DCMA Manual 3301-01

Agency Mission Assurance Construct

Office of Primary Responsibility	**Integrating Capability - Agency Mission Assurance**
Effective:	December 17, 2018
Releasability:	Cleared for public release
New Issuance	
Implements:	DCMA-INST 3301, “Agency Mission Assurance,” 14 May 2018
Internal Control:	Process flow and key controls are located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://360.dcma.mil/sites/policy/MA/SitePages/3301-01r.aspx
Approved by:	David H. Lewis, VADM, USN, Director

Purpose: This issuance in accordance with the authority in DoD Directive 5105.64, DoD Directive 3020.40, and DoD Instruction 3020.45 implements DCMA-INST 3301 “Agency Mission Assurance” and assigns responsibilities and provides procedures for the establishment and execution of the Mission Assurance Construct for DCMA.

TABLE OF CONTENTS

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to DCMA Headquarters (HQ), Operational Units (OU), and all other organizational entities within DCMA.

1.2. POLICY. It is DCMA policy to comply with the DoD-wide process to identify, assess, manage, and monitor risk to strategic missions. Strategic missions are defined as DCMA mission essential functions (MEFs).

a. DCMA will implement the Agency Mission Assurance (MA) Construct in order to establish the minimum risk management requirements for assets critical to the DCMA Mission.

b. The Agency MA construct will support strategic guidance priorities by providing the DCMA Director with recommendations to accept, mitigate, or remediate strategic risk through the Business Capabilities Framework and the DCMA Requirements Oversight Council (DROC) processes.

c. The Agency Mission Assurance Team will coordinate and collaborate MA execution through the Mission Assurance Working Group (MAWG). This includes sharing results of MA processes with MAWG representatives.

d. It is DCMA policy to execute this manual in a safe, efficient, effective, and ethical manner.

SECTION 2: RESPONSIBILITIES

2.1. OFFICE OF PRIMARY RESPONSIBILITY (OPR) FOR AGENCY MISSION ASSURANCE (MA). The OPR for Agency MA will:

a. Manage, lead and implement the Agency's MA construct as described in Section 3 of this issuance and serve as the Agency's single point of contact (POC) for Agency MA related matters.

b. Review and validate the Agency MEFs and MEF Output Tasks every 2 years.

c. Integrate and synchronize MA related programs and activities through the MAWG.

d. Develop and maintain Agency-level MA policy, tools, and training.

e. Conduct MA workshops and/or seminars with OU and Agency HQ Directorate MA POCs in the following:

(1) MA Construct.

(2) Task Critical Asset Identification.

(3) Task Critical Asset (TCA) Assessment.

(4) TCA Risk Management Requirements.

(5) TCA Monitoring Requirements.

f. Conduct MA related requirement reviews at the OUs.

g. Maintain the Common Operating Picture (COP) for the Agency.

h. Represent the Agency at external action officer-level MA forums.

i. Identify, consolidate, and report MA requirements for inclusion into the Agency's overarching budget.

j. Input TCA information into the DoD System of Record for MA.

k. Develop Mission Mitigation Plans (MMPs) for Agency mission risk linked to Defense Critical Assets (DCAs) within 90 days of designation.

l. Develop Risk Remediation Plans (RRPs) for Agency owned DCAs within 180 days of completion of a DoD Mission Assurance Assessment (MAA) report.

m. Maintain Agency procedures for internal reporting of impacts to Agency mission execution and the Defense Industrial Base.

2.2. COMMANDERS/DIRECTORS, OPERATIONAL UNITS (OUs). The Commanders/Directors of the OUs will:

a. Support the Agency MA construct by sharing information through participation in the Agency MAWG.

b. Integrate and synchronize the MA related programs and activities within the OU through MA forums.

c. Support the identification of potential TCAs for the Agency by providing required information on systems and assets with potential to impact DoD or DCMA missions.

d. Support the assessment of TCAs with subject matter expertise and dependency analysis.

e. Perform mission and/or asset owner responsibilities for the risk management of assets, systems, networks and applications identified as TCAs within the OU's operational control or geographical area.

f. Monitor the status of Agency TCAs within the OU's operational control or geographical area and report TCA capability degradation by means compliant with classification requirements.

g. Monitor, report and update risk management actions for TCAs as described in Section 3.5 of this issuance.

