BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-2402

29 AUGUST 2017

Operations

CRITICAL ASSET RISK MANAGEMENT PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading and ordering

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: HQ USAF/A3OA

Certified by: AF/A3O
(Mr. Steven A. Ruehl)
Pages: 46

This Air Force Instruction (AFI) implements the DoDI 3020.45, *Defense Critical Infrastructure Program (DCIP) Management.* It provides guidance and procedures to manage the identification, prioritization, and assessment of Defense Critical Infrastructure (DCI) and assigns responsibilities governing risk management including the acceptance, remediation, and/or mitigation of DCI risks.

This instruction designates AF/A3OA as the Air Force's (AF) single Office of Primary Responsibility (OPR) for the Air Force Critical Asset Risk Management (CARM) Program and authorizes it to establish and assign roles and responsibilities necessary for the execution of the program, thereby fulfilling AF DCIP obligations laid out in DODI 3020.45. The AF CARM Program's primary focus is the identification, assessment, analysis, and management of risk of loss to assets and supporting infrastructure deemed critical to execution of DoD and AF core capabilities, functions, and missions. This Instruction is applicable to Headquarters Air Force (HAF), Major Commands (MAJCOM), Field Operating Agencies (FOA), Direct Reporting Units (DRU), Primary Support Units (PSU), Combatant Commands (CCMD), and Air National Guard (ANG). This AFI may be supplemented at any level. Route an informational copy to AF/A3OA after certification and approval. Refer recommended changes and questions about this publication to the OPR using the AF Form 847, *Recommendation for Change of Publication;* route AF Form 847 from the field through the appropriate functional chain of command. The authorities to waive the requirements identified in this publication are identified with a tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1. for a description of the authorities associated with the tier numbers. Submit requests for waivers through the chain of command to the appropriate tier

Waiver Approval Authority, or alternately, to the Publication OPR for non-tiered compliance items. AF units on Joint Bases must continue to comply with AF guidance to ensure their Task Critical Assets (TCA)/systems/capabilities are adequately managed. In accordance with (IAW) Joint Basing Implementation Guidance, supported/supporting units will implement Memorandums of Agreement to establish standards of support. Units that cannot meet AF requirements by exhausting the Joint Basing Implementation Guidance adjudication process must coordinate with their MAJCOM to alleviate discrepancies. MAJCOMs that cannot resolve discrepancies will coordinate with the appropriate HAF office for final determination. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW the Air Force Records Disposition Schedule (RDS) in the Air Force Records Information Management System (AFRIMS).

Chapter 1

PROGRAM OVERVIEW

1.1. Executive Summary

1.1.1. The CARM Program was established to increase the reliability of assets/capabilities essential to the execution of DoD missions worldwide. The CARM program enables continuity in two ways: 1) by identifying those systems and assets on which AF missions rely for functionality, and 2) then implementing a risk management strategy designed to reduce or offset the risk of loss to these TCA/ systems/capabilities. The CARM risk management approach includes four macro processes (identify, assess, analyze, and manage mission risk) which seek to introduce mitigation and remediation measures across its capabilities to increase mission resiliency.

1.1.2. The Critical Asset Identification Process (CAIP), outlined in DoDM 3020.45 V1, *Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP),* is designed to be conducted across the DoD on a 3-year cycle or when there is a change in assigned missions or capabilities. The process begins at the mission owner level and then works downward through the AF structure. Assessment and analytical products identify threats and hazards to TCAs and provide leadership with courses of action (COA) to reduce or offset risk. These products contribute to risk decisions at the HAF, CCMD, MAJCOM/DRU, FOA, and Joint Staff (JS) levels.

1.1.3. The CARM program seeks to reduce risk by providing information to AF senior leadership (to include the Acquisitions and Sustainment communities), thus optimizing decisions on the allocation of remediation resources and future asset investment planning. Many AF Mission Assurance (MA) programs have overlapping responsibilities and focus areas. Coordination and information sharing among these programs multiplies the impact of each organization and increases the return on investment of expended resources. The CARM program seeks to maximize situational awareness and coordination at all levels of the AF structure, and acts to integrate CARM priorities and products within these communities.

1.2. Program Objectives

1.2.1. To ensure AF capabilities, functions, and missions can be executed globally via identifying those systems, assets, and infrastructure dependencies whose loss or degradation would negatively impact mission execution.

1.2.2. To establish and implement a risk management program for systems and assets critical to the execution of AF missions.

1.2.3. To define responsibilities, procedures, and standards so commanders can identify, validate, and prioritize TCAs and assess and manage risk to these TCAs in all threats/hazards environment.

1.2.4. Create a comprehensive and coordinated enterprise-wide approach to identify, assess, analyze, and manage risk for AF Tier 1 and Tier 2 TCAs. TCA tier definitions can be found in section 3.2.5.

1.2.5. In conjunction with security-related and other risk management activities, advocate for action to protect and secure TCAs through a comprehensive risk management program.

1.2.6. Foster collaboration and integrate CARM program guidance, procedures, and capabilities into the overarching disciplines, planning tools, products and processes of other risk management programs. This includes establishing information sharing capabilities as captured within the Integrated Defense Risk Management Process, and in accordance with the classification statutes outlined in DoDM 3020.45, V3.

1.2.7. Establish partnerships with other services, federal, state and local governments, host nations and the private sector to address CARM Program issues and inter-dependencies.

1.2.8. Synchronize assessment, mitigation, and remediation efforts with other AF MA programs. A list of MA programs can be found in section 1.4.1.

1.3. Scope

1.3.1. CARM program responsibilities extend to any AF organization with assigned missions and required capabilities. All MAJCOM/DRUs and FOAs that are responsible for TCAs (as appropriate) will establish CARM programs charged with performing risk management to TCAs and direct subordinate organizations to execute CARM responsibilities as necessary. Exemptions may be granted to installations with a demonstrated absence of DCI.

1.4. CARM and MA Integration Strategy

1.4.1. DoDD 3020.40 provides guidance for the integration and synchronization of DoD risk management programs, to include CARM. CARM programs will implement and execute CARM guidance and requirements within the overall DoD MA Strategy and Framework by establishing complementary partnerships and information cross-flows between the CARM program and AF MA efforts as needed. Designated MA programs/activities, as defined in DoDD 3020.40, are:

1.4.1.1. Continuity of Operations (COOP), as defined in DoDD 3020.26, *DoD Continuity Programs,* and AFI 10-208, *Air Force Continuity of Operations (COOP) Program.*

1.4.1.2. Antiterrorism (AT), as defined in DoDI O-2000.16, *DoD Antiterrorism (AT) Program Implementation: DoD AT Standards* and AFI 10-245, *Antiterrorism (AT).*

1.4.1.3. Cybersecurity (CS), as defined in DoDI 8500.01, *Cybersecurity,* and AFI 33-200, *Information Assurance Management.*

1.4.1.4. Emergency Management (EM) as defined in DoDI 6055.17, *DoD Installation Emergency Management Program,* and AFI 10-2501, *Air Force Emergency Management (EM) Program.*

1.4.1.5. Chemical, Biological, and Nuclear (CBRN) Survivability, as defined in DoDI 3150.09, *The Chemical, Biological, Radiological, and Nuclear Survivability Policy* and AFI 10-2607, *Air Force Chemical, Biological, Radiological, and Nuclear Survivability.*

1.4.1.6. Defense Security Enterprise (DSE), as defined in DoDD 5200.43, *Management of the Defense Security Enterprise* and AFPD 16-14, *Security Enterprise Governance.*

1.4.1.7. Law Enforcement (LE). Suspicious activity reporting, as defined in DoDI 2000.26, *Suspicious Activity Reporting.*

1.4.1.8. Force Health Protection, as defined in DoDD 6200.04, *Force Health Protection*, and DoDI 6200.03, *Public Health Emergency Management Within the DoD.*

1.4.1.9. Readiness Reporting, as defined in DoDD 7730.65, *DoD Readiness Reporting System*, and AFI 10-201, *Force Readiness Reporting* .

1.4.1.10. Insider Threat, as defined in DoDD 5205.16, *The DoD Insider Threat Program,* and AFI 16-1402, *Insider Threat Program Management.*

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Secretary of the Air Force (SECAF).

2.1.1. Serve as the primary AF stakeholder in determining the acceptable level of risk to all CARM program systems and assets which are presented to the SECDEF.

2.1.2. Serve as the approving signatory for Defense Critical Assets (DCA) nominations.

2.2. Chief of Staff of the Air Force (CSAF).

2.2.1. Serve in conjunction with the SECAF as a primary AF stakeholder in determining the acceptable level of risk to all CARM program systems and assets which are presented to the SECDEF.

2.2.2. Approve Tier 1 and Tier 2 TCA lists.

2.3. Assistant Secretary of the Air Force for Acquisition (SAF/AQ).

2.3.1. Maintain responsibility for the acquisition and sustainment of prioritized systems and assets identified as critical.

2.3.2. Incorporate CARM remediation and mitigation plans as appropriate, into industrial preparedness, contracting, services acquisition, science and technology (S&T), and life cycle management policies, procedures, and planning.

2.3.3. Interface with DoD senior leadership to address CARM Defense Industrial Base (DIB) issues. Advocate for resources to support high-priority DIB TCAs through DoD corporate processes as required.

2.3.4. As the CARM DIB functional area lead, provide a DIB functional area representative to the CARM Working Group (WG) when requested.

2.4. Administrative Assistant to the Secretary of the Air Force (SAF/AA).

2.4.1. Assist CARM through the Air Force Security Enterprise Executive Board (AFSEEB) structure, as described in DoDI 3020.45, to ensure requirements, timelines, and processes are addressed.

2.4.2. Assist CARM in explaining AF TCAs/systems to external stakeholders and DoD decision makers.

2.4.3. Inform the HAF CARM Program of any identified Committee on Foreign Investment in the United States (CFIUS) concerns in close proximity to DoD TCAs.

2.4.4. Provide a representative to the CARM WG when requested.

2.5. Chief, Information Dominance and Chief Information Officer (SAF/CIO A6).

2.5.1. Serve as the AF Information Networks (AFIN) functional area lead.

2.5.2. Provide overarching policy and oversight of cybersecurity policies and procedures applied to the AF cyber enterprise.

2.5.3. Coordinate with other federal CIOs on CARM cybersecurity issues related to CARM TCAs.

2.5.4. Provide Subject Matter Experts (SME) to assist in the identification, assessment, analysis, and management of TCA-related cyber issues.

2.5.5. Provide SMEs to participate in the Mission Assurance Assessments (MAA) process as requested.

2.5.6. Plan and develop procedures to ensure COOP for TCAs and related cyber systems that support AF operations.

2.5.7. Develop guidance and procedures to implement National, DoD, Joint Chiefs of Staff (JCS), and AF Information Assurance (IA) and cybersecurity direction for CARM applications.

2.5.8. Provide a cyber-representative to the CARM WG when requested.

2.6. Assistant Secretary of the Air Force, Financial Management and Comptroller (SAF/FM).

2.6.1. Serve as the AF appropriations, programming, and financial management functional area lead.

2.6.2. Provide SMEs to advise CARM on resourcing issues including AF manpower, remediation, the AF corporate budget, and AF finance policy.

