



# CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

---

J-6

DISTRIBUTION: A, B, C, J, S

CJCSI 3401.03A

15 July 2003

## INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND) JOINT QUARTERLY READINESS REVIEW (JQRR) METRICS

Reference: See Enclosure F.

1. Purpose. This instruction provides standardized information assurance (IA) and computer network defense (CND) metrics and supplemental joint policy guidance to support DOD organizations' self-assessment of their IA and CND status for readiness reporting (JQRR or other forums), determining resource requirements, and conducting risk assessments.
2. Cancellation. CJCSI 3401.03, 15 October 2002, "Information Assurance (IA) and Computer Network Defense (CND) Joint Quarterly Readiness Review (JQRR) Metrics," is canceled.
3. Applicability. This instruction applies to the Joint Staff, combatant commands, Services, and the following DOD combat support agencies: Defense Intelligence Agency (DIA), Defense Information Systems Agency (DISA), Defense Logistics Agency (DLA), National Imagery and Mapping Agency (NIMA), National Security Agency (NSA), Defense Threat Reduction Agency and Defense Contracting Management Agency.
4. Policy. See Enclosure A.
5. Definitions. See Glossary.
6. Responsibilities. See Enclosure B.
7. Summary of Changes. This administrative update is required in order to:
  - a. Align instruction language with CJCSI 3401.01, "Chairman's Readiness System" (reference a).

b. Update metric references, definitions and terminology based on publication of DOD Directive 8500.1, "Information Assurance (IA)" (reference c) DOD Instruction 8500.2, "Information Assurance (IA) Implementation" (reference d) and CJCSM 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND) (reference h)."

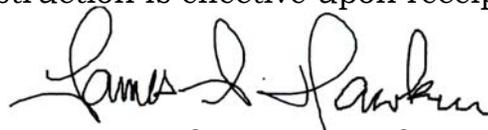
c. Provide task references for IA and CND metrics from the Universal Joint Task List (UJTL) (reference b).

d. Update instruction based on CND mission transfer to USSTRATCOM from USSPACECOM under Unified Command Plan (UCP) change.

e. Remove "For Official Use Only" marking from instruction to ensure wider distribution.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--  
<http://www.dtic.mil/doctrine>. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This instruction is effective upon receipt.



JAMES A. HAWKINS  
Major General, USAF  
Vice Director, Joint Staff

Enclosures:

- A -- Policy
- B -- Responsibilities
- C -- Information Assurance (IA) and Computer Network Defense (CND) Metrics
- D -- Information Assurance (IA) and Computer Network Defense (CND) Metrics - Optional
- E -- Intelligence Metrics Supporting IA and CND - Optional
- F -- References
- GL -- Glossary

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	<u>Copies</u>
.....	
Commandant, Joint Forces Staff College.....	2
Director, Joint Warfighting Center .....	2

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for CJCSI 3401.03A. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE
1 thru 2	O
i thru viii	O
A-1 thru A-6	O
B-1 thru B-2	O
C-1 thru C-12	O
D-1 thru D-52	O
E-1 thru E-14	O
F-1 thru F-2	O
GL-1 thru GL-10	O

(INTENTIONALLY BLANK)



(INTENTIONALLY BLANK)

TABLE OF CONTENTS

	PAGE
ENCLOSURE A--POLICY	
Purpose .....	A-1
Scope .....	A-1
General .....	A-1
Application .....	A-2
Reporting Examples.....	A-4
Classification.....	A-6
 ENCLOSURE B--RESPONSIBILITIES .....	 B-1
 ENCLOSURE C--Information Assurance (IA) AND Computer Network Defense (CND) METRICS.....	 C-1
 ENCLOSURE D--INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND) METRICS – OPTIONAL.....	 D-1
 ENCLOSURE E--INTELLIGENCE METRICS SUPPORTING IA AND CND – OPTIONAL .....	 E-1
 ENCLOSURE F--REFERENCES .....	 F-1
 GLOSSARY	
PART I--ABBREVIATIONS AND ACRONYMS .....	GL-1
PART II--DEFINITIONS .....	GL-5

(INTENTIONALLY BLANK)

## ENCLOSURE A

### POLICY

1. Purpose. This instruction provides standardized IA and CND metrics to consider in support of component readiness reporting, training program development, equipment acquisition, and risk assessments. Combatant commands and combat support agencies will use the core metrics (Enclosure C) in conjunction with preparing the IA and CND portion of their JQRR reports. The portion of the metrics focused on information systems and computer networks will also be used in assessing CND mission and IA readiness.
  
2. Scope. The Chairman's Readiness System is designed to provide DOD leadership a current, macro-level assessment of the military's readiness to execute the National Military Strategy as assessed by the combatant commanders, Services, and agencies. The assessment is presented to the Vice Chairman of the Joint Chiefs of Staff and Service OpsDepts in a briefing presented by the Services, US Special Operations Command and the Joint Staff.
  
3. General
  - a. The Defense Information Infrastructure has evolved into a complex Global Information Grid (GIG) of various information processing and distribution systems that are monitored and controlled by different organizations from geographically dispersed locations. To attain information superiority, we must significantly improve our capabilities for comprehensive and sustained network awareness and management.
  
  - b. Network Operations (NETOPS) is a concept that will enable us to meet these needs by means of the standardized organizational and operational integration of Network Management, Information Dissemination Management and IA.
  
  - c. IA is focused on protecting and assuring security of information and information systems. IA secures information and information systems to ensure the continued availability of accurate, relevant, and timely information to the required recipient and prevent its dissemination to our adversaries. IA incorporates protection, detection, response, restoration, and reaction capabilities and processes to shield and preserve information and information systems. The fundamental attributes of information assurance include:

(1) Availability: Employment of capabilities and processes ensuring timely and reliable access to data and services for authorized users.

(2) Authentication: Employment of security measures designed to establish the validity of a transmission, message, or originator, or as a means of verifying an individual's authorization to receive specific categories of information.

(3) Confidentiality: Employment of capabilities to assure that information is not disclosed to unauthorized persons, processes, or devices.

(4) Integrity: Employment of capabilities to protect against unauthorized modification or destruction of information.

(5) Nonrepudiation: Employment of capabilities and processes to assure the sender of the data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

d. IA for DOD information and information systems requires a defense-in-depth strategy that integrates the capabilities of people, operations, and technology to establish multilayer and multidimensional protection to ensure survivability and mission accomplishment.

e. CND is the operational component of IA focused on actions to protect, monitor, analyze, detect and respond to unauthorized activity within DOD computer networks. CND provides operational guidance to IA elements (people, processes, and technology) based on a risk assessment of ongoing military operational requirements, and potential threats and ongoing unauthorized activity to our computer networks. IA capabilities and measures are then modified to internally protect and defend our computer networks based on CND operational guidance.

f. The enclosed metrics lists will assist in the operational assessment of the CND mission area and IA.

#### 4. Application

a. Enclosure C is designed to help combatant commanders and combat support agencies conduct operational IA and CND assessments that can be used to support reporting of C4 deficiencies in the JQRR as well as determine other resource and training requirements. Enclosure C provides a small set of "core" metrics to be considered during the full

15 July 2003

JQRR cycle (Jan and July) providing a macro-level assessment of IA and CND readiness. Enclosures D and E are optional and are provided to furnish greater depth and possible unique areas to commanders' assessments or for specific JQRR scenarios.

(1) Enclosure C will assist in developing IA and CND assessments and strengthen the process by providing a list of IA and CND parameters to consider when deriving conclusions about IA and CND readiness. This guide will be used as the minimal core metrics for C4 IA and CND reporting.

(2) Common measurements should help enable components to conduct comprehensive IA and CND assessments. The consideration by combatant commanders, Services, and agencies of the same areas will help aggregate submissions and therefore (1) make better resource decisions at this level and (2) evaluate a reported shortfall worldwide.

b. The use of all the lists will also help with IA and CND readiness self-assessment and identifying resource shortfalls. Organizational use of the enclosed metrics, and linkage of deficiencies to either degraded joint mission essential tasks (reference b) or degraded agency mission essential tasks, can provide a snapshot status of current readiness and IA and CND deficiencies. Over time, this can develop into a chronology of shortfalls that indicate trends. This will allow organizations to make more informed resource decisions when addressing IA and CND readiness.

c. Application. The core metrics will be used to support IA and CND readiness assessments. Assessment of each IA and CND major area should be based on current operational requirements and threat environment, not on desired future capabilities or threats.

d. Each category is divided into subcategories with a space for assignment of a M-level, as defined in reference a.

(1) Combatant commands and combat support agencies should complete these metric assessments each full JQRR cycle (Jan and July) and retain it locally as a chronological record of IA and CND readiness.

(2) Combatant commands and combat support agencies should identify appropriate baseline (e.g., baseline number of personnel or equipment for a metric) for each metric criteria to meet their specific conditions based on DOD and organization requirements.

(3) Combatant commands and combat support agencies should determine M-level based on ability to meet IA and CND mission requirements of the given JQRR scenario, supported in large measure by accomplishing metric evaluations outlined in Enclosures C, D, and E.

(4) These enclosures can also be expanded locally to include additional metrics and criteria for other C4 and NETOPS mission areas.

e. Metric Statements and Criteria

(1) Metrics are derived from policy, guidance and requirements outlined in DOD directives and instructions (references c, d, e, and f); and Joint Staff publications (references g and h).

(2) Metrics have either numerical criterion or criteria based on an objective level that includes a subjective assessment on impact to accomplish required missions.

(3) Subjective assessment will be based on reference a.

5. Reporting Examples

a. Examples of readiness evaluated (subparagraphs) within IA and CND paragraph for full JQRR cycle (Jan and July) are shown as follows:

(1) Personnel metrics - 1.1.1: 81% (M-2) and 1.2.1: 71% (M-3).

(2) Training metrics - 2.1.1: 72% (M-3) and 2.2.1: 95% (M-1).

(3) Operations metrics - 3.1.1 (M-1), 3.1.2 (M-2), 3.2.1 (M-2) and 3.2.2 (M-2).

(4) Technology (equipment) metrics - 4.1.1 (M-1), 4.2.1 (M-3) and 4.2.2 (M-2).

