires/Effects
  - Intel Gain Loss (IGL)
  - Political Military Assessment (PMA)
  - Collateral Effects Estimate (CEE)
  - Operation Legal Review (OLR)
  - Blowback Assessment
  - No Foreign Policy Objection (NFPO)
  - Risk Assessment Report (RAR)/Capability Target Pairing (CTP)

USCYBERCOM Process 6 and ITs (Cont.)

- P6: Joint Targeting Cycle
  - *"Targeting is the process of selecting and prioritizing targets, matching the appropriate response to them, and considering operational requirements and capabilities."* (JP 3-60) Integrating and synchronizing planning, execution, and assessment is pivotal to the success of targeting.
- Individual Tasks (ITs)

  6.4 Target Validation
    - Joint Targeting Coordination Board (JTCB) – On behalf of the supported or supporting JFC, develop broad targeting priorities and other targeting guidance in accordance with the JFC's objectives as they relate operationally. Approve/Disapprove addition of targets to USCC target lists or target, capability and concept of fires release to COCOM.
    - The JTCB validates a target in context of the plan or operation order it supports.

Cyberspace Tasking Cycle



KEY

SOPs

Battle Rhythm (B2C2WG)

LEGEND

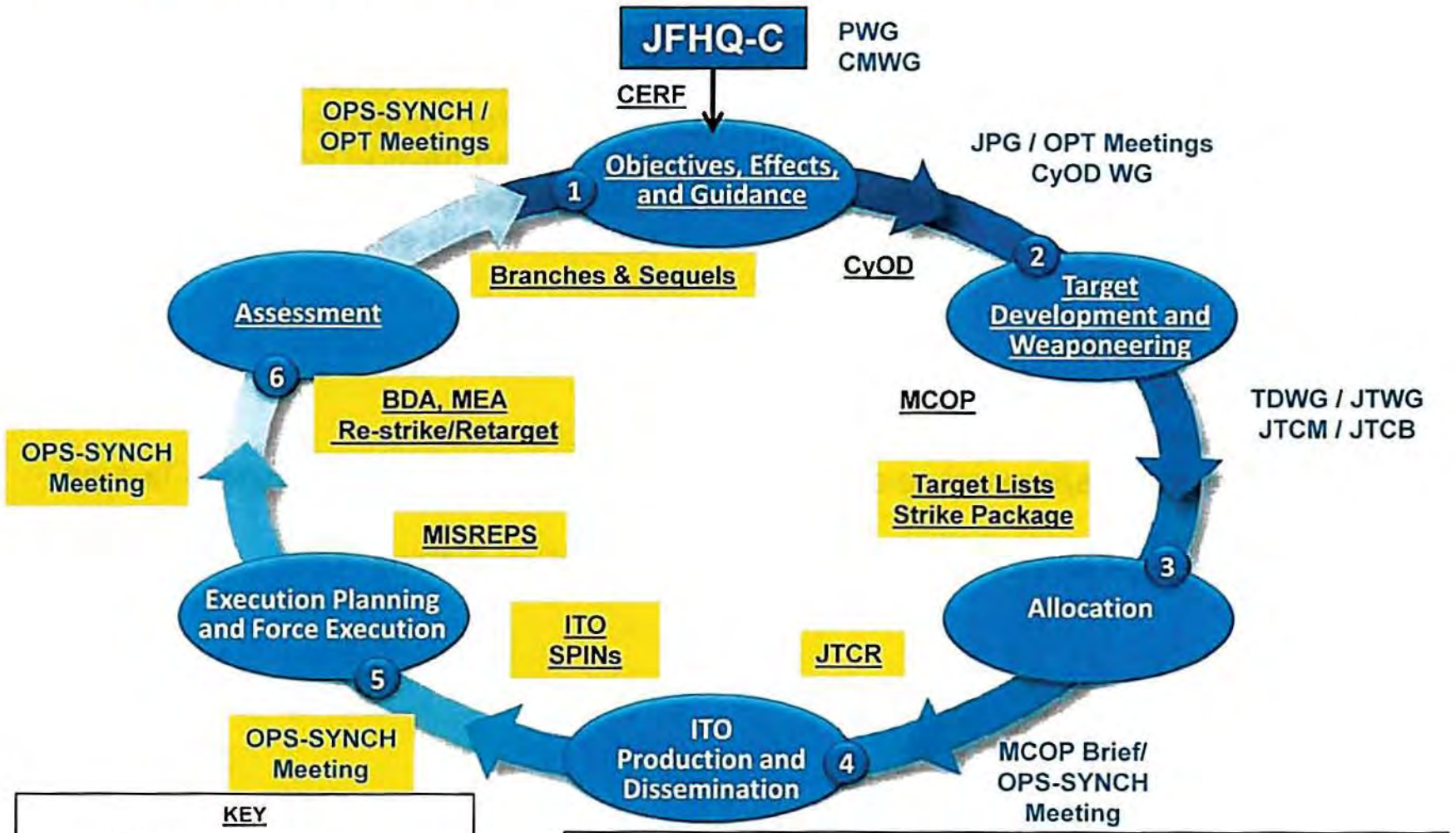
CERF – Cyber Effects Request Form
CYOD – Cyber Operations Directive
JTCR – Joint Tactical Cyber Request
MCOP – Master Cyber Operations Plan
ITO – Integrated Tasking Order
CCO – Cyber Control Order

USCYBERCOM Process 7 and ITs

- P7: Operations Synchronization
  - The Operations Synchronization (OPS-SYNC) meeting assesses operations executed during the last 24-hours; evaluates ongoing operations for the present day ITO and schedules and deconflicts operations out to 48-hours and beyond by annotating them on a MCOP. The current intelligence picture, collection emphasis message, target status, and readiness of forces and infrastructure inform this effort.

- Individual Tasks (ITs)
  - 7.1 Deconflicting CO throughout the domain
  - 7.2 Synchronizing CO with other kinetic or non-kinetic operations
  - 7.3 Providing updates/support to efforts spanning all phases of the Cyberspace Tasking Cycle
  - 7.4 Integrating legal services in support of planning and operations

Cyberspace Tasking Cycle



KEY

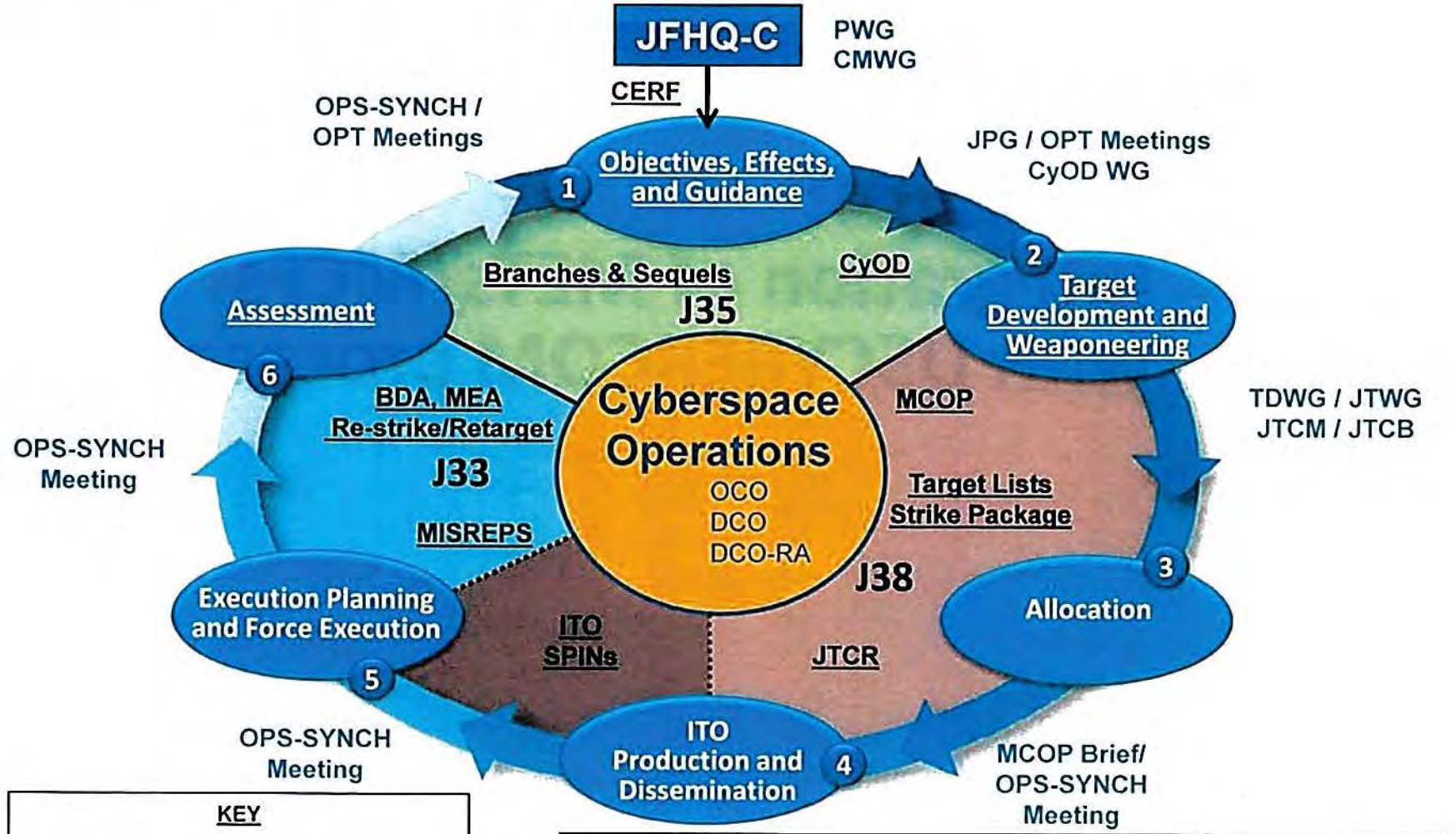
SOPs

Battle Rhythm (B2C2WG)