2.6.3. Provide a finance representative to the CARM WG when requested.

2.7. Secretary of the Air Force, Inspector General (SAF/IG).

2.7.1. Provide inspection policy IAW HAF functional requirements.

2.7.2. Ensure the Air Force Office of Special Investigations (AFOSI), in coordination with the HAF CARM Program office, provides policy and oversight regarding intelligence, threat and counterintelligence (CI) support provided by AFOSI to the CARM Program, and more specifically will:

2.7.2.1. Identify tailored CI collection requirements based on foreign intelligence and international terrorist threats that could affect the protection and assurance of Tier 1 TCAs. TCA tier definitions can be found in section 3.2.5.

2.7.2.2. Assign servicing AFOSI unit-specific roles and responsibilities for the identification, tracking, and dissemination of threat information to all AF commands owning or operating Tier 1 TCAs.

2.7.2.3. Coordinate with the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), Defense Intelligence Agency (DIA), and AF Intelligence Community (IC) to obtain threat information on AF TCAs consistent with U.S. law and military regulations concerning sharing of intelligence information and intelligence collection in the U.S. and on U.S. persons.

2.7.2.4. Provide CI summaries and indications and warnings (I&W) to appropriate authorities and commands with respect to activities in geographic areas where Tier 1

TCAs are located, to include but not limited to, AF installations, facilities, or other property.

2.7.2.5. Provide comprehensive CI support to the CARM Program IAW DoDI 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program,* AFI 71-101 V4, *Counterintelligence,* and related instructions.

2.7.2.6. Provide Defense Threat Assessment Summaries on an annual basis to CARM for locations that will receive a Higher Headquarters (HHQ) assessment.

2.7.3. Provide a representative to the CARM WG when requested.

2.7.4. Provide SMEs to participate in the MAA process as it pertains to Tier 1 TCAs and as requested.

2.8. Secretary of the Air Force, Installations, Environment and Energy (SAF/IE).

2.8.1. Serve as the CARM energy, and water and wastewater-systems functional area lead.

2.8.2. Provide SMEs to advise the CARM Program on enterprise-wide energy, water and wastewater-systems related issues.

2.9. Air Force Surgeon General (AF/SG).

2.9.1. Serve as the AF functional area lead for Health Affairs.

2.9.2. Provide a health functional area representative to the CARM WG when requested.

2.9.3. Provide SMEs to participate in the MAA process as it pertains to TCAs and as requested.

2.10. Deputy Chief of Staff, Manpower, Personnel and Services (AF/A1).

2.10.1. Serve as the AF functional area lead for Personnel.

2.10.2. Provide a personnel representative to the CARM WG when requested.

2.10.3. Assist the HAF CARM Program office in the assessment and validation of CARM program manpower requirements for MAJCOM/DRUs and FOAs CARM POCs.

2.10.4. Assist the HAF CARM Program office with the inclusion of Center/Wing CARM POCs in the official additional duties list.

2.10.5. Coordinate as appropriate with the HAF CARM Program to code HAF, MAJCOM/DRU, and FOA CARM positions with a Top Secret (TS) / Sensitive Compartmented Information (SCI) security clearance.

2.11. Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance (ISR) (AF/A2).

2.11.1. Serve as the AF Functional Area Lead for Intelligence, Surveillance, and Reconnaissance.

2.11.2. Provide ISR information as requested.

2.11.3. Provide an ISR representative to the CARM WG when requested to brief intelligence issues pertaining to TCAs.

2.12. Air Force Deputy Chief of Staff, Operations (AF/A3).

2.12.1. Serve as the AF functional area lead for Space.

2.12.2. Provide a Space or appropriate functional area representative to the CARM WG when requested.

2.12.3. Oversee and maintain overall responsibility for implementing a CARM program for the purpose of managing risk to AF TCAs.

2.12.4. Focus the CARM Program on DoD mission requirements.

2.12.5. Serve as the approving authority for finalized AF Risk Response Plans (RRP).

2.12.6. Establish a HAF CARM program office, which:

2.12.6.1. Develops and maintains a CARM primary and alternate point of contact (POC) appointed by memorandum.

2.12.6.1.1. Appointed personnel (program positions must be coded) will be coordinated with SAF/AAR, and possess a TS / SCI security clearance. (**T-1**)

2.12.6.2. Ensure that the CARM enterprise roster is updated annually with POC information and organizational task box and/or the Director of Staff organizational information (i.e. email and phone number, etc.) for HAF, MAJCOM/DRU and FOA contacts. This roster will be maintained by the HAF CARM Program office.

2.12.6.3. Advocate for funding of the CARM program by identifying and assigning a Program Element Monitor (PEM) to manage PE 35125F (Critical Infrastructure Program). The AF may coordinate with an established system program or program office to avoid duplication in CARM or other programs.

2.12.6.4. Advocate for the resourcing of risk reduction requirements put forth by the MAJCOM/DRUs and FOAs via the corporate process, but is not responsible for funding MAJCOM/DRU and FOA remediation or mitigation efforts.

2.12.6.5. Utilize the Planning, Programming, Budgeting and Execution (PPBE), Program Budget Review (PBR) and other sources to plan, program, and advocate for sufficient manpower resources to execute the CARM program.

2.12.6.6. Develop CARM program processes and procedures, to include the implementation of a risk management framework for AF TCAs, which implements the program's four macro processes: Identify, Assess, Analyze, and Manage mission risk.

2.12.6.7. Implement and direct the AF CAIP, as outlined in **Chapter 3** and **Attachment 2** of this AFI.

2.12.6.8. Ensure organization senior leaders (General Officer level) are aware of the organization's Tier 1 and Tier 2 TCA lists.

2.12.6.9. Obtain CSAF approval of Tier 1 and Tier 2 TCA lists.

2.12.6.10. Leverage and augment other JS and AF assessment teams as needed to meet AF TCA assessment requirements, while minimizing the impact on installations. Assist in developing three and five-year assessment schedules for Future Year Defense Program (FYDP), Air Force Corporate Structure (AFCS), PPBE, and PBR purposes.

2.12.6.11. Ensure remediation efforts, plans, and costs are documented, monitored, and reported.

2.12.6.12. Task MAJCOM/DRUs and FOAs (as appropriate) on an annual basis to conduct a review of Baseline Elements of Information (BEIs) for identified TCAs to maintain data fidelity and asset awareness.

2.12.6.13. Assist MAJCOM/DRUs and FOAs (as appropriate) to advocate for funding of identified risk response COAs by HAF/JS/Office of the Secretary of Defense (OSD) chartered MA executive boards. These boards include the AFSEEB, Defense Acquisition System Executive Boards, AF Corporate Processes, and other executive bodies.

2.12.6.14. Advocate for the resourcing of TCA risk management activities through the HAF-level SE/MA working/steering/executive groups. Coordinate system and asset details and issues with appropriate HAF organizations, owning MAJCOM/DRU or FOA, interested CCMDs, JS/J3, and the appropriate Under Secretary of Defense (USD) for Acquisition, Technology and Logistics (AT&L) and/or Assistant Secretary of Defense (ASD) Homeland Defense & Global Security (HD&GS) as needed. Identify and integrate their priorities for remediation, mitigation, and programming resources for TCAs as required.

2.12.6.15. Coordinate and integrate CARM policies, guidance, plans, and orders with other AF risk management and MA programs.

2.12.6.16. Establish and manage a HAF level CARM WG and participate in AF SE/MA, OSD, and JS sanctioned working groups as requested. Ensure SMEs are aware and participate or provide information when requested.

2.12.6.17. Serve as the AF representative to the semi-annual meeting of the DoD DCI Integration Staff.

2.12.6.18. Partner with AF/A4 to ensure that CARM Tier 1 and Tier 2 items are made available to DoD MA programs and to synchronize CARM-related assessment, mitigation, and remediation efforts. A list of DoD MA programs can be found in Section 1.4.1. CARM POCs will familiarize themselves with the basic tenets of these organizations and how they interact with CARM. CARM POCs will participate in the other MA organizations' Corporate Structure activities as needed.

2.12.6.19. Ensure CARM priorities and best practices are coordinated with HAF Civil Engineering (CE) and Installation Mission Support Center (IMSC) CE leads and considered in the installation planning process for the MA survivability, resiliency, and redundancy of all TCAs during facility construction and installation capitalization efforts that affect, house, or support identified TCAs.

2.12.6.20. Ensure CARM priorities and best practices are coordinated with AF SG and considered in the installation planning process for the MA survivability, resiliency, and redundancy of all medical or health related TCAs. This coordination should occur during the facility planning phase and continue through the construction, military construction, and installation capitalization efforts that affect, house, or support identified medical TCAs.

2.12.6.21. Establish a comprehensive set of performance measurements (metrics) to determine the overall effectiveness and compliance of MAJCOM CARM programs with standards and benchmarks to identify, assess, analyze, and manage risk to SECDEF reportable TCAs.

2.12.6.22. Submit a CARM program review and milestones report to OSD when requested.

2.12.6.23. Work with AF functional area leads to foster relationships with local government, civil agencies, and the private sector to address issues with high-interest TCAs.

2.12.6.24. Share information and integrate CARM Program guidance, procedures, and products with other AF MA disciplines where possible.

2.12.6.25. Provide Temporary Duty (TDY) funds (as available) for MAJCOM/DRU or FOA (as appropriate) POCs and HAF SMEs in support of the CARM Program.

2.12.6.26. Develop and implement a CARM program long-term strategy for outreach, education, and training to meet CARM Program goals and objectives.

2.12.6.27. Develop, modernize, manage, and sustain the Air Force Critical Asset Management System Next Generation (AF-CAMS NG) CARM system of record for the management of TCAs.

2.12.6.27.1. Ensure the AF CARM system of record Cybersecurity Assessment and Authorization (A&A) requirements are met and documented in the Enterprise Mission Assurance Support Service (EMASS).

2.12.6.27.2. Act as the approval authority for the establishment of the AF system of record user accounts.

2.12.6.27.3. Maintain an Information Technology (IT) contingency plan for the AF CARM system of record to provide documented procedures to ensure the successful recovery in the event of a short-term system outage. The contingency plan will provide detailed procedures for handling an AF-CAMS NG system outage to minimize any adverse impact on the system's ability to fulfill its mission.

2.12.6.28. Provide programmatic and procedural training enabling the execution of the CARM Program's four macro processes. Additional training information is located in **Chapter 4**.

2.13. Deputy Chief of Staff for Logistics, Civil Engineering, and Force Protection (AF/A4).

2.13.1. Serve as the AF functional area lead for Logistics, CE, and Force Protection (FP) functional areas as identified in DoDI 3020.45.

2.13.2. Provide Logistics, CE, and FP representatives to the CARM WG when requested.

2.13.3. Ensure CARM Program requirements are coordinated with HAF CE and IMSC engineering leads and considered in the installation planning process for the MA survivability, resiliency, and redundancy of all TCAs during facility construction and installation capitalization efforts that affect, house, or support these identified TCAs as outlined in DoDI 3020.45.

