CJCSI 3209.01A
23 August 2023

MISSION ASSURANCE CONSTRUCT IMPLEMENTATION

JOINT STAFF
WASHINGTON, D.C. 20318

(INTENTIONALLY BLANK)

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-3
DISTRIBUTION: A, B, C, S

CJCSI 3209.01A
23 August 2023

MISSION ASSURANCE CONSTRUCT IMPLEMENTATION

References:
See Enclosure H

1. Purpose. This instruction:

a. Establishes Chairman of the Joint Chiefs of Staff (CJCS) Mission Assurance (MA) policy.

b. Assigns responsibilities and procedures for identifying, assessing, managing, and monitoring risk to mission-essential capabilities and defense critical infrastructure.

2. Superseded/Cancellation. This instruction supersedes Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3209.01, 9 January 2012, “Defense Critical Infrastructure Program (DCIP),” and cancels the Mission Assurance Assessments Concept of Operations (CONOPS), April 2016.

3. Applicability. This instruction applies to the Office of the Secretary of Defense (OSD), Military Departments, Office of the CJCS and Joint Staff, Combatant Commands (CCMDs), Office of the Inspector General of the Department of Defense (DoD), Defense Agencies, DoD Field Activities, and all other organizational entities within the DoD (referred to collectively throughout this instruction as the “DoD Components”).

4. Policy

a. Chairman of the Joint Chiefs of Staff

(1) Develops and publishes guidance for implementing MA Construct activities across the DoD Components and establishes a baseline for fulfillment of responsibilities in reference a.

(2) Oversees the MA identification process for CCMD campaign plans, operation plans (OPLANs), concept plans (CONPLANs), and core joint mission-essential tasks (JMETs), as outlined in Enclosure C of this issuance; and arbitrates disputes on asset criticality between DoD Components.

(3) In coordination with DoD Components, develops, publishes, and annually reviews supplemental MA guidance for implementing and facilitating MA Construct activities across the DoD Components, including, at a minimum, guidance on:

(a) Identification process execution, including Baseline Element of Information (BEI) submission. The CJCS will include establishment of a governance forum for BEI development and approval.

(b) Mission Assurance Assessment (MAA) and MA self-assessment execution.

(c) Risk management plan (RMP) development and coordination, including risk reduction plan and mission mitigation plan (MMP) enclosures signed by the component head or deputy, for defense critical assets (DCAs) and Mission Assurance Coordination Board (MACB)-prioritized Defense Critical Infrastructure (DCI).

(d) Monitoring, including the MA system of record; task critical asset (TCA) reporting for real-world events, exercises, and contingencies; and risk reduction action execution.

(4) Manages, on behalf of the MACB, the identification, assessment, and RMP development for DCAs and MACB-prioritized DCI supporting mission-essential capabilities or defense critical missions, with support from appropriate DoD and OSD Components.

(5) Designates a system of record to store DCI data; assessment products and results; and RMPs for the MA community. The CJCS establishes and ensures inputs contain minimum BEI requirements, and reviews designated Tier 1 TCAs to support reference g implementation and data validity.

(6) Provides DCA nominations to the Assistant Secretary of Defense for Homeland Defense and Global Security (ASD(HD&HA)), in coordination with the DoD Components, including the OSD Components, along with the opinions of applicable mission and asset owners. In December of each year, validates or recommends DCA list changes to the ASD(HD&HA).

(7) Ensures the timely production, and posting to the MA system of record, of the CCMD's hazard assessment for any geographic area of responsibility (AOR), and the CCMD's supplement to the Defense Intelligence Agency's (DIA's) global baseline threat assessment.

(8) Implements and oversees the Mission Assurance Assessment Program (MAAP) in accordance with (IAW) CJCS policy on MAAs.

(a) Provides guidance for execution of the MAAP.

(b) Follows established periodicity criteria to designate assessment timelines.

1. Ensures DoD Components meet periodicity requirements.

2. Adjudicates mission owner assessment periodicity windows with each asset owner. Minimizes overlapping assessments or unnecessary duplication of efforts.

3. Reviews and grants waivers to periodicity requirements submitted by the DoD Components.

(c) Standardizes MAA activities across DoD, including issuing integrated MA benchmarks and standards for use by all teams, at a minimum, in coordination with other DoD Component heads.

(d) Provides guidance for collecting self-assessment and self-inspection results from MA-related programs and activities.

(e) Develops and manages execution of an annual DoD-wide MAAP schedule. Coordinates the schedule with the Defense Threat Reduction Agency (DTRA), Military Departments, and appropriate Defense Agencies to synchronize efforts and reduce the annual burden of multiple assessment team visits to the same location.

(f) Ensures a DTRA MAA is conducted on all DCAs and MACB-prioritized DCI.

1. DTRA MAAs have priority over Military Department or Defense Agency MAAs when assessing subordinate commands/installations housing DCAs or MACB-prioritized DCI.

2. To reduce duplication of effort, Military Department or Defense Agency MAA teams may accompany or supplement a MAA to assess other TCAs assessed at the subordinate command/installation not covered by the MAA.

(g) Ensures all MAA results are posted to the MA system of record.

(h) Briefs the MACB on MAAP risk findings for DCAs and MACB-prioritized DCI supporting defense critical missions.

(9) In support of the ASD(HD&HA), provides recommendations on joint MA-related training and education programs for the DoD.

(10) Designates the Director, Joint Staff as the MA ESG co-chair and the Vice Director, Joint Staff (VDJS) as the MA Senior Steering Group (SSG) co-chair.

b. The Mission Assurance Risk Management System (MARMS) is designated as the system of record for MA information, and is comprised of the following:

(1) Strategic Mission Assurance Data System (SMADS) stores BEI for TCAs.

(2) Enterprise Protection Risk Management facilitates scheduling and conduct of MA-related assessments.

(3) Mission Assurance Decision Support System (MADSS) facilitates production and storage of BEI needed for identification, nomination, validation, and approval of TCAs. MADSS is the primary system for mission decomposition, TCA system identification, and criticality BEI.

(4) Enterprise Mission Assurance Analysis Portal allows viewing of information needed for risk management, monitoring, and reporting of TCAs and DCAs.

(5) The MARMS Registry provides centralized storage, standardization, synchronization, and version control of MA data. Component Critical Asset Management Systems (CAMS) can be used to ensure asset data is up to date. However, CAMS data must be consistent with BEI standards set forth in reference j.

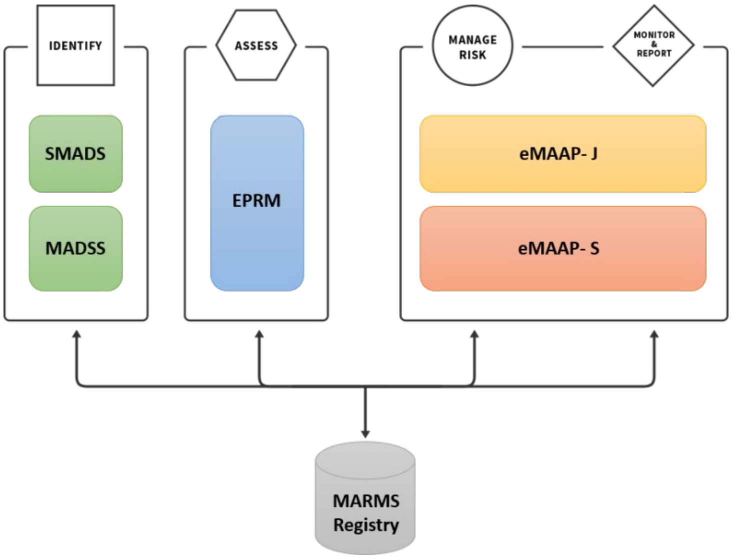

Figure 1. MARMS Functional Overview

5. Definitions. See Glossary.

6. Responsibilities. The DoD Component Heads will ensure the MA Construct is implemented to meet minimum baseline requirements IAW Enclosures A through G of this instruction.

7. Summary of Changes. This CJCSI transitions from the legacy Defense Critical Infrastructure Program (DCIP) to the current MA Construct Implementation and designates the system of record for MA information.

8. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on the Non-classified Internet Protocol Router Network (NIPRNET). DoD Components (to include the CCMDs), other Federal agencies, and the public may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at <http://www.jcs.mil/library>. Joint Staff activities may also obtain access via the SECRET Internet Protocol Router Network (SIPRNET) Directives Electronic Library websites.

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

For the Chairman of the Joint Chiefs of Staff:

Michael L Downs

MICHAEL L. DOWNS, Maj Gen, USAF
Vice Director, Joint Staff

Enclosures:
A – Responsibilities
B – MA Information Management
C – Identification
D – Assessments
E – Risk Management
F – Monitoring and Reporting
G – Alignment of MA within the Joint Staff
H – References
GL – Glossary

DISTRIBUTION

Distribution A, B, C, plus the following:

Secretary of Defense
Under Secretary of Defense for Acquisition and Sustainment
Under Secretary of Defense Comptroller/Chief Financial Officer, Department of Defense
Under Secretary of Defense for Intelligence and Security
Under Secretary of Defense for Policy
Under Secretary of Defense for Personnel and Readiness
Under Secretary of Defense for Research and Engineering
Assistant Secretary of Defense (Health Affairs)
Department of Defense Chief Information Officer

OPR for the subject directive has chosen electronic distribution to the above organizations via e-mail. The Joint Staff Information Management Division has responsibility for publishing the subject directive to the SIPRNET and NIPRNET Joint Electronic Library web sites.

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ENCLOSURE A

RESPONSIBILITIES

1. Heads of the DoD Components

a. By 1 December each year, DoD Component Heads will re-validate Tier 1 and Tier 2 TCAs and submit a memorandum to the CJCS, formatted IAW Appendix A to Enclosure C. Additionally, DoD components will verify that BEI for all TCAs have been shared or submitted to the MARMS Registry or appropriate MA system of record and provide an update on identification of strategic missions.

b. By 1 December each year, submit a memorandum to the CJCS, formatted IAW the template available from the office of primary responsibility (OPR) for this instruction, and accompanied by the associated criticality analyses and mission impact statements, recommending DCAs for addition, retention, and/or removal from the DCA list.

c. Ensure that BEI data that is shared to the MARMS Registry or appropriate MA system of record are complete, accurate, and formatted IAW BEI guidelines in reference j.

2. Director, Defense Threat Reduction Agency

a. Recommend changes to the architecture of MARMS as the MA system of record.

b. Continue all duties as outlined in references a and b. Provide necessary recommendations for implementation of the MA Construct to the Joint Staff J-36.

3. Vice Director, Joint Staff

a. Exercise decision authority over recommendations for changes to the MA system of record architecture.

b. Approve and publish a list of baseline BEI Data requirements and the formatting requirements for BEI.

d. Each year by 31 December, provide feedback to the MACB on DoD Component TCA Tier 1 submissions.

4. Joint Staff Deputy Director for Nuclear and Homeland Defense Operations, J-36. The Deputy Director for Nuclear and Homeland Defense Operations (DDNHDO) will:

a. Exercise day-to-day oversight and management of MA Construct implementation.

b. Exercise decision authority over asset criticality.

5. Chief, Homeland Defense Division, J-36

a. Chair a permanent MACB Working Group on MA BEI.

b. Recommend changes in BEI to the VDJS.

ENCLOSURE B

MA INFORMATION MANAGEMENT

1. BEI. To provide comparable MA data, standardized BEI will be visible to authorized users in MARMS. The MA BEI working group, chaired by the J-36 MA Branch and including commensurate action officer (AO)-level representation from DoD Components, is responsible for proposing changes to the baseline MA BEI.

a. CCMDs, Services, and Agencies that maintain risk management data systems will ensure that MA BEI data is submitted according to the standards set by reference i to the MARMS registry for that MA BEI dataset.

b. The MA BEI working group will meet as necessary to identify, coordinate, and propose any required changes to BEI.

(1) If the working group determines that BEI changes should be made, their recommendations will be further coordinated at the planner- and general officer/flag officer (GO/FO)/senior executive service (SES)- levels of participating DoD Components, prior to being forwarded to the VDJS for approval.

(2) The working group may publish a standardized list of Elements of Information (EI) to facilitate data standardization within the MA community. Based upon evolving requirements and mission priorities, the working group may select certain EI to be included as BEI in the standardized list of BEI.

2. TCA Processing. Disputes regarding TCA tier ratings will be resolved at the lowest possible level. For disputes that cannot be resolved at Component level, forward requests for adjudication to the VDJS, through the DDNHDO.