LEGEND

CERF – Cyber Effects Request Form	MCOP – Master Cyber Operations Plan
CYOD – Cyber Operations Directive	ITO – Integrated Tasking Order
JTCR – Joint Tactical Cyber Request	CCO – Cyber Control Order

Cyberspace Tasking Cycle



KEY

SOPs

Battle Rhythm (B2C2WG)

LEGEND

CERF – Cyber Effects Request Form
CYOD – Cyber Operations Directive
JTCR – Joint Tactical Cyber Request
MCOP – Master Cyber Operations Plan
ITO – Integrated Tasking Order
CCO – Cyber Control Order

Section 4: Integration of METs/MCFs with USCYBERCOM processes

Integration of METs/MCFs with USCYBERCOM processes

- The following slides outline how the major USCYBERCOM process integrate with the METs/MCFs of the JFHQ. It nests individual tasks under mission critical functions that support the mission essential tasks to show how the processes employed by USCYBERCOM support each of the tasks that the JFHQ-C will required to accomplish.

JFHQ-C MET 1 and MCFs Integrated with USCYBERCOM Processes

- MET 1: Exercise C2 of all attached CMF ISO CCMD mission. Command and Control Joint Force Headquarters – Cyber.
- Mission Critical Functions (MCF)

1.1 Exercise Command and Control of CMF maneuver teams

- P3 (b)(3) 10 U.S.C. § 130e
- P7 OPS-SYNCH:
  - IT 7.1 Deconflicting CO throughout the domain (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)
  - IT 7.2 Synchronizing CO with other lethal or non-lethal operations (Ref TA 3.3)

1.2 Report Readiness

- P3 (b)(3) 10 U.S.C. § 130e

1.3 Provide for Legal Services ISO planning & operations, except that all operational SIGINT legal advice will be provided by NSA OGC

- P7 OPS-SYNCH: IT 7.4 Integrating legal services in support of planning and operations (Ref OP 4.4.7 Provide for legal services)

JFHQ-C MET 1 and MCFs Integrated with USCYBERCOM Processes (Cont.)

1.4 Maintain Operational Information and Force Status (Also supports Tasks 2-5)

- P3 (b)(3) 10 U.S.C. § 130e (b)(3) 10 U.S.C. § 130e
- P7 OPS-SYNCH: IT 7.3 Providing updates/support to efforts spanning all phases of the Cyberspace Tasking Cycle

1.5 Conduct Joint Force Staff Operations

- P1 Cyberspace Tasking Cycle: Outlines the steps and processes necessary to conduct CO
- P4 Planning Teams: Properly organized teams following the Cyberspace Tasking Cycle will accomplish the staff actions needed to successfully employ CO

1.6 Conduct operational synchronization and integration with JCC/JFCCC

- P3 (b)(3) 10 U.S.C. § 130e
- P7 OPS-SYNCH :
  - IT 7.1 Synchronizing and Deconflicting CO throughout the domain (Ref TA 5.5.1 Conduct Force Link Up, TA 5.6.5.1 Coordinate employment of Computer Network Operations in Joint Operations Area)
  - IT 7.3 Forum to discuss status of I&W and operations assessments (Ref TA 2.4 Discuss Tactical Warning Information and Attack Assessment)

JFHQ-C MET 1 and MCFs Integrated with USCYBERCOM Processes (Cont.)

1.7 Conduct Knowledge Management and Information Management

- P3 (b)(3) 10 U.S.C. § 130e
- P7 OPS-SYNCH :
  - IT 7.1 Deconflict CO with the IC and adjacent units (Ref TA 5.6.5.1 Coordinate employment of Computer Network Operations in a Joint Operations Area)
  - IT 7.3 Share Operational Intelligence

JFHQ-C MET 2 and MCFs Integrated with USCYBERCOM Processes

- MET 2: Exercise SIGINT Authority, Mission Delegation and Intelligence Oversight (to include SIGINT IO and auditing) of all attached CMF ISO CCMD mission.
- Mission Critical Functions (MCF)

2.1 Manage the SIGINT collection process

- IT 5.1 PWG: Creates operational planning priorities that informs the intelligence collection priorities
- IT 5.2 CMWG: Prioritizes the JIPCL and develops collection guidance and priorities for ISR forces

2.2 Conduct asset management

- P3 (b)(3) 10 U.S.C. § 130e

2.3 Manage mission delegation

- P3 (b)(3) 10 U.S.C. § 130e
- IT 5.2 CMWG: Prioritizes the JIPCL and develops collection guidance and priorities for ISR forces

JFHQ-C MET 2 and MCFs Integrated with USCYBERCOM Processes

2.4 Oversee CMF Cryptologic Intelligence Oversight (CIO) program

- P3 (b)(3) 10 U.S.C. § 130e
  (b)(3) 10 U.S.C. § 130e

2.5 Provide advice and guidance on SIGINT policy and procedures

- P7 OPS-SYNCH: IT 7.4 Integrating legal services in support of planning and operations (Ref OP 4.4.7 Provide for legal services)

2.6 Provide Operations & Intelligence system support

- P3 (b)(3) 10 U.S.C. § 130e

JFHQ-C MET 3 and MCFs

- MET 3: Plan and direct Cyber ISR, Cyber OPE, Cyber Attack and – when directed – Cyber Defense actions to accomplish CCMD specified missions, and BPT conduct crisis action planning and CO in response to global threats.

- Mission Critical Functions (MCF)
  - 3.1 Prepare Plans and Orders
    - P1 Cyberspace Tasking Cycle: IT 1.4 ITO production and dissemination (Ref OP 5.3 Prepare Plans and Orders, OP 5.4.1 Approve Plans and Orders, TA 3.3.1 Prepare the Air Tasking Order)
    - P2 CERF: IT 2.3 Initiates operational planning (Ref TA 5.6.5.1 Coordinate Employment of Cyberspace operations)
    - P3 (b)(3) 10 U.S.C. § 130e (b)(3) 10 U.S.C. § 130e
    - P4 Planning Teams: IT 4.2 Prepare the ITO, MCOP, JIPTL, and SPINs (Ref TA 3.3.1 Coordinate Air Tasking Order)
  - 3.2 Conduct Mission Analysis
    - P4 Planning Teams: IT 4.1 Conduct Branch and Sequel planning IAW the Joint Operation Planning Process (JOPP) outlined in JP 5-0

JFHQ-C MET 3 and MCFs (Cont.)

3.3 Issue Planning Guidance

- P1 Cyberspace Tasking Cycle: IT 1.1 Objectives, Effects, and Commander's guidance is disseminated to the JFHQ staff via the CyOD (Ref TA 5.6.5.1 Coordinate Employment of Cyberspace Operations)
- P2 CERF: IT 2.1 Conveys Commander's objectives, end state and desired effects to the planning teams (Ref TA 5.6.5.1 Coordinate Employment of Cyberspace Operations)

3.4 Develop COA/Prepare staff estimates

- P4 Planning Teams: IT 4.1 Conduct planning IAW the JOPP outlined in JP 5-0

3.5 Issue Commander's Estimate

- P4 Planning Teams: IT 4.1 Conduct planning IAW the JOPP outlined in JP 5-0

3.6 Issue Plans and Orders

- P1 Cyberspace Tasking Cycle: IT 1.4 ITO Production and Dissemination (Ref OP 5.3 Prepare Plans and Orders, OP 5.4.1 Approve Plans and Orders, TA 3.3.1 Prepare the Air Tasking Order)
- P3 (b)(3) 10 U.S.C. § 130e

(b)(3) 10 U.S.C. § 130e

- P4 Planning Teams: IT 4.2 Prepare the ITO, MCOP, JIPTL, and SPINs (Ref TA 3.3.1 Coordinate Air Tasking Order)

JFHQ-C MET 3 and MCFs (Cont.)