2.13.4. Synchronize/de-conflict HHQ MA assessments supporting AT requirements in DoDI 2000.16 V1, *DoD Antiterrorism Standards*, with CARM requirements outlined in DoDI 3020.45.

2.13.5. Ensure the guidance provided in AFI 31-101, *Integrated Defense*, captures the requirement to include TCAs in the Integrated Defense Risk Management Process (IDRMP) and that the security afforded these assets is addressed in the Wing Integrated Defense Plan.

2.13.6. Partner with AF/A3 to ensure that CARM Tier 1 and Tier 2 TCAs are made available to DoD MA programs and to synchronize CARM-related assessment, mitigation, and remediation efforts. A list of DoD MA programs can be found in Section 1.4.1.

2.14. Deputy Chief of Staff for Strategic Plans and Requirements (AF/5/8).

2.14.1. Advise the HAF CARM Program on matters of strategic and resource planning.

2.14.2. Provide access to and interpretation of relevant Operational Plans (OPLAN) and Concept of Operations Plans (CONPLAN) as requested.

2.14.3. Provide a representative to the CARM WG when requested.

2.15. Director, Air Force Studies, Analyses, and Assessments (AF/9).

2.15.1. Advise the HAF CARM Program through the assessment and analysis of program structure, operations, and resource allocations as requested.

2.15.2. Provide a representative to the CARM WG when requested.

2.16. Deputy Chief of Staff, Strategic Deterrence and Nuclear Integration (AF/A10).

2.16.1. Provide a representative to the CARM WG when requested.

2.17. MAJCOM/DRUs.

2.17.1. Establish a CARM program office within the Headquarters organization for the purpose of identifying, assessing, analyzing, and managing mission risk to AF TCAs.

2.17.1.1. Any organization which can demonstrate a lack of TCAs will be exempt from CARM programmatic responsibilities.

2.17.2. Appoint a primary and alternate CARM POC on an annual basis, in writing, to manage their overall CARM program. A copy of the appointment letter will be provided to the HAF CARM Program office. (**T-1**) In addition:

2.17.2.1. MAJCOM/DRU CARM program appointed personnel must possess a TS / SCI security clearance. This may be waived to a SECRET level with a justification memorandum sent through the HAF CARM Program office.

2.17.2.2. Provide a validated list of organizations and installations exempt from the requirement to establish CARM programs to the HAF CARM Program office. Exemptions may be granted to installations with a demonstrated absence of TCAs.

2.17.2.3. CARM POCs will complete the annual CI Awareness Briefing as directed by AFI 71-101, V4.

2.17.3. Focus CARM activities on DoD mission requirements.

2.17.4. Establish POCs in Functional and Special Staff Directorates, as required, to socialize and advance CARM priorities; plus any System Program Office (SPO) / Program Management Office (PMO) program POCs for TCAs.

2.17.5. Maintain access to a facility capable of developing, communicating, and maintaining up to and including TS / SCI TCA-related data. This may be waived to a SECRET level with a justification memorandum sent through the HAF CARM Program office.

2.17.5.1. A Joint Worldwide Intelligence Communications System (JWICS) account will be established based on access and need-to-know. MAJCOM/DRUs will inform the HAF CARM Program office if this capability does not exist.

2.17.6. Provide CARM data to MAJCOM/DRU PEMs; SPOs/PMOs; IMSC; and A4 (as required) to advocate for the funding of remediation efforts or to support funding requests beyond the MAJCOM/DRU level (i.e. PPBE, PBR, AFCS).

2.17.7. Inform the HAF CARM Program office of CARM program staffing/funding requirements through the PPBE on a fiscal year basis. Submit these requirements to the respective MAJCOM/DRU Program Objective Memorandum (POM) OPR.

2.17.8. Establish and provide corporate process priorities and products for Tier 1 and Tier 2 TCA information on an as-requested basis for the AFSEEB (AFPD 16-14, *Security Enterprise Governance*) and AF Budget Corporate Processes (AFI 65-601, V3, *The Air Force Budget Corporate Process*), as well as sanctioned AF WGs.

2.17.9. Ensure that all Tier 1 and Tier 2 TCAs are listed in their command posts and subordinate installation command post matrices.

2.17.9.1. Ensure MAJCOM/DRU senior leadership is aware of and has approved the Tier 1 and Tier 2 TCA list on an annual basis or as changes to assets or senior leadership occur.

2.17.10. Oversee development and implementation of Numbered Air Force (NAF) and Center/Wing CARM programs as required.

2.17.11. Ensure the reporting of changes in the operational status of Tier 1 and Tier 2 TCAs as outlined and required in AFI 10-206, *Operational Reporting*.

2.17.12. Establish and manage a CARM WG or incorporate the requirement into an equivalent, existing MAJCOM/DRU WG (e.g. Threat, EM, or Integrated Defense (ID)) to:

2.17.12.1. Facilitate cross-functional dialogue on TCA identification, availability, and reliability and to support consequence management and COOP planning.

2.17.12.2. Develop strategies for remediating or mitigating identified vulnerabilities and risks to assessed TCAs and infrastructures to inform the HAF CARM Program office and HAF CARM WG. A detailed description of the roles and expectations of a CARM WG can be found in section 3.6.

2.17.13. Coordinate with the MAJCOM/DRU Readiness function, such as Defense Readiness Reporting System (DRRS), to identify and document Mission Essential Tasks (MET) / Mission Essential Functions (MEF), core functions, and required capabilities for which the command has overall responsibility for execution and annually update results in the AF CARM system of record.

2.17.13.1. Provide METs / MEFs identified by the CCMDs to each respective subordinate organization.

2.17.14. Execute the AF CAIP process by identifying, nominating, and validating Tier 1 and Tier 2 TCAs supporting assigned missions and documenting approved TCAs in the AF CARM system of record as required.

2.17.15. Enter and validate their discovered/identified critical systems' and assets' BEIs in the AF CARM system of record for AF programmatic and PPBE efforts to remediate or create redundant capabilities.

2.17.15.1. Conduct an annual review of BEIs for identified TCAs to maintain data fidelity and asset awareness.

2.17.16. Coordinate remediation and mitigation requests to systems, systems of systems, and their supply-chain and life cycle management with a system's PMO, SPO, and other organizations as needed.

2.17.17. Document major remediation projects, timelines, and changes in remediation/mitigation status of Tier 1 and Tier 2 TCAs in the AF CARM system of record.

2.17.17.1. Provide notification of unfunded remediation requirements to the HAF CARM Program office.

2.17.18. Request command-level functions with risk response equities (Communications, CE, etc.) provide updates on Tier 1 and Tier 2 TCAs remediation or mitigation projects when requested. Updates will include project number, status, associated work orders, costs, and expected completion times.

2.17.19. Provide updates on select asset remediation and mitigation status to the HAF CARM Program when requested.

2.17.20. Leverage Center/Wing CARM POC's relationships with local government, civil agencies, and the private sector to address risk to TCAs.

2.17.21. Information share and, when possible, integrate CARM Program guidance; procedures; and products into other MA disciplines and instructions of other AF contingency planning programs, risk management, and MA plans.

2.17.22. Attend and participate in the MAJCOM/DRU Threat, EM, and ID WGs and provide CARM Program-related data when requested.

2.17.23. Ensure DoD MA programs are aware of CARM Tier 1 and Tier 2 TCAs in accordance with proper security procedures. A list of DoD MA programs can be found in Section 1.4.1. CARM POCs will familiarize themselves with the basic tenets of these organizations and how they interact with CARM. CARM POCs will participate in the other MA organizations' Corporate Structure activities.

2.17.24. Manage and coordinate CARM outreach, education, and training.

2.17.25. Engage operational system and asset owners (MAJCOM/DRU and PMO/SPOs) to develop capability reviews and produce remediation/mitigation COA reviews when tasked.

2.17.26. Ensure Center/Wing level CARM POCs complete required CARM training upon being assigned, and recurring annually. Required courses will be designated by the HAF CARM Program office.

2.17.27. Ensure the development of Risk Response Plans (RRP) for select Tier 1 TCAs, as outlined in paragraph 3.4., as required and applicable.

2.17.28. Provide guidance to Centers/Wings regarding the inclusion of TCAs in existing installation exercises to include:

2.17.28.1. Provide CARM activity injects into existing command exercise programs for the test and evaluation and validation of critical security, mitigation, reconstitution, and emergency response plans.

2.17.28.2. Document lessons learned from operations, training, and exercises and incorporate (as appropriate) into CARM processes and activities addressing the protection, survivability, and assurance of TCAs.

2.17.29. Lead support efforts with Centers/Wings in execution of Mission Assurance Assessments (MAA) of TCAs. Assessment types and actions are described in section 3.3.

2.17.29.1. MAJCOM POCs will participate in MAAs as SMEs, as requested and resources permit.

2.17.30. Ensure guidance provided by the MAJCOM supplement (as appropriate) to AFI 31-101 captures the requirement to include TCAs in the IDRMP and that the security afforded these assets is addressed in the Wing Integrated Defense Plan. This guidance will incorporate CCMD/Sub-Unified Commander CARM requirements as necessary.

2.17.31. Conduct an annual review of program metrics and benchmarks established by the HAF CARM Program to determine the overall effectiveness and compliance of MAJCOM CARM programs with requirements to identify, assess, analyze, and manage risk to identified TCAs.

2.17.31.1. MAJCOM CARM POCs will determine Center/Wing program review requirements.

2.18. AF Installation and Mission Support Center (IMSC).

2.18.1. Provide CE, physical security, and AT subject matter expertise in support to MAJCOM/DRU, FOA, Center/Wing CARM program as requested.

2.18.2. IMSC PSUs, the Air Force Civil Engineer Center (AFCEC), will provide program management for infrastructure-related engineering efforts associated with TCAs on AF installations. (**T-1**)

2.18.3. IMSC PSU, the Air Force Security Forces Center (AFSFC), will conduct Air Force Mission Assurance Assessments (AFMAA) for AF installations as requested.

2.19. Air Force Components to the Combatant Commands.

2.19.1. Participate in the CARM WG as required.

2.19.2. Assist in identifying and prioritizing AF assets critical to the capabilities required by the Combatant Commander.

2.19.3. Coordinate with the MAJCOM/DRUs, FOAs, and AF functional area leads on the identification, assessment, and remediation of AF TCAs and non-AF owned and/or managed infrastructure.

2.19.4. Document major remediation projects, timelines, and changes in status of Tier 1 and Tier 2 TCAs in the AF CARM system of record. (**T-1**)

2.19.5. Provide notification of unfunded remediation requirements to the relevant HHQ functional manager and the HAF CARM Program office.

2.19.6. Work with the COCOM to identify the impact resulting from the loss, damage, or destruction of internal and external infrastructure critical to the CCMD's mission.

2.20. FOAs.

2.20.1. Establish a CARM program office within the organization for the purpose of assigning, identifying, assessing, analyzing, and managing mission risk to AF TCAs. (**T-1**)

2.20.1.1. Any organization which can demonstrate a lack of TCAs will be exempt from CARM programmatic responsibilities through their HHQ's organization.