3. Mission Assurance Reviews. The Joint Staff J-36 MA Branch will review CCMD MA-related policy and guidance annually via video teleconferencing (VTC) or Defense Communications Systems (DCS), and (if possible) triennially in person.

a. Annually, not later than (NLT) 1 June, the J-36 MA Branch will notify CCMDs of information they are required to submit to the Joint Staff, including:

(1) MA Self-Assessment based on CCMD requirements.

(2) CCMD MA-related instructions, plans, and guidance.

(3) CCMD MA-related training documents.

(4) CCMD MA-related threat and hazard monitoring and reporting. procedures

(5) CCMD MA-related mitigation plans.

(6) CCMD organizational chart and current MA office staffing guidance.

b. Annually NLT 1 September, the CCMDs will submit the requested information to the J-36 MA Branch under the signature of their MA O-6/GS-15 representative.

c. Annually NLT the end of October, the J-36 MA Branch will coordinate with CCMDs to schedule their MA reviews during the month of November.

d. Annually NLT the end of December, the J-36 MA Branch will publish an executive summary of all CCMD MA reviews, applicable trends/best practices, and the annual TCA re-validation results.

ENCLOSURE C

IDENTIFICATION

1. Purpose. Provide supplemental guidance for implementing and facilitating the identification process as prescribed in reference b.

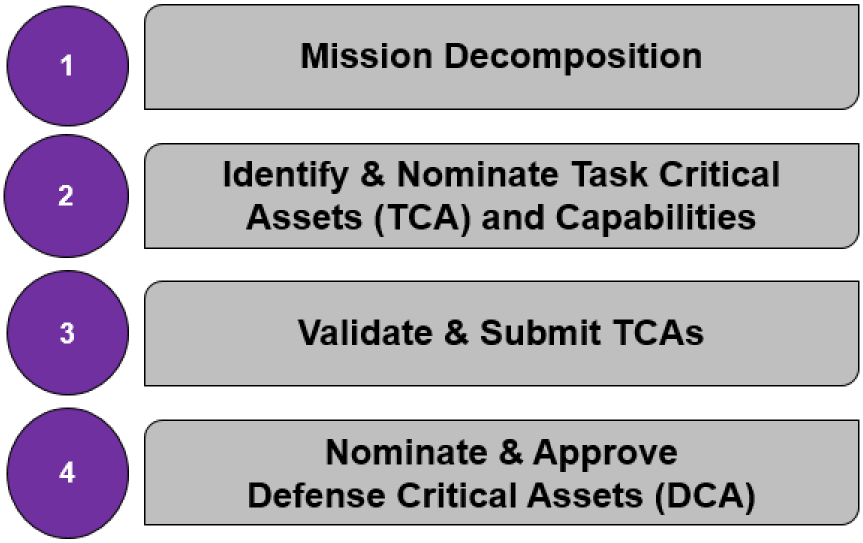
1
Mission Decomposition
2
Identify & Nominate Task Critical Assets (TCA) and Capabilities
3
Validate & Submit TCAs
4
Nominate & Approve Defense Critical Assets (DCA)

Figure 2. MA Identification Process

2. Process

a. Step 1 – Mission Decomposition. Mission decomposition is conducted by mission owners IAW reference b.

(1) While conducting the identification process, if mission-essential tasks (METs), mission-essential functions (MEFs), or DoD primary MEFs are not currently reported in the Defense Readiness Reporting System – Strategic (DRRS-S), DoD Components should provide recommendations to their readiness section for potential incorporation into the command's DRRS-S report. DRRS-S is a data entry point for the MARMS system, which is necessary to assist in the decomposition process. An accurate and robust decomposition process enables Services and Agencies to refine mission requirements so that they can train and resource appropriately.

(2) Mission owners define the standards and conditions that are necessary for capability success. These standards and conditions provide

clarity to asset owners and/or capability providers to identify critical assets and capabilities.

(a) Standards are static evaluation measures for each Service and/or Agency Mission-Essential Task List. In some situations, one standard may be sufficient to describe a capability. However, in most circumstances, a mission owner may have to specify more than one standard to accurately reflect essential capability requirements.

(b) Conditions are dynamic and consider the unique requirements and challenges of the AOR and strategic operations. Multiple conditions are usually required to accurately reflect the requisite capability.

(3) In addition the requirements in reference b, any deliberate planning effort (e.g., updated campaign plans or an OPLAN/CONPLAN revision) will initiate capability identification for review and confirmation at the CCMD level.

b. <u>Step 2 – Identify Task Assets and nominate TCAs</u>. Asset owners and/or capability providers identify task assets (TAs) and nominate TCAs that meet the mission owner's required mission standards and conditions. Mission owners should analyze and document mission dependencies and Time to Impact Mission (TTIM) of critical assets. Asset owners/capability providers analyze and document infrastructure dependencies and Time to Restore (TTR) of critical assets. Documentation of this information should be submitted in the appropriate program of record for inclusion into the MARMS registry or appropriate MA system of record module.

(1) Dependency analysis provides a thorough understanding of each mission, function, and capability conducted at a site, along with associated stakeholders, supporting assets, critical data, and resources necessary to execute IAW published plans and requirements. The completed dependency analysis aims to produce a better understanding for all stakeholders of the interdependencies inherent in complex missions and the consequences that loss of a capability or asset may have for the missions it supports.

(a) Mission dependencies are the relationships between a mission, task, or function and the asset/capability required for successful execution. Documentation of this relationship should show how a mission is degraded or fails if the asset/capability is degraded or fails.

(b) Infrastructure dependencies are relationships that are required for an asset to function (e.g., power, water, communication links/nodes, runways). Infrastructure dependency analysis must encompass DoD-owned, commercial, and/or foreign government-owned infrastructure as they apply to a particular asset. Dependency analysis should be performed completely for nodes within an installation and to no less than one node beyond the perimeter of the installation where the asset is located, if applicable.

(2) TTIM and TTR are important in constructing an accurate Mission Impact Statement.

(a) Mission owners identify the TTIM (how quickly the mission is impacted after the asset/capability is no longer functional).

(b) Asset owners and/or capability providers identify the TTR (the time required to reconstitute the asset to capability). Services and agencies should consider CCMD-input concerning TTR.

(3) A TA is any asset (e.g., supporting infrastructure, other dependencies) that directly supports the mission but does not satisfy the definition of a TCA. DoD Components may create their own designation for subsets of these assets, but these assets will be recorded in the MARMS Registry as TAs.

c. <u>Step 3 – Validate and Submit TCAs</u>. Conduct IAW reference a and submit to the CJCS via memorandum. The validation memorandum will confirm that the TCAs have been validated and the associated BEI has been shared to the MARMS registry or submitted to the appropriate MARMS Module. Appendix A provides a sample memorandum template.

d. <u>Step 4 – Nominate and Approve Defense Critical Assets</u>. Designate DCAs IAW reference a.

(1) For DoD MA purposes, if multiple assets function as a single unit in support of a capability and/or strategic mission and are co-located, they may be designated as a system and nominated as a DCA.

(a) An example of an MA system would be a logistics facility that has multiple TCAs in order to conduct its transportation/shipping operations. While assets are submitted in MARMS individually as TCAs, they could be nominated as one system for DCA designation.

(b) When evaluating a system, the DoD Component will assess redundancy and establish each single point of failure within the system that will result in either the loss or severe degradation of the capability.

(2) DoD Components provide DCA nomination and removal recommendations with GO/FO/SES endorsement to CJCS.

(a) Recommended nominations must include a complete, in-depth criticality analysis and a defined mission impact statement that meets the criteria in reference b for evaluation by the appropriate Components. This nomination should include a complete Mission decomposition in the associated MARMS module (MADSS) with loss impacts clearly annotated.

(b) Recommended removals must include in-depth reasoning for the asset’s removal. The recommendation should include a complete Mission decomposition in the associated MARMS module (i.e., MADSS), with loss impacts clearly annotated.

(c) All DCA nominations and removals must be properly documented in the CJCS-approved format and classified at the appropriate level; contact the J36 MA Branch for a copy of this template.

(3) Prior to submission, Services/agencies and CCMDs must coordinate and communicate their DCA nomination or removal recommendations to one another. The lead DoD Component will coordinate with all other organizations with equity in the DCA nomination or removal.

(4) Mission owners or asset owners/capability providers must ensure appropriate subordinate commands and internal branches are aware of the DCAs in their jurisdiction.

3. Criticality Scoring for Calculating Risk. For MAA process risk calculation:

a. Criticality scores are solely used to calculate risk during MAAs (see Enclosure D).

b. DoD Mission Owners assign a criticality score to each TCA, with 1.0 being most critical and 0.01 being least critical. Mission owners and asset owners/capability providers must consider the level of mission failure or degradation resulting from complete asset failure or loss. DoD Components may utilize an already established criticality scoring methodology. In lieu of a robust criticality scoring methodology, the following criticality scoring ranges will be utilized for standardization:

(1) TCA Tier 1: 1.0 to 0.85.

(2) TCA Tier 2: 0.84 to 0.65.

(3) TCA Tier 3 and Task Asset: 0.64 and below.

c. If DoD mission owners and asset owners differ on a tier rating for an asset, they should attempt to resolve the dispute at the component level. If the dispute cannot be resolved at the AO, planner, and GO/FO/SES-levels between component stakeholders, tier rating recommendations will be forwarded to the J-36 MA Branch for J-36 adjudication.

d. Assets may have different tier ratings and criticality scores for each strategic mission that a TCA supports. Assets will be managed based on the requirements associated with the highest validated tier rating.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE C

ANNUAL TCA VALIDATION AND STRATEGIC MISSION REVIEW TEMPLATE

DD MM YYYY

MEMORANDUM FOR JOINT STAFF J36 HOMELAND DEFENSE DIVISION
3000 Joint Staff Pentagon
Washington, DC 20318-3000

SUBJECT: Calendar Year 20XX Annual Task Critical Asset Validation and Strategic Mission Review

1. In accordance with DoD Instruction 3020.45, section 3.3, paragraph b. (1)., (DoD Component XXX) completed calendar year (CY) 20XX review of (DoD Component)-owned and/or operated Tier 1 and Tier 2 TCAs (TCA-1 and TCA-2). All assets are current, and their associated BEI has been shared to the AMRMS registry or the appropriate MA System of Record.

2. (CCMDS ONLY) In accordance with DoD Instruction 3020.45, section 3.3, paragraph b(1), (CCMD) owns BLANK strategic missions that require a triennial review.

a. (BLANK) of these missions were completed in CY 20XX *(List Missions).*

(1) STRATEGIC MISSION 1 review completed on DDMMYYYY.

(2) STRATEGIC MISSION 2 review completed on DDMMYYYY.

b. The remaining (BLANK) mission reviews will be completed by: *(List missions and estimated date of completion, if applicable).*

(1) STRATEGIC MISSION 3 review estimated to be complete on DDMMYYYY.

(2) STRATEGIC MISSION 4 review estimated to be complete on DDMMYYYY.

3. Please contact my POC, NAME at PHONE or EMAIL with any comments or questions.

NOTE: This template is UNCLASSIFIED when separated from classified attachments. This memorandum will be classified at the appropriate level IAW *reference c and/or applicable DoD component SCGs when completed. Include all applicable portion markings.*

ENCLOSURE D

ASSESSMENTS

1. Purpose. This enclosure provides minimum baseline guidance for the execution of MAAs IAW reference b. MAAs inform risk management processes at all levels and through all phases of operations, with inputs, outputs, and feedback into each of the four MA processes (Figure 3). The MA assessment process integrates information on mission dependencies, asset criticality, asset or area-specific hazards and threats, and vulnerabilities through which those hazards and threats may impact missions. Once combined, this information allows a more comprehensive understanding of the risks to mission that may adversely affect all levels throughout all phases of operations.

a. MAAs rely upon the identification process to identify what must be assessed. The MAA supports the risk management process by identifying potential risks to mission execution from which to develop and prioritize risk management actions.

b. MAAs are designed to identify and communicate vulnerabilities and mission risk to mission owners, asset owners, capability providers, and others who have the responsibility and authority to manage resources and risk. The assessment results are used by mission owners for awareness of risks to capabilities that have been validated and linked to strategic missions.

c. MAAs serve other purposes—they assist installation leaders in understanding the risk posed to strategic missions by assets within their AOR and enable leaders at all levels to make better informed risk management decisions. Additionally, MAAs provide a more comprehensive understanding of how hazards and threats impact missions through identified vulnerabilities, along with expert advice in identifying remediation and mitigation strategies.