3.7 Coordinate Battlespace maneuver & integrate with firepower

- P1 Cyberspace Tasking Cycle:
  - IT 1.3 Allocation
  - IT 1.4 Iterative, Cyclic process to plan, schedule and execute CO (Ref OP 3.1.2 Apportion fires, OP 5.3 Prepare Plans and Orders, OP 5.4.1 Approve Plans and Orders, TA 3.3.1 Prepare the Air Tasking Order)
- P3 (b)(3) 10 U.S.C. § 130e
- P7 OPS-SYNC: IT 7.1 Deconflict operations with the IC and adjacent units (Ref TA 5.6.5.1 Coordinate Employment of Cyberspace Operations)

3.8 Support Target System Analysis, Electronic Target Folders and Target List Production/Management

- P1 Joint Targeting Cycle: IT 1.1, IT 1.2 Develop Targets through the advanced level and place them on a targeting list (Ref OP 2.8 Provide Intelligence Support to Fires, TA 2.1 Produce Electronic Target Folders)
- P4 Planning Teams: IT 4.1 Submit intelligence requirements and requests for information as required to build a Target System Analysis (Ref OP 2.8 Provide Intelligence Support to Fires)

JFHQ-C MET 3 and MCFs (Cont.)

3.9 Support HPT/HVT development

- P4 Planning Teams:
  - IT 4.1 Submit intelligence requirements and requests for information as required to build a Target System Analysis (Ref OP 2.8 Provide Intelligence Support to Fires)
  - IT 4.2 Prioritize HPTs/HVTs
- P6 Joint Targeting Cycle: IT 6.3 Prepare cyberspace strike package for Commander's approval

3.10 Conduct operational rehearsals

- P4 Planning Teams: IT 4.1, IT 4.2 Identify and rehearse key processes and elements

3.11 Conduct operational maneuver

- P1 Cyberspace Tasking Cycle:
  - IT 1.3 Translate JTCR onto the MCOP
  - IT 1.4 Produce ITOs from the MCOP
  - IT 1.5 Generate SPINs
- P7 OPS-SYNC: IT 7.1 Deconflict operations with the IC and adjacent units (TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)

JFHQ-C MET 3 and MCFs (Cont.)

3.12 Conduct effects and tactical assessments

- P1 Cyberspace Tasking Cycle: IT 1.6 Assessment (MISREPS, MOP/MOE, BDA)
- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams: IT 4.1 Digest MISREPs and intelligence reports and produce effects and tactical assessments
- P7 OPS-SYNC: IT 7.3 Disseminate assessment information (Ref TA 2.4 Disseminate Tactical Warning Information and Attack Assessments)

3.13 Prioritize OPE and ISR efforts

- P1 Cyberspace Tasking Cycle:
  - IT 1.1 Objectives, Effects, and Guidance
  - IT 1.3 Allocation
- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams:
  - IT 4.1 Provide characterization of the cyberspace battlespace (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)
  - IT 4.3 Identify cyberspace activity as neutral, friendly, or adversarial (Ref TA 6.5 Provide for Combat Identification)
- IT 5.2 CMWG: Develop intelligence collection guidance and priorities for ISR forces

JFHQ-C MET 3 and MCFs (Cont.)

3.14 Conduct dynamic targeting

- P4 Planning Teams: IT 4.2 Conduct planning/crisis action planning and produce cyberspace strike packages as required to support dynamic targeting
- P6 Joint Targeting Cycle: IT 6.4 Validate targets at the JTCB and place them on a targeting list to be prosecuted as targets of opportunity

3.15 Participate in Task Forces (Joint/Interagency/International)

- P2 CERF: TA 2.4 Facilitates dialogue/DIRLAUTH and transparency throughout the process (Ref TA 5.6.5.1 Coordinate Employment of Cyberspace Operations

3.16 Conduct Computer Network Exploitation (CNE) enabling operations (Cyberspace ISR and Cyberspace OPE)

P1 Cyberspace Tasking Cycle: Iterative, Cyclic process for planning, scheduling, executing and assessing OPE and ISR missions

P3 (b)(3) 10 U.S.C. § 130e

JFHQ-C MET 4 and MCFs

- MET 4: Coordinate, integrate, synchronize, and de-conflict cyber operations of attached CMF with other JFHQ-C, NMF-HQ and USCC, operating in the same networks, at the tactical level, to maximize operational effectiveness. Coordinate as required with NSA Cryptologic Center Commanders.
- Mission Critical Functions (MCF)
  - 4.1 Synchronize, deconflict, and integrate operations/fires
    - P1 Cyberspace Tasking Cycle:
      - IT 1.3 Allocation (MCOP)
      - IT 1.4 ITO Production and Dissemination (Ref TA 5.6.5.1 Coordinate employment of Computer Network Operations in a Joint Operations Area)
    - P3 (b)(3) 10 U.S.C. § 130e
    - P7 OPS-SYNC:
      - IT 7.1 Deconflict CO throughout the domain (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)
      - IT 7.2 Synchronize CO with other lethal/non-lethal operations (Ref 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)
      - IT 7.3 Disseminate I&W information (Ref TA 2.4 Disseminate Tactical Warning Information and Attack Assessments)

JFHQ-C MET 4 and MCFs

4.2 Coordinate employment of Cyberspace Operations (CO)

- P1 Cyberspace Tasking Cycle: Iterative process that outlines the procedures necessary for conducting CO (Ref TA 5.6.5.1 Coordinate employment of Computer Network Operations in a Joint Operations Area)
- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams: IT 4.2, IT 4.3 Identify and rehearse key processes and elements
- P7 OPS-SYNC:
  - IT 7.1, IT 7.2 Deconflict and synchronize CO with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.5.1 Conduct Force Link up)
  - IT 7.2 Synchronize CO with other lethal/non-lethal operations (Ref 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)
  - IT 7.3 Disseminate I&W information (Ref TA 2.4 Disseminate Tactical Warning Information and Attack Assessments)

JFHQ-C MET 4 and MCFs

4.3 Manage use and assignment of terrain

- P1 Cyberspace Tasking Cycle:
  - IT 1.3 Allocation - Systematically assign forces to battlespace areas (Ref Op 3.1.2 Apportion Fires)
  - IT 1.3 Allocation - Establish primacy on cyberspace assets/devices (Ref TA 6.5 Provide for Combat Identification)
- P3 (b)(3) 10 U.S.C. § 130e
- IT 5.2 CMWG: Develop collection guidance and priorities for ISR forces
- P7 OPS-SYNC:
  - IT 7.1 Deconflict and synchronize CO with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.5.1 Conduct Force Link up)
  - IT 7.2 Synchronize CO with other lethal/non-lethal operations (Ref 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)

JFHQ-C MET 4 and MCFs

4.4 Synchronize and integrate operations

- P3 (b)(3) 10 U.S.C. § 130e
- P7 OPS-SYNC:
  - IT 7.1 Deconflict and synchronize CO with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.5.1 Conduct Force Link up)
  - IT 7.2 Synchronize CO with other lethal/non-lethal operations (Ref 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)
  - IT 7.3 Identify cyberspace activity as neutral, friendly, or adversarial (Ref TA 6.5 Provide for Combat Identification)

4.5 Conduct Operational Assessment

- P1 Cyberspace Tasking Cycle: IT 1.6 Assessment
- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams: IT 4.1 Digest MISREPs and intelligence reports and produce effects and tactical assessments
- P7 OPS-SYNC: IT 7.3 Disseminate assessment information (Ref TA 2.4 Disseminate Tactical Warning Information and Attack Assessments)

JFHQ-C MET 4 and MCFs

4.6 Employ tactical cyberspace firepower

- P1 Cyberspace Tasking Cycle: IT 1.5 Execution Planning and Force Execution (Ref OP 5.3 Prepare Plans and Orders, OP 5.4.1 Approve Plans and Orders, TA 3.3.1 Prepare the Air Tasking Order)
- P3 (b)(3) 10 U.S.C. § 130e
- P7 OPS-SYNC:
  - IT 7.1 Deconflict and synchronize CO with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.5.1 Conduct Force Link up)
  - IT 7.2 Synchronize CO with other lethal/non-lethal operations (Ref 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 3.2.3 Conduct Interdiction)

JFHQ-C MET 4 and MCFs

4.7 Coordinate and integrate Joint/Multinational and Interagency support

- P4 Planning Teams: IT 4.1 Conduct planning IAW the Joint Operational Planning Process (JOPP) outlined in JP 5-0 and coordinate with Joint/Multinational forces and the Interagency as required to deconflict plans
- P6 Joint Targeting Cycle:
  - IT 6.1 Develop targets and Vet them with the Interagency IAW CJCSI 3370.01
  - IT 6.4 Validate targets and cyberspace strike package at the JTCB IAW CJCSI 3370.01
- P7 OPS-SYNC:
  - IT 7.1 Deconflict and synchronize CO with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.5.1 Conduct Force Link up)
  - IT 7.2 Synchronize CO with other lethal/non-lethal operations (Ref 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 3.2.3 Conduct Interdiction)