2.20.2. Appoint a primary and alternate CARM POC on an annual basis, in writing, to manage their overall CARM program. (**T-2**) A copy of the appointment letter will be provided to the HAF CARM Program office and the FOA's HHQ's functional manager. (**T-2**) In addition:

2.20.2.1. FOA CARM appointed personnel (program positions must be coded) will possess a TS / SCI security clearance. This may be waived to a SECRET level with a justification memorandum sent through the FOA's HHQ's functional manager. (**T-2**)

2.20.2.2. CARM POCs will complete annual CI Awareness Briefing as directed by AFI 71-101, V4.

2.20.3. Focus CARM activities on DoD mission requirements.

2.20.4. Maintain access to a facility capable of developing, communicating, and maintaining up to and including TS / SCI TCA-related data. This may be waived to a SECRET level with a justification memorandum sent through the FOA's HHQ's functional manager. (**T-2**)

2.20.4.1. A JWICS account will be established based on access and need-to-know. FOAs will inform its HHQ's functional manager and the HAF CARM Program office if this capability does not exist. (**T-3**)

2.20.5. Execute a CARM program responsible for the following:

2.20.5.1. Ensure FOA PEMs responsible for AF TCAs have CARM data, as required, in order to advocate for the funding of remediation efforts or to support funding requests beyond the FOA level (i.e. PPBE, PBR, AFCS). (**T-1**)

2.20.5.2. Inform the HAF CARM Program office of CARM program staffing/funding requirements through the PPBE on a fiscal year basis. Submit these requirements to the respective FOA POM OPR. (**T-1**)

2.20.6. Ensure that all Tier 1 and Tier 2 TCAs are listed in installation command post matrices as appropriate. (**T-1**) CARM POCs will ensure COOP, Installation EM, Consequence Management, and Incident Response functions are aware of applicable TCAs and recommend CARM inclusion. (**T-1**)

2.20.6.1. Ensure FOA senior leadership is aware of and has approved the Tier 1 and Tier 2 TCA list on an annual basis, or as changes occur. (**T-2**)

2.20.7. Ensure the reporting of Tier 1 and Tier 2 TCAs using operational reporting as outlined and required in AFI 10-206. (**T-2**)

2.20.8. Establish and manage a CARM WG or incorporate the requirement into an equivalent, existing organizational WG (e.g. Threat or EM WG) (**T-2**) as appropriate to:

2.20.8.1. Facilitate cross-functional dialogue on TCA identification, availability, and reliability and to support consequence management and COOP planning. (**T-2**)

2.20.8.2. Develop strategies for remediating or mitigating vulnerabilities and risks to TCAs and infrastructures to inform the FOA's HHQs functional manager, HAF CARM Program office, and HAF CARM WG. (**T-1**)

2.20.8.3. A detailed description of the roles and expectations of a CARM WG can be found in section 3.6.

2.20.9. Execute implementation of the AF CAIP process by helping to identify, nominate, and validate Tier 1 and Tier 2 TCAs supporting assigned missions and documenting approved TCAs in the AF CARM system of record. (**T-1**)

2.20.10. Enter and validate their discovered/identified critical systems and assets' BEI in the AF CARM system of record for AF programmatic and PPBE efforts to remediate or create redundant capabilities. (**T-1**)

2.20.10.1. Conduct an annual review of BEIs for identified TCAs to maintain data fidelity and asset awareness. (**T-2**)

2.20.11. Coordinate remediation and mitigation requests to systems, systems of systems, and their supply-chain and life cycle management with a system's PMO, SPO, and other organizations as needed. (**T-2**)

2.20.12. Document major remediation projects, timelines, and changes in status of Tier 1 and Tier 2 TCAs in the AF CARM system of record. (**T-1**)

2.20.13. Provide notification of unfunded remediation requirements to the FOA HHQ's functional manager and HAF CARM office. (**T-1**)

2.20.14. Request functions with risk response equities (Communications, CE, etc.) provide updates on Tier 1 TCA remediation or mitigation projects as appropriate and when requested. Updates will include project number, status, associated work orders, costs, and expected completion times.

2.20.15. Provide updates on select asset remediation and mitigation status to the FOA HHQ's functional manager and the HAF CARM Program as appropriate and when requested. (**T-2**)

2.20.16. Engage operational system and asset owners (MAJCOM/DRU and FOA) to request capability reviews and produce remediation/mitigation COA reviews when tasked. (**T-1**)

2.20.17. Ensure the development of RRPs for select Tier 1 TCAs, as outlined in paragraph 3.4., and as required and applicable.

2.20.18. Assist in the development of exercises relating to TCAs (**T-2**) as appropriate to include:

2.20.18.1. Provide CARM activity injects into existing installation and command exercise programs for the test and evaluation, and validation of critical security, mitigation, reconstitution, and emergency response plans. (**T-2**)

2.20.18.2. Document lessons learned from operations, training, and exercises and ensure they are incorporated into CARM program processes and activities addressing the protection, survivability, and assurance of TCAs. (**T-2**)

2.20.19. Support MAAs of TCAs. (**T-1**) Assessment types and actions are described in section 3.3.

2.21. Air Force Critical Asset Owning Centers and Wings.

2.21.1. Execute CARM activities, to include the identification and management of risk to TCAs. (**T-1**)

2.21.1.1. Centers/Wings will be exempt if capable of demonstrating an absence of TCAs.

2.21.2. Appoint in writing primary and alternate CARM POCs to execute CARM activities to include the identification and management of risk to AF TCAs. (**T-2**) A copy of the POC appointment letter will be provided to the applicable MAJCOM/DRU. (**T-2**)

2.21.2.1. The appointment of CARM POCs should be assigned to the position for a minimum of one year to ensure the stability and continuity of operations.

2.21.2.2. CARM POCs will possess at a minimum a SECRET security clearance. In some circumstances, selected CARM POCs will require a TS or TS / SCI security clearance based on TCAs and missions assigned and supported. (**T-2**)

2.21.2.3. CARM POCs will complete required CARM training upon assignment and once annually for each following year. (**T-3**) Required courses will be designated by the HAF CARM Program office.

2.21.3. Establish and manage a CARM WG or incorporate the requirement into an equivalent, existing Center/Wing or Installation WG (e.g. Threat, EM, or ID WG) to facilitate cross-functional dialogue on TCA identification, availability, and reliability, as well as to support consequence management and COOP planning. (**T-2**) Additional details regarding the purpose and responsibilities of the CARM WG can be found in section 3.6.

2.21.4. Assist in the execution of MAAs as required by the MAJCOM/DRU CARM POC. (**T-2**)

2.21.5. Assist in the development of risk remediation or mitigation COAs for identified vulnerabilities and risks to TCAs and infrastructure as required by the MAJCOM/DRU CARM POC. (**T-2**)

2.21.6. Document major remediation projects, timelines, and changes in status of Tier 1 and Tier 2 TCAs in the AF CARM system of record. (**T-1**)

2.21.7. Provide notification of unfunded remediation requirements to the MAJCOM/DRU CARM POC. (**T-1**)

2.21.8. Collaborate with MA TCA stakeholders and resourcing functions to integrate CARM program guidance and requirements in the development and publication of installation plans and annual military construction (MILCON); and sustainment, restoration, and modernization (SRM) prioritization lists via the Installation Facilities Board. (**T-2**)

2.21.9. Manage and coordinate Center/Wing participation in the AF CAIP process by helping to identify, nominate, and validate Tier 1 and Tier 2 TCAs supporting assigned missions. This includes coordinating validated TCA data with appropriate stakeholders. (**T-2**)

2.21.9.1. CARM POCs will maintain a current list of their Wing's TCAs in accordance with proper security procedures. (**T-3**) CARM POCs will provide this list to their host Center/Wing and MAJCOM/DRU CARM POCs.

2.21.10. Ensure all additions or subtractions to their TCA list or significant changes to the status of TCA remediation or mitigation efforts, are reported to the relevant MAJCOM/DRU CARM POC. (**T-1**)

2.21.11. Ensure the reporting of changes in the operational status of their Tier 1 and Tier 2 TCAs as outlined and required in AFI 10-206.

2.21.12. Participate in the Center/Wing/Installation Threat and EM WGs to provide regular status of CARM program milestones to the responsible commanders. (**T-2**)

2.21.13. Brief installation senior leaders on the CARM program and their involvement as it pertains to TCAs and those critical assets formerly known as Supporting Infrastructure Critical Assets (SICA) that are now included under the TCA category. (**T-2**)

2.21.14. Ensure DoD installation MA programs are aware of CARM Tier 1 and Tier 2 TCAs in accordance with proper security procedures. (**T-1**) A list of DoD MA programs can be found in Section 1.4.1. CARM POCs will familiarize themselves with the basic tenets of these organizations and how they interact with CARM. CARM POCs will participate in the other MA organizations' Corporate Structure activities.

2.21.15. Ensure TCAs are included in the IDRMP and the resulting Wing Installation Defense Plan. (**T-2**)

2.21.16. Provide CARM activity injects into existing command exercise programs for the test and evaluation and validation of critical security, mitigation, reconstitution, and emergency response plans. (**T-2**)

2.21.17. Ensure that vulnerability data and risk management actions are shared with the Center/Wing Antiterrorism Officer (ATO) and the Defense Force Commander (DFC). (**T-2**)

2.22. Air Force Host Centers and Wings.

2.22.1. Execute the responsibilities found in section 2.22. if responsible for any TCAs. (**T-1**) Host Centers/Wings will be exempt if capable of demonstrating an absence of TCAs. If an exemption is awarded, Host Centers/Wings are only responsible for those activities identified in this section.

2.22.2. Work with those organizations within their installation who own TCAs to ensure proper support and awareness of assets. (**T-2**)

2.22.2.1. Where applicable, maintain a host-tenant agreement with asset-owning organizations within their installation that spells out the responsibilities of each organization in regards to the TCA. (**T-1**)

2.22.3. Maintain a current list of TCAs for the installation in accordance with proper security procedures. (**T-2**)

2.22.4. Participate in CARM WGs as requested by Centers/Wings on their installation. (**T-2**)

2.22.5. Report changes in the operational status of installation Tier 1 and Tier 2 TCAs as outlined and required in AFI 10-206. (**T-2**)

Chapter 3

CARM PROCESSES

3.1. The CARM Cycle.

3.1.1. The CARM Cycle performs risk management through a macro four-step process which informs senior leaders and justifies resources for risk remediation or mitigation efforts. The process begins with the identification of assets critical to the execution of DoD missions, which are then assessed to measure criticality and identify vulnerabilities and threats/hazards. Assessment findings are analyzed to calculate risk to the mission/asset and reported to the MAJCOM/DRUs, FOAs, and the JS, along with recommended COAs to reduce risk to the asset and mission. The process concludes when the AF manages the risk to the asset through the implementation of one or more of the recommended COAs in order to remediate or mitigate the risk.

3.2. Identification of TCAs.

3.2.1. Identification of TCAs ensures MAJCOM/DRUs; FOAs; and Installation Commanders and CARM program POCs maintain situational and operational awareness of risk to systems/assets critical to the execution of DoD missions.