2. Overview

a. MAAs integrate many assessment requirements of MA-related programs and activities (MARPAs) to present a more complete understanding of potential risks to missions across the DoD.

b. MAAs consist of several elements (dependency analysis, criticality verification, hazard and threat analysis, and vulnerability assessments) and rely upon the previously completed identification process to produce an assessment of risk to assets and missions. Any DoD Component that is required or prefers to maintain MAA teams will configure it to meet DoD requirements, the requirements in this instruction, and their own needs.

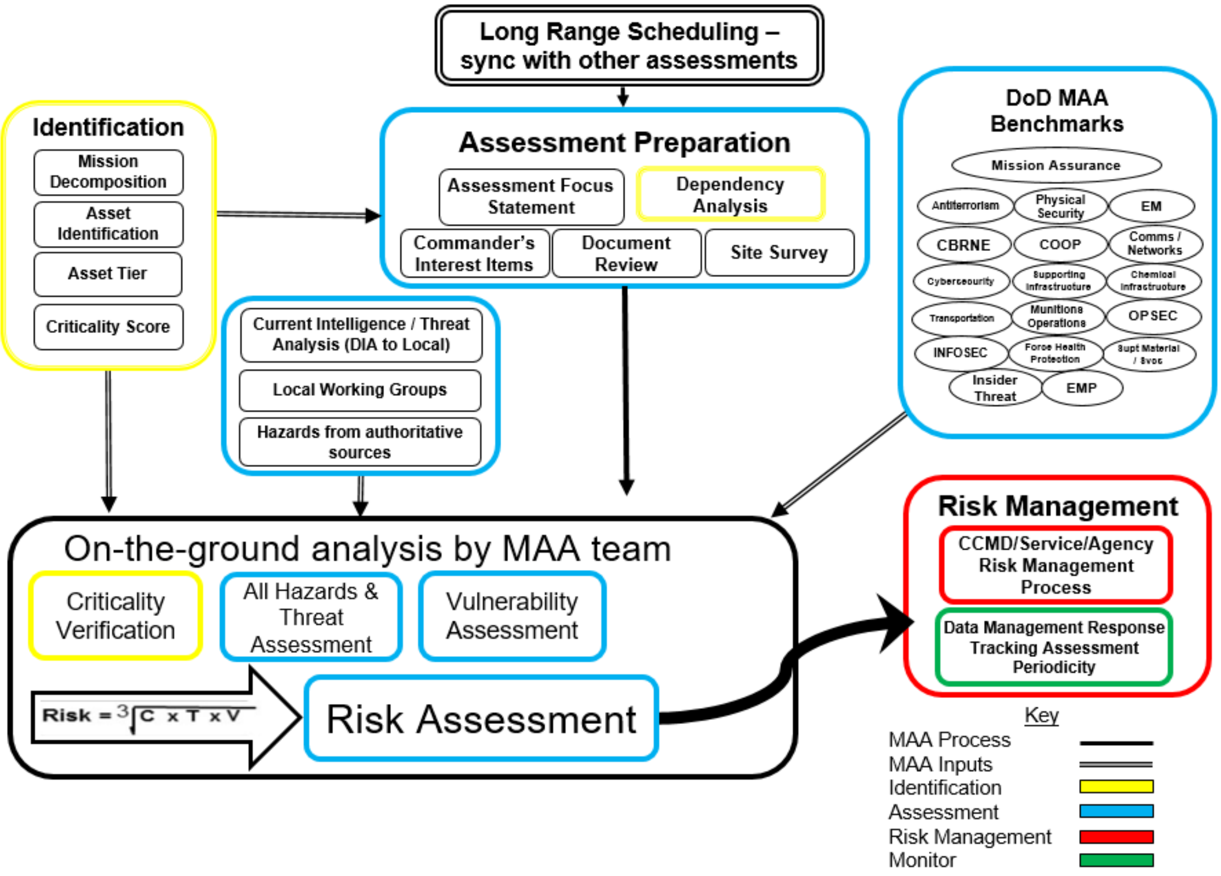

Figure 3. Mission Assurance Assessment Process

c. The DoD requires baseline standardization of MAAs across the DoD to support cross-functional multi-domain comparisons and analysis. All MAAs will align with the minimum baseline guidance in this instruction unless superseded by higher Department-level guidance. Subject matter experts (SMEs) will use this guidance at a minimum, along with their experience and best judgment, to categorize their observations. Standardized MA data enables the DoD to accurately compare observations made by different assessment teams. All MAAs will assess using the most recent version of the DoD MAA Benchmarks (reference d) as the minimum standard. DoD Components may publish MAA benchmarks to meet specific requirements, but these benchmarks must align with the DoD MAA Benchmarks to support baseline analysis and comparisons across all DoD.

d. These assessments involve a broad group of stakeholders, ranging from CCMDs conducting strategic missions, to installation tenant organizations conducting specific tasks at the installation level. The J-36 MA Branch will identify a lead DoD Component (known hereafter in this enclosure as the lead component) on the Integrated Assessment Schedule (IAS). Development of the IAS is outlined in 3.a.(1) below. The lead component will coordinate among all the organizations with equity in the assessment and the assessing organization to properly scope the assessment. The lead component will provide coordination between the hosting installation, the MAA team, and various stakeholders. If necessary, installation commanders can establish MAA working groups and committees to coordinate between the installation, the MAA team, and other various stakeholders.

e. During an MAA, the assessment team may discover vulnerabilities to some of the most critical assets in the DoD with subsequent implications of risk to DoD strategic missions. Therefore, it is vitally important that participants practice good operational security procedures and follow the applicable security classification guides, notably reference c. The survey and assessment teams should actively seek out any potentially applicable security classification guidance, including guides for specific programs, assets, or weapon systems, to ensure proper classification of information in the Mission Assurance Assessments Reports (MAAR). If multiple security classification guides apply to a MAA (e.g., Antiterrorism (AT) and Force Protection (FP)) then the team will apply and cite the most stringent classification requirements.

f. Results of the MAAs will be shared to the MARMS registry or submitted in the appropriate MA system of record. The assessing organization will ensure the Assessment, Vulnerability, Risk BEI and MAAR are shared to the MARMS registry. DoD Components with equity that require access to MAARs will then have access to them through MARMS or their own respective risk management systems for use in their risk management processes.

g. Appropriate information sharing ensures that critical information is disseminated through all levels of command. Stakeholders utilize the data to promote visibility of risk management through the MA Construct and in any additional ways that suit their internal risk management strategies and procedures (providing that security classification requirements are followed). The increased visibility of the reports allows decisions concerning mitigation, remediation, or acceptance of risk to be made at the appropriate level of command. It also reduces the possibility that organizations accept risk within functional stovepipes or at lower levels without the mission owner's knowledge.

3. Process

a. Assessment Preparation

(1) Integrated Assessment Schedule. The IAS is an annual DoD-wide MAAP schedule coordinated and published by the CJCS in order to integrate, synchronize, and deconflict related assessments across the DoD. The IAS is validated at the GO/FO/SES level of all included DoD Components and thus serves as the authoritative MAA schedule. The MAAs listed in the IAS support the Chairman in understanding risk to mission and making risk recommendations to the Secretary of Defense (SecDef).

(a) Assessment preparation begins as soon as the annual IAS is published by the Joint Staff J-3. The IAS will include all DoD Component-level and above MAAs. These consist of Joint Mission Assurance Assessments (JMAA), DTRA MAAs, CCMD MAAs, Service MAAs, and other DoD Component HHQ MAAs. JMAAs and DTRA MAAs may include a separate Red Team assessment and/or an Advanced Cybersecurity Analytics Team (ACAT) assessment when either the lead component requests it or MACB prioritization requires it.

1. All JMAAs are conducted at the direction of the Joint Staff by DTRA. DTRA MAAs are often not conducted at the direction of Joint Staff, but MAAs may be used to satisfy MAA periodicity requirements at the discretion of the J-36 MA Branch. All JMAAs and any DTRA MAAs will be referred to collectively as DTRA-led MAAs throughout the remainder of this publication.

2. Additional MA-related assessments, such as Integrated Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability and Endurability Certification and Assessment Program, Command Cyber Readiness Inspections, Command Cyber Operational Readiness Inspection, Cybersecurity Service Provider inspections, and other DoD MA assessments will be included on the IAS at the discretion of J-36 MA Branch in order to increase situational awareness within the MA community, practice unity of effort, and reduce the probability of assessment fatigue on installations. DTRA will be included in the scheduling process with the requesting organization to promote effective coordination.

3. The J-36 MA Branch will coordinate with assessing organizations and DoD Components to minimize the impact of multiple assessments where possible. Due to the size of some locations, the size and complexity of missions, critical and mission-essential capabilities, and

supporting systems and assets; such locations may receive assessments more frequently than the required asset assessment periodicity.

(b) The lead component for each DTRA-led MAA on the IAS will act as the OPR for coordination and composition of the Assessment Focus Statement (AFS).

1. For DTRA-led MAAs, the lead component is typically the CCMD that is the primary mission owner with the greatest mission equity in missions conducted on the installation being assessed. The lead component may also be the DoD Component HHQ that has significant responsibilities at the assessed location as determined through the coordination process.

2. For Service MAAs, the Service is typically the lead component unless otherwise coordinated during the IAS coordination process. Mission Owners may provide an Assessment Focus Statement.

(c) All DoD Components will provide their proposed MAA schedules to the J-36 MA Branch during the annual IAS development process, during which the schedule for the next FY is solidified and an additional out year is drafted.

1. The nomination process for the next FY and subsequent out year begins in December and is staffed at AO, planner (O-6/GS-15), and GO/FO/SES levels before being published the following summer prior to the FY to which it applies.

2. In the initial, AO, round of coordination, components validate assessments previously nominated for an out year and/or nominate additional assessments for either FY under discussion.

3. Components will complete all applicable portions of the nomination form (even for validations) to include: assessment dates (to include alternate dates), assets, lead component, stakeholders, augments, and observers.

4. Components requesting an ACAT assessment in conjunction with the nominated DTRA-led MAA must specify the network/system to be assessed and provide complete POC information for the Information Systems Security Manager and the Authorizing Official responsible for issuing Authority to Connect to the system(s) needing access.

(d) DTRA conducts strategic vulnerability analysis by identifying trends, lessons learned, and potential assessment gaps for strategic missions.

(e) During the IAS coordination process, each DoD Component will ensure that the MAAs on the draft IAS are deconflicted all the way to the installation and unit levels for all applicable assets prior to endorsing their final IAS coordination.

(f) After the IAS is published, the assessing organizations will provide a formal notification message to the lead component and other components with equity 180 days prior to scheduled execution. Notification will include leaders and stakeholders at the DoD Component and DoD-wide levels to ensure adequate integration and oversight for the assessment. Notification includes a breakdown of responsibilities between the stakeholders, anticipated timeline, required documentation, and deliverables upon completion.

(g) Schedule changes/updates: the J-36 MA Branch manages and updates the IAS. Changes will be reflected in subsequent IAS updates for visibility to the DoD Community.

1. Schedule changes to DTRA-led MAAs within the FY are coordinated and approved at the AO level with J-36 MA Branch oversight.

2. Schedule changes to DTRA-led MAAs that cross FYs and/or exceed periodicity windows for assets to be assessed require GO/FO level request from the lead component (with concurrence from components with coordinating equities) and approval by J-36.

3. Schedule changes to component-led assessments require concurrence from components with equities only. Notification of any changes are required to be sent to J-36 MA Branch for inclusion in the next published change to the IAS.

4. The J-36 MA Branch will maintain the most current, approved version of the updated IAS on MARMS.

(h) Cancellation of a DTRA-led MAA represents a lost capability and often means lost resources. Consequently, a cancellation request with supporting rationale must come from or be endorsed by the first GO/FO/SES in the chain of command of the lead component. That component will forward the request to the J-36 MA Branch on SIPRNET for decision. The cancellation request will include the justification for the cancellation of the assessment, documentation of concurrence of other IAS designated stakeholders, assessment periodicity requirement implications for any TCAs that were to be assessed, recommended risk management actions from the last MAA, ongoing compliance measures, and the plan for rescheduling the assessment. The cancellation request template (Appendix A) will be utilized for cancellation requests.