(5) Intelligence metrics - 6.1.1 (M-2).

b. The following examples of deficiencies are provided in the context of paragraph (5) C4 of JQRR reporting format. The following examples could have been used by an organization to determine a M-level change for C4 functional area of M-3 indicating significant IA and CND deficiencies that prevent the organization from performing some portions of required missions:

15 July 2003

(1) Number of networks and systems with monitoring tools sufficient (Metric 4.2.1.). **“Lack of network information protection and intrusion detection systems (IDS). Unclassified and classified computer networks are vulnerable to computer network attack (CNA), which could cause loss of critical information or capabilities. This loss of critical information or capabilities will impact on ability to provide theater strategic command and control, employ theater strategic firepower and forces, sustain theater forces and operate and manage theater communications and information systems. In support of recent operations 25 (30%) sites did not have basic tools to implement a minimum level of security on deployed networks and 24 (29%) did not have an IDS. Networks were not protected against intrusions and other network vulnerabilities (internal or external intrusions, viruses, malicious code, etc.) To rectify this shortage would cost \$2,500,000 for 25 information protection tool packages. Failure to correct this deficiency will prevent this command from performing required missions to coordinate theater-wide activities and take actions to protect and defend information and information systems in support of OPLAN XXXX.”**

(2) IA professional (IAO, IAM, CERT, or other IA professionals) sufficiently assigned to accomplish missions (Metric 1.2.1). **“Information assurance (computer network defense) personnel/manpower shortages. Impact: A low ratio of available personnel to mission requirements in information assurance, computer network defense, and computer emergency response teams (CERT) personnel. Combatant command IA/CND and CERT positions are manned at 74% and 68%, respectively. Filling combatant command IA, CND and CERT positions is critical due to significant training and qualification increasing the lag time to fill a billet. Failure to resolve this deficiency will prevent this command’s ability to ensure adequate coverage of systems handling information that is determined to be vital to the mission effectiveness of deployed and contingency forces for JQRR scenario. The consequences of loss of integrity or availability of these Mission Assurance Category I systems are unacceptable and could include the immediate and sustained loss of mission effectiveness.”**

(3) Number of secure voice equipment (e.g., secure telephone unit (STU)-III or secure telephone equipment (STE)) on-hand as percentage of required (Metric 4.4.2). **“Insufficient secure voice capability. During current operations, there was insufficient secure voice capability between US force units and allied/coalition forces. Although Service components quickly purchased 68 STU-III(s), this was insufficient (66% of required) to provide required secure voice**

15 July 2003

**capability. Allied/coalition partners also lacked sufficient numbers (34 additional required) of secure instruments. These shortages resulted in numerous operations security (OPSEC) violations. Many CONUS deploying units are purchasing the new secure equipment, which is not interoperable with releasable allied/coalition secure instruments. Failure to fix this deficiency will prevent coordination of military operations with key nodes for 3 coalition nations vital to OPLAN XXXX. COMSEC violations could place expected operational missions at risk of failure preventing successful completion of specific tasks.”** Note: This is an example of an optional metric (Metric 4.4.2) being used based on component determined deficiency area impacting on required missions.

c. An assessment using metrics may identify deficiencies, but not to the level warranting reporting in JQRR. However, maintaining metric results internally and providing courtesy copy separately to the Joint Staff, J-6 will assist local organizations, DOD and USSTRATCOM in identifying overall trends and prioritize resources for combatant commands, Services and Defense Agencies before deficiencies reach a level that could impact mission accomplishment.

d. IA and CND personnel and manpower deficiencies will be reported in the joint personnel functional area or linked to appropriate JMET degradation.

e. Intelligence deficiencies impacting on IA and CND will be reported in the intelligence, surveillance and reconnaissance functional area or linked to appropriate JMET degradation.

f. All other deficiencies will be reported in the IA and CND paragraph in the C4 functional area and/or linked to appropriate JMET and will be worked with other functional area OPRs as appropriate.

6. Classification. In accordance with reference i, completed assessment reports using IA metrics lists should be classified at a minimum level of SECRET. See reference a, Enclosure 2 for further guidance.

ENCLOSURE B

RESPONSIBILITIES

1. General. The Joint Staff, combatant commanders, Services, and agencies will perform the following tasks:
2. Director for Command, Control, Communications, and Computer Systems, J-6, the Joint Staff
  - a. Provide OPR for the IA and CND portion of JQRR C4 functional area. The Information Assurance Division, J-6K, is the OPR for the IA and CND portion of this functional area.
  - b. Coordinate with Director for Operations, J-3, on CND operational deficiencies. J-3 OPR for CND operational deficiencies is Deputy Director for Operations, Information Operations.
  - c. Coordinate with the Director for Manpower and Personnel, J-1 (JQRR OPR for Joint Personnel) on IA and CND personnel deficiencies.
  - d. Coordinate with the Director for Intelligence, J-2 (JQRR OPR for Intelligence, Surveillance, and Reconnaissance) on intelligence deficiencies in support of IA and CND.
  - e. Coordinate with the Director for Plans and Policy, J-5 on IA and CND policy deficiencies.
  - f. Coordinate with the Director for Operational Plans and Joint Force Development, J-7, on IA and CND (JQRR OPR for Joint War Planning and Training) war planning and training deficiencies.
  - g. Assess IA and CND readiness issues for joint warfighting capabilities assessment study consideration.
3. Services and US Special Operations Command. As appropriate, use the enclosed IA and CND metrics to provide greater insight into personnel, equipment, and training readiness.
4. Combatant commanders
  - a. Provide an IA and CND point of contact (POC) to the Information Assurance Division, J-6K, Joint Staff.

15 July 2003

b. Assess and report joint IA and CND readiness to Joint Staff, J-3, in accordance with reference a. Combatant commander assessments will include IA and CND deficiencies in the C4 functional area and specific comments on the responsiveness and adequacy of support by the combat support agencies. Combatant commands will link deficiencies to degraded ability to accomplish specified JMETS.

5. US Strategic Command (USSTRATCOM). In addition to responsibilities outlined in paragraph 4, USSTRATCOM will review combatant commander and combat support agency JQRR IA and CND deficiencies to assist in evaluation of DOD components' readiness to defend DOD computer networks and to advocate common DOD-wide operational requirements for CND mission.

6. Combat Support Agencies

a. Provide an IA and CND POC to the Information Assurance Division, J-6K.

b. Assess and report IA and CND readiness to J-3 in accordance with reference a. Combat support agencies will provide IA and CND assessments in the C4 functional area. CSAs will link deficiencies to degraded ability to accomplish specified JMETS. Assessments will include specific comments on their readiness and responsiveness to support combatant commanders. DISA, DIA, DLA, NIMA, and NSA should assist combatant commander staffs in assessing IA readiness.

7. All DOD components. Will use the enclosed metrics to provide greater insight into IA and CND planning, operations, training, and resources on operational readiness.

ENCLOSURE C

INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND) METRICS

<b>1.0</b>	<b>PERSONNEL</b>		
<b>1.1</b>	<b>System administrators sufficiently assigned to accomplish mission.</b>		<b>M-Level</b>
1.1.1 (Metric)  (Ref. g, p. B-26, para. o. (33); Ref. b, ST 6.3.5 and ST 7.2)	Number of full-time system administrators (military, government civilian, or contractor) assigned as percentage of required.	M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%	

1.2	<b>IA professionals (information system security officer (IAO), information system security manager (IAM), computer emergency response team (CERT), or other IA professionals) sufficiently assigned to accomplish mission.</b>		<b>M-Level</b>
1.2.1 (Metric)  (Ref. g, p. B-26, para. o. (33); Ref. b, ST 7.2)	Number of full-time information system security professionals (IAO, IAM, CERT, system security engineers or other system security personnel) assigned as percentage of required.	M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%	

2.0	TRAINING		
2.1	System administrators' certifications satisfactorily in place and documented.		M-Level
2.1.1 (Metric)  (Ref. d, p. 93, PRTN-1; Ref. g, p. B-26, para. o. (34); Ref. h, Encl. A, App. B, para. 6; Ref. b, ST 6.3.5 and ST 7.2.4)	Percentage of system administrators' (military, Government civilian and Contractors) trained and certified to DOD and organization established IA and CND training standards.	M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%	

<b>2.2</b>	<b>Broad-based user IA training and awareness program effectively implemented.</b>		<b>M-Level</b>
<p>2.2.1 (Metric)</p> <p>(Ref. d, p. 93, PRTN-1; Ref. g, p. B-26, para. o.(35); Ref. h, Encl. A, App. A, para. 9 Encl. A, App. B, para. 5.; Ref. b, ST 6.3.5 and ST 7.2.4)</p>	<p>Percentage of users (military, government civilian and contractor) with signed organization System User Agreement, and completed as required (at least annually) DOD and component IA training requirements.</p>	<p>M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%</p>	

<b>3.0</b>	<b>OPERATIONS</b>	
<b>3.1</b>	<b>Government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) equipment satisfactorily employed with current approved upgrades, modifications, and CERT advisories (information assurance vulnerability alert (IAVA), information assurance vulnerability bulletin (IAVB), and technical advisories) implemented, adequately documented (certified and accredited), and operational.</b>	
<p>3.1.1 (Metric)</p> <p>(Ref. f, p. 8, para. 5.12.5; Ref. d, p. 65, VIVM-1; Ref. g, p. B-20, para. o. (3); Ref. h, Encl. B, App. B; Ref. b, ST 6.3.5)</p>	<p>IAVA compliance status in accordance with DOD guidance.</p>	<p>M-1: 100% of computer assets compliant or operating with approved extensions and mitigation plans with <b>negligible</b> risk on information systems capability to perform required missions.</p> <p>M-2: 100% of computer assets compliant, or operating with approved extensions and mitigation plans with <b>limited</b> risk on information systems capability to perform required missions.</p> <p>M-3: Less than 100% of computer assets compliant, with MAC II or MAC III computer assets operating without approved extension and mitigation plan that could <b>prevent</b> performing some portions of required missions if exploited.</p> <p>M-4: MAC I computer assets noncompliant operating without approved extension and mitigation plan that could <b>preclude</b> mission accomplishment if exploited.</p>

<b>3.2</b>	<b>Adequate architecture for securing systems and networks in place.</b>		<b>M-Level</b>
<p>3.2.1 (Metric)</p> <p>(Ref. c, p. 6, para. 4.13; Ref. g, p. B-21, para. o. (7); Ref. j, p. 3, para. 5.4.1; Ref. b ST 5.1.2 and ST 5.1.6)</p>	<p>Percentage of networks that completed certification and accreditation (C&amp;A) in accordance with DOD Information Technology Security Certification and Accreditation Process (DITSCAP).</p>	<p>M-1: 100% of operating MAC I, MAC II and MAC III systems with C&amp;A.</p> <p>M-2: 100% of operating MAC I and MAC II systems with C&amp;A, but some MAC III systems operating without C&amp;A.</p> <p>M-3: 100% of operating MAC I systems with C&amp;A, but some MAC II systems operating without C&amp;A.</p> <p>M-4: MAC I or MAC II systems operating without C&amp;A.</p>	

3.3	<b>Access to computer networks is controlled.</b>		<b>M-Level</b>
<p>3.3.1 (Metric)</p> <p>(Ref. d, p. 59-60, ECAT-2, ECCD-2, ECND-2 and ECPA-1; Ref. g, p. B-26, para. o. (5); Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Unauthorized access (root, user, privileged) to MAC I, MAC II, and MAC III systems and networks since last reporting period.</p>	<p>M-1: No incidents of unauthorized access to MAC I or MAC II network and/or system.</p> <p>M-2: Unauthorized access to MAC III network and/or system.</p> <p>M-3: Unauthorized access to MAC II network and/or system.</p> <p>M-4: Unauthorized access to MAC I, or classified network and/or system.</p>	

3.3	Access to computer networks is controlled. (continued)		M-Level
<p>3.3.2 (Metric)</p> <p>(Ref. c, p. 8, para. 4-20; Ref. d, p. 65, VIVM-1; Ref. g, p. A-15, para. 2. g.; Ref. b, ST 6.3.5 and OP 5.1.9)</p>	<p>Periodicity and status of deficiencies from requested or unannounced outside organization or agency vulnerability analysis assessments (active penetration testing, red teaming and assessments of organization networks and/or systems).</p>	<p>M-1: Periodic assessments with no findings open, and all findings corrected within 30 days of identification.</p> <p>M-2: Periodic assessments and only minor security findings open for more than 60 days.</p> <p>M-3: Periodic assessments within past year with major security findings (vulnerabilities) open for more than 60 days on MAC II or MAC III systems that could <b>prevent</b> performing some portions of required missions if exploited.</p> <p>M-4: No assessment within past year, or major security findings (vulnerabilities) identified and currently open more than 30 days on MAC I systems that could <b>preclude</b> mission accomplishment if exploited.</p>	