JFHQ-C MET 6 and MCFs

6.10 Conduct Joint Force Staff Operations (Cont.)

- P6 Joint Targeting Cycle
  - IT 6.1 TDWG: Develop targets through the intermediate stage and vet them with the IC
  - IT 6.2 JTWG: Nominate and approve entities of interest for target development, and conduct advanced target development of vetted targets
  - IT 6.3 Build cyberspace strike package to present at JTCM & JTCB
  - IT 6.4 JTCB: Approve the target and cyberspace strike package for tactical engagement and place on JIPTL
- P7 OPS-SYNC:
  - IT 7.1, IT 7.2 Deconflict and synchronize CO with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.5.1 Conduct Force Link up)
  - IT 7.2 Synchronize CO with other lethal/non-lethal operations (Ref 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)
  - IT 7.3 Providing updates/support to efforts spanning all phases of the Cyberspace Tasking Cycle
  - IT 7.4 Integrating legal services in support of planning and operations (Ref OP 4.4.7 Provide for legal services)

JFHQ-C MET 6 and MCFs

6.10 Conduct Joint Force Staff Operations

- P1 Cyberspace Tasking Cycle: Iterative, Cyclic process that allows staff officers to plan, execute, and assess CO
- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams: Properly organized teams following the Cyberspace Tasking Cycle will accomplish the staff actions needed to successfully employ CO
- P5 Operational Priorities and Intelligence Collection Priorities:
  - IT 5.1 PWG: Analyze demand signal from CERFs and command guidance against current and operational planning priorities
  - IT 5.2 CMWG: Develop intelligence collection guidance and priorities for ISR forces
  - IT 5.2 CMWG: Deconflict Command/SCC requirements

JFHQ-C MET 6 and MCFs

6.9 Provide Security (ACCM) Management & oversee STO/SAP operations

- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams:
  - IT 4.1 Establish ACCM management program
  - IT 4.2 Submit JTCRs to add STO/SAP missions to the MCOP and ITO (Ref TA 5.6.5.1 Coordinate Employment of Cyberspace Operations)

JFHQ-C MET 6 and MCFs

6.7 Coordinate Logistic Services

- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams: IT 4.1 Coordinate with USCC as required for logistic support (Ref TA 4 Perform Logistics and Combat Service Support, TA 4.2 Provide Sustainment)

6.8 Manage Personnel Accountability & Strength Reporting

- P3 (b)(3) 10 U.S.C. § 130e

JFHQ-C MET 6 and MCFs

6.4 Serve as the USCC Coordinating Authority to coordinate and deconflict deliberate mission scheduling for unattached, co-located CMF (Cont.)

- P7 OPS-SYNC: IT 7.1, IT 7.2 Deconflict and synchronize Operations with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)

6.5 Serve as the USCC Coordinating Authority to coordinate and deconflict time sensitive operations for unattached, co-located CMF, Ops Sync

- P3 (b)(3) 10 U.S.C. § 130e
- P7 OPS-SYNC: IT 7.1, IT 7.2 Deconflict and synchronize CO with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)

6.6 Prioritize Architecture and Capabilities Development and Requirements (ISO Task 4)

- IT 5.2 CMWG: Review and prioritize capability requirements; Deconflict Command/SCC requirements

JFHQ-C MET 6 and MCFs

6.3 Serve as the USCC Coordinating Authority facilitating as required, Service Component ADCON through local coordination of admin, logistics & support requirements for all co-located (attached and unattached) CMF

- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams: IT 4.1 Coordinate with USCC as required for administrative, logistic and operational support (Ref TA 4 Perform Logistics and Combat Service Support, TA 4.2 Provide Sustainment)

6.4 Serve as the USCC Coordinating Authority to coordinate and deconflict deliberate mission scheduling for unattached, co-located CMF

- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams: IT 4.2 Submit JTCRs to add CO missions to the MCOP and ITO (Ref TA 5.6.5.1 Coordinate Employment of Cyberspace Operations)

JFHQ-C MET 6 and MCFs

6.1 Plan, Direct, and Execute Exercises (Cont.)

- P6 Joint Targeting Cycle:
  - IT 6.1 TDWG: Develop targets through the intermediate stage and vet them with the IC
  - IT 6.2 JTWG: Nominate and approve entities of interest for target development, and conduct advanced target development of vetted targets
  - IT 6.3 Build cyberspace strike package to present at JTCM & JTCB
  - IT 6.4 JTCB: Approve the target and cyberspace strike package for tactical engagement and place on JIPTL

6.2 Provide Resource Management

- P1 Cyberspace Tasking Cycle:
  - IT 1.3 Deconflict infrastructure/Assets (Ref TA 5.6.5.1 Coordinate Employment on CO)
  - IT 1.5 Establish SPINs and TTPs to protect tradecraft and capabilities (Ref TA 6.8 Conduct Defensive Countermeasure Operations)
- P3 (b)(3) 10 U.S.C. § 130e
- IT 5.2 CMWG: Develop intelligence guidance and priorities for ISR forces

JFHQ-C MET 6 and MCFs

6.1 Plan, Direct, and Execute Exercises (Cont.)

- P1 Cyberspace Tasking Cycle: Plan, execute, and assess CO (Ref OP 4.4.5 Train Joint Forces and Personnel, OP 5.4.6 Conduct Operational Rehearsals)
- P3 (b)(3) 10 U.S.C. § 130e
- P7 OPS-SYNC:
  - IT 7.1, IT 7.2 Deconflict and synchronize CO with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.5.1 Conduct Force Link up)
  - IT 7.3 Identify cyberspace activity as neutral, friendly, or adversarial (Ref TA 6.5 Provide for Combat Identification)
  - IT 7.3 Disseminate I&W and operational assessment information (Ref TA 2.4 Disseminate Tactical Warning Information and Attack Assessments)

JFHQ-C MET 6 and MCFs

- Coordinate JFHQ-C support functions for attached and for co-located CMF with USCC, NSA, service and functional components; direct CMF training, exercises, and readiness requirements.
- Mission Critical Functions (MCF):

  6.1 Plan, Direct, and Execute Exercises
  - P4 Planning Teams:
    - IT 4.1 Use intelligence reports to shape operational plans (Ref TA 2 Share Intelligence)
    - IT 4.1 Establish primacy on cyberspace assets/devices (Ref TA 6.5 Provide for Combat Identification)
    - IT 4.2 Establish SPINs and TTPs to protect tradecraft and capabilities (Ref TA 6.8 Conduct Defensive Countermeasure Operations)
  - P5 Operational Priorities and Intelligence Collection Priorities:
    - IT 5.1PWG: Analyze demand signal from CERFs and command guidance against current and operational planning priorities
    - IT 5.2 CMWG: Develop intelligence collection guidance and priorities for ISR forces

JFHQ-C MET 5 and MCFs (Cont.)

5.12 Conduct Intelligence Staff Operations

- P1 Cyberspace Tasking Cycle: Iterative, Cyclic process that allows intelligence staff officers to incorporate intelligence into plans and operations
- P5 Operational Priorities and Intelligence Collection Priorities:
  - IT 5.1 PWG: Analyze demand signal from CERFs and command guidance against current and operational planning priorities
  - IT 5.2 CMWG: Develop intelligence collection guidance and priorities for ISR forces

JFHQ-C MET 5 and MCFs (Cont.)

5.11Produce operational Intelligence

- P1 Cyberspace Tasking Cycle: Plan, execute, and assess Cyberspace ISR (Ref TA 1.2.5 Conduct Site Exploration)
- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams:
  - IT 4.1 Establish primacy on cyberspace assets/devices (Ref TA 6.5 Provide for Combat Identification)
  - IT 4.2 Establish SPINs and TTPs to protect tradecraft and capabilities (Ref TA 6.8 Conduct Defensive Countermeasure Operations)
- IT 5.2 CMWG: Develop intelligence collection guidance and priorities for ISR forces
- P7 OPS-SYNC: IT 7.3 Disseminate operational assessment information (Ref TA 2 Share Intelligence)

JFHQ-C MET 5 and MCFs (Cont.)

5.10 Provide SIGINT on Specified Targets

- P1 Cyberspace Tasking Cycle: Plan, execute and assess Cyberspace ISR (Ref TA 1.2.5 Conduct Site Exploration)
- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams:
  - IT 4.1 Establish primacy on cyberspace assets/devices (Ref TA 6.5 Provide for Combat Identification)
  - IT 4.2 Establish SPINs and TTPs to protect tradecraft and capabilities (Ref TA 6.8 Conduct Defensive Countermeasure Operations)
- IT 5.2 CMWG: Develop intelligence collection guidance and priorities for ISR forces

JFHQ-C MET 5 and MCFs (Cont.)

