BY ORDER OF THE
SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE
MANUAL 13-212, VOLUME 3

11 FEBRUARY 2022

Nuclear, Space, Missile, Command and Control

CYBERSPACE RANGE PLANNING AND OPERATIONS

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 or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A3TI
Senior USSF Coordinator: SCC/CD (Brig Gen Donald Cothern)
Certified by: AF/A3T (Maj Gen Albert G. Miller)
Supersedes: AFMAN 13-212 Volume 3, 17 October 2019
Pages: 43

This manual implements Air Force Policy Directive (AFPD) 13-2, *Air Traffic, Airfield, Airspace, and Range Management*; AFPD 16-10, *Modeling and Simulation;* and Department of Defense Directive (DoDD) 5101.19E, *DoD Executive Agents for the Cyber Test and Cyber Training Ranges*. This manual establishes the Cyberspace Range Planning and Operations that support Department of the Air Force (DAF) objectives and provides foundational guidance on how to plan and integrate a cyberspace infrastructure for current and future Department of the Air Force cyberspace ranges. This infrastructure will support cyber testing, training, evaluations, multi-domain exercises, experimentation, concept development, and mission rehearsals, as well as other related cyber activities. This publication applies to all civilian employees and uniformed members of the Regular Air Force, United States Space Force, Air Force Reserve and Air National Guard, and to contractors when required by the terms of their contracts. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility (OPR) listed above for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the OPR listed above using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in

this publication does not imply endorsement by the Department of the Air Force. The authorities to waive wing/unit/USSF equivalent level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Reference Department of the Air Force (DAF) Instruction (DAFI) 33-360, *Publications and Forms Management*, 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 AF/A3TI for non-tiered compliance items. See **paragraph 1.3** for additional details on waiver processing. Compliance with the attachments in this publication is mandatory.

SUMMARY OF CHANGES

This manual has been substantially revised and must be completely reviewed. Major changes include the addition of the Joint Information Operations Range (JIOR) to the Air Force as a primary cyberspace range and the funding sources that support the range, and the change from an AFMAN to a DAF Manual (DAFMAN). Additionally, it has been revised to update the flow of attachments and the contents of the cyberspace range capability matrices to be more accurate. Furthermore, the manual has also been updated to reflect the appropriate responsibility for integration of Air Force control systems cybersecurity efforts with energy and utility resiliency under the AF/A4. Finally, the manual has been updated to reflect the Air Force Futures Cross-functional Team (CFT) governance structure for developing infrastructure.

Chapter 1

INTRODUCTION

1.1. Overview. This manual provides guidance for commanders to operate assigned cyberspace ranges effectively, efficiently, and in accordance with the risk management framework (RMF) to meet training and test requirements. Additionally, this manual assigns the responsibilities and authorities to accomplish activities outlined in the manual, including the development of an Enterprise Range Plan Cyber Annex.

1.2. Scope.

1.2.1. This manual applies to all Department of the Air Force-operated cyberspace ranges. A cyberspace range is an event environment that supports cyber effects on information technology; weapons; control systems; command, control, communications, computers, intelligence, surveillance, and reconnaissance; and other network-enabled technologies for the purpose of experimentation, testing, training, or exercising on a real or simulated network.

1.2.2. Cyberspace ranges encompass the hardware, software, and connectivity; test facilities; and test beds and tailored scenarios and capabilities to conduct research, development, test and evaluation. Additionally, they provide other means and resources for testing, training and exercises, demonstration and developing software; personnel; organization and all information system networks or enclaves that represent the cyberspace environment.

1.2.3. While most of the range equipment consists of standard Internet Protocol systems such as servers, routers, and switches, it also includes specialized systems such as radio frequency systems, cellular technologies including but not limited to wireless communications technologies, simulators, control systems, avionics, and detailed threat systems.