4.0	TECHNOLOGY (EQUIPMENT) – HARDWARE AND SOFTWARE		
4.1	Sufficient Firewall, Router, and Guard Configurations available and implemented.		M-Level
<p>4.1.1 (Metric)</p> <p>(Ref. d, p. 64, CCED-2; Ref. g, p. A-9, para. 2.d.; Ref. h, Encl. C, App. K; Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Number of networks and/or systems with enclave boundary protection hardware and/or software (e.g. firewalls and guards) on-hand and properly configured as percentage of required. Shortfalls in protection of MAC I, MAC II or MAC III systems.</p>	<p>M-1: 100% of required to protect MAC I and MAC II systems available, and 90 to 100% of required to protect MAC III systems available.</p> <p>M-2: 100% of required to protect MAC I and MAC II systems available, and 80 to 89% of required to protect MAC III systems available.</p> <p>M-3: 100% of required to protect MAC I systems available, 90 to 100% of required to protect MAC II systems available, and 60 to 79% of required to protect MAC III systems available.</p> <p>M-4: 0 to 59% of required to protect MAC II and MAC III available, or MAC I networks and/or systems shortfall.</p>	

<b>4.2</b>	<b>Network situational awareness capability sufficient for fixed and deployed forces.</b>		<b>M-Level</b>
<p>4.2.1 (Metric)</p> <p>(Ref. d, p. 59, ECAT-2; Ref. g, p. A-15, para. 2.q.; Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Number of networks/systems with monitoring tools (network health, bandwidth utilization, and key servers and processes) on-hand as percentage of required. Shortfalls in monitoring capability of MAC I or MAC II networks/systems.</p>	<p>M-1: 100% of MAC I and MAC II systems covered by monitoring tools, and 90 to 100% of MAC III systems covered by monitoring tools.</p> <p>M-2: 100% of MAC I and MAC II systems covered by monitoring tools, and 80 to 89% of MAC III systems covered by monitoring tools.</p> <p>M-3: 60 to 79% of required available or a MAC II system shortfall in monitoring capability.</p> <p>M-4: 0 to 59% of required available or a MAC I system shortfall in monitoring capability.</p>	

<b>4.2</b>	<b>Network situational awareness capability sufficient for fixed and deployed forces. (continued)</b>		<b>M- Level</b>
<p>4.2.2 (Metric)</p> <p>(Ref. d, p. 60, ECID-1; Ref. g, p. A-10, para. 2. d.; Ref. h, Encl. C, App K; Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Number of intrusion detection system hardware/software (scanners, sensors, and analyzer) on-hand as percentage of required.</p>	<p>M-1: 90 to 100% required available, but MAC I and MAC II networks and systems covered by IDS.</p> <p>M-2: 80 to 89% required available, but MAC I networks and systems covered by IDS.</p> <p>M-3: 60 to 79% required available, or any MAC II network and system IDS shortfall.</p> <p>M-4: 0 to 59% required available, or any MAC I network and system IDS shortfall.</p>	
<b>5.0</b>	<b>SUPPORTING INFRASTRUCTURE (Note: No Metrics in this area in Enclosure C)</b>		

<b>6.0</b>	<b>INTELLIGENCE</b>	
<b>6.1</b>	<b>Intelligence support (indications and warning, analysis, and assessments) to computer network mission.</b>	
<p>6.1.1 (Metric)</p> <p>(Ref. e, p. 4, para. 5.15.1; Ref. g, p. B-14, para. h. (6); Ref. b, ST 2.1.1 and OP 2.1.1)</p>	<p>CND Priority Intelligence Requirements (PIR) are validated and impact of outstanding PIR assessed.</p>	<p>M-1: 90 to 100% operations plan (OPLAN) and concept plan (CONPLAN) PIR validated with outstanding PIR having <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: 75 to 89% of OPLAN and CONPLAN PIR validated with outstanding PIR have <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: 50 to 74% of OPLAN and CONPLAN PIR validated with outstanding PIR <b>prevent</b> performing some portion of required missions.</p> <p>M-4: Below 50% of OPLAN and CONPLAN PIR validated with outstanding PIR that could <b>preclude</b> satisfactory mission accomplishment.</p>

ENCLOSURE D

INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND) METRICS - OPTIONAL

Enclosure D provides a list of additional metrics. The list provides optional metrics, which can assist in more in-depth analysis or emphasize unique specific areas of importance to a command or organization's CND or IA readiness.

<b>1.0</b>	<b>PERSONNEL</b>	
<b>1.1</b>	<b>System Administrators sufficiently assigned to accomplish mission. (Note: Metric 1.1.1 located in Enclosure C.)</b>	<b>M-Level</b>
<b>1.2</b>	<b>System security professionals (IAO, IAM, CERT, or other IA professionals) sufficiently assigned to accomplish mission tasks. (Note: Metric 1.2.1 located in Enclosure C.)</b>	<b>M-Level</b>
1.2.2 (Metric)  (Ref. h, p. B-26, para. o. (33); Ref. b, ST 7.2)	Number of CERT or computer incident response team (CIRT) personnel assigned as percentage of required.	M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%

1.3	<b>Operations and law enforcement (e.g., criminal investigation of computer crimes and computer forensics) personnel sufficiently assigned to accomplish IA and CND tasks.</b>		<b>M-Level</b>
<p>1.3.1 (Metric)</p> <p>(Ref. h, p. B-26, para. o. (33); Ref. b, ST 7.2)</p>	<p>Number of operations (J-3) personnel requirements (military (joint, active and reserve), civilian and contractor) assigned as percentage of required.</p>	<p>M-1: 85 to 100%</p> <p>M-2: 75 to 84%</p> <p>M-3: 65 to 74%</p> <p>M-4: 0 to 64%</p>	
<p>1.3.2 (Metric)</p> <p>(Ref. h, p. B-26, para. o. (33); Ref. b, ST 7.2)</p>	<p>Number of law enforcement personnel (military (joint, active and reserve), civilian and contractor) assigned as percentage of required.</p>	<p>M-1: 85 to 100%</p> <p>M-2: 75 to 84%</p> <p>M-3: 65 to 74%</p> <p>M-4: 0 to 64%</p>	

1.4	<b>Network Information Management personnel sufficiently assigned to monitor status of the systems, networks, and nodes.</b>		<b>M-Level</b>
1.4.1 (Metric)  (Ref. h, p. B-26, para. o. (33); Ref. b, ST 7.2)	Number of network information management personnel (military (joint, active and reserve), civilian and contractor) assigned as percentage of required.	M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%	

<b>2.0</b>	<b>TRAINING</b>		
<b>2.3</b>	<b>Information System Security Professionals (IAO, IAM, CERT, system security engineers or other System Security Personnel) completed required IA and CND training. (Note: Metric 2.1.1 and 2.2.1 in Enclosure C.)</b>		<b>M-Level</b>
<p>2.3.1 (Metric)</p> <p>(Ref. c, p. 13, para. 5.10.7; Ref. d, p. 93, PRTN-1; Ref. g, p. B-26, para. o. (34) Ref. h, Encl. A, App. B, para. 12.d.; Ref. b, ST 7.2.4)</p>	<p>Percentage of designated approving authorities (DAA) that have completed required DOD and organization IA and CND training requirements.</p>	<p>M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%</p>	

2.3	<b>Information System Security Professionals (IAO, IAM, CERT, system security engineers or other System Security Personnel) completed required IA and CND training. (continued)</b>		<b>M-Level</b>
<p>2.3.2 (Metric)</p> <p>(Ref. c, p. 13, para. 5.10.7; Ref. g, p. B-26, para o. (34); Ref. h, Encl. A, App. B, para. 12.b. and 12.c.; Ref. b, ST 7.2.4)</p>	<p>Percentage of IAMs and IAOs that have completed required DOD and organization IA and CND training requirements.</p>	<p>M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%</p>	

2.3	<b>Information System Security Professionals (IAO, IAM, CERT, system security engineers or other System Security Personnel) completed required IA and CND training. (continued)</b>		<b>M-Level</b>
2.3.3 (Metric)  (Ref. c, p. 13, para. 5.10.7; Ref. g, p. B-26, para. o. (34); Ref. h, Encl. A, App. B, para. 12.a.; Ref. b, ST 7.2.4)	Percentage of CERT or CIRT that have completed required DOD and organization IA and CND training requirements.	M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%	

<b>2.4</b>	<b>Intelligence Personnel required IA and CND training completed.</b>		<b>M- Level</b>
2.4.1 (Metric)  (Ref. d, p. 93, PRTN-1; Ref. b, ST 7.2.4)	Percentage of intelligence personnel available that have completed required DOD and organization IA or CND training requirements.	M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%	

<b>2.5</b>	<b>Personnel liaison or attached required IA or CND training completed.</b>		<b>M- Level</b>
<p>2.5.1 (Metric)</p> <p>(Ref. d, p. 93, PRTN-1; Ref. g, p. B-26, para. o. (35); Ref. h, Encl. C, App. B, para. 5.; Ref. b, OP 4.4.5)</p>	<p>Percentage of external agency or supporting organization personnel (assigned or attached) to your command that have completed required DOD and organization IA and CND training requirements.</p>	<p>M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%</p>	

2.5	Personnel liaison or attached required IA or CND training completed.		M-Level
<p>2.5.2 (Metric)</p> <p>(Ref. d, p. 93, PRTN-1; Ref. g, p. B-26, para. o. (35); Ref. h, Encl. C, App. B, para. 5; Ref. b, OP 4.4.5)</p>	<p>Personnel for augmentation for surge or crisis operations (military {active and reserve}, civilian and contractor) that have completed required DOD and organization IA and CND training.</p>	<p>M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%</p>	

<b>2.6</b>	<b>Organization conducts IA and CND training and exercises.</b>		<b>M-Level</b>
<p>2.6.1 (Metric)</p> <p>(Ref. e, p. 6, para. 5.6.5; Ref. g, p. B-5, para. b. (6), p. B-8, para. c. (17), p. B-8, para. d. (1), and p. B-9, para. e. (4); Ref. b, ST 4.2.4)</p>	<p>IA CND objectives are integrated into organization level training and exercises.</p>	<p>M-1: IA and CND objectives (as appropriate) and training integrated into 85 to 100% of organizational level training and exercises.</p> <p>M-2: IA and CND objectives (as appropriate) and training integrated into 75 to 84% of organizational level training and exercises.</p> <p>M-3: IA and CND objectives (as appropriate) and training integrated into 65 to 74% of organizational level training and exercises.</p> <p>M-4: IA and CND objectives (as appropriate) and training integrated less than 64% of organizational level training and exercises.</p>	

<b>3.0</b>	<b>OPERATIONS</b>	
<b>3.1</b>	<b>Government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) equipment satisfactorily employed with current approved upgrades, modifications, and CERT advisories (information assurance vulnerability alert (IAVA), information assurance vulnerability bulletin (IAVB), and technical advisories) implemented, adequately documented (certified and accredited), and operational. (Note: Metric 3.1.1 in Enclosure C.)</b>	
<p>3.1.2 (Metric)</p> <p>(Ref. c, p. 4, para. 4.7; Ref. g, p. B-23, para. o. (12); Ref. b, ST 5.1.2)</p>	<p>MAC I and MAC II systems identified based on operational requirements and missions.</p>	<p>M-1: 90 to 100% of MAC I and MAC II systems identified, mapped, and documented.</p> <p>M-2: 80 to 89% of MAC I and MAC II systems identified, mapped, and documented.</p> <p>M-3: 70 to 79% of MAC I and MAC II systems identified, mapped, and documented.</p> <p>M-4: Less than 70% of MAC I and MAC II systems identified, mapped, and documented.</p>