2.3. DIRECTOR, INFORMATION TECHNOLOGY (IT). The IT Director will:

a. Provide and sustain IT systems and equipment necessary to support performance of the Agency MA requirements including classified information systems.

b. Support identification of potential TCA for the Agency by providing required information on systems and assets with potential to impact DoD or DCMA missions.

c. Support identification of Agency TCAs through utilization of the Agency's Enterprise Architecture.

d. Support assessment of IT TCAs with subject matter expertise and dependency analysis.

e. Incorporate TCAs in assessment plans as described in Section 3.4.

f. Perform mission and/or asset owner responsibilities for the risk management of IT assets, systems, networks and applications identified as TCAs.

g. Monitor the status of IT TCAs and report TCA capability degradation by means compliant with classification requirements.

h. Monitor, report and update the implementation of risk management actions for IT TCAs as described in Section 3.5. of this issuance.

2.4. DIRECTORS, CORPORATE OPERATIONS, HUMAN CAPITAL, TECHNICAL DIRECTORATE. Utilizing the assigned MA related programs and activities identified in DCMA Instruction (DCMA-INST) 3301, "Agency Mission Assurance," the Directors of Corporate Operations, Human Capital, and Technical Directorate will:

a. Support the Agency MA construct by sharing information through participation in the Agency MAWG and forums.

b. Support identification of potential TCAs for the Agency by providing required information on systems and assets with potential to impact DoD or DCMA missions.

c. Support assessment of TCAs with subject matter expertise and dependency analysis.

d. Incorporate TCAs in assessment plans as described in Section 3.4

e. Perform mission and/or asset owner responsibilities for the risk management of assets and systems identified as TCAs.

f. Monitor the status of Agency TCAs and report TCA capability degradation by means compliant with classification requirements.

g. Monitor, report and update the implementation of risk management actions for TCAs as described in Section 3.5 of this issuance.

2.5. COMPONENT HEADS/CAPABILITY MANAGERS. Includes HQ components, Centers, and DCMA Capability Leads within the Capability Model Framework. Component Heads and Capability Managers must:

a. Develop MMPs for Agency mission risk linked to TCAs.

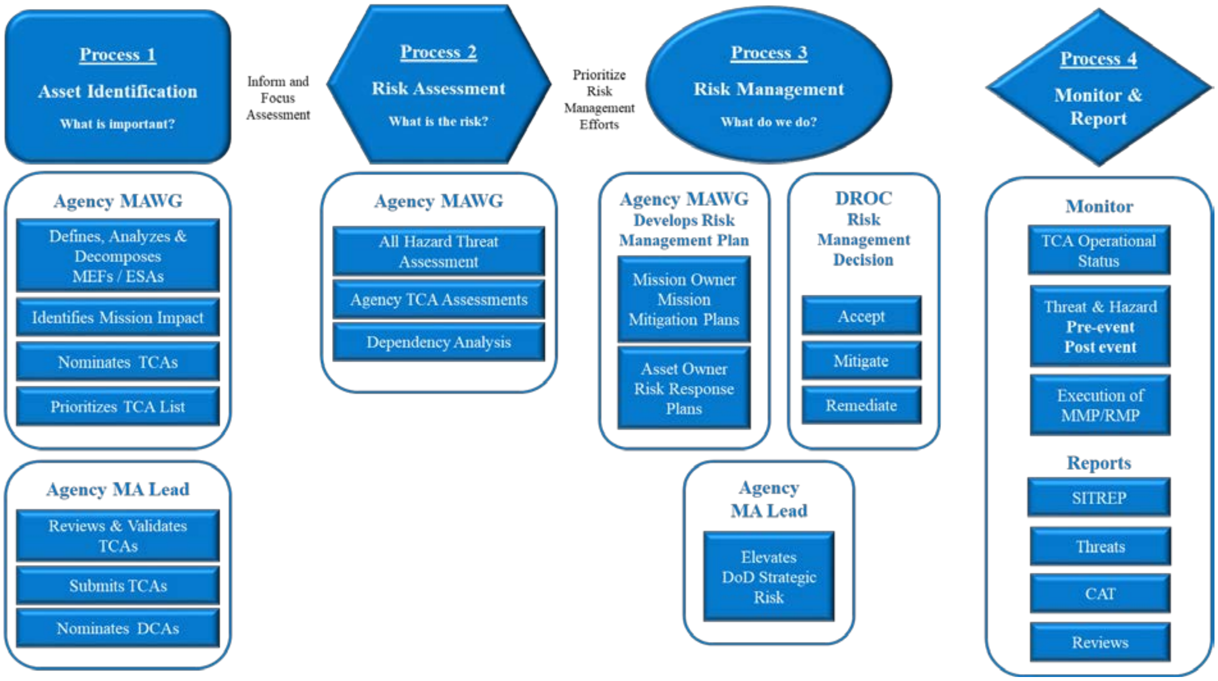
b. Develop RRPs for Agency owned DCAs.