(i) Cancellation of any other assessment on the IAS will be handled IAW the policy of the DoD Component conducting the assessment.

(j) The DDNHDO is the CJCS-delegated authority for the approval of MAA periodicity waivers and cancellation requests. Following coordination with all DoD Components annotated as having equity in MARMS and/or on the IAS, lead DoD Components will route the request to the J-36 MA Branch. If the waiver request is not already a part of a MAA cancellation request, utilize the Assessment Periodicity Waiver Request template (Appendix B).

(2) Assessment Focus Statement

(a) The AFS outlines the core effort for DTRA-led MAAs and includes missions, programs, and assets to be assessed.

1. During AFS development, the lead component will take inputs from the various stakeholders to determine the assessment scope.

2. The lead component will coordinate with the MAA team when developing the assessment scope to ensure feasibility based on team capacity.

3. The AFS developer will consider the assessing organization's capabilities and coordinate augmentation to assess any areas that are outside of the MAA team's capabilities.

(b) An AFS will be completed for all DTRA-led MAAs and other MAAs in which multiple DoD Components have listed equity on the IAS and within MARMS. Mission Owners may provide an Assessment Focus Statement for Services MAA's.

(c) The AFS for DTRA-led MAAs will be signed by at least the first O-6/GS-15 or equivalent in the lead component chain of command. Other assessment organizations will determine the appropriate approval authority for their documents.

(d) The AFS adds specificity to the IAS and will include at a minimum:

1. The mission(s) which will be assessed. Listed missions will be aligned to strategic missions and detail those established Mission Owner standards and conditions that were identified as critical to support for each asset.

2. A list of assets to be assessed with a brief description of each asset and the organization with budgetary (e.g., Planning, Programming, Budgeting, and Execution responsibility). These are typically DCAs or Tier 1 or Tier 2 TCAs, but Tier 3 TCAs and TAs may be recommended by any stakeholder and included in the AFS at the discretion of the lead component.

a. All assets listed on the AFS must have an associated criticality score for the mission being assessed, as described in Enclosure C of this instruction. If a criticality score is not available in MARMS, the lead component must coordinate with other equity holders to provide a score for the purpose of calculating risk as part of the assessment.

b. MAAs should be scoped to assess all TCAs and DCAs at each location to reduce assessment fatigue on command personnel, when feasible.

c. Stakeholders should resolve disputes regarding assets to be assessed at the lowest level possible and forward issues to the J-36 MA Branch if disputes cannot be resolved between components.

d. Any relevant information regarding potential new assets to be investigated or assessed should also be included in the AFS.

e. The AFS-listed assets do not preclude the assessment team from discovering new potential assets during the assessment and subsequently documenting those findings in the report.

3. Commander's Interest Items. Commander's Interest Items (CIIs) could be missions, program areas, or other areas of concern (not assets, which will be in the asset list) that are of special interest to the assessment stakeholders. The lead component will generally be responsible for selecting CII, but should take inputs across levels of command from the installation to the Joint Staff as appropriate. CIIs must be agreed upon by the MAA team to ensure feasibility and must be prioritized appropriately to ensure that they do

not detract from the team's ability to assess necessary critical assets and missions.

4. Points of Contact. Each point of contact (POC) must be listed with their name, phone number, and e-mail address. POCs (or suitable replacements) must be available during the entire assessment period, from IAS coordination through MAAR publication. The list of POCs will include:

a. A representative from each listed asset.

b. A representative from each DoD Component with equity.

c. A representative from the location/installation to act as MAA Coordinator.

(1) This individual will coordinate with installation/ location leadership, the assessing organization, site equities, and identified MARPA representatives.

(2) The location/installation MAA Coordinator will be responsible for liaising with the assessing organization and others regarding location-specific logistics and ensuring the lead component MAA Coordinator is informed of these arrangements.

(3) Location-specific logistics include but are not limited to: accommodations necessary for the assessment, such as classified work and briefing spaces, in-brief and outbrief times and locations, security permissions, and classified storage capability.

5. A list of any Tier 1 or Tier 2 TCAs at the location that will not be assessed, along with the rationale. This may be due to time restrictions during a mission-focused MAA, construction at the site, an imminent change in mission or location, or a recently completed assessment that would make the current MAA redundant. This information will be used for future assessment scheduling.

6. All relevant prior analysis results will be made available to the assessment team. If prior analysis data is not available in MARMS, assessment data must be provided to the assessment team as soon as possible during the assessment planning process.

7. When an AFS is required by this instruction, it must strictly follow the template provided in Appendix C. The AFS should simply scope the MAA and avoid repeating BEI.

(3) Assessment Team Preparation Overview. During the preparation phase of the MAA, the assessment team analyzes the selected mission(s), supporting capabilities, assets, dependencies, and CIIs at the assessment location to enable a properly scoped and efficiently scheduled assessment. The MAA team will become familiar with the site and adjust the team composition based on the missions, assets, and CIIs that will be assessed. Stakeholders at all levels will actively participate throughout the entire process to ensure that teams have a comprehensive understanding of the missions, capabilities, assets, dependencies, and CIIs that they will assess.

(4) Dependency Analysis

(a) The MA identification process utilizes mission decomposition to identify DCAs, TCAs, TAs, and critical capabilities. To be effective, an assessment team must collect and/or analyze both the mission dependencies and infrastructure dependencies of those assets. Assets may be people, facilities, or physical objects (e.g., Building 1201 or a network server), information systems or applications (e.g., an emergency message system), or information (e.g., real-time weather data). Assessment teams will collect and review applicable documents that provide an overview of command missions. These documents include installation and tenant standard operating procedures, technical documentation, OPLANs, CONPLANS, strategic mission documentation, other mission guidance, and any other documentation that provides a better understanding of mission and system dependencies. This process should identify stakeholders (e.g., interagency partners or other DoD mission owners) that were not known by the lead component. These additional organizations should be included throughout the assessment and added to the AFS as necessary.

(b) At a minimum, MAA teams will collect or develop:

1. Background information for the missions executed or supported by each asset identified on the AFS. This may include, but is not limited to, requirements to execute the mission in both competition and conflict, mission standards, and conditions of execution.

2. A list of hosts, major tenant organizations, and other supported commands (generally led by an O-6-equivalent or higher but may vary depending on the nature of the command) and their missions (if not

already provided). The assessing organization should assess newly added organizations to determine any new assets or dependencies that require analysis.

3. Comprehensive documentation of all supporting infrastructure that the assessed assets depend upon for mission execution. This should include DoD-owned, commercial, and foreign government-owned infrastructure. Installation MAAs should identify dependencies to no less than one node beyond the installation perimeter. As applicable, non–DoD-owned infrastructure will be included in this analysis and contacts should be obtained to permit as much assessment of the non-DoD infrastructure as possible.

(5) Pre-Assessment Site Survey

(a) The pre-assessment site survey (PSS) is an essential element of an MAA that supports the linkage of assets identified in the AFS with the component and DoD-wide tasks and missions. The preferred method of conducting a PSS is in person, although they may be conducted virtually via video teleconference or web conference if a team is familiar with the assessment site or in extenuating circumstances.

1. A key leader engagement meeting will be conducted prior to the PSS to enhance asset/installation participation and set expectations for the PSS and assessment.

2. While the MAA may focus on a particular asset or specific mission, installations are required to participate and support the MAA teams, lead component, and other stakeholders during AFS development, PSS activities, and MAA execution.

(b) The key objectives of the PSS are:

1. Finalize the list of assets to be assessed. Receive mission briefs from all the relevant units (as identified in the AFS) to establish a thorough understanding of the assets and infrastructure necessary to support mission execution. The list of assets to be assessed may be modified in coordination with MAA stakeholders.

2. Finalize CII list with inputs from the MAA Coordinator at the location and/or installation, lead component, CII originator, and others, as necessary.

3. Finalize the assessment team composition and augmentation based on the site characteristics and missions to be assessed.

4. Review the All-Hazards Threat Assessment (AHTA), the Defense Critical Infrastructure Threat Assessment (DCITA) (if applicable), and criticality scoring from the AFS with all stakeholders.

5. Coordinate logistics and team access with the host organization and MAA Coordinator.

6. Review assessment schedule.

7. Review provided documents to identify any missing information.

8. Provide the host organization and MAA Coordinator an overview of the assessment timeline and CONOPS.

(c) The site survey will typically consist of:

1. Office calls with senior leaders.

2. Mission briefs by the relevant commands, including all those with assets listed in the AFS.

3. MAA overview briefing by a representative from the assessing organization.

4. Site visits of all assets and dependencies identified in the AFS.

(d) Modifications to the assessment from what is outlined in the AFS will be coordinated with all the stakeholders and noted in the MAAR.

(6) ACAT Assessment Preparation. For DTRA-led MAAs, the lead component is responsible to ensure that asset owners coordinate with DTRA to identify the specific network(s) of interest and corresponding Authorizing Official point of contact for ACAT Assessments. As outlined in reference b, asset owners are required to grant Authority to Connect to DTRA within 60 calendars days of the location inclusion on the IAS.

b. Criticality Assessment

(1) The MA identification process is the foundation for the assessment process. Mission owners, asset owners, and capability providers (as applicable) perform a criticality review of each asset during the identification process as outlined in reference b and further clarified in Enclosure B of this instruction. After an asset has been reviewed and validated as a TCA (by a DoD Component) or DCA (by SecDef), its criticality has been established.

(2) Asset tiering is used to schedule assessments, determine the assessment periodicity, and identify the organizations responsible for conducting the assessment as stated in reference b. For each asset involved in an assessment, assessors will use identification process results (to include asset criticality scoring) as determined by mission and asset owner(s) as the basis of the MAA. An MAA may provide feedback to stakeholders via the MAAR that may influence changes to previously determined criticality scores and/or asset tiering and assist with updates to loss impact statements. For instance, unique mission capabilities or redundant resources may be discovered during the MAA and provided to stakeholders for use in the next identification cycle.

(3) The MAA must address mission impact as it relates to criticality and vulnerability. Mission impact must consider the TTIM (capability and/or mission) and TTR (capability and/or mission) from the potential hazard or threat listed in the AHTA.

c. All-Hazards Threat Assessment

(1) AHTA guidance is provided by reference e and further specified in this instruction to meet the requirements for its use in MA IAW reference b. The AHTA identifies and characterizes the hazards and threats, to include natural events, human-caused events (accidental and intentional), and technologically caused events. In addition, the AHTA process identifies the probability of the occurrence of these threats and hazards based on historical data, prevailing environmental conditions, and detailed intelligence threat analysis.

(a) The AHTA will not determine the degree to which the installation or assets are susceptible to an identified threat or hazard—that is evaluated during the vulnerability assessment.

(b) The threat and hazard categories and descriptions, scoring criteria, and methodology are published by DTRA in collaboration with other DoD Components IAW reference e.

(2) This assessment is the responsibility of asset owners, command leadership, and capability providers (as applicable). The AHTA will be informed by the DIA all-source global baseline assessment and Geographic Combatant Command (GCC) threat assessments. For DCAs and other MACB-prioritized DCI (see enclosure G), the DCITA should provide the validated source input on threats beyond those at the local level and should be provided to the installation at least 90 days prior to the scheduled date of the vulnerability assessment. It is then adapted for the local area through collaboration between relevant working groups and the installation community. The AHTA should be developed with the active engagement of personnel familiar with local conditions and mission requirements.

(a) In accordance with reference e, the AHTA is approved by the authority with jurisdiction over the installation (e.g., wing commander, installation commander). If the site is not an installation, then the commander of that site will approve the AHTA for the purposes of a MAA. For all DTRA-led MAAs, the assessing organization will remind the installation that the GCC baseline threat and hazard assessment supplement and any applicable DCITAs will inform their AHTA. An installation may create a Top Secret AHTA supplement depending on the nature of the threats that may affect that location or asset.

(b) For maximum standardization, the AHTA should use the best available authoritative data sources to determine the probability of occurrence of a given hazard or threat. At a minimum, the AHTA will include a description of each hazard and threat along with an estimate of the likelihood of the identified event occurring. This allows consideration of the historical frequency and a range of likely intensity for the hazard, or the known capability of hostile actors and potential likelihood of these capabilities being employed as threats, when applicable. Commands may also collaborate with other commands in the same geographical area to ensure the best data is utilized to inform the AHTA.