5.9 Conduct Single Source Exploitation

- P1 Cyberspace Tasking Cycle: Plan and conduct Cyberspace ISR (Ref OP 5.6.5.4 Conduct Computer Network Exploitation (CNE) Enabling Operations)
- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams:
  - IT 4.1 Establish primacy on cyberspace assets/devices (Ref TA 6.5 Provide for Combat Identification)
  - IT 4.2 Establish SPINs and TTPs to protect tradecraft and capabilities (Ref TA 6.8 Conduct Defensive Countermeasure Operations)
- P7 OPS-SYNC:
  - IT 7.1, IT 7.2 Deconflict and synchronize CO with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.5.1 Conduct Force Link up)
  - IT 7.3 Disseminate I&W and operational assessments (Ref TA 2.4 Disseminate Tactical Warning Information and Attack Assessments)

JFHQ-C MET 5 and MCFs (Cont.)

5.8 Conduct Cyberspace ISR (Cont.)

- P1 Cyberspace Tasking Cycle:
  - IT 1.5 Conduct Cyberspace ISR (Ref OP 5.6.5.4 Conduct Computer Network Exploitation (CNE) Enabling Operations)
- P7 OPS-SYNC:
  - IT 7.1, IT 7.2 Deconflict and synchronize CO with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.5.1 Conduct Force Link up)
  - IT 7.2 Synchronize CO with other lethal/non-lethal operations (Ref 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)
  - IT 7.3 Identify cyberspace activity as neutral, friendly, or adversarial (Ref TA 6.5 Provide for Combat Identification)
  - IT 7.3 Disseminate I&W and operational assessments (Ref TA 2.4 Disseminate Tactical Warning Information and Attack Assessments)

JFHQ-C MET 5 and MCFs (Cont.)

5.7 Develop Operational Targets (Cont.)

- P4 Planning Teams: IT 4.1 Conduct target system analysis on adversarial networks (Ref TA 2.3 Produce Imagery Target Graphics)
- P6 Joint Targeting Cycle:
  - IT 6.1 TDWG: Develop targets through the intermediate stage and vet them with the IC
  - IT 6.2 JTWG: Nominate and approve entities of interest for target development, and conduct advanced target development of vetted targets
  - IT 6.4 JTCM: Deconflict targets with the IC and Joint forces and coordinate cyberspace strike package
  - IT 6.4 JTCB: Approve the target for tactical engagement and place on JIPTL

5.8 Conduct Cyberspace ISR

- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams:
  - IT 4.1 Establish primacy on cyberspace assets/devices (Ref TA 6.5 Provide for Combat Identification)
  - IT 4.2 Establish SPINs and TTPs to protect tradecraft and capabilities (Ref TA 6.8 Conduct Defensive Countermeasure Operations)

JFHQ-C MET 5 and MCFs (Cont.)

5.6 Provide Intelligence Support to Plans, Operations, and Fires

- P1 Cyberspace Tasking Cycle: Iterative, Cyclic process that allows intelligence integration into the planning and execution of CO
- P4 Planning Teams:
  - IT 4.1 Use intelligence reports to shape operational plans (TA 2 Share Intelligence)
  - IT 4.1 Conduct target system analysis on adversarial networks (Ref TA 2.3 Produce Imagery Target Graphics)
  - IT 4.2 Digest MISREPs and intelligence reports and produce effects and tactical assessments (Ref OP 2.8.1 Provide Intelligence Support to Fires, OP 2.8.4 Provide Intelligence Support to Combat Assessments)
- P7 OPS-SYNC: IT 7.3 Disseminate I&W and operational assessments (Ref TA 2.4 Disseminate Tactical Warning Information and Attack Assessments)

JFHQ-C MET 5 and MCFs (Cont.)

5.4 Conduct Intelligence Preparation of the Battlefield (IPB)

- P1 Cyberspace Tasking Cycle: Plan and conduct Cyberspace ISR (Ref TA 1.2.5 Conduct Site Exploration)
- P4 Planning Teams: IT 4.1 Conduct target system analysis on adversary networks (Ref TA 2.3 Produce Imagery Target Graphics)

5.5 Gain & Maintain Situational Understanding

- P1 Cyberspace Tasking Cycle: Plan, execute and assess Cyberspace ISR (Ref OP 5.6.5.4 Conduct Computer Network Exploitation (CNE) Enabling Operations)
- P3 (b)(3) 10 U.S.C. § 130e
  (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams: IT 4.1 Use intelligence reports to shape operational plans (Ref TA 2 Share Intelligence)
- P7 OPS-SYNC:
  - IT 7.1 Deconflict and synchronize CO with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.5.1 Conduct Force Link up)
  - IT 7.2 Synchronize CO with other lethal/non-lethal operations (Ref 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower)
  - IT 7.3 Identify cyberspace activity as neutral, friendly, or adversarial (Ref TA 6.5 Provide for Combat Identification)
  - IT 7.3 Disseminate I&W and operational assessments (Ref TA 2.4 Disseminate Tactical Warning Information and Attack Assessments)

JFHQ-C MET 5 and MCFs (Cont.)

5.2 Direct Joint Intelligence Support Element (JISE) operations (Cont.)

- P7 OPS-SYNC: IT 7.1, IT 7.2 Synchronize and deconflict operations with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.6.5.1 Coordinate Employment of CNO)

5.3 Perform Collection Management (Planning & Prioritization, Requirements Management, & Tasking Cyber ISR Assets)

- P1 Cyberspace Tasking Cycle: IT 1.3 Allocation (Ref Op 3.1.2 Apportion Fires)
- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams:
  - IT 4.1 Establish primacy on cyberspace assets/devices (Ref TA 6.5 Provide for Combat Identification)
  - IT 4.2 Establish SPINs and TTPs to protect tradecraft and capabilities (Ref TA 6.8 Conduct Defensive Countermeasure Operations)
- IT 5.2 CMWG: Develop intelligence collection guidance and priorities for ISR forces
- P7 OPS-SYNC: IT 7.1, IT 7.2 Synchronize and deconflict operations with the IC and adjacent units (Ref TA 3.3 Coordinate Battlespace Maneuver and Integrate with Firepower, TA 5.6.5.1 Coordinate Employment of CNO)

JFHQ-C MET 5 and MCFs

- MET 5: Conduct intelligence operations; including managing CMF intelligence requirements and the collection, production, and dissemination of intelligence.
- Mission Critical Functions (MCF):

5.1 Process and exploit collected operational information

- P1 Cyberspace Tasking Cycle: Iterative, Cyclic process where intelligence drives operations
- P4 Planning Teams: IT 4.1 Use intelligence reports to shape operational plans (TA 2 Share Intelligence)

5.2 Direct Joint Intelligence Support Element (JISE) operations

- P1 Cyberspace Tasking Cycle: IT 1.3 Allocation (Ref Op 3.1.2 Apportion Fires)
- P3 (b)(3) 10 U.S.C. § 130e
- P4 Planning Teams:
  - IT 4.1 Establish primacy on cyberspace assets/devices (Ref TA 6.5 Provide for Combat Identification)
  - IT 4.2 Establish SPINs and TTPs to protect tradecraft and capabilities (Ref TA 6.8 Conduct Defensive Countermeasure Operations)
- IT 5.2 CMWG: Develop intelligence collection guidance and priorities for ISR forces

JFHQ-C MET 4 and MCFs

4.8 Coordinate with cryptologic enterprise elements (NSA)

- P4 Planning Teams:
  - IT 4.1 Conduct planning IAW the Joint Operation Planning Process (JOPP) outlined in JP 5-0 and coordinate with NSA as required to deconflict plans
  - IT 4.1 Establish primacy on cyberspace assets/devices (Ref TA 6.5 Provide for Combat Identification)
- P6 Joint Targeting Cycle:
  - IT 6.1 Develop targets and Vet them with the Interagency IAW CJCSI 3370.01
  - IT 6.4 Validate targets and cyberspace strike package at the JTCB IAW CJCSI 3370.01

JFHQ-C MET 6 and MCFs

6.11 Conduct command designated coordination operations

- P1 Cyberspace Tasking Cycle: Outlines B2C2WGs necessary to ensure proper coordination and integration with IC and adjacent/higher units
- IT 5.2 CMWG: Develop intelligence collection guidance and priorities for ISR forces, and Deconflict Command/SCC requirements
- P6 Joint Targeting Cycle:
  - IT 6.1 TDWG: Develop targets through the intermediate stage and vet them with the IC
  - IT 6.2 JTWG: Nominate and approve entities of interest for target development, and conduct advanced target development of vetted targets
  - IT 6.3 Build cyberspace strike package to present at JTCM & JTCB
  - IT 6.4 JTCB: Approve the target and cyberspace strike package for tactical engagement and place on JIPTL

JFHQ-C MET 6 and MCFs

6.12 Coordinate and direct weapon capability development

- P4 Planning Teams:
  - IT 4.1 Conduct target system analysis on adversarial networks (Ref TA 2.3 Produce Imagery Target Graphics)
  - IT 4.1, IT 4.2 Identify capability requirements and submit them for prioritization and development
  - IT 4.2 Conduct advanced target development (Weaponeering)
- IT 5.2 CMWG: Develop intelligence collection guidance and priorities for ISR forces, and Deconflict Command/SCC requirements