c. Support identification of potential TCA for the Agency by providing required information on systems and assets with the potential to impact DoD or DCMA missions.

SECTION 3: PROCEDURES

3.1. AGENCY MA CONSTRUCT. MA seeks to prioritize DCMA efforts and resources toward addressing the most critical strategic mission execution concerns. The MA Construct's four processes are identification, assessment, risk management, and monitoring. Their relationship to one another and their associated products are illustrated in Figure 1.

Figure 1. Mission Assurance Construct

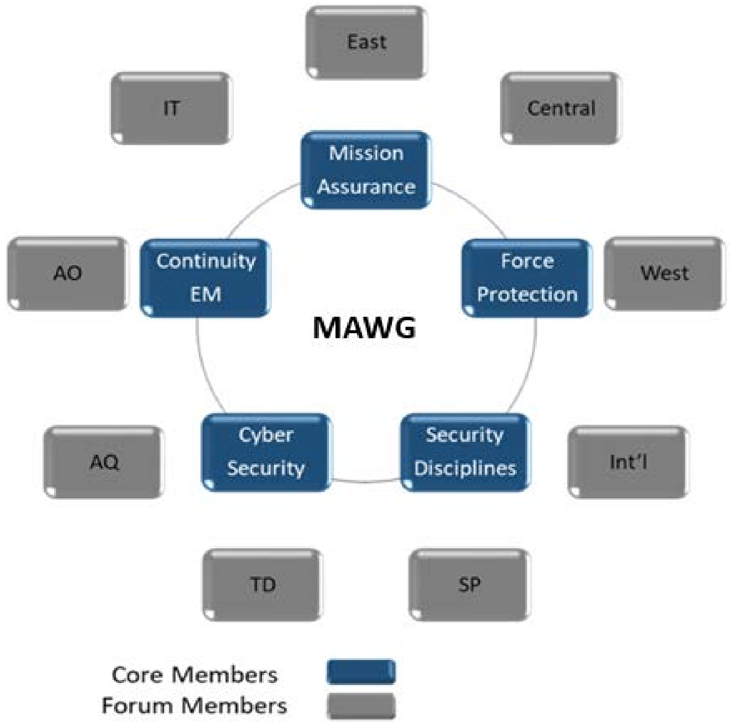


3.2. INFORMATION SHARING. Sharing information through coordination and collaboration is vital to the success of the MA Construct. Information has strategic value to DCMA and DoD. It must be safeguarded, appropriately secured, and shared with authorized DCMA and DoD personnel and mission partners throughout the information's lifecycle. DCMA Components performing MA activities will share information, DoD policy, and mission requirements with Agency MA and MA related programs identified in Figure 2 as necessary to implement the MA Construct.

a. Agency MAWG. Establish an Agency MA working group at appropriate organizational levels to support the identification, assessment, risk management, and monitoring of strategic mission-related risks.

b. Agency MAWG Composition. The Agency MAWG is to be minimally composed of the following MA related programs and activities identified in Figure 2 and are described in detail in Section 3.7. of this issuance.