(c) For an MAA, threat and hazard probability will be scored on a scale from 0.01 to 1.00 for each threat or hazard combination listed on the AHTA workbook tab in the DoD MAA workbook from reference e. When using the AHTA tool, selecting the range subsets will automatically populate a score.

d. Vulnerability Assessment

(1) The vulnerability assessment is an on-the-ground evaluation to determine asset vulnerability to the hazards and threats identified in the AHTA. Assessors will note conditions that could impact mission execution. Vulnerabilities must be associated with an assessed asset or a functionally

related asset to allow consideration of criticality in the risk assessment. Programmatic vulnerabilities not directly affecting an asset may also be recorded in the MAAR and submitted in MARMS as required.

(2) All hazards and threats listed in the AHTA, regardless of the probability of occurrence, will be considered by the assessment team when assessing the vulnerability. The MAA team will pair relevant threats and hazards with asset vulnerabilities to identify which assets are susceptible to each threat and hazard.

(3) The MAA team composition must include SMEs to address all DoD MAA Benchmarks (reference d) applicable to the assessment. The exact composition of the teams should be adjusted to meet the assessment requirements but must maintain sufficient expertise to assess every applicable benchmark area. An MAA team will include experts in dependency analysis, risk management, physical security, infrastructure engineering, cybersecurity, antiterrorism, communications, and emergency management at a minimum. Additional SMEs are available from various DoD components as necessary, based on the nature of the assets or missions and coordination between the lead component and assessing organization. Lead components must coordinate early with assessing organizations to determine if any outside expertise is required and determine a plan for acquiring that expertise. Early planning and coordination are essential to ensure proper MAA team composition is available for the assessment.

(4) The MAA team will make observations of vulnerabilities or other findings. These observations will focus on the impacts a vulnerability has on accomplishing the assigned mission and the ability to perform MEFs, instead of solely on compliance with policy and regulation. Vulnerabilities may exist even when an organization is fully compliant and, conversely, non-compliance may not result in any significant or exploitable vulnerability. Assessors should attempt to connect any deviation from the standards to the assessed assets and identified hazards and/or threats. The assessors will use the DoD MAA Benchmarks (reference d) in addition to their experience to determine whether vulnerabilities exist.

(5) The DoD MAA Benchmarks (reference d) provide guidance from the MARPA. They identify standards that assessors should consider when identifying significant or exploitable vulnerabilities.

(a) The DoD MAA Benchmarks also provide references to the applicable policy guidance. They are reviewed by the J-36 MA Branch and formally coordinated with DoD Components every two years. Joint Staff J-36 may publish minor updates without formal coordination at their discretion in order to keep the benchmarks up to date with current policy guidance.

(b) DTRA publishes supplemental guidelines for the DoD MAA Benchmarks to provide recommended assessor questions to assess each benchmark in reference f.

(6) In addition to infrastructure analysis and vulnerability assessment requirements outlined above, DTRA-led MAAs for DCAs, MACB-prioritized DCI, and other tiered assets prioritized based on mission and available resources will include:

(a) Adversarial approach analysis to evaluate the asset, site, and supporting infrastructure and identify potential attack vectors to disrupt mission accomplishment.

(b) An ACAT to conduct on-network information and traffic collection to evaluate critical networks and control systems and identify vulnerabilities and determine risk to mission execution.

1. Asset owners will coordinate with DTRA to grant ATC within 60 calendar days of the location's designation to receive an ACAT on the published IAS. The lead component for the assessment will ensure this has occurred as part of their overall coordinating responsibilities leading up to the assessment. DTRA will report to the CJCS and Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance (DASD(DC&MA)) any sites or assets for which owners are unable or unwilling to grant ATC. If the ATC is not granted within 30 calendar days of this notification, the ACAT for that location will be cancelled.

2. In cases where an MAA has been designated to receive an enhanced cyber analysis, asset owners who desire an MAA without it may request a formal waiver from the MA SSG co-chairs for this requirement.

3. Asset owners will provide DTRA with the latest mission based cyber risk assessment results for all applicable TCAs and DCAs being assessed.

(c) Analysis by the Defense Contract Management Agency's center of excellence for Defense Industrial Base supply chain network analysis, providing identification of critical industrial capabilities, foreign supplier dependencies, single or sole sources of supply, and associated industrial base risks (when applicable).

(d) Analysis by Defense Information Systems Agency on vulnerabilities for networks and mission-essential long-haul communications.

(7) Assessors will categorize the vulnerability of an asset by considering its level of exposure to an identified hazard or threat in its current state at the time of the assessment, including all protection and response capabilities available. The following guidelines for categorizing vulnerabilities will be used:

(a) Low. The vulnerability is of minor concern.

1. No known weaknesses through which adversaries, natural hazards, or accidental disruptions would be capable of causing the loss of or disruption to the asset's mission.

2. Mitigation is fully implemented, assessed, and effective.

(b) Moderate. The vulnerability is of moderate concern based on the exposure of the vulnerability and ease of exploitation.

1. At least one known weakness exists through which adversaries, natural hazards or accidental disruptions would be capable of causing the loss or disruption to the asset's mission.

2. Effective mitigation measures are in place.

(c) Significant. The vulnerability is of significant concern, based on the exposure of the vulnerability and ease of exploitation.

1. Multiple known weaknesses through which adversaries, natural hazards, or accidental disruptions would be capable of causing the loss of or disruption to the asset's mission functionality.

2. Some effective mitigation measures are in place or planned but not implemented; compensatory measures are in place and at least minimally effective.

(d) High. The vulnerability is exposed and exploitable.

1. Known weaknesses through which adversaries, natural hazards, or accidental disruptions would be capable of causing the loss of or disruption to the asset's mission functionality.

2. No effective mitigation measures are in place or planned; mitigation measures are planned but not implemented; no compensatory measures are in place or those that are in place are not effective.

e. MA Assessment Scoring

(1) Employing the definitions and guidelines previously described, SMEs will apply numerical scores to their qualitative observations. Qualitative terms linked to vulnerability scores may be used to assist the assessor with determining an appropriate vulnerability score. These scores allow MAA teams to quantify their assessment of risk to mission. The quantitative results are only the starting point for making risk decisions and may give a false sense of precision if applied incorrectly; leaders require refined analysis of the observations for subsequent risk management. The scoring guidelines are broad enough to provide flexibility for the various teams and SMEs, while providing sufficient standardization across the DoD.

(2) Each supporting assessment (criticality, AHTA, and vulnerability) uses a scale of 0.01 to 1.00 to quantify their evaluation. Assessors will ensure that their scoring is logical and consistent to score their observations of hazard, threats, or vulnerabilities. Assessors should avoid using minor numerical distinctions for subjective observations since there is limited significance between small score differences. Assessors should generally choose the middle of the category score and adjust further only with specific amplifying information. For risk, hazard and threat, and vulnerability categories, use the following scale:

(a) High. 1.00 to 0.80.

(b) Significant. 0.79 to 0.50.

(c) Moderate. 0.49 to 0.21.

(d) Low. 0.20 to 0.01.

(3) All MAAs will use the following formula to determine the risk category:

$$R=\sqrt[3]{C \times H/T \times V}$$

R = Risk

C = Criticality Score
H/T = Hazard or Threat Score (not divided by)
V = Vulnerability Score

(a) DoD Components may use their own formulas internally to meet their own requirements but must input their MA assessment scoring into MARMS IAW the above guidance and reference a.

(b) Any alternate scoring by DoD Components must be separate and in addition to using the above guidance.

f. Risk Assessment

(1) Preliminary Results

(a) Upon completion of the MAA, the team will provide an outbrief to the installation leaders, mission owners, asset owners, and capability providers (if applicable). If an organization desires an outbrief but is not present at the designated time and location, they are responsible for making such arrangements with the assessment team. The purpose of this outbrief is to provide stakeholders a general overview of significant findings and the opportunity to answer specific questions.

(b) Using a preliminary analysis of the three assessments (criticality, AHTA, and vulnerability), the team will highlight those observations that are of particular concern, generally those identified with significant or high-risk ratings. The preliminary analysis may address any commander’s interest items, health and safety concerns, or discoveries made by the team that were not outlined in the AFS or dependency analysis. The team may provide initial recommendations for addressing the observations. The outbrief is not a final product but provides initial feedback to the leaders on anticipated observations and conclusions, prior to the team completing its full assessment report.

(2) Post Assessment Review

(a) The risk assessment begins when the MAA supporting assessments are complete. This process continues from the preliminary conclusions identified during the outbrief and develops a full understanding of the risk to mission. The assessment will include root cause analysis to identify the source of the risk rather than just the observed symptoms of a problem.

(b) The MAAR will be provided to all stakeholders via MARMS, and the assessing organization will notify each DoD Component with equity (as listed on the AFS) of its completion. Mission owners, asset owners, and capability providers (if applicable) may utilize the assessment team's risk findings in their standing risk management processes. The risk scored inputs compare risks across the enterprise and provide a starting point for commanders to understand their risks. These risk scores should be used as an input to each commander's risk management process to help inform his/her official risk assessment.

(c) The MAA results (including MAAR files) will be maintained in the MARMS registry for a minimum of 15 years. A hard copy of the MAAR will be maintained by the assessing organization for a minimum of 10 years or the report publication of a subsequent assessment.

4. Mission Assurance Assessment Report

a. The results and MAAR will be completed and posted to MARMS by the assessing organization within 60 days of the completion of the vulnerability assessment. Assessing organization will complete BEI and post to MARMS within 90 days of completing assessment. When significant findings warrant immediate notification, as in the case of high risks or unsafe conditions, the MAA team will provide those findings to the stakeholders at the outbrief and notify the lead component and all asset owners if a representative is not present at the outbrief.

b. Additional timeline requirements for DTRA-led MAAs of DCA and MACB prioritized DCI include:

(1) Assessment team outbrief will be provided to the DASD(DC&MA), CJCS, and senior asset-owner leadership within 15 calendar days of completion of the assessment, with the final report provided within 60 calendar days.

(2) Availability of DTRA, DIA, and/or other appropriate centers of excellence to discuss their findings with the MACB and answer any additional questions.

c. The MAAR will address the validation of the criticality of the assessed assets, the installation hazards and threats, and the identified vulnerabilities. The core element of the MAAR is the discussion of observations that result in risk to mission. That risk will be discussed in the MAAR in the context of missions listed in the AFS, highlighting both mission impact and potential consequence of the loss. The report will include:

(1) A brief discussion of the MAA process, providing context to the stakeholders.

(2) An executive summary stating the overall mission risk associated with each asset, a brief description of all identified significant and high-risk findings, and any other information appropriate for executive consumption. The executive summary will also reference all threats assessed as high or significant likelihood in the DCITA and whether there were identified vulnerabilities which might be exploited, leading to high or significant mission risk.

(3) The final dependency and risk analysis report should include:

(a) A detailed description of all the assets including supported and supporting missions. The report should also annotate any asset BEI that was found to be inaccurate, and any information helpful to a mission owner in reviewing an asset's criticality.

(b) A detailed analysis of dependencies between assessed missions and assets and the installation's DoD and non-DoD supporting infrastructure (for installation-based assessments, to one node beyond the installation perimeter).

(c) Expected mission impacts if any asset or dependency is lost, corrupted, or no longer trusted.

(d) The final AHTA and hazard/asset or threat/asset pairing.

(e) A final output summary database of risks with their associated risk levels and recommended mitigations.

(f) A section outlining what was assessed, to include detailed observations for each determined vulnerability or programmatic concern identified as a risk to the mission. These observations may be accompanied by recommendations to address the vulnerability and an estimate of how much the recommendations would reduce the vulnerability to a requisite level.

d. The team will make recommendations for mission owners, asset owners, and capability providers (if applicable) to reevaluate asset criticality or local hazards and threats if additional supported missions or relevant threats and hazards are identified during the MAA.

e. All observations will be associated with at least one DoD MAA Benchmark and recorded in the report. The specific formatting may be modified to meet Service and Component the requirements, but each MAAR will use a standard template and scoring to facilitate trend analysis. All MAA resulted and final documentation will be shared to the MARMS registry or appropriate MA system of record. The team may also identify best practices when applicable.

f. The completed MAAR will be kept on file by the assessing organization, shared to the MARMS registry and provided to the DoD Component-level organizations with equity in the assessment as identified in the AFS. The increased visibility of the report permits decisions concerning mitigation, remediation, or acceptance of risk to be made at the appropriate level. It will support their respective risk management processes as discussed in Enclosure E of this instruction.