Way Ahead

- Staff IOC/FOC Certification Framework with Service Cyber Components
- Conduct Troops to Task analysis
- Either modify existing tactical actions contained in the UJTL to reflect CO or submit new TA for inclusion in the UJTL
- Develop individual "Joint Qualification Requirements"
- Feasibility of Support considerations
  - (b)(3) 10 U.S.C. § 130e
  - Work stations
  - Training support
  - Minimum systems & security requirements

Terms Of Reference

Terms of Reference

- Blowback – Assesses the potential risk of retribution from the target(s) if the operation is detected and attributed to USCYBERCOM; assesses the vulnerability of the GIG to potential cyber retribution
- Boards, Bureaus, Centers, Cells, and Working Groups (B2C2WG) – Staff functions for planning, coordinating, and prioritizing operations
- Capability Target Pairing (CTP) – CTP is a report required for the ELA waiver and ensures proper Operational Testing and Evaluation (OT&E)
- Cyberspace ISR – *"Cyberspace ISR includes ISR activities in cyberspace conducted to gather intelligence from target and adversary systems that may be required to support future operations, including OCO or DCO"* (JP 3-12)
- Cyberspace Effects Request Form (CERF) - The CERF is a format used to request operational support in the cyberspace domain
- (b)(3) 10 U.S.C. § 130e
- Collateral Effects Estimate (CEE) – Estimates the collateral effects of each target/capability pairing; first order effects on unintended targets involved with the operation are evaluated using the CEE logic

Terms of Reference (Cont.)

- Cyberspace Operations Directive (CyOD) – The CyOD focuses command activities on operational priorities across all three Lines of Operation (LOO), including DGO, DCO, and OCO and the Cyber Collection Guide (CCG) for the Operations Directorate
- Cyberspace Operational Preparation of the Environment (OPE) – OPE consists of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations
- Cyberspace Strike Package – The cyberspace strike package is the primary product presented to the chairman of the JTCB for the purpose of informing the Commander's decision regarding the execution of an operation
- Defensive Cyberspace Operations – Response Actions (DCO-RA) – Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend DoD cyberspace capabilities or other designated systems
- Evaluated Level of Assurance (ELA) – Established technical assurance levels that define criteria for OCO Technical Assurance Standards (TAS) evaluations (DoDI 3600.02)

Terms of Reference (Cont.)

- Integrated Tasking Order (ITO) – Articulates the taskings for Joint CO for a 24 hour period
- Intelligence Gain Loss (IGL) – Indentifies the intelligence gain and loss associated with target(s) and planned effects; Probability of Detection (PoD) and Probability of Attribution (PoA) are evaluated with regards to the operation and capability; Perceived PoA/PoD is also evaluated.
- Joint Collection Management Board (JCMB) – FO/GO decision board to review command priorities and discuss intelligence collection, access, and capability requirements; provide collection guidance, priorities, and direction for the employment of cyber forces; communicate prioritized requirements and synchronize collection actions supporting command planning and operations. The JCMB also identifies and prioritizes intelligence capacity and capability shortfalls.
- Joint Tactical Cyber Request (JTCR) – Specifies the timing and tempo of activities conducted in and through cyberspace to achieve the supported commander's objective(s)

Terms of Reference (Cont.)

- Master Cyber Operations Plan (MCOP) – The time-phased cyberspace operations scheme of maneuver for a minimum 72 hour period that synthesizes commander's guidance, desired effects, supported component's schemes of maneuver, available resources, and friendly and enemy capabilities
- No Foreign Policy Objection (NFPO) – Assesses the absence of any objections from the Department of State with relation to foreign policy
- Political Military Assessment (PMA) – Assess the potential political and military response to perceived or actual attribution of the operation as characterized in the order and TAB C to Appendix 16 to Annex C to an Order (Concept of Fires)
- Record of Fires – A comprehensive database of all executed cyberspace operations documentation (e.g. ITOs, MISREPs, MISUMs)
- Risk Assessment Report (RAR) – Assesses the risk associated with the design and operation of a particular capability
- Sub-elements – Those formally recognized parts of a larger organization (e.g. combat plans is a sub-element of an Air Operations Center)

Back Up Slides

Example JQR

		JOB QUALIFICATION STANDARD (JQS)									
		OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD									
				CERTIFICATION							
Critical Tasks	Task number	Core Tasks (*)	TASKS/KNOWLEDGE JQS TECHNICAL REFERENCE OBJECTIVE:	Start date	Completion Date	Trainee's Initials	Trainer's Initials	Certifying Official's Initials	Proficiency Codes

4. (U) OCO Mission Lead JQS Format

(U//~~FOUO~~) The OCO ML/MS JQS consist of tasks using the above format that will be assessed during UI and OJT periods prior to certification of candidate. The proficiency codes will designate the level of proficiency that will be measured for each task. Proficiency codes will also identify whether a task is either Knowledge and/or Performance based. Technical References and Objectives will be used as necessary to guide the candidates in determining recourses necessary and delivery methods of training needed to master a task. Failure to meet Core tasks identified in the JQS will constitute immediate certification failure and result in remediation and re-certification.

4.1 (U) JQS Categories

(~~S//REL~~) The following are the OCO ML/MS organizational categories for this JQS and are defined in the J38 CONOP and Master Training Plan.

CATEGORY	DESRIPTION
A	USCYBERCOM Joint Operations Center
B	Current Offensive Cyber Operations
C	Plans/Weapons & Tactics
D	Targeting
E	Assessments

4.2 (U//~~FOUO~~) Knowledge Tasks: Are to be fulfilled by researching the tasks and recording notes in the OJT Personal training record. Designated Qualified Battle Captains and or Mission Leads, as well as Staff SME can initial off on these tasks on the JQS within their mission area. Candidates are encouraged to thoroughly study tasks, training manuals and resources available. At the end of assigned training period, candidates will hand in completed JQS in preparation for final assessments and certification.

4.3 (U//~~FOUO~~) Performance Tasks: Are to be fulfilled by completing the action described on the JQS while under instruction (UI), OJT and supervised by primary trainee on shift. Nominees will record results and hours in OJT personal training record. When JQS tasks are completed successfully, the primary Qualified Battle Captains and or Mission Leads, as well as Staff Mission Area Subject Matter Experts (SME) will review the OJT personal training record and initial off on JQS.

4.4 (U//~~FOUO~~) On the Job Training (OJT). The OJT plan is designed around the JOC schedule.

a. 15 UI Shifts: Designed to train with certified individual on position assigned.
b. 3 Stand Alone Shifts: Weekend Day (Fri-Sun) on own individual basis. Work position to annotate any gaps not addressed in the previous 15 UI Shifts
c. 4 UI follow-on shifts: Work with certified individual as lead for assigned position to address any gaps not covered in the original 15 UI Shifts

Example JQR (Cont.)

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

		JOB QUALIFICATION STANDARD (JQS)								
		OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD								
				CERTIFICATION						
Critical Tasks	Task number	Core Tasks (T)	TASKS/KNOWLEDGE JQS TECHNICAL REFERENCE: OBJECTIVE	Standards	Completion Date	Trainee's Initials	Trainer's Initials	Certifying Official's Initials	Proficiency Codes

4.5 (~~S//REL~~) USCC JOC Security and Functional Access

(~~S//REL~~) All JOC OCO ML/MS candidates will check with the J38 Division SEL to verify that all security access and Phase I training is completed IAW J38 Individual Development Plan prior to starting JQS. Candidates are expected to validate that all mandatory annual and USSS training requirements are completed and updated to training records.

For Mandatory NSA Training see link below, confirm completion dates are updated to training records and JQS:

http://www.adet.nsa/adet_nesweb/Programs/Academic-Services/NSA-CSS-Mandatory-Training/military.cfm

Functional Access Requirements	Date
SID Obtained	
NSANET Account	
SIPRNET Account	
NIPRNET Account	
SIPR PKI Token	
NSANET IC PKI Certificates	
Create INTELINK account on all networks	
Register PKI w (b)(3) 10 U.S.C. § 130e	
Access to information portal (b)(3) 10 U.S.C. § 130e	
Set up email group and distri access	
Upload JOC OCO PKI Certificates	
Setup JOC C2 chat account access	
Annual Training: Use Go Connect for Ref)	

OVSC1000 Basic IO Training	
-CLAS1000 Elements of Classification and Marking	
OVSC 1500 (go ecampus)	
OPSE1301 OPSEC	
Red Tab Requirements:	
-CoS Intelligence Oversight Training	
Dual Authorities brief	
-OVSC 1100 (go VUport)	
OVSC 1800 (go ecampus)	
SIGINT Level B Requirement:	
- CRSKT/V0 Watch Isting Awareness	

4.6 Under Instruction (UI) Duty Shifts. Candidates will complete the training on this JQR/JQS with their assigned Trainer/Instructor in the following manner.

a. Complete prescribed UI duty shift assignments as the primary ML and or Mission Specialist (MS) with a qualified Mission Area Subject Matter Expert (SME). Your assigned trainer is:

X _____

Trainer's Signature & Date Entered Training

[JOB QUALIFICATION REQUIREMENT]

Example JQR (Cont.)