Figure 2. MAWG Composition

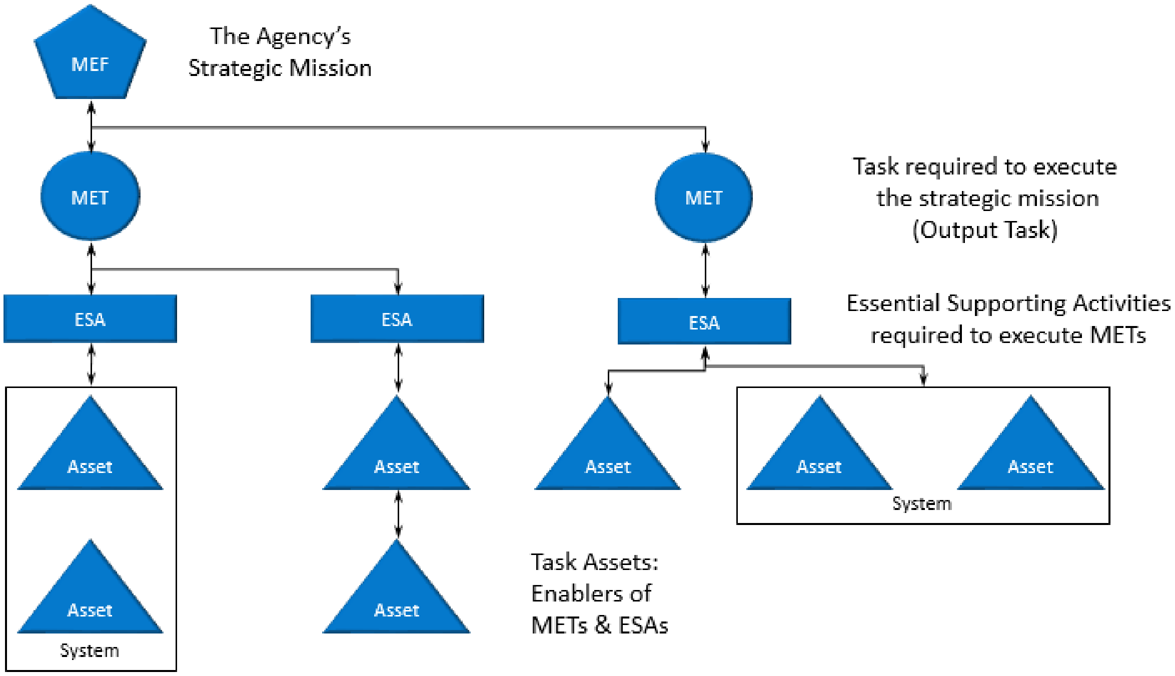


3.3. IDENTIFICATION PROCESS. The goal of the MA identification process is to synchronize and integrate information from the MA related programs and OUs to identify a list of systems and assets that if compromised could adversely impact DCMA MEFs or DoD Missions. These systems and assets, known as TCAs, are then prioritized based on criticality and impact factors. These TCAs provide the foundation of the MA construct. The identification process includes: Mission Decomposition, Mission Impact Analysis, Agency TCA Identification and Nomination, Validation and Submission of TCA List, and DCA Nomination.

a. Mission Decomposition. Mission decomposition discovers Task Assets (TAs). TAs may be people, facilities or physical objects, information systems, applications, or information used to support a Mission Essential Task (MET) or Essential Supporting Activities (ESA). TAs are identified by examining, identifying, and mapping functional processes, workflows, activities, systems, data, and facilities inherent in executing a MET also known as a MEF Output Task. The three steps in mission decomposition are:

- Identify Agency MEFs
- Identify METs and ESAs
- Identify required systems and assets

Figure 3. Mission Decomposition


MEF
The Agency's Strategic Mission
MET
MET
Task required to execute the strategic mission (Output Task)
ESA
ESA
ESA
Essential Supporting Activities required to execute METs
Asset
Asset
System
Asset
Asset
Asset
Asset
Asset
System
Task Assets: Enablers of METs & ESAs

b. Conduct Agency Mission Impact Analysis. A mission impact analysis will be conducted for every TA and considers the effect of criticality factors and the level of disruption to DCMA and DoD missions.