5. Subordinate Command Mission Assurance Assessments

a. The guidance in this instruction is applicable to DoD Component-level MAAs, as required by reference b. Any assessment intended to meet the periodicity requirements stated in reference b and other MA policy will be conducted IAW this guidance. This instruction provides baseline requirements and does not preclude commanders from adding additional requirements.

b. Subordinate command MAAs should adopt component-level methodology to the maximum extent possible and will comply with the following requirements:

(1) Subordinate command MAA schedules will be routed through applicable DoD Components and submitted to the J-36 MA Branch for inclusion in the IAS to ensure that these assessments are adequately de-conflicted and periodicity requirements are satisfied.

(2) DoD Component-level MAAs take precedence over subordinate command MAAs.

(3) The J-36 MA Branch has the authority to coordinate assessment dates of subordinate command MAAs during the IAS coordination process in order to reduce excessive assessments. Any changes to subordinate command MAA dates on a published IAS should be coordinated with the consent of the

appropriate subordinate command. The subordinate command should notify any stakeholders of any scheduling changes to the MAA.

6. Annual MA Self-Assessments. IAW reference b, DoD Components will perform annual self-assessments or self-inspections as required by MA-related programs and activities, ensure subordinate commands perform the annual self-assessment/inspection requirements, and record results in the appropriate MARMS module.

7. Higher Headquarters MARPA Review. MAAs may fulfill HHQ program review and vulnerability assessment requirements for MA-related programs and activities when permitted by that MARPA's applicable DoD governance. If specified, all DoD MAA Benchmarks in that section must be assessed. This accommodation could eliminate the commander's requirement to complete an additional review of specific MARPAs.

a. HHQ program reviews are not the primary assessment priority and should not interfere with the primary purpose of the MAA. Commanders may request that MAA teams (DTRA-led or otherwise) satisfy a HHQ program review requirement in their CIIs in the AFS; the assessing organization will review the request and evaluate its merits against allocated time and resources. HHQ requirements will only be considered after the completion of the on-site assessment.

b. Observations made in support of the HHQ program review may not have a direct relation to mission risk, but still require remediation and monitoring. Substantial programmatic weaknesses identified in the HHQ program review that could lead to the loss of life or mission failure if left unmitigated should be classified as vulnerabilities.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE D

JMAA or DTRA MAA CANCELLATION REQUEST TEMPLATE

DD MMM YYYY

MEMORANDUM FOR JOINT STAFF DEPUTY DIRECTORATE FOR NUCLEAR
HOMELAND DEFENSE
3000 Joint Staff Pentagon
Washington, DC 20318-3000

SUBJECT: Request for Cancellation of Fiscal Year 20XX Joint Mission Assurance Assessment or Defense Threat Reduction Agency Mission Assurance Assessment

1. Headquarters (HQ), United States XXX Command (HQ USXXX) requests to shift the fiscal year (FY) 20XX Joint Mission Assurance Assessment (JMAA)/ Defense Threat Reduction Agency (DTRA) Mission Assurance Assessment (MAA) for XXX Location, (DD MMM – MMM YYYY) until FY 20XX *(Do not insert specific dates; J-36 MA Branch reserves rescheduling prerogative). (State reason for cancellation: any change of schedule to a later FY is considered a cancellation that requires rescheduling. Requests to shift assessments within a FY do not require a memorandum; coordinate directly with J-36 MA Branch.)*

2. *(State other commands with equities and whether they have concurred with cancellation being requested.)* CCMD XXX concurs with this request. Location XXX concurs with this request. XXX (Agency) concurs with this request. XXX (Service) concurs with this request.

3. *(State plan to complete future MAA requirement.)* We will leverage the current FY 20XX/20XX IAS nomination process to request new assessment dates for XXX Location.

4. *(State if you are requesting a periodicity waiver from the Joint Staff for [MAA] requirement. State length of waiver being requested and reason for the waiver request. Also state how you are mitigating the lack of required MAA at the site [e.g., internal assessment, other MARPA assessments].)*

5. My POC is Rank Name at DSN XXX-XXX-XXXX or SIPRNET e-mail XXX.

NOTE: This template is UNCLASSIFIED when separated from classified attachments. This memorandum will be classified at the appropriate level IAW reference c when completed. Include all applicable portion markings.

APPENDIX B TO ENCLOSURE D

MAA PERIODICITY WAIVER REQUEST TEMPLATE

DD MMM YYYY

MEMORANDUM FOR JOINT STAFF JOINT STAFF DEPUTY DIRECTORATE
FOR NUCLEAR HOMELAND DEFENSE
3000 Joint Staff Pentagon
Washington, DC 20318-3000

SUBJECT: Request for Waiver of Mission Assurance Assessment Periodicity Requirement

1. Headquarters, United States XXX Command (HQ USXXX) requests to waive the Assessment Periodicity Requirement for XXX asset, (SMADS ID: XXXXX) until fiscal year (FY) 20XX. (*Do not insert specific dates. J-36 MA Branch reserves scheduling prerogative. State reason for request.)*

2. *(State other commands with equities and whether they have concurred with waiver being requested.)* CCMD XXX concurs with this request. Location XXX concurs with this request. XXX (Agency) concurs with this request. XXX (Service) concurs with this request.

3. *(State plan to complete Mission Assurance Assessment requirement.)* We will leverage the FY 20XX/20XX IAS nomination process to request new assessment dates for XXX Location.

4. *(State how you are mitigating the lack of required MAA at the site.)*

5. My POC is Rank Name at DSN XXX-XXX-XXXX or SIPRNET e-mail XXX.

NOTE: This template is UNCLASSIFIED when separated from classified attachments. This memorandum will be classified at the appropriate level IAW reference c when completed. Include all applicable portion markings.

(INTENTIONALLY BLANK)

APPENDIX C TO ENCLOSURE D

ASSESSMENT FOCUS STATEMENT TEMPLATE

DD MMM YYYY

MEMORANDUM FOR DIRECTOR, NUCLEAR ENTERPRISE SUPPORT
DIRECTORATE (J10), DEFENSE THREAT REDUCTION
AGENCY

SUBJECT: Endorsement of the Combatant Command Assessment Focus Statement for Joint Mission Assurance Assessment at INSTALLATION

1. In accordance with (IAW) the fiscal year (FY) 20XX Integrated Assessment Schedule, the Defense Threat Reduction Agency (DTRA) will conduct a Joint Mission Assurance Assessment at INSTALLATION IAW Chairman of the Joint Chiefs of Staff Instruction 3209.01A. This assessment is a significant vulnerability assessment tool that we will use to complete our risk assessment of assets supporting Combatant Command strategic missions.

2. The focus of this assessment will be MISSION OF INTEREST. The attached Assessment Focus Statement, developed in coordination with the other stakeholders, identifies several key assets that are critical to supporting that mission at INSTALLATION.

3. Please contact my POC, NAME at PHONE XXX-XXX-XXXX or EMAIL XXX with any concerns or questions.

Attachments:
As stated

cc:
Joint Staff J-36 w/ enclosures
Asset Owners w/ enclosures

NOTE: This template is UNCLASSIFIED when separated from classified attachments. This memorandum will be classified at the appropriate level IAW reference c when completed. Include all applicable portion markings.

Attachment A: AFS Memo

DD MMM YYYY

SUBJECT: Assessment Focus Statement for Fiscal Year 20XX Joint Mission
Assurance Assessment at INSTALLATION.

1. The Defense Threat Reduction Agency (DTRA) will conduct a fiscal year (FY) 20XX Joint Mission Assurance Assessment (JMAA) at INSTALLATION. The Pre-Assessment Site Survey (PSS) will be conducted from d Mmm yyyy to d Mmm yyyy. The On-the-Ground Assessment will be conducted from d Mmm yyyy to d Mmm yyyy.

2. The primary mission focus of this assessment will be MISSION OF INTEREST. *(Additional missions may be identified but should be limited to 2–3 to maintain assessment focus.)*

3. The stakeholders listed below have reviewed their equities at INSTALLATION and identified the following Commander's Interest Items. Primary and alternate points of contact are listed in Enclosure 2.

a. Primary Mission Owner – CCMD COMMANDER'S INTEREST ITEMS. *Commander's interest items may range from threats to protection programs. They should not include specific assets, which will be listed in paragraph 4. If there are no additional CIIs and a standard MAA review of the benchmarks is sufficient, please state that here.*

b. Installation Commander – *CII example: Request the JMAA take a close look at the AT/FP barrier plans. The funding currently available and projected for the near future appears to be too low to adequately resource the plans. Request the JMAA team review the currently resourced plans and provide recommendations for prioritizing efforts to minimize risk.*

c. OTHER STAKEHOLDERS AS LISTED ON THE INTEGRATED ASSESSMENT SCHEDULE. CII.

d. *AS REQUIRED ADDITIONAL STAKEHOLDERS. CII.*

4. The assets supporting *MISSION* and their required Standards and Conditions are listed in Enclosure 3.

5. *List assets that will not be assessed during this assessment. This does not need to be an exhaustive list but should identify Tier 1 and Tier 2 assets that*

would typically be assessed by a JMAA but are not required during this assessment. List the reason why the asset should not be assessed. If a recent assessment was conducted, provide the date and POC that can provide a copy of the report.

6. DTRA is authorized to coordinate directly with the mission owners and asset owners listed in this AFS to obtain additional information required to complete the JMAA. A DTRA mission analyst will contact the POCs to ensure that correct missions, OPLANS/CONPLANS, and mission essential tasks (MET) are identified along with the expected TTIM and TTR. DTRA will provide a list of deliverables, responsible offices, and the projected timeline for the assessment.

Attachment B: Points of Contact

Assessment lead and alternate POCs for the DoD Component and Installation stakeholders as listed on the Joint Staff Integrated Assessment Schedule. Additional stakeholders may be identified as necessary.

Primary Mission Owner	POC Name	POC #	POC NIPR	POC SIPR	POC JWICS
	Alt. POC Name	Alt POC #	Alt POC NIPR	Alt POC SIPR	Alt POC JWICS
Installation Commander	Commander	CDR #	CDR NIPR	CDR SIPR	CDR JWICS
	MAA POC Name	POC #	POC NIPR	POC SIPR	POC JWICS
	Comm POC	Comm #	Comm NIPR	Comm SIPR	Comm JWICS
	Plans POC	Plans #	Plans NIPR	Plans SIPR	Plans JWICS
	Utilities POC	Utilities #	Utilities NIPR	Utilities SIPR	Utilities JWICS
	AT/FP POC	At/FP #	AT/FP NIPR	AT/FP SIPR	AT/FP JWICS
IAS Listed Stakeholder 1	POC Name	POC #	POC NIPR	POC SIPR	POC JWICS
	Alt. POC Name	Alt POC #	Alt POC NIPR	Alt POC SIPR	Alt POC JWICS
IAS Listed Stakeholder 2	POC Name	POC #	POC NIPR	POC SIPR	POC JWICS
	Alt. POC Name	Alt POC #	Alt POC NIPR	Alt POC SIPR	Alt POC JWICS
IAS Listed Stakeholder 3	POC Name	POC #	POC NIPR	POC SIPR	POC JWICS
	Alt. POC Name	Alt POC #	Alt POC NIPR	Alt POC SIPR	Alt POC JWICS
Additional Stakeholder 1	POC Name	POC #	POC NIPR	POC SIPR	POC JWICS
	Alt. POC Name	Alt POC #	Alt POC NIPR	Alt POC SIPR	Alt POC JWICS
Additional Stakeholder 2	POC Name	POC #	POC NIPR	POC SIPR	POC JWICS
	Alt. POC Name	Alt POC #	Alt POC NIPR	Alt POC SIPR	Alt POC JWICS
Additional Stakeholder 3	POC Name	POC #	POC NIPR	POC SIPR	POC JWICS
	Alt. POC Name	Alt POC #	Alt POC NIPR	Alt POC SIPR	Alt POC JWICS

Attachment C: Asset Matrix

INSTALLATION Asset Matrix (Prioritized by Asset ID and Tier Ratings – Tier 1, 2, TA). In addition to the assets identified in the matrix below, other assets may be assessed as time permits.

JMAA Number and Dates						
Assets to be Assessed						
Asset	SMADS Asset ID	Tier Rating, Criticality Score	Supported CCMD / Agency	Supported Plan	Supported MET(s) / MEF(s)	Standards and Conditions

ENCLOSURE E

RISK MANAGEMENT

1. Purpose. Establish processes, timelines, and templates for executing MA risk management actions for DCAs and MACB-prioritized DCI. DoD Components will establish their own processes to manage risk for other TCAs supporting their designated missions.