3.2.2. Asset identification facilitates resourcing opportunities by identifying, analyzing, documenting, and validating the core system and asset requirements of the AF Enterprise. Requirements are entered by MAJCOM/DRUs, FOAs (as appropriate), or the AF Corporate Process into the AF baseline budget generated by the PPBE to execute assigned missions, functions, and capabilities at acceptable levels under the required conditions.

3.2.3. The CAIP, utilized by the DoD and the AF, identifies, nominates, validates, and analyzes TCAs and systems based on mission impact. The CAIP is a nine-step process executed over a time frame determined by the JS. A detailed breakdown of the CAIP steps and processes can be found in DoDM 3020.45 V1. A quick reference chart of the steps and process overview can be found in **Attachment 2**.

3.2.4. CARM programs will perform the CAIP, as described in DoDM 3020.45 V1, by identifying TCAs defined by this AFI, internal and external to DoD installation boundaries. For the purposes of this Instruction, the term TCA encompasses both Task Critical Assets (TCA) and critical assets formerly known as SICAs. Once an asset is determined to be critical, it is assigned a tier rating based on the level of impact its loss would inflict on the mission it supports.

3.2.5. CARM program tier definitions are below and in compliance with the DoD TCA tier definitions listed in DoDM 3020.45, V1. These definitions are to be utilized to assign tier ratings to identified TCAs. The Tier definitions are:

3.2.5.1. Tier 1 TCA – A system or asset of which the loss, incapacitation, or disruption could result in mission (or function) failure at the DoD, Military Department, CCMD, Sub-Unified Command, Defense Agency, or Defense Infrastructure Sector Lead Agency (DISLA) level.

3.2.5.1.1. Defense Critical Asset (DCA) - TCAs of such extraordinary importance to operations in peace, crisis, and war, that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the DOD to fulfill its missions. DCAs are not an independent tier of assets, but are a high-priority subset of Tier 1 TCAs.

3.2.5.2. Tier 2 TCA – A system or asset of which the loss, incapacitation, or disruption could result in severe mission (or function) degradation at the DoD, Military Department, CCMD, Sub-Unified Command, Defense Agency, or DISLA level.

3.2.5.3. Critical Assets, formerly known as SICAs, are infrastructures directly used to support the functioning or operation of a TCA such that the supporting infrastructure TCA's loss, degradation, or denial will result in the inability of TCAs to function or operate as intended in the execution of their associated METs/MEFs. An example would include an electrical substation that provides power to an identified TCA for which backup power generation is not available.

3.2.6. Task Asset (TA) – An asset that is directly used to support execution of one or more operations, activities, or METs/MEFs.

3.2.6.1. TAs determined to be critical to the execution of a mission are upgraded to TCAs and assigned a tier level based on the impact their loss would have on the mission.

3.2.7. The CARM Program risk management process is cyclical in nature and the CAIP timeline synchronizes the efforts of this process, aims to prevent duplication of effort, and establishes procedures and time requirements for the flow of CARM program guidance to all AF commands.

3.2.8. AF-CAMS NG is the AF CARM system of record for data associated with AF TCAs.

3.2.8.1. MAJCOM/DRUs and FOAs (as appropriate) are responsible for entering all of their TCAs into the AF CARM system of record and validating TCAs.

3.2.8.2. The CARM Program sustains and modernizes a Secret Internet Protocol Router Network (SIPRNet) database application for general programmatic tracking of critical systems and assets to assist with providing remediation and programmatic status on AF remediation efforts. The AF CARM system of record is not an operational reporting tool, nor is it built or certified for those types of functions.

3.2.8.3. The AF CARM system of record captures critical systems and assets for programming remediation efforts. The system is designed to serve as a common entry point for the MAJCOM/DRUs and FOAs (as appropriate) and is one-way web shared with CCMDs, JS/J33, and ASD (HD&GS) databases and representatives as appropriate.

3.3. TCA Assessment Processes.

3.3.1. The CARM Program utilizes products from three separate assessments to determine risk to AF TCAs and develop risk management strategies. The three assessments are 1) Balanced Survivability Assessments (BSA), 2) Joint Mission Assurance Assessments (JMAA) conducted by the Defense Threat Reduction Agency (DTRA), and 3) Air Force Mission Assurance Assessments (AFMAA) conducted by the AFSFC.

3.3.2. BSAs are mission survivability assessments which identify vulnerabilities and assess the mission impact should those vulnerabilities be successfully exploited. BSAs also recommend measures to remediate or mitigate the identified vulnerabilities. The assessments are mission, rather than geographically oriented, and focus on the systems, networks, architectures, infrastructures, and assets supporting the specific missions targeted by the assessment. BSAs are performed at the request of responsible commanders or directors.

3.3.2.1. BSAs consist of three phases: 1) pre-assessment phase, 2) assessment phase, and 3) post-assessment phase. BSA findings reports are distributed only to the assessed organization, the JS, the relevant CCMD(s) and service(s), the assessment requesting organization, and any organization mandated by DoD or service guidance. For additional details regarding the activities, timelines, and products generated by the BSA, please reference DoDI 3000.08, *Balanced Survivability Assessments*.

3.3.3. JMAAs identify potential risks to mission execution through risks to critical systems and assets based on the combination of likely threats or hazards with identified vulnerabilities. These include inter-and-intra-dependencies needed to accomplish required DoD mission requirements. JMAAs integrate the findings of three distinct assessments: 1) criticality assessment, 2) all hazards/threats assessments (AHTA), and 3) vulnerability assessment. JMAAs are based on DoD MAA benchmarks. Together, these are used to form a risk assessment for leadership use in prioritizing response actions.

3.3.3.1. Criticality assessments are conducted by asset and mission owners and categorize the importance of assets to the DoD missions they support. Criticality, along with vulnerabilities and threats/hazards, are used to determine the risk to a mission posed by specific assets. Criticality assessments are driven by the information gleaned via the latest CAIP and include various BEI data, including at a minimum, asset name and description, consequence of loss statement, and applicable stakeholders. Additionally, beneficial data points include missions/functions/plans supported by the asset, Impact of Loss (i.e., Tier I (mission failure) or Tier II (severe mission degradation), Time to Mission Impact, Time to Restore Mission Capability, and Criticality Rating.

3.3.3.2. The AHTA is a comprehensive list of known threats and hazards likely to occur on or in the vicinity of the installation. It covers man-made threats (terrorism, insider threat, cyber threats, etc.), natural hazards (geological, meteorological, and biological), and accidents. The installation AHTA should be tailored to the local environment and specific to the installation, identifying threats and hazards that may cause impact to assets, missions, or personnel. Each identified threat or hazard will receive a rating based on agreed-upon definitions, which indicates the likelihood of its occurrence.

3.3.3.2.1. The AHTAs fulfills the DoD requirement for annual installation threat assessments. It is initially drafted and then updated by on-site POCs, typically from the products created within the Threat WG and the EM WG. For the purposes of the HHQ assessments, the assessment team may review the existing installation AHTA, or develop a new document if no pre-existing product is available or deemed satisfactory. The AHTA provides the assessment team an understanding of the threats/hazards which must be considered during the assessment and will factor into mission risk determinations. Additionally, it is also reviewed during the vulnerability

assessment by the ATO and EM SMEs with the applicable on-site POCs to ensure a comprehensive product.

3.3.3.3. HHQ AFMAAs are conducted at the installation by the MAA team. These on-the-ground assessments determine the susceptibility of a system or asset to the identified threats and hazards. The three key phases to the AFMAA are 1) assessment preparation, 2) on-site assessment, and 3) post-assessment coordination.

3.3.3.3.1. The assessment preparation phase readies both the assessment team and the assessment recipient for the AFMAA vulnerability assessment. This includes the development of a Notification Message, Assessment Focus Statement (AFS), execution of a pre-assessment site survey (PSS), provision of applicable POC information, and required documentation from the location to the assessment team, and other logistical coordination (i.e., security requirements, on-site requirements such as work space, transportation, etc.). The assessment team will familiarize itself with the installation and the assets/infrastructures which are to be assessed, while the installation will develop an understanding of what can be expected throughout the process and what support and documentation must be provided to the assessment team. These activities will be primarily coordinated directly between the assessment team and installation POCs, but the assistance of Center/Wing CARM POCs may be requested throughout the process.

3.3.3.3.2. The Notification Message for the pending assessment is delivered by the assessing organization through the applicable chain of command to the recipient installation and signifies the beginning of the pre-assessment preparation phase. The notification includes a breakdown of responsibilities between stakeholders, an anticipated timeline, required documentation, and deliverables due upon completion of the assessment.

3.3.3.3.3. The AFS is a document usually drafted by the mission owner or asset owner with inputs from various stakeholders to include relevant CCMD(s) and service(s). In certain circumstances, the AF may be tasked to develop the AFS for installations where it is not a mission owner. The AFS outlines the programs, missions, assets, and special interest items to be assessed at the location, along with an assessment POC. This document will guide the assessment team's focus.

3.3.3.3.4. The PSS is a site visit by the assessment team to obtain additional insight to installation layout and local assessment partners, address pending issues or concerns, and prepare the assessment recipient for the AFMAA vulnerability assessment. Although PSS participation may vary depending on the features of the location being assessed, standard PSS activities include presentations by the local leadership and Team Chief; a windshield tour of the installation being assessed; and mission briefs and asset tours for each asset being assessed. Additionally, this visit is used to close out any key preparation activities that have not already been completed.

3.3.3.3.5. The on-site assessment is the physical execution of the AFMAA vulnerability assessment, which focuses on identifying vulnerabilities of the system or asset as well as the infrastructure components supporting the function of that system or asset. Components of the on-site assessment typically include an in-brief presentation with key installation and tenant leadership, asset tours to include a

mission brief on the asset, SME interviews with asset POCs, SME interviews with installation POCs to review support to and protection of the assets/tenants, daily hot washes to review findings and outstanding items, and an out-brief with installation and tenant leadership providing a preliminary overview of the assessment findings.

3.3.3.4. The post-assessment coordination is primarily conducted internally by the assessment team following the completion of the on-site assessment; although there may also be follow-up with on-site POCs to close out any remaining assessment action items. The internal coordination involves the drafting of an Assessment Team Report (ATR) highlighting the vulnerabilities identified during the assessment and providing a potential recommendation or COA to address each.

3.3.3.4.1. If an identified asset vulnerability is susceptible to specific threats or hazards identified in the AHTA, the report will note this pairing and also provide a rating for the vulnerability based on agreed upon definitions.

3.3.3.4.2. The threat/hazard and vulnerability pairing, along with the criticality rating of an asset, are used to calculate risk. A geometric mean is used for this calculation and the associated rating is another data point commanders can use for resource allocation decisions. The ATR is provided to the installation, MAJCOM/DRU, FOA, and HAF so coordination can occur across all levels for these resource allocation decisions.

3.3.3.5. The JS coordinates the selection of assessment recipients through an annual DoD-wide data call, which concludes and produces a schedule of forthcoming assessments in the late third quarter or early fourth quarter of the preceding year.