1.2.4. The cyberspace ranges are part of the Department of the Air Force's Operational Training and Test Infrastructure (OTTI). **Attachment 3** is intended to be the definitive list of Department of the Air Force primary cyberspace ranges; however, this manual covers all cyberspace ranges. Department of the Air Force organizations conducting Cyberspace Range activities, as defined in Department of Defense (DoD), *DoD Executive Agents for the cyber Test and Cyber Training Ranges,* Directive 5101.19E aligned to cyberspace ranges at locations other than those listed in **Attachment 3** must contact the parent major command (MAJCOM or Field Command) for review. **(T-1)**

1.2.5. If the range review determines the activity is within the scope and intent of this DAFMAN, a request for change should be submitted to Air Combat Command (ACC) and Headquarters Air Force OTTI Division (AF/A3TI) to update **Attachment 3**.

1.3. Waiver request.

1.3.1. Waiver requests will be submitted using the AF Form 679, *Air Force Publication Compliance Item Waiver Request/Approval,* and will include the information specified in DAFI 33-360, paragraph 1.9.4.2. The waiver authority may impose additional requirements.

1.3.1.1. Non-Tiered and T-0 waiver requests must also include the following:

1.3.1.2. Range name, location, Range Operating Authority and a point of contact.

1.3.1.2.1. Description of the conditions at issue to include:

1.3.1.2.2. Potential alternatives and their impact on test and training operations, maintenance, cost, and other factors deemed appropriate by the requesting agency.

1.3.1.2.3. Supporting Cyberspace Range architecture, charts, graphics, or other illustrations as appropriate.

1.3.1.3. A detailed plan to alleviate the condition.

1.3.1.4. Previously granted waiver, if any.

1.3.2. AF/A3TI will coordinate non-Tiered, T-0 and T-1 waiver requests with Headquarters Air Force Test and Evaluation (AF/TE) for Test and Evaluation (T&E) range matters when appropriate.

1.3.3. AF/A3TI will coordinate all waiver requests with ACC, Airspace, Ranges and Airfield Operations Division (ACC/A3A) so they can maintain appropriate situational awareness as the lead Command.

1.4. Supplements. This publication may be supplemented at any level. Route all supplements for coordination prior to certification and approval. **(T-1)** Supplements may change or add procedures, as applicable, to this manual, but changes can be no less restrictive than this manual. All supplements may use the most suitable format (i.e., integrated or standalone) and must be published in accordance with DAFI 33-360 on the Department of the Air Force electronics publications website. For MAJCOM and Field Command supplements, MAJCOMs and Field Commands must submit a copy to AF/A3TI for review and coordination prior to publication.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. The Assistant Secretary of the Air Force for Acquisition, Technology and Logistics (SAF/AQ).

2.1.1. Will serve as the focal point for development and procurement of cyber capabilities and perform all program element monitor (PEM) responsibilities for cyber capabilities.

2.1.2. Coordinate range-related acquisition programs and program element (PE) changes with AF/A3TI.

2.1.3. Provide technical advice and direct technical program assessments as needed.

2.1.4. Understand and communicate dependencies of weapon systems on infrastructure.

2.1.5. Oversee policy updates and implications for contracting and vendor acquisition requirements.

2.1.6. Act as the focal point for cyber-related science and technology research and development programs and monitor new technology for inclusion in Cyberspace Range planning.

2.1.7. Ensure that the creation of cyber capabilities that will be used as weapons and/or weapons systems are reviewed for legal sufficiency by AF/JAO prior to fielding and use.

2.1.8. Ensure that the creation of cyber capabilities that are intended to be used as weapons are properly reported to Congress, thru OSD.

2.2. The Deputy Under Secretary of the Air Force, International Affairs (SAF/IA).

2.2.1. Will provide policy and disclosure oversight to the DAF for the management of Foreign Military Sales cases and bilateral/multi-lateral training which utilizes AF systems and ranges.

2.2.2. Serve as the focal point for cooperative agreement with partner nations for the development of systems and capabilities.

2.3. The Assistant Secretary of the Air Force for Installations, Environment, and Energy (SAF/IE).

2.3.1. Will provide policy and oversight of all operational range environmental support such as operational range assessments and responses, natural and cultural resource management, hazardous material and hazardous waste management, and compliance with applicable environmental requirements that includes live ranges with cyber-integrated components.

2.3.2. Will oversee strategic basing, and environment, safety, and occupational health for cyberspace ranges.

2.4. The Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations (AF A2/6).

2.4.1. Will formulate, plan, refine, integrate, and oversee the direction, policy and execution of Air Force capabilities for Offensive Cyber Operations, Defensive Cyber Operations, and DoD Information Network operations (e.g., continuous monitoring, specialized toolkits, Mission-Relevant Terrain in cyberspace).