2. Overview

a. The MA SSG and MA ESG review component risk recommendations based on integrated inputs from: assessment results; threats and hazards; mission dependencies; and mitigation and remediation options.

b. The MA SSG evaluates the initial risk management recommendations before forwarding them to the MA ESG.

c. Based on the MA SSG and MA ESG decisions, ODASD(DC&MA) will communicate the risk to the SecDef through the MA Annual Report or as a separate action or info memo.

3. Overall process and timelines. This is a five-step process:

a. Step 1 – CCMDs Develop MMP

(1) MMPs describe mission impact and mitigation options if an asset is destroyed or unavailable. They should be mission-focused and based upon the capability an asset provides and not the asset itself.

(2) Mission owners (generally CCMDs) will submit GO/FO/SES-approved MMPs to the J-36 MA Branch within 90 days of designation as a DCA or MACB-prioritized DCI.

(3) The MMP will use the enclosed template (Appendix A). Components may add additional information, but will include the following information (at a minimum):

(a) Asset Information.

(b) Asset Description.

(c) Capability Provided.

(d) Mission Impacts of Catastrophic Loss.

(e) Mitigation Options.

(f) Risk Levels and Acceptability.

(g) Conclusions/Recommendations.

b. Step 2 – Asset Owner Makes Initial Presentation at the MA SSG

(1) Presentation date will be scheduled by the MA SSG ODASD(DC&MA) Secretariat, normally for 30–90 days after an assessment is completed.

(2) Asset owners will present a criticality overview and a summary of High and Significant vulnerabilities. Asset owners will also ask for assistance from other components if it is required.

c. Step 3 – Asset Owner Makes In-Progress Review at the MA SSG

(1) Presentation date will be scheduled by the MA SSG ODASD(DC&MA) Secretariat and is normally four months after the initial presentation to the MA SSG (two MA SSGs later).

(2) Asset owners will present an in-progress review on the status of their plans of action and milestones for addressing the High and Significant vulnerabilities. Asset owners will also ask for assistance from other components if it is required.

(3) Asset owners may make recommendations on some or all the vulnerabilities if they have firm POAMs in place.

d. Step 4 – Asset Owner Makes Final Recommendations at the MA SSG

(1) Presentation date will be scheduled by the MA SSG ODASD(DC&MA) Secretariat and is normally four months after the in-progress review presentation to the MA SSG (two MA SSGs later).

(2) Asset owners will present final courses of action and milestones for addressing the High and Significant vulnerabilities.

(3) The MA SSG will either accept the plans and transition the actions to Annual Monitoring or ask the Asset owner to return to address questions on their plans.

e. Step 5 – Asset Owner Provides Annual Updates to the MA SSG until all Open Actions are Completed. Asset owners will provide status on their remediation action and anticipated completion date. Asset owners will also state if they need assistance, or they are resourced to close the vulnerability.

4. MA SSG Preparation Process and Timeline. There are multiple steps leading up to each MA SSG. The MA SSG co-chairs may adjust these steps for an MA ESG.

a. Draft Slides Due. Components deliver draft MA SSG slides to the ODASD(DC&MA) Secretariat. The Secretariat merges component slides into the draft package for AO review.

b. Action Officer Review of the Draft MA SSG Slides. ODASD(DC&MA) and J-36 MA Branch host AO-level meeting with components to review and recommend changes to the MA SSG slides.

c. Delivery. Components deliver updated slides with changes from the AO review.

d. Planner Review of the Draft MA SSG Slides. ODASD(DC&MA) and J-36 MA Branch host planner-level meeting with components to review and recommend changes to the MA SSG slides.

e. Updated Delivery. Components deliver updated slides with changes from the planner review.

f. Read-Ahead and Draft Slides to Co-Chairs. ODASD(DC&MA) and J-36 MA Branch provide the co-chairs with the draft slides and read-ahead talking points to prepare their principals for the co-chair meeting.

g. Co-Chair Meeting. MA SSG co-chairs meet and finalize the slides and meeting execution plan.

h. Publish MA SSG Slides. ODASD(DC&MA) publishes final slides to the MA SSG membership.

i. MA SSG. Meeting execution.

j. MA SSG. Summary of Conclusions (SoC).

APPENDIX A TO ENCLOSURE E

MISSION MITIGATION PLAN TEMPLATE

[Insert Command Logo]

[Insert Asset Owner]

Mission Mitigation Plan

For

[Insert Asset Name]
[Insert Asset Location – (Base, State/Country)]

Approved by: **[Insert Approving Official Name, Rank, Title]**

As of: **[Insert Approval Date]**

NOTE: This template is UNCLASSIFIED when separated from classified attachments. This document will be classified at the appropriate level IAW the reference c when completed. Include all applicable portion markings.

Classified by:
Derived from:
Declassify on:

This Mission Mitigation Plan describes mission impact and mitigation options for [Insert Mission Owner] mission execution if the following Task Critical Asset is destroyed or unavailable.

1. Asset Information

a. Name: *(self-explanatory)*

b. Location: *(self-explanatory)*

c. AOR: *(self-explanatory)*

d. Asset Owner: *(self-explanatory)*

e. Mission Owner(s): *(List all Mission Owners, not just your organization)*

f. Primary Staff Element: *(Which non-DCI staff element on your staff is most concerned with this asset? Who does the DCI office work with to gather data about this asset? J23, J45, J6, etc.)*

g. Mission-Essential Task, Mission-Essential Function, Condition, and Standard: (What *is the impacted MET/MEF along with the Condition and Standard from your plan?)*

2. Asset Description

a. *What is the asset? Describe the asset in layman's terms. This information is obtained from an authoritative database. Description should focus on support of plans or missions and not simply a listing of JMETs that may fail.*

b. *What does the asset do to support your mission? Describe the function of the asset in layman's terms.*

3. Mission Impacts of Catastrophic Loss

a. *Include a restatement of your mission impact statement, but with a level of detail that reflects the mission impacts. Be specific. (Example: XX% sortie generation loss or XXX short tons.)*

b. *What does that mean to your plans/operations? (Example: OPLAN XXX Phase III delayed XX days or complete mission failure for OPLAN XXX Phase II.) Add additional information that describes the loss impact in layman's terms.*

4. Mitigation Options

a. What can DoD do to mitigate the loss of this asset?

(1) What are the impacts of this mitigation? Global Force Management? Other?

(2) Who else needs to act to implement this mitigation?

b. What is your organization doing to mitigate the loss of this asset?

(1) Additional Planning? Be specific.

(2) Exercises? Studies? Etc.?

c. Mitigation Options will be in two categories:

(1) Validated – options that have been exercised and validated.

(2) Planned – options that are conceptual and have not been exercised or validated.

5. Risk Levels and Acceptability

a. What is the Risk Level with no mitigation options, and is it acceptable or unacceptable?

b. What is the Risk Level when executing each mitigation option, and is that residual risk acceptable or unacceptable?

c. What is the desired end state for risk?

6. Conclusions/Recommendations

a. Acceptability of current level of risk associated with this asset.

b. Recommendations from your organization to the DoD/Joint Staff.

c. Additional conclusions.

[Insert Signature Block of Approving Official]

(INTENTIONALLY BLANK)

ENCLOSURE F

MONITORING AND REPORTING

1. Purpose. Specifies the formal monitoring and reporting process between all parties, including the CJCS, CCMDs, Services, and Agencies.

2. Overview. MA monitoring and reporting processes enable all DoD Components to maintain situational awareness of the risks related to their missions.

a. The monitoring process consists of operational status, threat and hazard monitoring, risk management implementation tracking, and the use of MARMS to support monitoring and reporting activities.

b. Monitoring and reporting requirements ensure that risk mitigation and/or acceptance decisions are made at the appropriate level, whether that is tactical, operational, or strategic.

3. Process. Asset owners and/or capability providers must monitor operational status, credible threats, and forecasted hazards to critical assets. Required reports will be provided to the National Military Command Center (NMCC) and all mission owners who have equity in, are users of, or rely upon the asset.

a. In order to facilitate timely execution of mission mitigation strategies, mission owners require operational status changes to be reported concurrently with those reported to the NMCC.

b. The reporting requirements contained herein apply to Tier 1 TCAs as specified in reference h. Asset owners/capability providers should similarly report the loss or degradation of Tier 2 TCAs to all DoD Components who have listed equity in MARMS.

c. Operational Reporting Requirements

(1) For initial notification, commanders must report the loss, incapacitation, or degradation of TCAs via Operational report (OPREP)-3 (Event and Incident Operational Report) IAW the requirements of reference h. Reports must be made as soon as the loss or degradation is discovered.

(2) The asset owner/capability provider will continue to provide required information according to the Situation Report (SITREP) requirements of reference h until the asset is able to fully provide the required capability.

4. Categories and Format. Reporting falls into three categories: changes in operational status, threat or hazard, and risk management implementation.

a. Change in Operational Status

(1) Asset Owner. Any change that impacts the operational status of a TCA, resulting in non-mission-capability or partial mission-capability, will be reported by the asset owner/capability provider as soon as the loss or degradation is realized. The asset owner/capability provider will include the following information, at a minimum, in their SITREP or OPREP:

(a) TCA name.

(b) Tier Level 1 or 2 TCA.

(c) SMADS ID Number.

(d) TCA description.

(e) Date/time of incident.

(f) Location of incident.

(g) Summary of the incident in narrative form.

(h) Impact to TCA capability.

(i) Time to impact mission.

(j) Mission owners that this TCA supports.

(k) Estimated time to restore.

(l) Commander or representative reporting: (name, rank, unit, DSN).

(m) POC: (name, rank, email address, DSN).

(2) Mission Owner. The NMCC will immediately request mission impacts from mission owners. Upon receipt of operational reporting either

from an asset owner or the NMCC, the mission owner will, at a minimum, report the following to the NMCC and asset owner/capability provider (as applicable):

(a) Assessed impact of the event on the missions affected by the loss or degradation of the asset.

(b) Any mitigation efforts or strategies that are taking place or recommended for implementation.

(c) Any shortfalls or requests for assistance to the Joint Staff to mitigate the loss or degradation of the asset (e.g., assistance from the Department of State to coordinate capability support from a partner nation).

(d) The reporting requirements above will account for changes in operational status and daily reporting during exercises and contingencies. Operations centers will incorporate appropriate Commander's Critical Information Requirements (CCIRs) to accomplish this task.

(e) The NMCC will determine the dissemination criteria for any CCIR, SITREP, or OPREP.

(f) GCCs will establish a monitoring process for all commercial or foreign government-owned TCAs within their AORs. GCCs will report operational status changes in commercial or foreign government-owned TCAs in their AOR to all DoD Components with equity in the asset.

b. Threat or Hazard.

(1) CCMDs, Services, and any agency or entity with asset or mission ownership will monitor potential threats and hazards to TCAs, and provide threat or hazard advisories via CCIR, OPREP, or SITREP to the NMCC and other DoD Components, as appropriate. Threats or hazards will be reported if a commander considers the threat likely to impact their mission, or the impact severity is such that the commander would take mission mitigation or remediation actions.

(2) At a minimum the report should include:

(a) TCA name.

(b) Tier Level 1 or 2 TCA.

(c) SMADS ID Number.

(d) TCA description.

(e) TCA location.

(f) Nature of the threat or hazard (e.g., hurricanes, wildfires, flooding, earthquakes).

(g) Imminence of the threat or hazard.

(h) Assessed likelihood of the threat or hazard.

(i) Any mission owners/stakeholders who have equity in the asset.

(j) Any mitigation or remediation efforts that are ongoing or recommended.

(k) Any shortfalls or requests to the DoD for assistance to mitigate or remediate the threat or hazard.

(l) POC: (name, rank, email address, DSN).

(3) Operations centers will incorporate appropriate SITREPs, OPREPs, or CCIRs to accomplish this task and disseminate to DoD Components with equity in the asset.

c. <u>Risk Management Implementation Reporting</u>

(1) DoD Component Heads will:

(a) Maintain awareness of risk management action execution.

(b) Address concerns with appropriate DoD Components.

(c) Adjudicate unresolved concerns through the MACB.

(d) Provide annual updates to the MACB on unresolved risk management actions for DCAs and other MACB prioritized DCI.