3.1	<b>Government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) equipment satisfactorily employed with current approved upgrades, modifications, and CERT advisories (information assurance vulnerability alert (IAVA), information assurance vulnerability bulletin (IAVB), and technical advisories) implemented, adequately documented (certified and accredited), and operational. (continued)</b>		<b>M-Level</b>
<p>3.1.3 (Metric)</p> <p>(Ref. d, p. 55, DCCS-2 p. 65, VIVM-1; Ref. g, p. B-28-29, para. o. (43) and o. (44); Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Current approved upgrades, modifications, and patches (technical bulletins and advisories) on systems implemented, adequately documented, and operational.</p>	<p>M-1: 100% approved upgrades, modifications, and patches are implemented and documented for MAC I and MAC II systems.</p> <p>M-2: Less than 100% approved upgrades, modifications and patches implemented and documented for MAC I systems, and <b>some</b> deficiencies (less than 100%) in MAC II systems with <b>limited</b> impact on network security.</p> <p>M-3: Less than 100% approved upgrades, modifications and patches implemented and documented for MAC I and MAC II systems with <b>significant</b> security deficiencies that could <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: Less than 100% approved upgrades, modifications and patches implemented (<b>major</b> security deficiencies) for MAC I and MAC II systems that could <b>preclude</b> satisfactory mission accomplishment.</p>	

3.1	<b>Government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) equipment satisfactorily employed with current approved upgrades, modifications, and CERT advisories (information assurance vulnerability alert (IAVA), information assurance vulnerability bulletin (IAVB), and technical advisories) implemented, adequately documented (certified and accredited), and operational. (continued)</b>		<b>M-Level</b>
<p>3.1.4 (Metric)</p> <p>(Ref. f, Encl. 6; Ref. d, p. 65, VIVM-1; Ref. g, p. B-20, para. o. (3); Ref. h, Encl B App. A; Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Sufficient capability to monitor IAVA compliance status for DOD systems and develop corresponding operational risk assessments from IAVA noncompliance.</p>	<p>M-1: Sufficient capabilities (<b>minor</b> deficiencies) to complete operational risk assessments due to IAVA noncompliance with <b>negligible</b> impact.</p> <p>M-2: Sufficient capabilities (<b>some</b> deficiencies) to complete operational risk assessments due to IAVA noncompliance with <b>limited</b> mission impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in capabilities to complete operational risk assessments due to IAVA noncompliance that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in capabilities to complete operational risk assessments due to IAVA noncompliance that <b>preclude</b> satisfactory mission accomplishment.</p>	

3.1	<b>Government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) equipment satisfactorily employed with current approved upgrades, modifications, and CERT advisories (information assurance vulnerability alert (IAVA), information assurance vulnerability bulletin (IAVB), and technical advisories) implemented, adequately documented (certified and accredited), and operational. (continued)</b>		<b>M-Level</b>
<p>3.1.5 (Metric)</p> <p>(Ref. e, p. 2, para. 4-6.2; Ref. d, p. 65, VIVM-1; Ref. g, p. A-18, para. 2.y.; Ref. b, ST 6.3.5, OP 5.1.9 and OP 6.3.4)</p>	<p>Regular and proactive vulnerability analysis, assessments and evaluations program to identify deficiencies.</p>	<p>M-1: Vulnerability assessment (VA) program implemented that identifies network vulnerabilities at least semiannually on MAC I systems.</p> <p>M-2: VA program implemented that identifies network vulnerabilities at least annually on MAC I and MAC II systems.</p> <p>M-3: VA program implemented but assessment conducted on annual or less frequent basis on MAC I and MAC II systems.</p> <p>M-4: VA program does not exist.</p>	

3.1	<b>Government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) equipment satisfactorily employed with current approved upgrades, modifications, and CERT advisories (information assurance vulnerability alert (IAVA), information assurance vulnerability bulletin (IAVB), and technical advisories) implemented, adequately documented (certified and accredited), and operational. (continued)</b>		<b>M-Level</b>
<p>3.1.6 (Metric)</p> <p>(Ref. e, p.2, para. 4.6.2; Ref. h Encl. B, App. D; Ref. b, ST 6.3.5 and OP 5.1.9)</p>	<p>Red Team or Blue Team employed to evaluate the security procedures.</p>	<p>M-1: Red or Blue teaming conducted to evaluate the information and information systems procedures at least semiannually, with <b>minor</b> deficiencies noted and corrected.</p> <p>M-2: Red or Blue teaming conducted to evaluate the information and information systems procedures at least annually, with <b>some</b> deficiencies noted and corrected.</p> <p>M-3: Red or Blue teaming conducted to evaluate the information and information systems procedures within past year with <b>significant</b> deficiencies noted that have not been corrected.</p> <p>M-4: Red or Blue teaming conducted to evaluate the information and information systems procedures within past year with <b>major</b> deficiencies noted that have not been corrected.</p>	

3.2	<b>Adequate architecture for securing systems and networks in place. (Note: Metric 3.2.1 in Enclosure C.)</b>		<b>M-Level</b>
<p>3.2.2 (Metric)</p> <p>(Ref. c, p. 6, para. 4.14.3; Ref. d, p. 56, DCID-1 and p. 89, ECIC-1; Ref. g, p. A-11, para. 2. i.; Ref. h, Encl. C, App. I; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Number of approved and properly configured secret and below interoperability (SABI) and top secret and below interoperability (TSABI) connections as a percentage of required.</p>	<p>M-1: 100% required MAC I and MAC II system connections approved and operational.</p> <p>M-2: 100% required MAC I system connections and less than 100% MAC II system connections approved and operational.</p> <p>M-3: Less than 100% MAC I system connections approved and operational that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: Less than 100% MAC I system connections approved and operational that <b>preclude</b> satisfactory mission accomplishment.</p>	

3.3	<b>Access to computer networks is controlled. (Note: Metric 3.3.1 and 3.3.2 in Enclosure C.)</b>		<b>M-Level</b>
<p>3.3.3 (Metric)</p> <p>(Ref. d, p. 91-92, EBRP-1, EBRU-1; Ref. g, p. B-21, para. o. (5) (b); Ref. h, Encl. C, p. C-15, para. 4.; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Remote access for users and system administrators controlled and systems configured according to manufacturer and DOD guidelines.</p>	<p>M-1: Policy and procedures for controlling and configuring remote access for MAC I and MAC II systems are documented and implemented.</p> <p>M-2: Policy and procedures for controlling and configuring remote access are MAC I systems are documented and being implemented, with some deficiencies in MAC II and MAC III systems.</p> <p>M-3: Policy and procedures for controlling and configuring remote access are being developed and documented, with deficiencies in MAC I systems.</p> <p>M-4: No policies or procedures exist for controlling and configuring remote access.</p>	

3.4	<b>Capability to monitor incident and vulnerability reports and operational impact of incidents on networks.</b>		<b>M-Level</b>
<p>3.4.1 (Metric)</p> <p>(Ref. d, p. 65, VIIR-1; Ref. f, para. 5.5.12; Ref. g., p. B-24, para. o. (17); Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Sufficient capability to monitor incident and technical vulnerability reports.</p>	<p>M-1: Receive 90 to 100% of incident and technical vulnerability reports: <b>Minor</b> deficiencies with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: Receive 80 to 89% of incident and technical vulnerability reports: <b>Some</b> deficiencies with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: Receive 70 to 79% of incident and technical vulnerability reports: <b>Significant</b> deficiencies that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: Receive less than 70% of incident and technical vulnerability reports: <b>Major</b> deficiencies that <b>preclude</b> satisfactory mission accomplishment.</p>	

3.4	<b>Capability to monitor incident and vulnerability reports and operational impact of incidents</b>		<b>M-Level</b>
<p>3.4.2 (Metric)</p> <p>(Ref. d, p. 64; Ref g. p. B-24, para. o. (18); Ref. h, Encl. B, App. B; Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Operational impact of incidents since last reporting period and time required to correct and restore networks and systems.</p>	<p>M-1: Incidents had <b>negligible</b> operational impact on performing required missions; and networks and systems restored in less than 6 hours for all incidents.</p> <p>M-2: Incidents had <b>limited</b> operational impact on performing required missions; and networks and systems restored in less than 6 hours for some incidents.</p> <p>M-3: Incidents had operational impact that <b>prevented</b> performing some portions of required missions; and networks and systems restored in greater than 6 hours for all incidents.</p> <p>M-4: Incidents had operational impact that <b>precluded</b> satisfactory mission accomplishment; and networks and systems restored in greater than 6 hours for some incidents.</p>	

3.5	Incident reporting of unauthorized activity.		M-Level
<p>3.5.1 (Metric)</p> <p>(Ref. d, p. 65, VIIR-2; Ref. E, para. 5.12.7; Ref g. p. B-20, para. o. (4); Ref. h, Encl. B, App. B; Ref. b, ST 5.1.6 and OP 5.1.9)</p>	<p>Sufficient reporting procedures established, implemented, and tested.</p>	<p>M-1: <b>Minor</b> deficiencies in reporting and coordination procedures (established, implemented, and tested; noted deficiencies corrected) for combatant commands, Services, or agencies with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in reporting and coordination procedures for combatant commands, Services, or agencies (not regularly tested; reporting deficiencies exist) with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in reporting and coordination procedures for combatant commands, Services, or agencies (established, recurring reporting deficiencies) that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in reporting and coordination procedures for combatant commands, Services, or agency that <b>preclude</b> satisfactory mission accomplishment.</p>	

3.6	<b>Adequate information operations condition (INFOCON) system and procedures to direct, and implement identified response actions necessary to defend combatant commands computer networks.</b>		<b>M-Level</b>
<p>3.6.1 (Metric)</p> <p>(Ref. e, p. 8, para. 5.12.5; Ref. g, p. B-20, para. o. (2); Ref. h, Encl. B, App. C; Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Adequate INFOCON plans, policies, and procedures are developed and implemented.</p>	<p>M-1: <b>Minor</b> deficiencies in INFOCON plans, policies, procedures, and measures implemented with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies (not fully implemented) in INFOCON plans, policies, procedures, and measures implemented with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in INFOCON plans, policies, procedures, and measures implementation that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in INFOCON plans, policies, procedures, and measures implementation that <b>preclude</b> satisfactory mission accomplishment.</p>	

3.6	<b>Adequate INFOCON system and procedures to direct, and implement identified response actions necessary to defend computer networks. (continued)</b>		<b>M-Level</b>
<p>3.6.2 (Metric)</p> <p>(Ref. e, p. 8, para. 5.12.5; Ref. g, p. B-20, para. o. (2); Ref. h, Encl. B, App. C; Ref. b, ST 4.2.4, ST 6.3.5 and OP 6.3.4)</p>	<p>INFOCON system and procedures integrated and evaluated within organization exercises and operations.</p>	<p>M-1: INFOCON system and procedures implemented, only <b>minor</b> deficiencies noted with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: INFOCON system and procedures implemented, <b>some</b> deficiencies noted with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: INFOCON system and procedures implemented, <b>significant</b> deficiencies noted that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: INFOCON system and procedures implemented, <b>major</b> deficiencies noted that <b>preclude</b> satisfactory mission accomplishment.</p>	

3.6	<b>Adequate INFOCON system and procedures to direct, and implement identified response actions necessary to defend computer networks. (continued)</b>		<b>M-Level</b>
<p>3.6.3 (Metric)</p> <p>(Ref. e, p. 6, para. 5.7.1.2; Ref. g, p. B-7, para. c. (7); Ref. h, Encl. B, App. C; Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Capability in place to direct global changes to DOD-wide INFOCON levels.</p>	<p>M-1: INFOCON level change relayed globally in 1 hour of CDRUSSTRATCOM decision.</p> <p>M-2: INFOCON level change relayed globally within 1 to 3 hours of CDRUSSTRATCOM decision.</p> <p>M-3: INFOCON level change relayed globally within 3 to 6 hours of CDRUSSTRATCOM decision.</p> <p>M-4: INFOCON level change relayed globally more than 6 hours after CDRUSSTRATCOM decision.</p>	