c. Agency TCA Identification and Nomination. A TCA is an asset or system of such extraordinary importance that its incapacitation or destruction would have a serious debilitating effect on a MET or ESA that will cause severe degradation (Tier 2 TCA) or failure (Tier 1 TCA) of the supported strategic mission/MEF. Tier 3 TCAs represent assets that will become Tier 1 or Tier 2 TCAs when linked to urgent, critical needs. Using the results of Mission Impact Analysis, the MAWG will nominate prioritized TCAs to the Agency MA Lead.

d. Validation and Submission of TCA List. The Agency MA Lead will validate the nominated Agency TCAs and submit the Agency approved TCA list to DoD MA system of record. The Agency approved TCA list will be provided to DoD and DCMA asset owners.

e. DCA Nomination. DCA designation should be reserved for assets whose loss, incapacitation, or disruption could result in mission failure or severe degradation of multiple strategic missions, including direct defense of the homeland, a vital national capability, a DoD-level MEF, a DoD principal MEF, or a national essential function. The Agency MA Lead will nominate Agency TCAs that meet the criteria above as DCAs to DoD as described in DoDI 3020.45 "Mission Assurance Construct."

f. Timeline. Agency MA will complete the identification process every 2 years (in coordination with the MEF revalidation cycle) for each strategic mission and revalidate Tier 1 and 2 TCAs annually.

3.4. RISK ASSESSMENT PROCESS. The goal of the MA risk assessment process is to understand the risk to TCAs by incorporating threat and vulnerability assessments from all MA-related programs and activities and dependency analysis. MA integrates these assessments to form a determination of risk for each TCA.

a. All Hazard Threat Assessment (AHTA). AHTAs are the baseline assessment for all MA programs and activities to determine specific hazards and threats, ranging from natural events, human-caused events (accidental and intentional), or technologically caused events.

b. Agency TCA Vulnerability Assessments.

(1) The assessment process draws upon the expertise of all applicable MA-related programs and activities to achieve success. The MAWG and forums should collaborate, assign leads for specific tasks based upon subject matter expertise, and share results to further MA and individual program and activity goals.

(2) The Agency MAWG will integrate assessments of all MA-related programs and activities to reduce redundancy and provide a more complete risk picture for TCAs when developing assessment plans. Agency MA will re-assess Tier 1 and 2 TCAs every 5 years at a minimum.

(3) Agency asset owners are required to facilitate access to TCAs or provide pertinent information to complete assessments.

(4) TCAs not owned by the Agency will be assessed to the furthest extent possible which may include assessments from other sources such as: DoD components, federal agencies, state or local authorities, or private entities.

c. TCA Dependency Analysis. TCA dependency analysis examines the critical infrastructure and services required for the TCA to perform its function. Dependencies may compound a vulnerability.

d. Determination of Risk. Risk to mission is determined by criticality, mission impact, AHTA, TCA assessment, and dependency analysis and is reviewed by the Agency MAWG. Risk determination is the output of MA Assessment and informs MA Risk Management.

3.5. RISK MANAGEMENT PROCESS. The goal of the risk management is to develop strategies to achieve an acceptable level of risk through acceptance, mitigation or remediation.

a. Agency MAWG develops a risk management plan (RMP). An RMP describes risks to a mission arising from an asset's operational factors and the decisions balancing risk cost with mission benefits.

(1) MMPs. Mission mitigation planning focuses on actions to be taken in response to a warning or after an incident occurs to restore TCA capability rapidly. It includes contingency or Continuity of Operations (COOP) planning by mission owners devising alternative methods to continue mission execution. MMPs will be exercised regularly.