(2) Once an RMP is approved by the SecDef, asset owners/capability providers and mission owners will make annual reports to the MA SSG of mitigation/remediation progress on the plan. If the plan is proceeding on the

timelines laid out in the RMP, reports may be submitted for review without formal presentation. If at any time prior to the annual review it is determined that the RMP is not IAW the approved timeline, the DoD Component with responsibility for the delinquent action will provide a report to the MA SSG co-chairs and inform the other DoD Components with equity.

5. Criticality List. All TCAs and their associated BEI will be available in the MARMS asset management module.

(INTENTIONALLY BLANK)

ENCLOSURE G

ALIGNMENT OF MISSION ASSURANCE WITHIN THE JOINT STAFF

1. Purpose. Synchronize MA within the Joint Staff and establish an MA forum IAW reference a. While other DoD Components may shape MA within their own organizations in a manner like the processes outlined herein, this enclosure is specific to the Joint Staff in order to align internal processes and avoid duplication of effort.

2. Overview

a. The DDNHDO is the GO/FO lead for integrating MA efforts across the Joint Staff. The J-36 MA Branch is the lead for day-to-day activities. The J-36 MA Branch performs DCI and MA Construct oversight, but relies upon policies and responsibilities which reside outside the J-36.

b. Table 1 identifies the Joint Staff OPR for each MARPA and equity. Each OPR is the CJCS's principal coordinator for this area. Each OPR should build and maintain a network of functional experts from the Joint Staff Directorates (J-Dirs) and the other DoD Components to collaborate and synchronize MA-related issues (e.g., J-3 is the OPR for CBRNE hazards).

MARPA	**Joint Staff OPR**
Defense Security Enterprise	JSSO
Insider Threat	JSSO
Adaptive Planning	J-3
AT	J-3
CBRNE Preparedness	J-3
Continuity of Operations	J-3
Defense Critical Infrastructure (DCI)	J-3
Emergency Management	J-3
Law Enforcement	J-3
Readiness Reporting	J-3
Energy Resilience	J-4
Fire Prevention and Protection	J-4
Munitions Operations Risk Management	J-4
Operational Energy	J-4
Cybersecurity	J-6
CBRN Survivability	J-8
Force Health Protection	JS Surgeon

Table 1. Mission Assurance Related Programs and Activities

3. Process

a. The J-36 MA Branch may convene a Joint Staff MA Forum when routine coordination amongst J-Dirs does not resolve an issue.

b. The Joint Staff MA Forum is separate and distinct from the MACB. The MACB is the DoD-level advocacy forum for implementing the MA Construct, whereas the Joint Staff MA Forum addresses MA issues across the Joint Staff.

c. The Joint Staff MA Forum is chaired by the J-36 MA Branch Chief and includes AO-level representation from applicable J-Dirs. If a Joint Staff MA Forum meeting is required, the J-36 MA Branch Chief will:

(1) Define the issue (problem set).

(2) Schedule forum with applicable participants and publish agenda.

(3) Chair the forum.

(4) Publish SoC.

(5) Implement the actions to address the issue(s).

ENCLOSURE H

REFERENCES

a. DoDD 3020.40, incorporating Change 1, 11 September 2018, “Mission Assurance”

b. DoDI 3020.45, 2 May 2022, “Mission Assurance Construct”

c. Defense Critical Infrastructure Line of Effort Security Classification Guide, 27 July 2018

d. 2020 DoD Mission Assurance Assessment Benchmarks, 14 April 2020

e. DoDI 6055.17, “DoD Emergency Management (EM) Program,” Incorporating Change 3, 12 June 2019

f. 2020 Defense Threat Reduction Agency, DoD Mission Assurance Assessment Guidelines, 24 September 2020.

g. CJCSM 3105.01 Series, “Joint Risk Analysis Methodology”

h. CJCSM 3150 Series, “Joint Reporting Structure”

i. DJSM 0089-19 Baseline elements of Information for Mission Assurance

ADDITIONAL REFERENCES

1. Antiterrorism (AT) and Force Protection Condition (FPCON) System Security Classification Guide (SCG), 12 December 2018

2. CJCSI 3100.01E, "Joint Strategic Planning System (JSPS)," 21 May 2021

3 CJCSI 3280.01 Series, "National Military Command System (NMCS)," 7 April 2017

4. CJCSI 6635.01, "National Military Command System (NMCS) Primary Command Center Personnel Performance Objectives and Assessment Criteria," 6 August 2018

5. CJCSI 6810.04 Series, "Nuclear Command, Control, and Communications Personnel Performance Objectives and Assessment Criteria," 22 October 2019

6. CJCS OPORD 3-CY, "Continuity of Operations (COOP) for the Chairman of the Joint Chiefs of Staff"

7. Deputy Assistant Secretary of Defense Memorandum, "Approval of the Mission Assurance Risk Management System Governance Plan," 17 December 2019

8. DASD(DC&MA) memo, "Designation of the Defense Threat Reduction Agency as the Mission Assurance Center of Excellence for Mission Assurance Assessments," 30 December 2019

9. DASD(DC&MA) memo, "Designation of the Naval Surface Warfare Center, Dahlgren Division, as the Mission Assurance Center of Excellence for Mission Analysis and Engineering, and Commercial Infrastructure Network and Interdependency Analysis"," 30 December 2019

10. DJSM 0008-21, "Delegation of Authority for Mission Assurance Assessment Schedule Cancellations and Periodicity Waivers," 19 January 2021

11. DoDD 3020.26, "DoD Continuity Policy," 14 February 2018

12. DoDD 3020.44, "Defense Crisis Management," Incorporating Change 2, 22 August 2019

13. DoDD 3100.10, "Space Policy," Incorporating Change 1, 4 November 2016

14. DoDD S-3710.01, “National Leadership Command Capability (NLCC),” 27 May 2015

15. DoDD 5200.43, “Management of the Defense Security Enterprise,” Incorporating Change 3, 14 July 2020

16. DoDD 7730.65, “Department of Defense Readiness Reporting System (DRRS),” Incorporating Change 1, 31 May 2018

17. DoDI 2000.12, “DoD Antiterrorism (AT) Program,” Incorporating Change 3, 8 May 2017

18. DoDI O-2000.16, Volume 1, “DoD Antiterrorism (AT) Program Implementation: DoD AT Standards,” Incorporating Change 3, 7 May 2021

19. DoDI 3020.39, “Mission Assurance Policy for the Defense Intelligence Enterprise (DIE),” Incorporating Change 2, 21 September 2020

20. DoDI 3020.42, “Defense Continuity Plan Development,” 17 February 2006

21. DoDI 3020.52, “DoD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Preparedness Standards,” Incorporating Change 1, 22 May 2017

22. DoDI 3150.09, “CBRN Survivability Policy,” Incorporating Change 2, 31 August 2018

23. DoDI 5200.08, “Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB),” Incorporating Change 3, 20 November 2015

24. DoDI 5240.19, “Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP),” Incorporating Change 2, 6 November 2020

25. DoDI 8320.02, “Sharing Data, Information and Information Technology (IT) Services in the Department of Defense,” Incorporating Change 1, 24 June 2020

26. DoDI 8320.07, “Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense,” Incorporating Change 1, 5 December 2017

27. DoDI 8500.01, “Cybersecurity,” Incorporating Change 1, 7 October 2019

28. DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," Incorporating Change 3, 29 December 2020

29. DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," 24 May 2011

30. DoDI 8540.01, "Cross Domain (CD) Policy," Incorporating Change 1, 28 August 2017

31. DoD Mission Assurance Strategy, Deputy Secretary of Defense, April 2012

32. JROCM 096-16, Information System Initial Capabilities Documents for MARMS, 6 September 2016

33. JSM 5100.01 Series, "Organization and Functions of the Joint Staff"

34. Joint Staff memo, "Designation of Mission Assurance (MA) Systems of Record," 8 November 2019

35. Mission Assurance Risk Management System (MARMS) Governance Plan, 30 October 2019

36. Mission Assurance Risk Management System Concept of Operations, Spiral One, 10 June 2014

37. Mission Assurance Risk Management System Capabilities Based Assessment, Functional Needs Analysis Report, 23 October 2014

38. Mission Assurance Risk Management System Requirements Definition Package, 13 June 2017

39. National Infrastructure Protection Plan (NIPP): Partnering for Critical Infrastructure Security and Resilience, 21 November 2018

40. PPD-21, Critical Infrastructure Security and Resilience, 12 February 2013

GLOSSARY

PART I – ABBREVIATIONS AND ACRONYMS

Items marked with an asterisk (*) have definitions in Part II

ACAT	Advanced Cybersecurity Analytics Team
AFS	Assessment Focus Statement
AHTA	All-Hazards Threat Assessment
AOR	area of responsibility
ASD(HD&GS)	Assistant Secretary of Defense for Homeland Defense and Global Security
AT	antiterrorism
BEI	Baseline Element of Information
CAMS	Critical Asset Management Systems
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear and high-yield explosive
CCDR	Combatant Commander
CCMD	Combatant Command
CII	Commander’s Interest Item
CIO	Chief Information Officer
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
COA	course of action
CONOPS	Concept of Operations
CONPLAN	Concept Plan
CRA	CJCS Risk Assessment
DASD(DC&MA)	Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance
DCA	Defense Critical Asset
DCI	Defense Critical Infrastructure
DCIP	Defense Critical Infrastructure Program
DCITA	Defense Critical Infrastructure Threat Assessment
DepSecDef	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DRRS	Defense Readiness Reporting System

DTRA	Defense Threat Reduction Agency
EI	Element of Information
EM	emergency management
FP	force protection
FHP	force health protection
GCC	Geographic Combatant Command
GMAP	Global Mission Assurance Portal
GO/FO	general officer/flag officer
HQ	headquarters
HHQ	higher headquarters
IAS	Integrated Assessment Schedule
IAW	in accordance with
JMAA	Joint Mission Assurance Assessment
JMAP	Joint Mission Assurance Portal
JMET	Joint Mission-Essential Task
MA*	Mission Assurance
MAA	Mission Assurance Assessment
MAAP	Mission Assurance Assessment Program
MAAR	Mission Assurance Assessment Report
MACB	Mission Assurance Coordination Board
MADSS	Mission Assurance Decision Support System
MARMS	Mission Assurance Risk Management System
MARPA	Mission Assurance-related program and activity
MA ESG	Mission Assurance Executive Steering Group
MA SSG	Mission Assurance Senior Steering Group
MEF	Mission-Essential Function
MET	Mission-Essential Task
MIL STD	military standard
MMP	mission mitigation plan
MOA	memorandum of agreement
MOU	memorandum of understanding
NEF	National-Essential Function
NIPRNET	Non-classified Internet Protocol Router Network
NJOIC	National Joint Operations and Intelligence Center
NLT	not later than

NMCC	National Military Command Center
OCA	Original Classification Authority
OPLAN	Operations Plan
OPR	office of primary responsibility
OSD	Office of the Secretary of Defense
POC	point of contact
RMP	risk management plan
SecDef	Secretary of Defense
SES	senior executive service
SIPRNET	SECRET Internet Protocol Router Network
SMADS	Strategic Mission Assurance Data System
SME	subject matter expert
TA	task asset
TCA*	task critical asset
TTIM	time to impact mission
TTP	tactics, techniques, or procedures
TTR	time to restore
UJTL	Universal Joint Task List
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(C)/CFO	Under Secretary of Defense Comptroller/Chief Financial Officer, Department of Defense
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(R&E)	Under Secretary of Defense for Research and Engineering

PART II – DEFINITIONS

Mission Assurance information. Information (data and databases) pertaining to DoD execution of assigned missions derived from and supporting the designated MA security, protection, and risk management programs. Information includes, but is not limited to, asset lists or subsets; asset BEI; criticality data; threat and hazard information at the global, region, area, installation, and local level; assessment reports; RMPs; operational status reports; program resource information and reports; readiness reporting; program process plans; and MACB and MACB working group information. Information may be in the form of electronic files or hard copies or be available on web-enabled applications and databases, geospatial products, or imagery and photos (DoDI 3020.45).

Task critical asset. 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 capability or mission-essential task it supports. Task critical assets are used to identify defense critical assets.

Tier 1 TCA. Defined in DODI 3020.45 Change 1.

Tier 2 TCA. Defined in DODI 3020.45 Change 1.

Tier 3 TCA. Defined in DODI 3020.45 Change 1.

(INTENTIONALLY BLANK)
Inner Back Cover

INTENTIONALLY BLANK
(BACK COVER)