<p>3.6.4 (Metric)</p> <p>(Ref. d, p. 59, ECAT-2; Ref. g, p. A-15, para. 2.q.; Ref. b, OP 5.1.2)</p>	<p>Sufficient capability to monitor the on-going responses to unauthorized activity and computer defensive actions.</p>	<p>M-1: Capability to monitor responses for all Mission Assurance Category (MAC) I and MAC II systems.</p> <p>M-2: Partial capability to monitor response actions for all MAC I and MAC II systems with <b>limited</b> impact on required missions.</p> <p>M-3: Partial capability to monitor response actions for MAC I and MAC II systems which <b>prevent</b> performing some portion of required missions.</p> <p>M-4: Partial capability to monitor response actions for MAC I systems that <b>preclude</b> mission accomplishment.</p>	
---	---	--	--

3.7	<b>Capability restoration relies on established procedures and mechanisms for prioritized restoration of essential functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer.</b>		<b>M-Level</b>
<p>3.7.1 (Metric)</p> <p>(Ref. c, p. 4, para. 4.7 &amp; p. 8, para. 4.20; Ref. d, p. 85, COTR-1; Ref. b, ST 5.1.2)</p>	<p>Key network systems are identified and prioritized for restoration in response to a future network event.</p>	<p>M-1: 100% of MAC I and MAC II systems and networks are identified and prioritized for restoration.</p> <p>M-2: 90 to 99% of MAC I and MAC II systems and networks are identified and prioritized for restoration.</p> <p>M-3: 80 to 89% of MAC I and MAC II systems and networks are identified and prioritized for restoration.</p> <p>M-4: Less than 80% of MAC I and MAC II the systems and networks are identified and prioritized for restoration.</p>	

3.7	<b>Capability restoration relies on established procedures and mechanisms for prioritized restoration of essential functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer.</b> <b>(continued)</b>		M-Level
3.7.2 (Metric)  (Ref. d, p.64, COTR-1; Ref. g, p. B-27, para. (39); Ref. h, Encl. C p. C-18, para. c. (2); Ref. b, ST 5.1.6 and OP 5.1.9)	Capability, plans, and procedures in place to respond to network events and restore network services.	M-1: Network events are fixed and services restored with <b>negligible</b> impact on capability to perform required missions.  M-2: Network events are fixed and services restored with <b>limited</b> impact on capability to perform required missions.  M-3: Network events are fixed and services restored that <b>prevent</b> organization from performing some portion of required missions.  M-4: Network events are fixed and services restored that <b>preclude</b> satisfactory mission accomplishment.	

3.7	<b>Capability restoration relies on established procedures and mechanisms for prioritized restoration of essential functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer.</b> <b>(continued)</b>		M-Level
3.7.3 (Metric)  (ref. k, p. 6, para. 5.3.1; ref. d, p. 64, COED-2; Ref. b, ST 5.1.2 and OP 5.1.8)	Organization develops, coordinates, and rehearses procedures and continuity of operations plan (COOP) to support combatant commanders information systems requirements.	<p>M-1: Procedures and COOP rehearsed with <b>minor</b> deficiencies documented (after-action reports and lessons learned), with <b>negligible</b> impact on required missions.</p> <p>M-2: Procedures and COOP rehearsed with <b>some</b> deficiencies documented (after-action reports and lessons learned), with <b>limited</b> impact on required missions.</p> <p>M-3: Procedures and COOP rehearsed with <b>significant</b> deficiencies documented (after-action reports and lessons learned) that <b>prevent</b> organization from performing some portion of required missions.</p> <p>M-4: <b>Major</b> deficiencies noted (no procedures or COOP) that <b>preclude</b> satisfactory mission accomplishment.</p>	

3.7	<b>Capability restoration relies on established procedures and mechanisms for prioritized restoration of essential functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer.</b> <b>(continued)</b>		M-Level
3.7.4 (Metric)  (Ref. d, p. 84, CODP-1; Ref. b, ST 6.3.5 and OP 6.3.4)	Sufficient redundant communications paths with allies, coalition partners, DOD, combatant commands, Services, and agencies during contingency operations when computer networks are threatened or being attacked.	<p>M-1: Multiple (2 or more) redundant secure communication paths are identified and available if primary communication path is lost.</p> <p>M-2: One secure redundant communication path is identified and available with <b>limited</b> impact on required missions if primary communication path is lost.</p> <p>M-3: Redundant communication alternatives (nonsecure) are identified and available which could <b>prevent</b> organization from performing some portions of required missions if primary communication path is lost.</p> <p>M-4: No redundant communications paths are identified and available that could <b>preclude</b> satisfactory mission accomplishment.</p>	

3.8	<b>Adequate policies in place to protect, detect and react quickly to attacks or threats of attacks on DOD computer networks and systems.</b>		<b>M-Level</b>
<p>3.8.1 (Metric)</p> <p>(Ref. g, p. B-22, para. (11); Ref. b, ST 5.1.2 and OP 6.3.4)</p>	<p>Adequate policies, rules of engagement (ROE), treaties, formal agreements, interorganizational memorandums of agreement (MOA) or memorandums of understanding (MOU) to support effective operations for required missions.</p>	<p>M-1: Adequate laws, policies, ROE, treaties, formal agreements, interorganizational MOA and MOU (<b>minor</b> deficiencies) with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in laws, policies, ROE, treaties, formal agreements, interorganizational MOA and MOU with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in laws, policies, ROE, treaties, formal agreements, interorganizational MOA and MOU that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in laws, policies, ROE, treaties, formal agreements, interorganizational MOA and MOU that <b>preclude</b> satisfactory mission accomplishment.</p>	

3.9	<b>CND and IA operational requirements identified to protect, detect, react and restore DOD computer networks from attack.</b>		<b>M-Level</b>
<p>3.9.1 (Metric)</p> <p>(Ref. f, p. 4, para. 5.5.4; Ref. b, ST 5.1.2)</p>	<p>Organization operational requirements, identified and prioritized for computer network defense.</p>	<p>M-1: Organization has identified and prioritized CND operational requirements (internal and in coordination with USSTRATCOM).</p> <p>M-2: Organization has identified CND operational requirements <b>some</b> deficiencies (not prioritized or coordinated with USSTRATCOM) with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: Organization has <b>significant</b> deficiencies in identifying and prioritizing operational requirements that <b>prevent</b> organization from performing some portion of required missions.</p> <p>M-4: Organization has <b>major</b> deficiencies in identifying and prioritizing operational requirements that <b>preclude</b> satisfactory mission accomplishment.</p>	

<b>4.0</b>	<b>TECHNOLOGY (EQUIPMENT) – HARDWARE AND SOFTWARE</b>	
<b>4.1</b>	<b>Sufficient Firewall, Router, and Guard Configurations available and implemented. (Note: Metric 4.1.1 in Enclosure C.)</b>	<b>M-Level</b>
<p>4.1.2 (Metric)</p> <p>(Ref. d, p. 102, EBBD-1; Ref. g, p. A-9, para. 2.d; Ref. h, Encl. C, App. K; Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Number of firewalls installed and configured properly (periodic updates per local and DOD guidance) on network boundaries to protect computer networks from unauthorized access.</p>	<p>M-1: 100% of required to protect MAC I and MAC II systems available, and 90 to 100% of required to protect MAC III systems available.</p> <p>M-2: 100% of required to protect MAC I and MAC II systems available, and 80 to 89% of required to protect MAC III systems available.</p> <p>M-3: 100% of required to protect MAC I systems available, 90 to 100% of required to protect MAC II systems available, and 60 to 79% of required to protect MAC III systems available.</p> <p>M-4: 0 to 59% of required to protect MAC II and MAC III available, or MAC I networks and systems shortfall.</p>

4.1	<b>Sufficient Firewall, Router, and Guard Configurations available and implemented. (continued)</b>		<b>M- Level</b>
<p>4.1.3 (Metric)</p> <p>(Ref. d, p. 61, ECVP-1; Ref. h, p. C-3, para. 2. c. (1); Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Number of antivirus suites installed and monitored on networks and network boundaries to protect computer networks from virus infection.</p>	<p>M-1: 100% of MAC I and MAC II systems covered by antivirus suites, and 90 to 100% of MAC III systems covered by antivirus suites.</p> <p>M-2: 100% of MAC I and MAC II systems covered by antivirus suites, and 80 to 89% of MAC III systems covered by antivirus suites.</p> <p>M-3: 60 to 79% of required available, or MAC II systems shortfall in antivirus capability.</p> <p>M-4: 0 to 59% of required available, or MAC I systems shortfall in antivirus capability.</p>	

4.1	<b>Sufficient Firewall, Router, and Guard Configurations available and implemented. (continued)</b>		<b>M- Level</b>
<p>4.1.4 (Metric)</p> <p>(Ref. d, p. 61, ECVP-1; Ref. h, Encl. C p. C-3, para. 2. c. (1); Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Number of antivirus suites installed and monitored at desktop level to protect computer networks from virus infection.</p>	<p>M-1: 100% of MAC I and MAC II systems covered at desktop level by antivirus suites, and 90 to 100% of Category III systems at desktop level covered by antivirus suites.</p> <p>M-2: 100% of MAC I and MAC II systems at desktop level covered by antivirus suites, and 80 to 89% of MAC III systems covered at desktop level by antivirus suites.</p> <p>M-3: 60 to 79% of required available at desktop level, or a MAC II systems shortfall in antivirus capability at desktop level.</p> <p>M-4: 0 to 59% of required available at desktop level, or a MAC I shortfall in antivirus capability at desktop level.</p>	

4.2	<b>Network situational awareness capability sufficient for fixed and deployed forces. (Note: Metric 4.2.1 and 4.2.2 in Enclosure C.)</b>		<b>M-Level</b>
<p>4.2.3 (Metric)</p> <p>(Ref. e, p. 4, para. 5-5-10; Ref. g, p. A-18, para. z. (2) (b); Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Capability (technology and equipment) to display a network common operational picture (NETCOP) (network health, bandwidth utilization, circuit status, key servers and processes) of MAC I and MAC II systems and networks.</p>	<p>M-1: Full capability to display network common operational picture on 100% of MAC I and MAC II systems and networks.</p> <p>M-2: Near full capability to display network common operational picture on MAC I and MAC II systems and networks with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: Limited capability to display network common operational picture on MAC I and MAC II systems and networks that <b>prevent</b> performing some portion of required missions.</p> <p>M-4: No capability to display network common operational picture on MAC I or MAC II systems and networks that <b>preclude</b> satisfactory mission accomplishment.</p>	

<b>4.2</b>	<b>Network situational awareness capability sufficient for fixed and deployed forces. (continued)</b>		<b>M- Level</b>
<p>4.2.4 (Metric)</p> <p>(Ref. d, p. 69, DCPR-1; Ref. i; Ref. h, Encl. C, App. I; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Capability (technology and equipment) to analyze documentation (maps) DOD, Gateway, SABI and TSABI interconnections and operational significance to associated networks.</p>	<p>M-1: 100% SABI and TSABI interconnection mapping documentation for classified computer network interconnections and unclassified computer network interconnections.</p> <p>M-2: 100% SABI and TSABI interconnection mapping documentation is available for classified computer network interconnections and less than 90% of unclassified computer network interconnection.</p> <p>M-3: 99 to 90% SABI and TSABI interconnection mapping documentation is available for classified and less than 80% of unclassified computer network interconnections.</p> <p>M-4: Less than 70% SABI and TSABI interconnection mapping documentation is available for computer network interconnections.</p>	

