Sec. 342 Report on Joint Strategy for Readiness and Training in a Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Denied Environment.

(U) In Section 342 of The National Defense Authorization Act for Fiscal Year 2013 (Public Law 112-239), Congress required that the Secretary of Defense (SECDEF), in consultation with the Chairman of the Joint Chiefs of Staff (CJCS), submit "a report on the readiness of the joint force to conduct operations" in a C4ISR denied environment including "a description of the steps taken and planned to be taken..." with respect to six specific topic areas:

a. (U) Identify threats to include weapons and those states with such capabilities.

(U) Threats to and vulnerabilities of C4ISR systems are documented in System Threat Assessment Reports (STAR) and other classified documents, and can be provided upon request for specific systems. Additionally, Combatant Commanders (CCDRs) maintain listings of regional or mission-specific threats and vulnerabilities. Broadly, any potential adversary represents a threat to permissive C4ISR.

b. (U) Vulnerabilities of your C4ISR systems.

(U) As reported in item (a), threats to and vulnerabilities of C4ISR systems are catalogued in System Threat Assessment Reports (STAR) and can be provided upon request for specific systems.

c. (U) How do you reconstitute those systems and prevent further denial and counter-attack capabilities?

(U) CCDRS and their staffs spend many man-hours reviewing their Operation and Contingency Plans, developing frameworks and procedures for using alternative methods, diversifying communications paths and media, and pursuing the ability to use distributed operations in a denied environment. As CCDRs identify these vulnerabilities and dependencies, they develop tactics, techniques, and procedures (TTP) for operating or restoring nets in C4ISR denied environments.

d. (U) Types of joint operations that would be feasible in a denied environment

(U) Services and CCDRs organize, train, and equip to operate in a degraded environment. Specifically, the DoD, at every level, trains in multiple exercises every year to hone operations and conduct various military missions, from peacekeeping through strategic operations, in degraded environments.

Additional studies, such as "Resilient Basis for Satellite in Joint Operations (S)", also address the threats, vulnerabilities, ability to reconstitute, and the feasibility of joint operations in a SATCOM denied environment.

e. (U) Training and exercise opportunities you have used to support sustained operations in denied environments.

(U) The CJCS has directed all CCDRs to integrate objectives into exercises that promote development of operations in realistic environments, including denied environments. Additionally, each of the CCDRs has internal exercises to focus on their mission specific areas of concern.

f. (U) TTP changes you have developed to support denied environment operations

(U) The CJCS has directed all the CCDRs to execute exercises in realistic environments, including denied environments. Scope and impact of these objectives continue to mature over time, with annual reports on exercise effectiveness, lessons learned, and recommendations for future exercises. All of these activities feed directly into TTP development and refinement.

(U) The SECDEF, through the CJCS, has tasked the Combatant Commanders (CCDRs) and Services in a separate EXORD to provide a detailed denied cyber assessment in the Spring of 2014, therefore this report does not cover cyber vulnerabilities of C4ISR.

(U) Additional information regarding each of the topic areas above is provided in the attached classified annex.