(2) Risk Remediation Plans (RRPs). Risk remediation planning is the asset owner's proactive reduction of TCA risk to an acceptable level. Corrective actions include enhancing the security, protection, operations, or redundancy to improve TCA resilience. Preventative actions include changes to doctrine, organization, training, materiel, leadership, personnel, and facilities.

b. Risk Management Decision (RMD). RMPs will be presented to Agency senior leadership for a decision to accept, mitigate or remediate risk. Risk acceptance is an option when made by the appropriate authority and shared with all stakeholders.

c. Elevate DoD strategic risk. DoD strategic risks will be elevated through the DCA risk management process per DoDI 3020.45.

3.6. MONITORING PROCESS. The goal of MA monitoring is for all DCMA Components to maintain situational awareness on the risks related to their MEFs and ESAs. The monitoring process consists of threat monitoring, reporting operational status of TCAs, and risk management implementation tracking.

a. Monitoring. Monitoring allows commanders and senior leaders to make timely and informed decisions and informs all stakeholders on TCA operational status, emerging threats & hazards, and the progress of risk management execution.

(1) TCA Operational Status. Monitoring the operational status of TCAs is required to limit the impacts to mission.

(2) Threats and Hazards. Threats and hazards addresses natural, technological, and man-made emergencies such as earthquakes, epidemics, floods, hurricanes, radiological release, industrial accidents, terrorist events, or other reportable situations that adversely impact the operation of a TCA.

(a) Pre-event monitoring provides commanders and senior leaders with situational awareness, through watches, warnings and advisories utilizing the Agency's common operating picture in advance of an impending threat or hazard.

(b) Post-event monitoring ensures timely execution of mitigation plans and recovery. Long term post-event monitoring may also include executing corrective actions recommended in incident after action reports.

(3) Risk Management Execution. Monitoring risk management actions ensures that the mitigation and remediation plans are fulfilled in order to make a TCA more resilient.

b. Reporting. Reporting informs commanders and senior leaders of changes to operational status of TCAs or risk to mission.

(1) Internal reporting of TCA capability degradation must be compliant with classification requirements and may be accomplished through the Agency Situational Reporting (SITREP) procedure located on the Agency MA Instruction (DCMA-INST 3301) resource page. Additional reporting may be required to support contingencies, exercises and other threats and hazards.

(2) External reporting requirements for TCAs are primarily accomplished by updating and recording information and events in the DoD MA system of record identified on the resource page of this manual. The DoDI 3020.45 also identifies the following reporting requirements to the Chairman of the Joint Chiefs of Staff (CJCS):

(a) As an asset owner, DCMA must report changes in TCA operational status.

(b) As a mission owner, DCMA must supplement asset owner reporting on other DoD TCAs with mission impacts and the implementation of MMPs.

3.7. MA RELATED PROGRAM AND ACTIVITY INTEGRATION. The MAWG is the primary means of integrating force protection, security, continuity, emergency management (EM), and cybersecurity disciplines into the MA Construct. The MAWG operates at the Agency level and is designed to synchronize and integrate all MA program efforts and addresses routine MA actions for coordination across the corporate structure as depicted in Section 3.2., Figure 2.

a. The designated OPR for each MA-related program and activity will update their associated policy to align and support MA goals in improving the resilience of the execution of strategic missions.

b. Each MA-related program or activity provides vital security, protection, or risk management expertise or results that further the goals of MA.

(1) Anti-Terrorism (AT), in accordance with Volume 1 of DoDI O-2000.16, “DoD Antiterrorism (AT) Program Implementation,” directs the Agency to establish, implement, and maintain a comprehensive AT program using an integrated systems approach, designed to protect Agency elements and personnel from terrorist attacks. AT efforts support the MA Construct during each process to ensure the threat of terrorism is considered and accounted for during the execution of strategic missions.

(2) COOP, in accordance with DoDD 3020.26, “Department of Defense Continuity Programs,” ensures the continuation of current approved Agency MEFs across the spectrum of threats. COOP is the Agency’s primary mission mitigation strategy supporting Risk Management.

(3) Cybersecurity, in accordance with DoDI 8500.01 “Cybersecurity,” implements a multi-tiered cybersecurity risk management process to protect Agency interests, operational

capabilities, personnel, organizations, and assets. MA leverages cybersecurity in the MA construct to identify, assess, and manage cyber-related risks that endanger strategic mission execution.