4.3	<b>Capability restoration relies on established procedures and mechanisms for prioritized restoration of essential functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer.</b>		<b>M-Level</b>
<p>4.3.1 (Metric)</p> <p>(Ref. d, p. 63, COBR-1, p. 64, COSW-1; Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Key network equipment is identified and logistical procedures are in place to replace that equipment with backup equipment or emergency requisition.</p>	<p>M-1: 95 to 100% of MAC I and MAC II systems hardware covered in restoration plans.</p> <p>M-2: 85 to 94% of MAC I and MAC II systems hardware covered in restoration plans.</p> <p>M-3: 75 to 84% of MAC I and MAC II systems hardware covered in restoration plans.</p> <p>M-4: Less than 75% of MAC I and MAC II network hardware covered in restoration plans.</p>	

4.4	<b>Sufficient US, allied and coalition secure voice and fax capabilities available and effectively employed for mission accomplishment.</b>		<b>M-Level</b>
<p>4.4.1 (Metric)</p> <p>(Ref. m, p. A-2, para. 4.; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Number of Defense Switched Network (DSN) and commercial telephone as percentage of required.</p>	<p>M-1: 90 to 100% required available and shortfall has <b>negligible</b> impact on performing required missions.</p> <p>M-2: 80 to 89% required available and shortfall has <b>limited</b> impact on performing required missions.</p> <p>M-3: 60 to 79% required available and/or shortfalls that <b>prevent</b> performing some portions of required missions.</p> <p>M-4: 0 to 59% required available and/or shortfalls that <b>preclude</b> satisfactory mission accomplishment.</p>	
<p>4.4.2 (Metric)</p> <p>(Ref. m, p. A-2, para. 4.; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Number of secure voice equipment assets (e.g. STU-III or STE) on-hand as percentage of required.</p>	<p>M-1: 90 to 100% required available and shortfall has <b>negligible</b> impact on performing required missions.</p> <p>M-2: 80 to 89% required available and shortfall has <b>limited</b> impact on performing required missions.</p> <p>M-3: 60 to 79% required available and/or shortfall that <b>prevent</b> performing some portions of required missions.</p> <p>M-4: 0 to 59% required available and/or shortfall that <b>preclude</b> satisfactory mission accomplishment.</p>	

4.4	<b>Sufficient US, allied and coalition secure voice and fax capabilities available and effectively employed for mission accomplishment. (continued)</b>		<b>M-Level</b>
4.4.3 (Metric)  (Ref. m, p. A-2, para. 4.; Ref. b, ST 5.1.2 and OP 5.1.2)	Number of secure Defense Red Switch Network (DRSN) equipment assets on-hand as percentage of required.	M-1: 90 to 100% required available and shortfall has <b>negligible</b> impact on performing required missions.  M-2: 80 to 89% required available and shortfall has <b>limited</b> impact on performing required missions.  M-3: 60 to 79% required available and shortfall that <b>prevent</b> performing some portions of required missions.  M-4: 0 to 59% required available and shortfall that <b>preclude</b> satisfactory mission accomplishment.	

4.5	<b>Sufficient US, allied and coalition secure video capabilities available and effectively employed for mission accomplishment.</b>		<b>M-Level</b>
<p>4.5.1 (Metric)</p> <p>(Ref. m, p. A-2, para. 4.; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Number of secure video equipment assets on-hand as percentage of required.</p>	<p>M-1: 90 to 100% required available and shortfall has <b>negligible</b> impact on performing required missions.</p> <p>M-2: 80 to 89% required available and shortfall has <b>limited</b> impact on performing required missions.</p> <p>M-3: 60 to 79% required available and/or shortfall that <b>prevent</b> performing some portions of required missions.</p> <p>M-4: 0 to 59% required available and/or shortfall that <b>preclude</b> satisfactory mission accomplishment.</p>	

4.6	<b>Sufficient US, allied and coalition network capabilities available and effectively employed for mission accomplishment.</b>		<b>M-Level</b>
<p>4.6.1 (Metric)</p> <p>(Ref. m, p. A-2, para. 4.; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Number of Non-Secure Internet Protocol Router Network (NIPRNET) access available as percentage of required.</p>	<p>M-1: 90 to 100% required available and shortfall has <b>negligible</b> impact on performing required missions.</p> <p>M-2: 80 to 89% required available and shortfall has <b>limited</b> impact on performing required missions.</p> <p>M-3: 60 to 79% required available and/or shortfall that <b>prevent</b> performing some portions of required missions.</p> <p>M-4: 0 to 59% required available and/or shortfall that <b>preclude</b> satisfactory mission accomplishment.</p>	
<p>4.6.2 (Metric)</p> <p>(Ref. 1, p. B-11, para. 9.; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Number of Secure Internet Protocol Network (SIPRNET) access available as percentage of required.</p>	<p>M-1: 90 to 100% required available and shortfall has <b>negligible</b> impact on performing required missions.</p> <p>M-2: 80 to 89% required available and shortfall has <b>limited</b> impact on performing required missions.</p> <p>M-3: 60 to 79% required available and/or shortfall that <b>prevent</b> performing some portions of required missions.</p> <p>M-4: 0 to 59% required available and/or shortfall that <b>preclude</b> satisfactory mission accomplishment.</p>	

4.6	<b>Sufficient US, allied and coalition network capabilities available and effectively employed for mission accomplishment. (continued)</b>		<b>M-Level</b>
<p>4.6.3. (Metric)</p> <p>(Ref. b, ST 2.3)</p>	<p>Number of Joint Worldwide Intelligence Communications System (JWICS) access available as percentage of required.</p>	<p>M-1: 90 to 100% required available and shortfall has <b>negligible</b> impact on performing required missions.</p> <p>M-2: 80 to 89% required available and shortfall has <b>limited</b> impact on performing required missions.</p> <p>M-3: 60 to 79% required available and/or shortfall that <b>prevent</b> performing some portions of required missions.</p> <p>M-4: 0 to 59% required available and/or shortfall that <b>preclude</b> satisfactory mission accomplishment.</p>	
<p>4.6.4 (Metric)</p> <p>(Ref. b, ST 5.1.2)</p>	<p>Number of Planning and Decision Aid System (PDAS) access available as percentage of required.</p>	<p>M-1: 90 to 100% required available and shortfall has <b>negligible</b> impact on performing required missions.</p> <p>M-2: 80 to 89% required available and shortfall has <b>limited</b> impact on performing required missions.</p> <p>M-3: 60 to 79% required available and/or shortfall that <b>prevent</b> performing some portions of required missions.</p> <p>M-4: 0 to 59% required available and/or shortfall that <b>preclude</b> satisfactory mission accomplishment.</p>	

4.7	<b>Public Key security capabilities (Public Key Infrastructure (PKI)/Public Key Enabled (PKE)).</b>		<b>M-Level</b>
<p>4.7.1  (Ref. c, p. 5, para. 4.8.2; Ref. d, p. 59, IAKM-2 and p. 81, IAKM-1; Ref. g, p. B-25, para. o. (26); Ref. b, ST 6.3.3 and OP 6.3.2)</p>	<p>Percentage of new and upgraded operating systems (OS), software applications, and other communications and equipment PKE.</p>	<p>M-1: 100% of new OS, software applications, and other communications and equipment that require authentication, digital signatures, or encryption are PKE.</p> <p>M-2: 90 to 99% of new OS, software applications, and other communications and equipment that require authentication, digital signatures, or encryption are PKE.</p> <p>M-3: 80 to 89% of new OS, software applications, and other communications and equipment that require authentication, digital signatures, or encryption are PKE .</p> <p>M-4: Less than 80% of new OS, software applications, and other communications and equipment that require authentication, digital signatures, or encryption are PKE.</p>	

4.7	<b>Public Key security capabilities (Public Key Infrastructure (PKI)/Public Key Enabled (PKE).</b>		<b>M-Level</b>
<p>4.7.2  (Ref. c, p. 5, para. 4.8.2; Ref. d, p. 59, IATS-2 and p. 81, IATS-1; Ref. g, p. B-25, para. o. (27) Ref. b, ST 6.3.3 and OP 6.3.2)</p>	<p>PKI certificates assigned to full-time personnel (military, civilian, and contractor).</p>	<p>M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%</p>	

5.0	SUPPORTING INFRASTRUCTURE		
5.1	Sufficient funding identified for CND mission and IA programs.		M-Level
<p>5.1.1 (Metric)</p> <p>(Ref. d, p. 37, para. E.3.3.4, p. 57, DCPB-1; Ref. f, p.4, para. 5.5.11; Ref. g, p. B-21, para. o. (6))</p>	<p>Sufficient funding available to provide CND mission and IA programs support.</p>	<p>M-1: Budgeting requirements forecasted and funded at 80 to 100% of requested requirements with <b>minor</b> deficiencies that have <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: Budgeting requirements forecasted and funded at 50 to 79% of requested requirements with <b>some</b> deficiencies that have <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: Budgeting requirements forecasted and funded at 20 to 49% of requested requirements with <b>significant</b> deficiencies that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: Budgeting requirements forecasted and funded at 0 to 19% of requested requirements with <b>major</b> deficiencies that <b>preclude</b> satisfactory mission accomplishment.</p>	

5.2	Adequate facilities are available to support required mission. (continued)		M-Level
5.2.1 (Metric)	Sufficient facilities are available to enable the planning and execution of network operations and CND (personnel and equipment) during crisis and surge operations.	<p>M-1: <b>Minor</b> deficiencies in physical space available with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in physical space available with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in physical space available that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in physical space available that <b>preclude</b> satisfactory mission accomplishment.</p>	

5.2	Adequate facilities are available to support required mission. (continued)		M-Level
<p>5.2.2 (Metric)</p> <p>(Ref. d, p. 92, PEPF-2, PEPS-1, and PESP-1, p. 93, PEVC-1; Ref. g, p. B-29, para. o. (45); Ref. h, Encl. C, App. D; Ref. b, ST 6.3, 6.3.2; OP 6.3.3)</p>	<p>Command and Organization provides a secure environment (physical, personnel, network, emanations) to counteract attempts to disrupt operations.</p>	<p>M-1: <b>Minor</b> deficiencies in physical security with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in physical security with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in physical security that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in physical security that <b>preclude</b> satisfactory mission accomplishment.</p>	

<b>5.2</b>	<b>Adequate facilities are available to support required mission. (continued)</b>		<b>M- Level</b>
<p>5.2.3 (Metric)</p> <p>(Ref. d, p. 63, COBR-1; Ref. b, ST 6.3.5 and OP 6.3.4)</p>	<p>Key network equipment is identified and logistical procedures are in place to replace that equipment with backup equipment or emergency requisition.</p>	<p>M-1: Restoration plans cover 95 to 100% of MAC I and MAC II systems and network hardware.</p> <p>M-2: Restoration plans cover 85 to 94% of MAC I and MAC II systems and network hardware.</p> <p>M-3: Restoration plans cover 75 to 84% of MAC I and MAC II systems and network hardware.</p> <p>M-4: Restoration plans cover less than 75% of MAC I and MAC II systems and network hardware.</p>	

5.2	Adequate facilities are available to support required mission. (continued)		M-Level
<p>5.2.4 (Metric)</p> <p>(Ref. b, ST 5.1.2)</p>	<p>Host C4/IA capabilities and technical expertise support attached personnel and equipment connected to hosting network.</p>	<p>M-1: Host organization support augmenting personnel and equipment on their internal network, and only <b>minor</b> deficiencies (policies and procedures developed and implemented) with <b>negligible</b> impact on augmenting organization to perform required missions.</p> <p>M-2: Host organization support augmenting personnel and equipment on their internal networks, and has <b>some</b> deficiencies (policies and procedures developed and being implemented) with <b>limited</b> impact on augmenting organization to perform required missions.</p> <p>M-3: Host organizations support augmenting personnel and equipment on their internal networks, and has <b>significant</b> deficiencies (developing policies and procedures) that <b>prevent</b> augmenting organization from performing some portions of required missions.</p> <p>M-4: Host organizations supporting augmenting personnel and equipment on their internal networks, and has <b>major</b> deficiencies (no policies and procedures) that <b>preclude</b> augmenting organization satisfactory mission accomplishment.</p>	