2.4.2. Formulate, plan, refine, integrate, and oversee the direction, policy, training, and execution of Air Force capabilities for the intelligence, surveillance, and reconnaissance of Air Force networks and supporting infrastructure.

2.4.3. Serve as lead for collecting, reporting and disseminating intelligence between United States Cyber Command (USCYBERCOM), intelligence communities, and DAF functional organizations.

2.4.4. Work with USSF Chief Operations Officer Director of Intelligence, Surveillance, Reconnaissance (SF/S2) and USSF Chief Operations Officer Director of Cyber and Spectrum Ops Integration (SF/S6C) to ensure USSF equities are included.

2.5. The Chief Information Officer (SAF/CN).

2.5.1. Will enforce the RMF in accordance with DoD Instruction 8510.01, *Risk Management Framework (RMF) for Department of Defense Information Technology (IT)***.**

2.5.2. Shall provide oversight and policy authority for cyberspace-related AF Special Access Programs in accordance with AFPD 16-7, *Special Access Programs,* and AFI 16-701, *Management, Administration, and Oversight of Special Access Programs.*

2.6. The Deputy Chief of Staff for Operations (AF/A3). In accordance with Headquarters Air Force Mission Directive 1-54, *Deputy Chief of Staff, Operations, Plans & Requirements*, and in coordination with USSF Chief Operations Officer (SF/COO), AF/A3 is responsible for matters concerning ranges. As Lead Integrator for OTTI, AF/A3 appoints an Authorizing Official for OTTI systems to SAF/CN for appointment in accordance with AFI 17-130, *Cybersecurity Program Management*. AF/A3, through the Director of Training and Readiness (AF/A3T), establishes range policy, programming, and requirements.

2.6.1. Director of Training and Readiness (AF/A3T) will:

2.6.1.1. When appointed, serve as the OTTI Authorizing Official, responsible for the cybersecurity review and approval of cybersecurity accreditation for cyberspace range operations.

2.6.1.2. Designate AF/A3TI as the OPR for all Air Force range policy and management.

2.6.1.3. Work with USSF Chief Human Capital Officer (CHCO) Education, Training & Development (SF/S1D) to ensure USSF equities are included.

2.6.2. Operational Training Infrastructure Division (AF/A3TI) will:

2.6.2.1. Develop range policy, programming, and requirements in accordance with AFPD 13-2 and in coordination with AF/TE.

2.6.2.2. Review and coordinate on ACC's Enterprise Range Plan Cyber Annex.

2.6.2.3. Advocate for Air Force cyberspace range sustainment funding.

2.6.2.4. Serve as the Headquarters level focal point for development and procurement of cyberspace range training systems, threat emulators and engagement scoring systems.

2.6.2.5. Perform PEM responsibilities in coordination with ACC for cyberspace training range development and procurement in association with the Cyberspace Training (84762F) and Support to Information Operations Capabilities (33166F) Program Elements.

2.6.2.6. Provide cyberspace range-related information to the Cyberspace Range Steering Group as requested.

2.6.2.7. Provide semi-annual feedback to Headquarters Air Force on cyberspace range capabilities and status.

2.6.2.8. Coordinate statutory and regulatory cyber security requirements in accordance with AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT).*

2.6.2.9. Coordinate with the executive agent for cyberspace training ranges, to include serving as Air Force representatives in initiatives such as the Persistent Cyber Training Environment (PCTE) Executive Board, Joint Cyber Training Enterprise (JCTE) Executive Board and the DoD Cyberspace Range Working Group.

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

2.7.1. Will coordinate and facilitate Military Construction requests for cyberspace range facilities.

2.7.2. Will facilitate the cross-functional integration of the Department of the Air Force's control systems cybersecurity, defense and resiliency efforts..

2.8. The Director of Air Force Test and Evaluation (AF/TE).

2.8.1. Will perform Headquarters level portfolio management and oversight, in conjunction with SAF/AQ for the following T&E infrastructure and support areas: cyberspace test range operations and maintenance (O&M); Threat Simulator Development; Major T&E Investment; Operational T&E; T&E Support; and Facility, Sustainment, Repair and Modernization (FSRM).