Critical Tasks	Task number	Core Tasks [*]	JOB QUALIFICATION STANDARD (JQS) OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD TASKS/KNOWLEDGE JQS: TECHNICAL REFERENCE: OBJECTIVE:	CERTIFICATION: Start date	Completion Date	Trainee's Initials	Trainer's Initials	Certifying Official's Initials	Proficiency Codes
			USCYBERCOM Joint Operations Center (1.0-1.1.2 with noted exceptions)						
OP1.2.5	2.0	*	Identify, recommend, and document processes and procedures to enable 24X7, JOC & OCO operation ISO CMDR USCC. JQS: 1.0 TR: JBS, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2a
OP1.2.5	2.24	*	Enforce information management and security controls JQS: 1.1 TR: JBS, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OP1.2.5	2.24	*	Establish adequate access controls to all OCO information based on principles of least privilege and need-to-know IAW Command classification guides. JQS: 1.1.0 TR: JBS, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2b
OP1.2.5	2.29.0		Evaluate effectiveness of all IT platforms for OCO (b)(3) 10 U.S.C. § 130e CERF, R2D2, J2T Portal) JQS: 1.1.1 TR: JBS, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2a
OP1.2.5	2.29.0	*	Execute USCC JOC Continuity of Operations (COOP) Plan JQS: 1.1.2 TR: JBS, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						4c

Example JQR (Cont.)

JOB QUALIFICATION STANDARD (JQS)
OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD

Critical Tasks	Task number	Core Tasks [*]	TASKS/KNOWLEDGE JQS: TECHNICAL REFERENCE: OBJECTIVE:	CERTIFICATION: Start date	Completion Date	Trainees Initials	Trainers Initials	Certifying Officials Initials	Proficiency Codes
			Current Offensive Cyber Operations(2.0-2.5.6.3 with noted exception:)						
OP1.2.5 OP3.1.2 OP3.1.2	2.3.0 5.0.0 5.1.0 5.1.1		Generate, route and maintain SA on all OCO orders coming into or sent from USCYBERCOM (FRAGOS, OPORDS, EXORDS) JQS: 2.0 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1.2.5	2.23.1		Make recommendations to the Cyber Battle Captain on OPR for CERF entries. (i.e. than 180 = JS; than 180 J35) JQS: 2.1 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OP1.2.5	2.4.0		Generate and Approve Daily SPINS that accompany ITO JQS: 2.2 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1.2.5	2.1.0		Maintain Situational Awareness and Manage IT platforms for the JOC & OCO (b)(3) 10 U.S.C. § 130e CERF, R2D2, J2T Portal) JQS: 2.3 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OP1.2.5	2.1.0	+	Maintain Situational Awareness and Manage USCYBERCOMMAND JOC Portal JQS: 2.3.0 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1.2.5	2.1.0	+	Maintain Situational Awareness and Manage (b)(3) 10 U.S.C. § 130e JQS: 2.3.1 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						4d
OP1.2.5	2.1.0		Maintain Situational Awareness and Manage the Cyber Effects Request Form (CERF)Portal JQS: 2.3.2 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						4c
OP1.2.5	2.1.0		Maintain Situational Awareness for the Operational Data Analysis Tool (ODAT) JQS: 2.3.3 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2b

Example JQR (Cont.)

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

		JOB QUALIFICATION STANDARD (JQS)									
		OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD									
				CERTIFICATION							
Critical Tasks	Task number	Core Tasks [*]	TASKS/KNOWLEDGE JQS: TECHNICAL REFERENCE: OBJECTIVE:	Start date	Completion Date	Trainee's Initials	Trainer's Initials	Certifying Official's Initials	Proficiency Codes
OPI 2.5	2.1.0		Maintain Situational Awareness for the 624th OC R2D2 Portal JQS: 2.3.4 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2b
OPI 2.5	2.1.0		Maintain Situational Awareness for the Cyber Common Operating Picture (CyberCOP) Portal JQS: 2.3.5 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OPI 2.5	2.1.0		Maintain familiarization with J2W, DCO, DGO & NTOC IT platforms and products that support current operations. JQS: 2.3.6 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2a
OPI	1.0		Execute and enforce detailed IO CNO operational related Plans and orders and requirements at an operational level. JQS: 2.4 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OPI	1.0.0		Act as J38 Chief in his/her absence (Aligned with the Commander's intent) JQS: 2.4.0 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OPI	1.0.1	*	Enforce and Execute the Integrated Tasking Order JQS: 2.4.1 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						4c
OPI	1.2.2	*	Issue ITO to subordinate units and partners for execution JQS: 2.4.1.0 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						4c

Example JQR (Cont.)

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

			JOB QUALIFICATION STANDARD (JQS) OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD	CERTIFICATION					
Critical Tasks	Task number	Core Tasks (*)	TASKS/KNOWLEDGE JQS: TECHNICAL REFERENCE: OBJECTIVE:	Start date	Completion Date	Trainee's Initials	Trainer's Initials	Certifying Official's Initials	Proficiency Codes
OP1.2.5 OP3.1.2	2.5.0 5.0.1	*	Manage and Maintain QA of Integrated Tasking Order (ITO) JQS: 2.4.1.1 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1.2.5	2.17.1	*	Direct post execution assessment and reporting of ITO actions JQS: 2.4.1.2 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						4c
OP1.2.5	2.7.1	*	Assess ITO actions according to indications and warnings JQS: 2.4.1.3 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						4c
OP1.2.5	2.8.1	*	Coordinate ITO actions according to indications and warnings JQS: 2.4.1.4 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						4c
OP1.2.5	2.17.0	*	Execute ITO actions according to indications and warnings JQS: 2.4.1.5 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						4c
OP1.2.5	2.9		Assist the JOC CBC in developing a common operational picture (COP). JQS: 2.5 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OP1.2.5	2.19.0	*	Report to leadership if Commander Critical Information Requirement has been met and submit CCIRs when necessary. JQS: 2.5.0 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						4c

Example JQR (Cont.)

		JOB QUALIFICATION STANDARD (JQS) OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD								
				CERTIFICATION						
Critical Tasks	Task number	Core Tasks [*]	TASKS/KNOWLEDGE JQS: TECHNICAL REFERENCE: OBJECTIVE:	Start date	Completion Date	Trainee's Initials	Trainer's Initials	Certifying Official's Initials	Proficiency Codes
OP1.2.5	2.9		Submit or respond to requests for de-confliction of CNO operations. JQS: 2.5.1 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2b
OP1.2.5	2.11	*	Initiate Briefs and Reports on adversarial and friendly situations. JQS: 2.5.2 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1.2.5	2.12.0		Send weekly SITREP from USCYBERCOM to the JIATF that explains past weeks Offensive Cyber Operations. JQS: 2.5.3 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2c
OP1.2.5	2.13.0		Host Ops Synchronization Meeting; meeting designed for all parties to synchronize operations. JQS: 2.5.4 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2c
OP1	1.2	*	Establish and maintain positive control of Cyber Forces. JQS: 2.5.5 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1.2.5	2.21		Maintain relationships with USCC Directorates, DoD Components, Intelligence Agencies, Law Enforcement (LE), US Government and partner organizations involved in cyber planning or other related mission areas. JQS: 2.5.5.0 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2b
OP1.2.5	2.21		Coordinate with USCC Directorates, DoD Components, Intelligence Agencies, Law Enforcement (LE), US Government and partner organizations. JQS: 2.5.5.1 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2b

Example JQR

		JOB QUALIFICATION STANDARD (JQS)								
		OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD								
				CERTIFICATION						
Critical Tasks	Task number	Core Tasks [*]	TASKS/KNOWLEDGE JQS: TECHNICAL REFERENCE: OBJECTIVE:	Start date	Completion Date	Trainee's Initials	Trainer's Initials	Certifying Official's Initials	Proficiency Codes
OP1	1.2.0 1.1.2	*	Identify and illustrate the TACON and OPCON USCC Cyber Force Structure and relationships. JQS: 2.5.5.2 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1	1.1.4	*	Establish ALERTCON Status with USCC controlled firing units. JQS: 2.5.5.3 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1	1.1.5	*	Recommend Changes of ALERTCON Status for USCC controlled firing units. JQS: 2.5.5.4 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1	1.2.0	*	Maintain Operational control during of firing units during Title 50 and Title 10 operations. JQS: 2.5.5.5 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3
OP1	1.1 1.2	*	Establish and maintain operational communications. JQS: 2.5.6 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OP1	1.1.0	*	Establish and maintain operational communications with Subordinate OP Center. JQS: 2.5.6.0 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2b
OP1	1.1.1 1.1.3	*	Establish and maintain operational communications with Firing Units, Service Components and COCOM CSE JQS: 2.5.6.1 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c

Example JQR (Cont.)