5.3	Personnel have required security clearances.		M-Level
<p>5.3.1 (Metric)</p> <p>(Ref. d, p. 7, para. 5.7.11; Ref. g, p. A-13, para. 2.n.)</p>	<p>Number of personnel (military, civilian and contractor) with security clearances as percentage of required.</p>	<p>M-1: 85 to 100% M-2: 75 to 84% M-3: 65 to 74% M-4: 0 to 64%</p>	
5.4	Adequate continuity of operations planning and facilities at alternate site(s).		M-Level
<p>5.4.1 (Metric)</p> <p>(Ref. k, p. 6, para. 5.3.1; Ref. d, p. 63 and p. 64, CODP-3 and COEB-2; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Continuity of operations plan (COOP) enables the execution in a degraded environment or at alternate locations</p>	<p>M-1: <b>Minor</b> deficiencies in plan with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in plan with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in plan that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in plan that <b>preclude</b> satisfactory mission accomplishment.</p>	

5.4	<b>Adequate continuity of operations planning and facilities at alternate site(s). (continued)</b>		<b>M-Level</b>
<p>5.4.2 (Metric)</p> <p>(Ref. d, p. 64, CODP-3; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>COOP supports collaboration with higher HQ and subordinate commands and components to facilitate effective execution.</p>	<p>M-1: <b>Minor</b> deficiencies in plan with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in plan with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in plan that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in plan that <b>preclude</b> satisfactory mission accomplishment.</p>	

5.4	Adequate continuity of operations planning and facilities at alternate site(s). (continued)		M-Level
<p>5.4.3 (Metric)</p> <p>(Ref. d, p. 63, COAS-2; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Alternate facility sufficient (physical, personnel, network, emanations) to assure continued operations in a degraded environment.</p>	<p>M-1: <b>Minor</b> deficiencies in physical space available with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in physical space available with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in physical space available that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in physical space available that <b>preclude</b> satisfactory mission accomplishment.</p>	

5.4	<b>Adequate continuity of operations planning and facilities at alternate site(s). (continued)</b>		<b>M-Level</b>
<p>5.4.4 (Metric)</p> <p>(Ref. d, p. 63, COBR-1; Ref. b, ST 5.1.2 and OP 5.1.2)</p>	<p>Sufficient C4I capability at alternate facility.</p>	<p>M-1: Alternate site is available with full backup capability; only <b>minor</b> deficiencies with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: Alternate site is available with critical backup capability; only <b>some</b> deficiencies with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: Alternate site is available with <b>significant</b> deficiencies in backup capability that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: Alternate site is available with <b>major</b> deficiencies in backup capability that <b>preclude</b> satisfactory mission accomplishment.</p>	
5.5	<b>Databases supporting computer network defense mission.</b>		<b>M-Level</b>
<p>5.5.1 (Metric)</p>	<p>The Joint Threat Incident Database (JTID) is operational and populated with current data and accessible to DOD components.</p>	<p>M-1: Data entered within 12 hours of an event.</p> <p>M-2: Data entered between 12 and 24 hours of an event.</p> <p>M-3: Data entered between 24 and 36 hours of an event.</p> <p>M-4: Data entered more than 36 hours after an event.</p>	

ENCLOSURE E

INTELLIGENCE METRICS SUPPORTING IA AND CND - OPTIONAL

Enclosure E provides a list of additional metrics. The list provides optional metrics, which can assist in more in-depth analysis or emphasize intelligence support to a command or organization's CND or IA readiness.

<b>6.0</b>	<b>INTELLIGENCE</b>	
<b>6.1</b>	<b>Intelligence support (indications and warning, analysis, and assessments) to computer network mission. (Note: Metric 6.1.1 in Enclosure C.)</b>	<b>M-Level</b>
6.1.2 (Metric)	Developed and implemented indications and warning (I&W) problem with strategic and tactical indicators and criteria to provide warning of a computer network attack.	<p>M-1: <b>Minor</b> deficiencies in strategic I&amp;W indicators and criteria with <b>negligible</b> impact to required missions.</p> <p>M-2: <b>Some</b> deficiencies in strategic I&amp;W indicators and criteria that <b>prevent</b> I&amp;W from performing some portion of required missions.</p> <p>M-3: <b>Significant</b> deficiencies in strategic I&amp;W indicators and criteria that <b>preclude</b> satisfactory mission accomplishment.</p> <p>M-4: <b>Major</b> deficiencies in strategic I&amp;W indicators and criteria that <b>precludes</b> satisfactory mission accomplishment.</p>

6.1	<b>Intelligence support (indications and warning, analysis, and assessments) to computer network mission. (continued)</b>		<b>M-Level</b>
6.1.3 (Metric)	All-source theater and global intelligence assessments are available and provided in a timely manner (via message traffic or JWICS/SIPRNET E-mail notifications).	<p>M-1: Assessment(s) sent to appropriate global addressees within 1 hour of recognition of the event.</p> <p>M-2: Assessment(s) sent to appropriate global addressees within 1 to 4 hours of recognition of the event.</p> <p>M-3: Assessment(s) sent to appropriate global addressees within 4 to 7 hours of recognition of the event.</p> <p>M-4: Assessment(s) sent to appropriate global addressees more than 7 hours after recognition of the event.</p>	

6.1	<b>Intelligence support (indications and warning, analysis, and assessments) to computer network mission. (continued)</b>		<b>M-Level</b>
6.1.4 (Metric)	Global and regional CND baseline threat assessments available and updated to support required missions.	<p>M-1: <b>Minor</b> deficiencies in capability to rapidly access and update global and regional CND threat assessments with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in capability to access and update global and regional CND threat assessments with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in capability to access current global and regional CND threat assessments that <b>prevent</b> performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in capability to access current CND-specific global and regional threat assessments that <b>preclude</b> satisfactory mission accomplishment.</p>	

6.1	<b>Intelligence support (indications and warning, analysis, and assessments) to computer network mission. (continued)</b>		<b>M-Level</b>
6.1.5 (Metric)	Global and regional CND baseline threat assessments are accurately tailored to the assigned mission.	<p>M-1: Assessments meet the assigned mission requirements.</p> <p>M-2: Assessments have some applicability to assigned mission with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: Assessments have <b>significant</b> deficiencies (not specifically tailored) that <b>prevent</b> performing portions of required missions.</p> <p>M-4: Assessments have <b>major</b> deficiencies that <b>preclude</b> satisfactory mission accomplishment.</p>	

6.1	<b>Intelligence support (indications and warning, analysis, and assessments) to computer network mission. (continued)</b>		<b>M-Level</b>
6.1.6 (Metric)	Capability to fuse operational intelligence from a variety of sources (technical network analysis and traditional intelligence and disciplines) allowing positive CND action(s)	<p>M-1: <b>Minor</b> deficiencies in processes and procedures to fuse intelligence from a variety of sources to field actionable CND intelligence with <b>negligible</b> impact on capability to perform required missions</p> <p>M-2: <b>Some</b> deficiencies in processes and procedures to fuse intelligence from a variety of sources to field actionable CND intelligence with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in processes and procedures (data collection capability but is unable to translate this to actionable intelligence) that <b>prevent</b> performing some portion of required missions.)</p> <p>M-4: <b>Major</b> deficiencies in processes and procedures to fuse intelligence from a variety of sources to field actionable CND intelligence that <b>precludes</b> satisfactory mission accomplishment.</p>	

6.1	<b>Intelligence support (indications and warning, analysis, and assessments) to computer network mission. (continued)</b>		<b>M-Level</b>
6.1.7 (Metric)	<p>Processed traffic analysis data from NSA, DISA, and the CERTs is sufficient and timely to perform CND mission.</p>	<p>M-1: Only <b>minor</b> deficiencies in available processed traffic analysis data received with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: Only <b>some</b> deficiencies in available processed traffic analysis data received with <b>limited</b> impact on capability (command action) to perform required actions.</p> <p>M-3: <b>Significant</b> deficiencies in available processed traffic analysis data that <b>prevent</b> performing some portions of required actions (command action).</p> <p>M-4: <b>Major</b> deficiencies in available processed traffic analysis that <b>preclude</b> satisfactory mission accomplishment.</p>	

6.2	Capability to attribute the source of computer network attacks.		M-Level
6.2.1 (Metric)	Sufficient data to determine attack and attribution of attacker.	<p>M-1: <b>Minor</b> deficiencies in capability to assess attribution with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in capability to assess attribution with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in capability to assess attribution (data quality insufficient for network event activity) that <b>prevent</b> performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in capability to assess attribution (data not useful to assess attack origin) that <b>preclude</b> satisfactory mission accomplishment.</p>	

6.2	Capability to attribute the source of computer network attacks. (continued)		M-Level
6.2.2 (Metric)	Capability to support an intelligence assessment of state-sponsored computer network attack (CNA) activities.	<p>M-1: <b>Minor</b> deficiencies in capability to assess and attribute state-sponsored CNA with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in capability to assess and attribute state-sponsored CNA with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in capability to assess and attribute states-sponsored CNA that <b>prevent</b> performing some portion of required missions.</p> <p>M-4: <b>Major</b> deficiencies in capability to assess or attribute state-sponsored CNA that <b>preclude</b> satisfactory mission accomplishment.</p>	

6.2	Capability to attribute the source of computer network attacks. (continued)		M-Level
6.2.3 (Metric)	Capability to support an intelligence assessment of nonstate-sponsored (terrorist or criminal) computer network attack CNA activities.	<p>M-1: <b>Minor</b> deficiencies in capability to assess and attribute nonstate-sponsored CNA with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in capability to assess and attribute nonstate-sponsored CNA with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in capability to assess and attribute nonstate-sponsored CNA that <b>prevent</b> performing some portion of required missions.</p> <p>M-4: <b>Major</b> deficiencies in capability to assess or attribute nonstate-sponsored CNA that <b>preclude</b> satisfactory mission accomplishment.</p>	

6.2	Capability to attribute the source of computer network attacks. (continued)		M-Level
6.2.4 (Metric)	Capability to reconstruct unauthorized activity and attack.	<p>M-1: <b>Minor</b> deficiencies in capability to reconstruct unauthorized activity with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in capability to enable reconstruction of unauthorized activity with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in capability to enable reconstruction of unauthorized activity that <b>prevent</b> performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in capability to enable reconstruction of unauthorized activity that <b>preclude</b> satisfactory mission accomplishment.</p>	

6.3	<b>CND intelligence requirements, resources, and procedures sufficient.</b>		<b>M- Level</b>
6.3.1 (Metric)	National intelligence support requirements for CND mission sufficiently defined and adequately collected against.	<p>M-1: <b>Minor</b> deficiencies in national intelligence requirements with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in coordinated national intelligence requirements (not forwarded for approval) with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in national intelligence requirements (development phase) that <b>prevent</b> organization from performing some portion of required missions.</p> <p>M-4: <b>Major</b> deficiencies in national intelligence requirements that <b>preclude</b> satisfactory mission accomplishment.</p>	