3.3.3.5.1. DoDI 3020.45 states installations with DCAs and select Tier 1 TCAs, as identified by the Chairman of the Joint Chiefs of Staff (CJCS), will be assessed at a minimum every three (3) years, while installations with Tier 1 and Tier 2 TCAs will be assessed at a minimum every five (5) years. CCMDs, Services, and Agencies may coordinate with the CJCS to waive periodicity requirements for up to two (2) years if required. Waivers can be granted a maximum of two (2) years for any specific JMAA. (**T-0**)

3.3.3.5.2. Significant changes to any of the major factors utilized to determine risk to an asset may necessitate reassessment of the asset inside its scheduled three (3) or five (5) year cycle.

3.3.3.6. The HAF CARM Program will collaborate with HAF/A4 MA office to provide AF submissions to the JS assessment data call. Submissions should include justification (number and tier of TCAs, missions supported, change in missions supported, time since last assessment, etc.) and availability to be assessed. Submissions will also take into consideration the maximum amount of resources the AF can commit to pre and post-assessment activities. All assessments will be coordinated through the A4 and SAF/IG Gatekeeper Program in order to eliminate duplication of effort and minimize disruption within the assessed unit’s organizations.

3.3.4. The AFMAA is the only assessment program pertaining to the CARM Program, which focuses exclusively on AF assets and infrastructure. The AFMAA team structure and assessment format parallel that of the JMAA. As such, the assessment stages, procedures, outputs, and team composition described in Section 3.3.3 also apply to the AFMAA.

3.3.4.1. While the JMAAs are conducted by DTRA, AFMAAs are coordinated and executed by the AFSFC. The annual schedule of AFMAAs are developed by AFSFC in coordination with AF/A3OA with primary consideration of the assessment requirements dictated by AF Mission Assurance and Antiterrorism programs. These timelines are established by The Deputy Secretary of Defense Mission Assurance Assessment Program Interim Implementation Memo and the AT Program Instruction DODI O-2000.16, V1.

3.3.4.2. The CARM Program will supply a Mission Analyst to participate in AFMAAs involving TCAs. Mission Analysts attend the PSS, assist in asset identification, AFS development, and criticality and risk analysis.

3.4. Mission Risk Analysis.

3.4.1. Per paragraphs 2.17.27 and 2.20.17, RRPs will be developed to document the criticality data, threats, hazards, and vulnerabilities to TCAs identified during an assessment; as well as provide possible risk reduction COAs developed by assessment team SMEs, installation POCs, MAJCOM/DRUs, or FOAs. The purpose of the COAs are to reduce risk to capability and increase mission resilience. The MAJCOM/DRU Commander, or designee, will select a COA or determine the level of asset risk to be acceptable prior to RRP finalization.

3.4.1.1. RRPs will be developed if multiple criteria are met. These criteria may include risk assessment findings of moderate or higher, a recommendation requiring a material solution not Tactics, Techniques, and Procedures (TTP) related, and sufficient existing policy for the owning organization to take action.

3.4.1.2. RRPs will be classified in accordance with DoDM 3020.45 V3, *Defense Critical Infrastructure Program Security Classification Manual,* and related security classification guides.

3.4.2. RRP risk reduction COAs' recommendations fall under two main categories: remediation and mitigation actions.

3.4.2.1. Remediation actions are long-term improvement efforts intended to reduce risk by redressing design or operational environment flaws capable of having adverse effects on the availability of a TCA, not actions to improve functionality or structure.

3.4.2.2. Mitigation actions are taken in response to a warning or after an incident has occurred and are intended to minimize or lessen the incident's potentially adverse effects on a given mission.

3.4.2.3. Each COA recommendation will include a summary of the suggested action, expected risk reduction effectiveness, and estimates of time/investment needed to implement the action.

3.4.3. RRPs are drafted by the asset-owning MAJCOM/DRU or FOA utilizing the appropriate assessment reports and will be coordinated with the HAF CARM Program office or FOA SPO/PMO within 180 days of the formal assessment report release. Personnel should reference **Attachment 3** for a RRP template.

3.4.4. The HAF CARM Program will provide input to the RRP and coordinate the document across the HAF A-Staff and other stakeholders as needed.

3.4.5. The AF/A3 is responsible for final approval of RRPs. The HAF CARM Program office will forward the approved RRP to the JS for finalization.

3.4.6. The HAF CARM Program office will distribute the approved RRP and risk response decision(s) across the HAF A-Staff, relevant MAJCOM/DRU or FOA, and respective CCMDs.

3.4.7. MAJCOM/DRUs and FOAs must document risk response decisions in the AF CARM system of record so the respective chain of command can review risk decisions made at lower echelon levels and formulate additional guidance or direction for management of risk to TCAs. Risk response documentation will include a summary of risk reduction alternatives considered, their expected risk reduction effectiveness, and estimates of required time/investment.

3.5. Risk Management.

3.5.1. The HAF CARM Program will collaborate with HAF/A4 MA to advocate on behalf of the MAJCOM/DRUs and FOAs (as appropriate) for remediation or mitigation actions in chartered executive forums and processes. Forums include the AFCS, AFSEEB, AF Security Enterprise Mission Assurance (SE/MA) Working Group, MA Senior Steering Group, Executive Steering Group, and General Officer Steering Group as MA guidance emerges.

3.5.2. MAJCOM/DRUs and FOAs (as appropriate) will coordinate with appropriate functional offices to implement approved risk response actions.

3.5.3. MAJCOM/DRUs and FOAs (as appropriate) will identify funding requirements to implement risk response actions through the PPBE process and inform the HAF CARM Program of any unfunded risk reduction requirements identified in finalized RRPs.

3.5.4. For large scale remediation or mitigation efforts, the HAF CARM Program will advocate through the AF corporate process for funding and assist MAJCOM/DRUs and FOAs (as appropriate) in coordinating the inclusion of the identified measures in future asset investment planning.

3.5.5. The HAF CARM Program will perform periodic reviews of approved RRPs to determine whether identified risk reduction COAs are undergoing implementation or require follow up action. Inactivity on approved remediation or mitigation efforts may be reported to the JS in accordance with the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3209.01, *Defense Critical Infrastructure Program*.

3.5.6. MAJCOM/DRUs and FOAs (as appropriate) will maintain current and accurate records of identified TCAs and risk remediation efforts in the AF CARM system of record.

3.5.7. The HAF CARM Program will task MAJCOM/DRUs and FOAs (as appropriate) on an annual basis to conduct a review of BEIs for identified TCAs to maintain data fidelity and asset awareness.

3.6. CARM WG.

3.6.1. The CARM WG serves at the primary working level advisory forum for the development, vetting, and coordination of CARM-related policies, procedures, and actions. This may include:

3.6.1.1. Identification, prioritization, and assessment of TCAs.

3.6.1.2. Coordinating, resourcing, and tracking of risk management decisions and actions.

3.6.1.3. Providing situational awareness of TCA availability and reliability.

3.6.1.4. Facilitating cross-functional and cross-organizational dialogue.

3.6.1.5. Supporting consequence management and COOP decisions.

3.6.2. CARM WG membership should reflect AF functional organizations with equity in TCAs or responsibilities which overlap with CARM (such as the MA community). Membership may also include private sector partners when applicable and security protocols allow. CARM POCs will shape membership based on the requirements of their program and supported TCAs.

3.6.3. CARM WGs should be established at the HAF, MAJCOM/DRU, FOA, and asset-owning Center/Wing levels.

3.6.4. The CARM WG can be incorporated into an equivalent, existing MAJCOM/DRU, FOA, Center/Wing, or Installation WG (e.g. Threat, COOP, or EM WG).

3.7. Classification Guidance.

3.7.1. CARM programs shall classify information regarding CARM activities, systems, or assets in accordance with DoDM 3020.45 V3, or as required by the system/asset or capability owner security classification guides.

3.8. Baseline Elements of Information (BEI).

3.8.1. BEIs represent the minimum data required to be captured on assets identified as critical. They do not relieve organizations of other assigned CARM or TCA data exchange responsibilities, such as support of functional are characterization or vulnerability assessment results. This data is required to document a system or asset in the AF CARM system of record and other CCMD established databases.

3.8.2. CARM programs may reference Enclosure 5 of DoDM 3020.45 V1 for a list of BEIs.

Chapter 4

CARM PROGRAM TRAINING AND OUTREACH

4.1. The CARM training and outreach program will provide recipients with an understanding of program methodologies and processes, address any programmatic updates or changes that may impact the field, increase cross-program and cross-function coordination, and enable personnel to execute the four stages of the CARM cycle. Training will be provided through outreach and the leveraging of existing technologies for remote delivery.

4.2. Several methods of remote delivery will be utilized to instruct personnel on the basic tenets of the CARM program and in the navigation of the AF CARM system of record. Electronic Learning Training modules provide individual, self-paced training and are available to all Common Access Card holders through the Advanced Distributed Learning System (ADLS).

4.3. The HAF CARM Program office will conduct CARM Reviews with the MAJCOM/DRU, FOA, and Component to the Combatant Command CARM programs as requested. CARM Reviews will consist of in-person discussions between the HAF and MAJCOM/DRU, FOA, or Component to the Combatant Command CARM staffs regarding CARM Program status, lessons learned/best practices, challenges faced by the field, and issues with which the HAF might assist. Participation in these sessions is not limited to CARM POCs but may include representatives from partner programs and stakeholders (e.g. the MA or CE community, and the relevant CCMD). CARM Reviews will feature a series of focused discussions on the following topics:

4.3.1. Review of the AFI-mandated MAJCOM responsibilities and tasks.

4.3.2. Overview of programmatic and policy updates or changes.

4.3.3. Review of CAIP data and ongoing TCA remediation/mitigation efforts.

4.3.4. Briefing CARM TCA data management capabilities and status.

4.3.5. Beyond the mandatory elements, CARM Reviews may be customized to the desire or need of the CARM field office in order to address specific areas of concern for attendees. Inclusion of partner programs and stakeholders to discuss specific issues with which the HAF CARM Program office could assist is encouraged (HAF advocacy or coordination among HHQ elements) and can serve to promote cross-coordination among programs. The HAF will supply reach-back to provide clarity on any concepts or policies which the MAJCOM/DRU, FOA, or Component to the Combatant Command request.

4.3.6. MAJCOM/DRUs and FOAs will coordinate with the HAF CARM Program office to schedule Mobile Training Team (MTT) sessions for CARM personnel and cooperating programs at the MAJCOM/DRU and FOA levels.

4.4. The specifics of the CARM training program can be found on the CARM SharePoint site. Content will include database navigation tutorials, the FAQs, and a link to the DoD web-sharing tool for live instruction.