Critical Tasks	Task number	Core Tasks [*]	JOB QUALIFICATION STANDARD (JQS) OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD TASKS/KNOWLEDGE JQS: TECHNICAL REFERENCE: OBJECTIVE:	CERTIFICATION Start date	Completion Date	Trainee's Initials	Trainer's Initials	Certifying Official's Initials	Proficiency Codes
OP1	1.1.2	*	Initiate communications with units TACON to USCYBERCOM. JQS: 2.5.6.2 TR: J3S. JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1	1.2.0	*	Initiate communications subordinate commands OPCON to USCYBERCOM. JQS: 2.5.6.3 TR: J3S. JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2b
			Plans/Weapons & Tactics (3.0-3.90 with noted exceptions)						
OP1.2.5	2.2		**Execute and maintain deliberate, dynamic and /or crisis plans TSP/TST.** JQS: 3.0 TR: J3S. JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2b
OP2.S	3.4.1	*	Monitor indications and warnings WRT Intel triggers to support ITO actions. JQS: 3.1 TR: J3S. JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1.2.5	3.5.1	*	Through the CSE, make sure current day's executions are in line with COCOM CDR's objectives. JQS: 3.2 TR: J3S. JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c
OP1.2.5	2.23.0		Maintain Situational Awareness of current events throughout the globe and be prepared to support effective delivery of Cyber Effects Request Process (CERF). JQS: 3.3 TR: J3S. JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2c
OP1.2.5	2.20		Implement and evaluate a course of action to address a declared significant cyber event. JQS: 3.4 TR: J3S. JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2c

Example JQR (Cont.)

		JOB QUALIFICATION STANDARD (JQS)									
		OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD									
				CERTIFICATION							
Critical Tasks	Task number	Core Tasks [*]	TASKS/KNOWLEDGE JQS: TECHNICAL REFERENCE: OBJECTIVE:	Start date	Completion Date	Trainee's Initials	Trainer's Initials	Certifying Official's Initials	Proficiency Codes
OP1	1.1.6	*	Initiate Recall procedures in response to TSP/TST, Crisis Action. JQS: 3.5 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2c
OP1.2.5 OP3.1.6	2.2.0 2.6.0 6.1.1		Execute Pre-Approved Actions (PAA's) at moment's notice. JQS: 3.6 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2a
OP1.2.5	2.2.1		Build out communications plans as TSP/TST, crisis action situations arise. JQS: 3.7 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2b
OP3	4.3		Oversee and Assist in operational utilization and employment of weapons and capabilities. JQS: 3.8 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OP1.2.5	2.16		Maintain timely SA of imminent or hostile adversarial intentions or activities—to include adversarial intentions to conduct computer network attack (CNA)—which may impact the command's OCO mission, resources, or capabilities. JQS: 3.8.0 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OP3	4.4.0	*	Maintain Situational Awareness of capabilities available for title 10 actions and what effects these capabilities can be paired to do. JQS: 3.8.1 TR: J3S, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3c

Example JQR (Cont.)

		JOB QUALIFICATION STANDARD (JQS) OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD									
					CERTIFICATION						
Critical Tasks	Task number	Core Tasks [*]	TASKS/KNOWLEDGE JQS: TECHNICAL REFERENCE: OBJECTIVE:		Start date	Completion Date	Trainee's Initials	Trainer's Initials	Certifying Official's Initials	Proficiency Codes
OP3	4.3.0	+	Maintain situational awareness TTPs and capability to effects pairing. JQS: 3.8.2 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							2a
OP3	4.1.0		Assist J38 Plans and Targeting branches in target to effects pairing. JQS: 3.8.3 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							2b
OP1.2.5	2.30	+	Review security assessment reports, OPSEC and configuration management concerns of OCO infrastructures and capabilities. Oversee capability development to ensure the capability meets USCYBERCOM requirements. JQS: 3.8.4 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							3c
OP1.2.5	2.25		Prepare for and participate in exercises and mission war games. JQS: 3.9 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							3a
OP1.2.5	2.26		Participate in TTX and war gaming efforts JQS: 3.9.0 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							2a
OP1.2.5	2.27		Participate in command exercises and provide feedback via after action reports. JQS: 3.9.1 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							3b
OP1.2.5	2.28		Provide input (verbal or written) to lessons learned document that conveys results of missions, exercises, or war gaming activities. JQS: 3.9.0 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							3b

Example JQR (Cont.)

		JOB QUALIFICATION STANDARD (JQS)									
		OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD									
					CERTIFICATION						
Critical Tasks	Task number	Core Tasks [*]	TASKS/KNOWLEDGE JQS: TECHNICAL REFERENCE: OBJECTIVE:		Start date	Completion Date	Trainees Initials	Trainers Initials	Certifying Official's Initials	Proficiency Codes
			Targeting (4.0-4.0.3 with noted exceptions)							
OP3	4.0		**Gather data to support the synchronization of non-kinetic effects into the joint targeting cycle.** JQS: 4.0 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							5b
OP3	4.0.0	*	Maintain situational awareness of the target development and maintenance cycle on existing target folders and generation of new target packages. JQS: 4.0.1 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							3c
OP2.8	3.1.0	*	With assistance of the J2W submit RFI's for further information on current situation, target information, HVI, and HVT's JQS: 4.0.2 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							5c
OP2.8	3.4.0		Maintain Situational Awareness of all targets approved, nominated, and what status in the targeting cycle they are at any given time. JQS: 4.0.3 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							2a
OP2.8	3.3.1	*	Maintain Situational Awareness of the IO production and approval chain to support CSE in theater. Identify suspense time of IO production and approval in order for firing units to host/replace IO, etc. JQS: 4.0.3 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD							4c

Example JQR (Cont.)

			JOB QUALIFICATION STANDARD (JQS) OFFENSIVE CYBER OPERATIONS (OCO) MISSION LEAD	CERTIFICATION						
Critical Tasks	Task number	Core Tasks [*]	TASKS/KNOWLEDGE JQS: TECHNICAL REFERENCE: OBJECTIVE:	Start date	Completion Date	Trainee's Initials	Trainer's Initials	Certifying Official's Initials	Proficiency Codes
			Assessment: (5.0-5.0.3 with noted exception)						
OP2.8	3.2		Validate intelligence estimates to support the planning cycle. JQS: 5.0 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OP2.8	3.5.1	*	Establish and maintain communications with pier ops centers pertaining to OCO (GOC, NTOC, NSOC, ROC, COCOM Op centers) JQS: 5.0.0 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OP3.1.6	6.5.0		Maintain Situational Awareness of all CNE operations in support of USCC title 10 actions. JQS: 5.0.1 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OP3.1.6	6.0.0	*	Provide Combat Assessment Reports (BDA, MOP, & MEA). JQS: 5.0.2 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2a
OP3.1.6	6.0.1		Oversee Assessment Plan generation and implementation. JQS: 5.0.3 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2a
OP3.1.6	6.2.2		Review capability assessments for capability to effects pairing JQS: 5.0.4 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2a
OP3.1.6	6.4.0		Oversee and make recommendations for capability to effects pairing. JQS: 5.0.5 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2a
OP3.1.6	6.2.0		Evaluate attack and re-attack recommendations using (BDA, MOP, MEA) data. JQS: 5.0.6 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2a
OP3.1.6	6.1.0	*	Maintain situational awareness and propose recommendations using (BDA, MOP, MEA) data. JQS: 5.0.7 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						3b
OP3.1.6	6.2.1		Assess Pre-Approved Actions (PAA's) against CIPE assessments and courses of actions in keeping with mission objectives and authorities JQS: 5.0.8 TR: J38, JOC & OCO CONOP & MTR (b)(3) 10 U.S.C. § 130e OJT OBJ: QT TBD						2a

Example JQR (Cont.)

QUALITATIVE TERMINOLOGY	
CONDITION	
WITH REFERENCE	Individual may reference applicable training references.
WITHOUT REFERENCE	Individual may not utilize training references.
STANDARD	
WITH MINIMAL ERROR	Individual may make minimal errors that do not alter the stated task objective.
WITHOUT ERROR	No error may be committed

JQR VALUE SCALE	DEFINITION: The Individual Proficiency Codes	
*TASK PERFORMANCE LEVELS	1	Can do simple parts of the task. Needs to be held or shown how to do most of the task. (EXTREMELY LIMITED)
	2	Can do most parts of the task. Needs help only on hardest parts. May not meet load demands for speed or accuracy. (PARTILLY PROFICIENT)
	3	Can do all parts of the task. Needs help only a spot check of completed work. Meets minimum load demands for speed and accuracy. (COMPETENT)
	4	Can do the complete task quickly and accurately. Can tell or show others how to do the task. (HIGHLY PROFICIENT)
**TASK KNOWLEDGE LEVELS	a	Can name parts, tools and simple facts about the task. (NOMENCLATURE)
	b	Can determine step-by-step procedures for doing the task. (PROCEDURES)
	c	Can explain why and when the task must be done and why each step is needed. (OPERATING PRINCIPLES)
	d	Can predict, identify, and resolve problems about the task. (ADVANCED THEORY)
EXPLANATION		
*A task knowledge scale value may be used alone or with a task performance scale to define a level of knowledge for a specific task. (Example: b and 1b)		