6.3	<b>CND intelligence requirements, resources, and procedures sufficient. (continued)</b>		<b>M- Level</b>
6.3.2 (Metric)	CND sections of Intelligence Support Plan (ISP) have sufficiently identified intelligence resources necessary for required missions.	<p>M-1: <b>Minor</b> deficiencies in intelligence resources identified in CND portion of ISP with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in intelligence resources identified in CND portion of ISP with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in intelligence resources identified in CND portion of ISP that <b>prevent</b> organization from performing some portions of their required missions.</p> <p>M-4: <b>Major</b> deficiencies in intelligence resources identified in CND portion of ISP that <b>preclude</b> satisfactory mission accomplishment.</p>	

6.3	<b>CND intelligence requirements, resources, and procedures sufficient. (continued)</b>		<b>M- Level</b>
6.3.3 (Metric)	Sufficient databases and tools available to aid in analysis, assessment, reporting, and planning support.	<p>M-1: <b>Minor</b> deficiencies in available databases and tools to assist in timely data capture, analysis, reporting and planning support with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies (requires manipulation) in available databases and tools to assist in data capture, analysis, reporting and planning support with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in databases and tools (elementary) that prevent development of operational support products and <b>prevent</b> some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in databases and tools for capture of data, analysis, reporting, and planning support that <b>preclude</b> satisfactory mission accomplishment.</p>	

6.3	<b>CND intelligence requirements, resources, and procedures sufficient. (continued)</b>		<b>M- Level</b>
6.3.4 (Metric)	Intelligence support procedures for CND established in organization plans and tactics, techniques, and procedures (TTP).	<p>M-1: <b>Minor</b> deficiencies in intelligence support procedures in plans and TTP with <b>negligible</b> impact on capability to perform required missions.</p> <p>M-2: <b>Some</b> deficiencies in intelligence support procedures in plans and TTP with <b>limited</b> impact on capability to perform required missions.</p> <p>M-3: <b>Significant</b> deficiencies in intelligence support procedures in plans and TTP that <b>prevent</b> organization from performing some portions of required missions.</p> <p>M-4: <b>Major</b> deficiencies in intelligence support procedures in plans and TTP that <b>preclude</b> satisfactory mission accomplishment.</p>	

ENCLOSURE F

REFERENCES

- a. CJCSI 3401.01 Series, "Chairman's Readiness System"
- b. CJCSM 3500.04 Series, "Universal Joint Task List"
- c. DOD Directive O-8500.1, 24 October 2002, "Information Assurance (IA)"
- d. DOD Instruction O-8500.2, 6 February 2003, "Information Assurance (IA) Implementation"
- e. DOD Directive O-8530.1, 8 January 2001, "Computer Network Defense"
- f. DOD Instruction O-8530.2, 9 March 2001, "Support to Computer Network Defense (CND)"
- g. CJCSI 6510.01 Series, "Information Assurance (IA) and Computer Network Defense (CND)"
- h. CJCSM 6510.01, 25 March 2003, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)"
- i. DOD Instruction S-3600.2, 6 August 1998, "Information Operations (IO) Security Classification Guidance (U)"
- j. DOD Instruction 5200.40, 30 December 1997, "Defense Information Technology Security Certification and Accreditation Process (DITSCAP)"
- k. DOD Directive, 26 May 1995, "Continuity of Operations (COOP) Policy and Planning"
- l. CJCSI 6211.02 Series, "Defense Information System Network (DISN): Policy, Responsibilities and Processes"
- m. CJCSI 6215.01 Series, "Policy For Department of Defense Voice Networks"
- n. NSTISSI No. 4009 rev1, September 2000, "National Information Systems Security (INFOSEC) Glossary"

- o. Federal Standard 1037C, 7 August 1996, “Telecommunications:  
Glossary of Telecommunications Terms”
  
- p. Joint Pub 1-02, “Department of Defense Dictionary of Military and  
Associated Terms”

## GLOSSARY

### PART I--ABBREVIATIONS AND ACRONYMS

#### C

C4	command, control, communications, and computers
C&A	certification and accreditation
CERT	computer emergency response team
CIRT	computer incident response team
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CNA	computer network attack
CND	computer network defense
CONPLAN	concept plan
COOP	continuity of operations plan
COTS	commercial-off-the-shelf

#### D

DAA	designated approving authority
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DLA	Defense Logistics Agency
DOD	Department of Defense
DRSN	Defense Red Switch Network
DSN	Defense Switched Network

#### G

GIG	Global Information Grid
GOTS	government-off-the-shelf

#### I

I&W	indications and warning
IA	information assurance
IAVA	information assurance vulnerability alert
IDS	intrusion detection system
INFOCON	information operations condition
INFOSEC	information systems security
IO	information operations
IS	information system
ISP	Intelligence Support Plan
IAM	information assurance manager

IAO information assurance officer

J

JMETS Joint Mission Essential Tasks  
JQRR Joint Quarterly Readiness Review

M

MAC mission assurance category  
MOA memorandum of agreement  
MOU memorandum of understanding

N

NETOPS network operations  
NETCOP network common operational picture  
NIMA National Imagery and Mapping Agency  
NIPRNET Non-Secure Internet Protocol Router Network  
NSA National Security Agency  
NSTISSI National Security Telecommunications and  
Information Systems Security Instruction

O

OPLAN operation plan  
OPR office of primary responsibility  
OPSEC operations security  
OS operating system

P

p. page  
PABX public automated branch exchange (telephone)  
para. paragraph  
PIR priority intelligence requirements  
PKE public key enabled  
PKI public key infrastructure  
POC point of contact

R

Ref. Reference  
ROE rules of engagement

S

SABI secret and below interoperability  
SIPRNET SECRET Internet Protocol Router Network  
STE secure telephone equipment  
STU secure telephone unit

T

TSABI top secret and below interoperability  
TTP tactics, techniques, and procedures

U

USSPACECOM US Space Command

V

VA vulnerability assessment

W

WWW World Wide Web

(INTENTIONALLY BLANK)

## PART II--DEFINITIONS

access control - Limiting access to information system resources only to authorized users, programs, processes, or other systems. (reference n)

accreditation - Formal declaration by a designated approving authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. (references n)

accountability - Process allowing auditing of IS activities to be traced to a source that may be held responsible. (reference n)

architecture - 1. *Computer Architecture*. Of a computer, the physical configuration, logical structure, formats, protocols, and operational sequences for processing data, controlling the configuration, and controlling the operations. Note: Computer architecture may also include word lengths, instruction codes, and the interrelationships among the main parts of a computer or group of computers. 2. *Network Architecture* a. The design principles, physical configuration, functional organization, operational procedures, and data formats used as the bases for the design, construction, modification, and operation of a communications network. b. The structure of an existing communications network, including the physical configuration, facilities, operational structure, operational procedures, and the data formats in use. (reference o)

audit - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (reference n)

authentication - Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. (reference n)

backup - Copy of files and programs made to facilitate recovery, if necessary. (reference n)

certification - Comprehensive evaluation of the technical and nontechnical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. (references n and k)

computer network defense (CND) - Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DOD information systems and computer networks. NOTE: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information. CND protection activity employs information assurance protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, detection activities, including trend and pattern analysis, are performed by multiple disciplines within the Department of Defense, e.g., network operations, CND Services, intelligence, counterintelligence, and law enforcement. CND response can include recommendations or actions by network operations (including information assurance), restoration priorities, law enforcement, military forces and other US Government agencies. (reference e)

confidentiality - Assurance that information is not disclosed to unauthorized persons, processes, or devices. (reference n)

contingency plan - Plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, to ensure the availability of critical resources, and to facilitate the continuity of operations in an emergency situation. (reference n)

Defense in depth - The DOD approach for establishing an adequate IA posture in a shared risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and, the selection of IA solutions based on their relative level of robustness. (reference c)

denial of service (attack) - Result of any action or series of actions that prevents any part of an IS from functioning. (reference n)

designated approving authority (DAA) - The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk - This term is synonymous with designated accrediting authority and delegated accrediting authority. (reference c)

digital signature - Cryptographic process used to ensure message originator authenticity, integrity, and nonrepudiation. Same as electronic signature. (reference n)

DOD Information Technology Security Certification and Accreditation Process (DITSCAP) - The standard DOD process for identifying information security requirements, providing security solutions, and managing information system security activities. (reference k)

Firewall - System designed to defend against unauthorized access to or from a private network. Firewalls can be implemented in hardware and software, or a combination of both. (reference n)

Guards - Process limiting the exchange of information between systems. (reference n)

information assurance - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (reference c)

information operations condition (INFOCON) - The INFOCON is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. INFOCON recommends actions to uniformly heighten or reduce defensive posture, to defend against computer network attacks, and to mitigate sustained damage to the DOD information infrastructure, including computer and telecommunications networks and systems.

information systems security (INFOSEC) - Protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. (reference n)

information assurance manager (IAM) - the individual responsible for the information assurance program of a DOD information system or organization. While the term IAM is favored within the Department of Defense, it may be used interchangeably with the IA tile Information Systems Security Manager. (reference c)

information assurance officer (IAO) - An individual responsible to the IAM for ensuring the appropriate IA posture is maintained DOD information system or organization. While the term IAO is favored within the Department of Defense, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems

Security Custodian, Network Security Officer, or Terminal Area Security Officer. (reference c)

integrity - Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. (reference n)

Joint Quarterly Readiness Review (JQRR) - Provides the DOD leadership a current, macro-level assessment of the military's readiness to fight and meet the demands of the National Military Strategy as assessed by the combatant commands, Services, and DOD combat support agencies. (reference a)

Mission Assurance Category (MAC) - Applicable to DOD information systems, the mission assurance category reflects the importance of information relative to the achievement of DOD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

Mission Assurance Category I (MAC I) - Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a Mission Assurance Category I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.

Mission Assurance Category II (MAC II) - Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure an adequate IA posture is achieved.

Mission Assurance Category III (MAC III) - Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques or procedures generally commensurate with commercial best practices. (reference c)

network operations (NETOPS) - The organizations and procedures required to monitor, manage and control the Global Information Grid. Network operations incorporate network management, information dissemination management, and information assurance.

network common operational picture (NETCOP) - A graphical depiction of warfighting information available in an area of responsibility (AOR). A NETCOP displays network resources showing their operational status and linkage to other sources. When supplemented with additional automated tools and sensors, is used to create and maintain GIG situational awareness.

Nonrepudiation - Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. (reference n)

operating system - An integrated collection of routines that service the sequencing and processing of programs by a computer. Note: An operating system may provide many services, such as resource allocation, scheduling, input and output control, and data management. Although operating systems are predominantly software, partial or complete hardware implementations may be made in the form of firmware. (reference o)

physical security - The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (reference o)

Public Key Infrastructure (PKI) - Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. (reference n)

red team - Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of information systems. (reference n)

remote access - 1. Pertaining to communication with a data processing facility from a remote location or facility through a data link. 2. A PABX service feature that allows a user at a remote location to access by telephone PABX features, such as access to wide area telephone service (WATS) lines. Note: For remote access, individual authorization codes are usually required. (reference o)

risk assessment - Process of analyzing threats to and vulnerabilities of an IS and the potential impact the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and cost-effective countermeasures. (reference n)

router - In data communications, a functional unit used to interconnect two or more networks. Note 1: Routers operate at the network layer (layer 3) of the ISO Open Systems Interconnection--Reference Model. Note 2: The router reads the network layer address of all packets transmitted by a network, and forwards only those addressed to another network. (reference o)

system administrator - Individual responsible for the installation and maintenance of an information system, providing effective IS utilization, adequate security parameters, and sound implementation of established information systems security policy and procedures. (reference n)

threat - Any circumstance or event with the potential to harm an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. (reference n)

vulnerability - Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited. (reference n)

vulnerability assessment - Systematic examination of an IS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (reference n)