SCOTT A. VANDER HAMM, Maj Gen, USAF
Assistant Deputy Chief of Staff, Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

U.S.C. Title 10, *United States Code Title 10, Armed Forces,* August 10, 1956

PPD-21,*Presidential Policy Directive 21,* February 12, 2013

DoDD 3020.26, *Department of Defense Continuity Programs*, January 9, 2009

DoDD 3020.40, *Mission Assurance (MA)*, November 29, 2016

DoDD 4180.01, *DoD Energy Policy*, April 16, 2014

DoDD 5200.43, *Management of the Defense Security Enterprise*, October 1, 2012, Incorporating Change 1, April 24, 2013

DoDD 5205.16 ,*The DoD Insider Threat Program*, September 20, 2014

DoDD 6200.04, *Force Health Protection (FHP)*, October 9, 2004

DoDD 7730.65, *Department of Defense Readiness Reporting System (DRRS)*, May 11, 2015

DoDI O-2000.16, DoD *Antiterrorism (AT) Program Implementation: DoD AT Standards*, November 17, 2016

DoDI 2000.26, *Suspicious Activity Reporting*, September 23, 2014

DoDI 3000.08, *Balanced Survivability Assessments (BSAs)*, January 5, 2010, Incorporating Change 1, November 19, 2010

DoDI 3020.52, *DOD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Preparedness Standards*, May 18, 2012

DoDI 3020.45, *Defense Critical Infrastructure Program (DCIP) Management*, April 21, 2008

DoDI 3150.09, *The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy*, April 8, 2015

DoDI 4170.11, *Installation Energy Management*, December 11, 2009

DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)*, October 9, 2008

DoDI 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program*, January 31, 2014

DoDI 6055.17, *DoD Installation Emergency Management Program*, January 13, 2009; Incorporating Change 1, November 19, 2010

DODI 6200.03, *Public Health Emergency Management Within the DoD*, March 5, 2010, Incorporating Change 2, October 2, 2013

DoDI 8500.01, *Cybersecurity*, March 14, 2014

DoDM 3020.45, V1 *Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP)*, October 24, 2008

DoDM 3020.45, V3 *Defense Critical Infrastructure Program (DCIP): Security Classification Manual (SCM)*, February 15, 2011

CJCSI 3209.01, Defense *Critical Infrastructure Program*, December 18, 2014

AFPD 10-25, *Air Force Emergency Management Program*, April 28, 2014

AFPD 16-14, *Security Enterprise Governance*, July 24, 2014

AFI 10-201, *Force Readiness Reporting*, March 3, 2016

AFI 10-206, *Operational Reporting*, June 11, 2014

AFI 10-245, *Antiterrorism (AT)*, June 25, 2015

Adopted Forms

AF Form 679, Air *Force Publication Compliance Item Waiver Request*

AF Form 847, Recommendation *for Change of Publication*

Abbreviations and Acronyms

AF—Air Force

AF/A1—Deputy Chief of Staff, Manpower and Personnel

AF/A2—Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance

AF/A3—The Air Force Deputy Chief of Staff, Operations

AF/A4—Deputy Chief of Staff, Logistics, Civil Engineering, and Force Protection

AF/A5/8—Deputy Chief of Staff, Strategic Plans and Requirements

AF/A10—Deputy Chief of Staff of Strategic Deterrence and Nuclear Integration

AF/SG—Surgeon General of the Air Force

AFCS—Air Force Corporate Structure

AFI—Air Force Instruction

AFIN—Air Force Information Networks

AFMAA—Air Force Mission Assurance Assessment

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFPDO—Air Force Policy Directive Office

AFRIMS—Air Force Records Information Management Office

AFS—Assessment Focus Statement

AHTA—All Hazard Threat Assessment

ANGRC—Air National Guard Readiness Center

AOR—Area of Responsibility

ASD (HD&GS)—Assistant Secretary of Defense (Homeland Defense & Global Security)

AT—Antiterrorism

ATO—Antiterrorism Officer

BEI—Baseline Element of Information

BSA—Balanced Survivability Assessment

CA—Critical Asset

CAIP—Critical Asset Identification Process

CARM—Critical Asset Risk Management

CARM WG—Critical Asset Risk Management Working Group

CBRN—Chemical, Biological, Radiological, and Nuclear

COCOM—Combatant Command

CE—Civil Engineer

CI—Counter-Intelligence

CJCS—Chairman of the Joint Chiefs of Staff

COAs—Courses of Action

CONPLAN—Contingency Plans

COOP—Continuity of Operations

CSAF—Chief of Staff of the Air Force

DCI—Defense Critical Infrastructure

DCIP—DoD Critical Infrastructure Program

DFC—Defense Force Commander

DIB—Defense Industrial Base

DIA—Defense Intelligence Agency

DHS—Department of Homeland Security

DISLA—Defense Infrastructure Sector Lead Agents

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DRU—Direct Reporting Unit

EM—Emergency Management

FAQ—Frequently Asked Question

FBI—Federal Bureau of Investigation

FOA—Field Operating Agency

FYDP—Future Year Defense Planning

HAF—Headquarters Air Force

HHQ—Higher Headquarters

IA—Information Assurance

IAW—In Accordance With

ID—Integrated Defense

IDRMP—Integrated Defense Risk Management Process

IG—Inspector General

IMSC—Installation Mission Support Center

ISR—Intelligence, Surveillance, and Reconnaissance

IT—Information Technology

JCS—Joint Chiefs of Staff

JMAA—Joint Mission Assurance Assessment

JS—Joint Staff

JWICS—Joint Worldwide Intelligence Communications System

LE—Law Enforcement

MA—Mission Assurance

MAA—Mission Assurance Assessment

MAJCOM—Major Command

MEF—Mission Essential Functions

MET—Mission Essential Tasks

MTT—Mobile Training Team

OPR—Office of Primary Responsibility

OSD—Office of Secretary of Defense

PBR—Program Budget Review

PEM—Program Element Monitors

PMO—Program Management Office

POC—Point of Contact

POM—Program Objective Memorandum

PPBE—Planning, Programming, Budget and Execution

PSS—Pre-Assessment Site Survey

PSU—Primary Subordinate Unit

RRP—Risk Response Plans

SAF/AQ—Assistant Secretary of the Air Force, Acquisition

SAF/CIO A6—Chief, Information Dominance and Chief Information Officer

SAF/FM—Assistant Secretary of the Air Force, Financial Management and Comptroller

SAF/IG—Secretary of The Air Force Office of The Inspector General

SCI—Special Compartmented Information

SCM—Security Classification Manual

SECAF—Secretary of the Air Force

SECDEF—Secretary of Defense

SE/MA—Security Enterprise / Mission Assurance

SICA—Supporting Infrastructure Critical Asset

SIPRNet—Secret Internet Protocol Routed Network

SMADS—Strategic Mission Assurance Database System

SME—Subject Matter Expert

SPO—Special Program Office

SRM—Sustainment, Restoration, and Modernization

S&T—Science and Technology

TCA—Task Critical Asset

TDY—Temporary Duty

TTP—Tactics, Techniques, and Procedures

USAF—U.S. Air Force

USD—Under Secretary of Defense

VA—Vulnerability Assessment

WG—Working Group

Terms

Air Force Critical Asset Management System Next Generation (AF—CAMS NG) – Risk management/mission assurance related program that identifies Air Force owned task critical assets that are essential to executing combatant command and Air Force Title 10, 32, and 50 mission requirements in an all threats and hazards environment.

Air Force Information Networks (AFIN)—The globally interconnected end-to-end set of AF unique information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support

personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security.

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

Combatant Command (CCMD)—United States Department of Defense unified or specified command with a broad and continuing mission under a single commander established and so designated by the President, through the Secretary of Defense, and with the advice and assistance of the Chairman of the Joint Chiefs of Staff.

Continuity of Operations (COOP)—An internal effort within individual components of the Executive, Legislative, and Judicial Branches of Government assuring the capability exists to continue uninterrupted essential component functions across a wide range of potential emergencies, including local or regional natural disasters, health-related emergencies, accidents, technological and/or attack-related emergencies. COOP involves plans and capabilities covering the same functional objectives of Continuity of Government, must be maintained at a high level of readiness, and be capable of implementation both with and without warning. COOP is not only an integral part of Continuity of Government and Enduring Constitutional Government (ECG), but is simply "good business practice" - part of the Department of Defense's fundamental mission as a responsible and reliable public institution.

Criticality—A metric used to describe the consequence of loss of an asset, based on the effect the incapacitation or destruction of the asset would have on DoD operations and the ability of the Department of Defense to fulfill its missions.

Critical Infrastructure Program (CIP)—The identification, assessment, and security enhancement of cyber and physical assets and associated infrastructures essential to the execution of the National Military Strategy. It is a complementary program linking the mission assurance aspects of the Antiterrorism, Force Protection, Information Assurance, Continuity of Operations, and Readiness programs.

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

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

Defense Critical Infrastructure Program (DCIP)—A DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the national military strategy.

Defense Industrial Base (DIB)—The DoD, U.S. Government, and private sector worldwide industrial complex with capabilities to perform research, development, and design and to produce and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

Defense Readiness Reporting System (DRRS)—A federated system of systems designed to provide the DoD a single comprehensive readiness reporting system with a standard metric uniformly applied across the Department. DRRS integrates the Status of Resources and Training System reporting process, the Joint Forces Readiness Review process, and Installation Readiness reporting into a single readiness report system.

Dependency—The reliance of an asset, system, network, node, or collection thereof on input, interaction, or other requirement from other sources in order for the asset to function properly.

Functional Area Lead—Single focal point for planning and coordination of assurance activities within each sector. Air Force functional area leads will coordinate with the DoD functional area leads.

Hazard—Non-hostile incidents such as accidents, natural forces, and technological failure that cause loss or damage to infrastructure assets.

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

Integrated Defense (ID)— The integration of multidisciplinary active and passive, offensive and defensive capabilities, employed to mitigate potential risks and defeat adversary threat to Air Force operations.

Joint Worldwide Intelligence Communications System (JWICS)—The sensitive compartmented information portion of the Defense Information Systems Network, which incorporates advanced networking technologies that permit point to point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing.

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

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

Mission Essential Task (MET)—A mission task selected by a commander deemed essential to mission accomplishment and defined using the common language of the Universal Joint Task List in terms of task, condition, and standard. Differs from a joint mission essential task in that it may reflect missions tasked within a sole DoD Component's authority.

Mission Essential Task List (METL)—A list of METs/MEFs selected by a commander to accomplish an assigned or anticipated mission that includes associated tasks, conditions, and standards and also requires the identification of command-linked and supporting tasks.

Mitigation—Actions taken in response to a warning or after an incident occurs that are intended to lessen the potentially adverse effects on a given military operation or infrastructure.

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

Resiliency—The characteristic or capability to maintain functionality and structure (or degrade gracefully) in the face of internal and external change.

Risk—The Probability and severity of loss linked to threats or hazards and vulnerabilities.

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

Sensitive Compartmented Information Facility (SCIF)— An accredited area, room, group of rooms, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed where procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular sensitive compartmented information authorized for use or storage within the sensitive compartmented information facility.

Secret Internet Protocol Routed Network (SIPRNet)—The worldwide SECRET-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry.

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

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

Vulnerability—A weakness or susceptibility of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard.

Attachment 2

QUICK REFERENCE CHART AND PROCESS OVERVIEW

Table A2.1. AF Critical Asset Identification Process (CAIP).