(4) The Agency Security Directorate, as per DoDD 5200.43, "Management of the Defense Security Enterprise" and the guiding policy documents of each of its security programs, recognizes security as an essential supporting activity of the Agency and its proper execution has a direct impact on all Agency missions and capabilities. The Agency Security Directorate aligns with MA to ensure security safeguards exist from each appropriate security discipline to support strategic mission execution

(5) Emergency management (EM), in accordance with DoDI 6055.17, "DoD Emergency Management (EM) Program," maintains Agency readiness and sustains MA by establishing and maintaining a comprehensive, all-hazards EM program. MA leverages the work of EM to assess, risk manage, and monitor threats and hazards that endanger strategic mission execution.

(6) Force health protection in accordance with DoDD 6200.04, "Force Health Protection (FHP)," directs Agency commanders, supervisors, and personnel to promote health protection. This effort supports MA by identifying and addressing health-related issues that endanger strategic mission execution.

(7) Insider threat, in accordance with DoDD 5205.16, "The DoD Insider Threat Program," seeks to prevent, deter, detect, and mitigate the threat insiders may pose to Agency facilities, personnel, missions, or resources. Threats may include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of Agency resources or capabilities. MA leverages insider threat efforts during the assessment, risk management, and monitoring processes and seeks to prevent, deter, detect, and mitigate such threats that endanger strategic mission execution.

(8) Operational energy, in accordance with DoDD 4180.01, "DoD Energy Policy," assesses and manages energy-related risks to operations, training, and testing, including assets, supporting infrastructure, equipment, supplies, platforms, and personnel. Operational energy supports MA by focusing on identifying and resolving energy-related risks that endanger strategic mission execution.

(9) Readiness Reporting, as per DoDD 7730.65, "Department of Defense Readiness Reporting System (DRRS)," manages and reports readiness of DoD and subordinate components to execute the national military strategy. MA leverages readiness reporting to assess the Agency's readiness to execute strategic missions and highlight and address high or significant risks.

c. OU representatives from these various programs efforts will collaborate through their MA forums to identify, assess, manage and monitor the risks to strategic mission execution.

d. Enterprise Architecture. The DCMA enterprise architecture supports MA by providing an integrated business architecture that enables mission analysis and decomposition.

GLOSSARY

G.1. DEFINITIONS.

Asset. A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations.

Asset Owner. The DoD Component or subcomponent with planning, programming, budgeting, and execution (PPBE) responsibility for a DoD asset, or organizations that own or operate a non-DoD asset.

Common Operating Picture (COP). A COP is a single identical display of relevant information shared by more than one Command. A COP facilitates collaborative planning and assists all echelons to achieve situational awareness.

Defense Critical Infrastructure (DCI). The composite of DoD and non-DoD assets are essential to project, support, and sustain military forces and operations worldwide. DCI is a combination of TCAs and DCAs.

Defense Critical Asset (DCA). An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the DoD to fulfill its missions.

Essential Supporting Activities (ESAs). ESAs are activities that must be performed in order to support DCMA's performance of its MEFs. Typically, ESAs are common to most agencies (paying staff, providing a secure workplace, ensuring computer systems are operating, etc.), but do not directly accomplish the mission. ESAs are facilitating activities that enable DCMA to perform MEFs; they are important and urgent, but accomplishing the ESA does not accomplish the output task or MEF.

Hazard. A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation.

Infrastructure. The framework of interdependent physical and cyber-based systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, to the smooth functioning of government at all levels, and to society as a whole.

Integrate. The arrangement of efforts to reduce redundancy and operate as a whole.

Mission Assurance (MA). A process to protect or ensure continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to executing DoD mission-essential functions in any operating environment or condition.

MA Construct. The DoD-wide risk management approach that synchronizes and integrates multiple security, protection, and risk management efforts throughout the DoD to manage risk to the Department's strategic missions. The MA Construct is made up of four processes: identification, assessment, risk management, and monitoring.