STEP	TASK
1	Mission owners decompose assigned missions to identify capabilities required to implement each mission. (**T-1**) **Deliverable:** A list of validated missions, as applicable, executed at each command level down to the Center/Wing level (Wing roll-up of Squadron mission tasks). OPRs, where formal METs/MEFs do not apply, identify to the HAF CARM Program office how these are expressed (e.g., OPLANS or CONPLANs).
2	MAJCOM/DRUs, FOAs, ANGRC, and functional areas initiate Task Asset identification and analysis. (**T-1**) **Deliverable:** MAJCOM/DRUs, FOAs and ANGRC, (as appropriate) A3 Division Chief memorandum/email confirmation.
3	MAJCOM/DRUs, FOAs, ANGRC, and functional areas submit nominated TCAs to HAF from Step 2 based on the mission data from Step 1. (**T-1**) **Deliverable:** MAJCOM/DRU, FOA, ANGRC, and (as appropriate) CV approves TCA nominations and releases report. All TCA nominations, including recommended tier level, are loaded into AF-CAMS NG. System-generated TCA reports are sent to the HAF CARM Program office.
4	HAF, MAJCOM/DRUs, FOAs (as appropriate), ANGRC, and functional areas review/validate nominated TCAs. (**T-1**) **Deliverable:** AF-validated TCA nominations and updated AF TCA data in AF-CAMS NG.
5	HAF submits AF TCA validated data to the JS/J33. **Deliverable:** AF-validated TCA data and AF/A3 approval and release of AF TCA validated data to JS**.**
6	JS/J33 compiles TCA submissions (COCOMs, Military Departments, Defense Agencies, and DISLAs) consolidates duplicates and coordinates updates. **Deliverable:** JS release of TCA list to DCI community.
7	Defense infrastructure functional area lead conducts an interdependency analysis of TCAs, when requested. **Deliverable:** Request interdependency analysis through the JS and ASD (HD&GS) as required.
8	MAJCOM/FOAs (as appropriate), ANGRC, and functional areas review and submit DCA-nominations to HAF. (**T-1**) HAF submits AF-approved DCA nominations to JS/J33. **Deliverable:** MAJCOM CV-approved DCA nomination listing. AF-approved DCA nominations submitted to JS.
9	JS Submits DCA nominations list to ASD (HD&GS) and is reviewed and approved. **Deliverable:** ASD (HD&GS)-approved DCA list to the DCI community.

A2.1. During the initial step of the CAIP process , DoD mission owners (CCMDs, Defense Agencies, Military Departments) will decompose their assigned missions and core functions to identify the specific METs/MEFs each requires to be implemented by the resource providers. This information allows resource providers such as Services or Field Activities to select the individual METs/MEFs their organizations execute in support of assigned missions. This process is then replicated at each subordinate organizational level until a list of METs/MEFs required to execute missions are identified down to the Wing level. CARM POCs do not usually perform mission decomposition, but utilize its results to identify the assets which enable the implementation of those missions supported by their respective organizations.

A2.1.1. The authoritative sources for DoD METs are the Universal Joint Task List (UJTL), which comprises all of DoD's joint missions, and the Air Force Universal Task List (AFUTL), which compliments the UJTL missions for which the AF has specific responsibilities. MEFs are organizationally derived, and used to augment applicable METs. Services and other resource providers may assign responsibility for missions to subordinate organizations. MAJCOM/DRU, FOA (as appropriate), and Wing Commanders are responsible for identifying those METs supported by their organizations. The relevant METs are then loaded by each organization into the DRRS or a similar mission readiness database. CARM POCs should leverage their organization's Readiness Officer to navigate this system and to retrieve applicable entries.

A2.1.2. Each of a Command's assigned METs/MEFs contains standards and conditions which define acceptable levels of execution. Combined, these represent an accepted expression of a mission and a quantifiable means to measure mission impact.

A2.2. METs and MEFs obtained from DRRS will then serve as the foundation for asset identification and nomination activities performed by CARM POCs and WGs. CARM POCs should provide a list of installation or command-supported METs/MEFs to CARM WG members. From that list, CARM WG members should identify the specific METs/MEFs their organizations support and then provide SMEs capable of determining the specific assets utilized to execute those tasks.

A2.3. Assets determined to operate in support of assigned METs/MEFs will qualify as TAs. If further analysis by CARM POCs and the CARM WG determines that the degradation or removal of a TA will cause mission degradation or failure, (as determined by the MET/MEF's standards and conditions), then the asset must be nominated for TCA validation. Expanded analysis of each nominated TCA will be conducted at the HHQ level to determine if a redundant capability exists within the larger AOR. If no viable alternative capability is detected, the asset is validated as a TCA at the HAF level and submitted to the JS.

A2.4. Validation of nominated assets as critical to the execution of assigned METs/MEFs is a core function of the CAIP process. The essential requisites for validation include:

A2.4.1. Confirming and documenting the METs/MEFs that are assigned and executed. This reinforces the TCA identification process that starts with the mission. TCAs cannot exist without an associated mission or function.

A2.4.2. Documenting TCAs and associated data points for any mission. All TCA nominations will be approved by each Center/Wing Commander prior to the initiation of the validation process. (T-1) Responsibility for asset data entry into the AF CARM system of record will be determined by the MAJCOM/DRU or FOA (as appropriate). The nominated TCAs will be reviewed and validated by the respective MAJCOM/DRU and FOA (as appropriate). Upon completion, the HAF CARM Program will conduct an informal review of the data for mission impact and completeness. After the HAF CARM Program review, the AF/A3 will approve and release the AF Tiers 1 and 2 TCA data to the JS/J33 for review and coordination. This process includes:

A2.4.2.1. Documenting and verifying the scope of impact of loss or degradation of a TCA.

A2.4.2.2. Providing BEI data to be approved by each level of command and subsequently reviewed and validated by the next echelon of command.

A2.5. The JS will review the mission impact statement associated with each validated DCA and nominate those which meet DCA criteria to the ASD (HD&GS) for review. The ASD (HD&GS) approved list of DCAs will be provided to the appropriate DoD Components.

Attachment 3

RISK RESPONSE PLAN (RRP) TEMPLATE

Figure A3.1. Risk Response Plan (RRP) Template.

(Insert Command Logo)

Defense Critical Infrastructure Program

(Insert Asset Owner)

Risk Response Plan

For

(Insert Asset Name)
(Insert Asset Location – (i.e., Base, State/Country))

Approved by: (Insert Approving Official Name, Rank, Title)

As of: (Insert Approval Date)

I. Executive Summary

Service specific opening information: Why are we doing this RRP, what are the assessed risks to the assets and missions supported, and what are the command recommendations (i.e., accept, mitigate, remediate, or some combination of these options).

II. Asset Information: Criticality Assessment Summary

Asset Name	Self-explanatory		
Asset Owner	Self-explanatory	**Asset Number**	SMADS or CAMS ID #
Asset Description	Describe the asset and what it does, ex. "Key C3ISR node enabling the tasking, collection, exploitation, and dissemination of ISR data." Describe it to the uninitiated.		
Asset Location	Bldg., Base, State/Country (for terrestrial assets), AOR		
Mission Owners	List all mission owners (CCMDs, Services, Agencies, etc.)		
METs/MEFs Supported PLANS	What is/are the impacted METs/MEFs Supported PLANs, along with Condition(s) and Standard(s) identified for this asset?	**Mission Impact**	Tier I (mission failure) or Tier II (severe degradation)?
		Time to Impact	Time to Mission Impact
		Time to Restore	Time to Restore Critical Asset Capability
Consequence of Loss Statement	Describe what happens to the mission should the asset fail, ex. "Loss of the asset would result in the inability to operationally align expertise with specific theater collection priorities and assets. This results in failure to satisfy joint and coalition intelligence needs, as well as production with other services and national agencies."		

(*The Mission Owners, METs/MEFs Supported PLANs (and associated impact and time data), and Consequence of Loss Statement may be duplicated in this table, as appropriate.*)

Based on the above information, (this asset) was determined to have a criticality rating of _____.

III. Threat/Hazard Assessment Summary

Summarize the likely/probably threats/hazards to the asset. This will focus on the most likely or probable threats and hazards and will be those threats/hazards linked to identify vulnerabilities of the asset. This section will also include associated scoring for each threat/hazard.

Critical Asset	Threat/Hazard	Threat/Hazard Rating
Asset A (Bldg. 1)	A/C Failure	**High**
	Terrorism - VBIED	**Low**
Asset B (Bldg. 2)	A/C Failure	**High**
	Fire Damage	**Medium**

IV. Vulnerability Assessment Summary

Include key highlights from the last VA – who conducted it, and when. Summarize the vulnerabilities associated with the most likely or probable threats/hazards. This section will also include associated scoring for each vulnerability.

Critical Asset	Vulnerability Description	Vulnerability Rating
Asset A (Bldg. 1)	Rm. 100 no longer has adequate redundancy with its A/C units and if one unit fails mission equipment will receive insufficient cooling and could overheat and fail.	**High**
	Vehicles can park within 10 feet of the building due to lack of barriers or fencing.	**Medium**
Asset B (Bldg. 2)	One of three A/C units supporting Rms. 10, 11, and 15 have been malfunctioning and personnel have had to open doors and bring in portable fans to prevent mission equipment from overheating and failing.	**Critical**
	This building lacks an automatic fire suppression system. While fire extinguishers are present for personnel to utilize, should an alarm sound this facility is not manned 24/7.	**Medium**

V. Bisk Assessment Summary

Provide risk ratings for the asset based on the likely/probably threats/hazards and associated vulnerabilities. Ensure focus is on Critical/High/Significant Risks. Identify COAs for each of these risks. These COAs can, and should, cover immediate/short-term mitigation options through long-term, resource-intensive remediation options.

For (asset name), which has a criticality rating of _____, the threat/hazard and vulnerability pairs result in the following risk ratings:

A. Risk A: (List threat/hazard and vulnerability (ex. A/C failure and inadequate cooling redundancy) – Risk Rating)
B. Risk B: (Threat/hazard and vulnerability – Risk Rating)

For each of these identified risks above, the following COAs have been identified:

A. Risk A, COA #1: (Briefly describe the COA and include project numbers, cost, ESD/ECD if and when available)
B. Risk A, COA #2: (Briefly describe the COA)
C. Risk A, COA #3: (Briefly describe the COA)
D. Risk B, COA #4: (Briefly describe the COA)
E. Risk B, COA #5: (Briefly describe the COA)
F. Risk C, COA #6: (Briefly describe the COA)

VI. Risk Response

Describe what your organization may have already done or can do based on the proposed COAs for each risk, and identify how this revises the risk. Provide project numbers, titles, cost, resource provider, ESD, ECD, LIMFACs, etc.).

The below table represents the anticipated change in vulnerability and risk after implementation of each of the identified COAs:

	Vul. Descrip.	Vul. Rating	Risk Rating	COA	Revised Vul.	Revised Risk
Risk A, COA #1	Inadequate Cooling	High	Critical	Have load-shedding plan	High	Critical
Risk A, COA #2	Inadequate Cooling	High	Critical	Have portable equip. avail.	Medium	High
Risk A, COA #3	Inadequate Cooling	High	Critical	Add another A/C unit	Low	Low
Risk B, COA #4	VBIED	Medium	High	Update barrier plan for higher FPCONs	Medium	High

VII. Conclusions & Recommendations

Propose way ahead by your organization on COAs. Include recommendations or requests your organization has for the DoD/JS/Mission Owners and include additional conclusions as necessary.