Mission Essential Function (MEF). The specified or implied tasks performed by, or derived from, statute, Executive order, or other appropriate guidance, and those organizational activities performed under all circumstances to achieve DoD Component missions or responsibilities in a continuity threat or event. Failure to perform or sustain these functions would significantly affect DoD's ability to provide vital services or exercise authority, direction, and control.

Mission Essential Task (MET). Tasks based on mission analysis and approved by the Commander that are necessary, indispensable, or critical to the success of a mission. Defined in DoDD 7730.65.

Mission Mitigation Plan. A plan developed by a mission owner reflecting how to respond to the loss or incapacitation of identified DCI.

Mission Owner. The DCMA Component having responsibility for executing all or part of a mission assigned by statute or the Secretary of Defense.

Mitigation. Actions taken in response to a warning or after an incident occurs that lessen the potentially adverse effects on operations or infrastructure.

Network. A group or system of interconnected or cooperating entities, normally characterized as nodes (assets) and the connections that link them.

Remediation. Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified.

Risk Assessment. A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks.

Risk Management. A process by which decision makers accept, reduce, or offset risk and subsequently make decisions that weigh overall risk against mission benefits. Risk management is composed of risk assessment and risk response.

Risk-Management Plan (RMP). A plan describing the risks to a mission arising from an asset's operational factors and the decisions that balance risk cost with mission benefits.

Risk Remediation Plan (RRP). A plan describing the asset owner's proactive reduction of TCA risk to an acceptable level. Corrective actions include enhancing the security, protection, operations, or redundancy to improve TCA resilience. Preventive actions may include changes to doctrine, organization, training, materiel, leadership, personnel, and facilities.

Risk Response. Actions taken to remediate or mitigate risk or reconstitute capability in the event of loss or degradation.

Task Assets (TAs). TAs may be people, facilities or physical objects, information systems, or applications or information that are used to support a MET or ESA.

Task Critical Asset (TCA). An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD or OSD Components to execute the task or mission-essential task it supports. TCAs are used to identify DCAs.

TCA Tier 1. An asset whose loss, incapacitation, or disruption would result in mission failure at the DoD Component level of a MET or essential capability aligned to strategic missions.

TCA Tier 2. An asset whose loss, incapacitation, or disruption would result in severe mission degradation at the DoD Component level of a MET or essential capability aligned to strategic missions.

TCA Tier 3. An asset not currently assigned to support a strategic mission, but will become a Tier 1 or Tier 2 TCA when designated by its parent component to support a strategic mission.

Threat. An adversary having the intent, capability, and opportunity to cause loss or damage.

GLOSSARY

G.2. ACRONYMS.

AHTA	all-hazards threat assessment
AT	antiterrorism
COOP	continuity of operations
COP	common operating picture
DCA	defense critical asset
DCI	defense critical infrastructure
DoDD	DoD directive
DoDI	DoD instruction
DROC	DCMA Requirements Oversight Council
EM	emergency management
ESA	essential supporting activities
HQ	headquarters
IT	Information Technology
FHP	force health protection
MA	mission assurance
MAWG	mission assurance working group
MEF	mission essential function
MET	mission essential task
MMP	mission mitigation plan
OPR	office of primary responsibility
OU	Operational Unit
POC	point of contact
RMP	risk management plan
RRP	risk remediation plan
TA	task asset
TCA	task critical asset

REFERENCES

Chairman of the Joint Chief of Staff Instruction 3100.01C, "Joint Strategic Planning System," November 20, 2015

DoD Directive 3020.26, "Department of Defense Continuity Programs," February 14, 2018

DoD Directive 3020.40, "Mission Assurance", November 29, 2016

DoD Directive 4180.01, "DoD Energy Policy," April 16, 2014 as amended

DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," January 10, 2013

DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 1, 2012, as amended

DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014 as amended

DoD Directive 6200.04, "Force Health Protection (FHP)," October 9, 2004

DoD Directive 7730.65, "Department of Defense Readiness Reporting System (DRRS)," May 11, 2015

DoD Instruction 3020.45 "Mission Assurance Construct," August 2018

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014

DoD Instruction O-2000.16 (volume 1), "DoD Antiterrorism (AT) Program Implementation," November 17, 2016