2.8.2. Serve as AF OPR for congressional reporting on AF Cyberspace Test Range Budget Exhibit.

2.8.3. Serve as AF OPR for coordinating with the DoD Executive Agent for Cyberspace Test Ranges' Test Resource Management Center (TRMC).

2.8.4. Work with SF/TE under VCSO/USSF to ensure space equities are included.

2.9. ACC.

2.9.1. Will develop and publish the Enterprise Range Plan Cyber Annex.

2.9.2. Serve as the lead for the Air Force Cyberspace Range Steering Group and develop the Cyberspace Range Steering Group charter to include identifying members and stakeholders.

2.9.3. Serve as the lead Command for the overall program management of Center Scheduling Enterprise (CSE) to include development of utilization guidance, system implementation, and sustainment. The CSE is a computerized man-in-the-loop system designed for the scheduling of all missions requiring the use of ranges or support resources.

2.9.4. Create and maintain security classification guide for ACC owned cyberspace ranges.

2.9.5. Identify, manage, and advocate for funding of cyberspace range requirements.

2.9.5.1. Collect, coordinate, and prioritize requirements for cyberspace range capabilities.

2.9.5.2. Sponsor PEM for cyberspace training ranges, operations, and sustainment.

2.9.5.3. Develop and publish a process for soliciting MAJCOM and Field Command input.

2.9.5.4. Serve as lead Command for development and procurement of cyberspace range training systems, threat emulators and engagement scoring systems.

2.9.5.5. Perform all PEM responsibilities for cyberspace training range development and procurement in association with the Cyberspace Training (84762F) and Support to Information Operations Capabilities (33166F) Program Elements as well as Facility, Sustainment, Repair and Modernization (FSRM) dollars.

2.9.6. Host a biennial integrated Air Force Airspace and Range Conference which includes multi-domain ranges (cyberspace, space, Information Operations, etc.).

2.9.7. Provide oversight to ensure that cyberspace range systems meet cybersecurity risk management framework (RMF) requirements in accordance with AFI 17-101. Provide standardized implementation guidance for RMF-related contracts.

2.9.8. Update/manage assigned cyberspace ranges and coordinate support for cyberspace range activities.

2.9.9. Develop policy, advocate for resources, define requirements, and manage the oversight of MAJCOM and Field Command cyberspace ranges.

2.9.10. Serve as Cyberspace Range Central Authority to collect requirements, advocate for funding at higher headquarters, provide prioritization framework for oversight of cyberspace range training and ACC owned test resources, and monitor for usage and availability of all AF cyberspace ranges.

2.9.11. Designate command or staff element responsible for overseeing connectivity (e.g., local, Joint Information Operations Range (JIOR), Joint Mission Environment Test Capability (JMETC) Multiple Independent Levels of Security (MILS) Network (JMN), and commercial Internet), and access to Air Force operational cyberspace workforce (e.g., Mission Defense Teams, Cyber Protection Teams).

2.9.12. Designate command or staff element will develop and publish a process for cyber units to request connectivity to cyberspace ranges.

2.9.13. **Work with Space Operations Command (SpOC) to ensure USSF equities are included.**

2.10. AFMC.

2.10.1. Support a PEM for the Cyber T&E investment PEs.

2.10.2. Create and maintain security classification guide for AFMC owned cyberspace ranges to complement the unit-level and program class guides if required.

2.10.3. Identify, manage, and advocate for funding of cyberspace test infrastructure requirements.

2.10.4. Collect, coordinate, and prioritize Cyberspace Test Range Foreign Materiel Acquisition requirements.

2.10.5. Coordinate and deconflict AFMC Cyberspace Test Range priorities across MAJCOMs and Field Commands as required.

2.10.6. Fulfill necessary management and oversight functions for AFMC-owned cyberspace ranges not otherwise identified as Primary Range Providers. These functions include but are not limited to: developing policy, advocating for resources, managing requirements, and range prioritization

2.10.7. Manage cybersecurity Risk Management Framework (RMF) processes by ensuring that an appropriately cleared Approving Official (AO) or Delegated Approving Official (DAO) is appointed for all Cyberspace Test-related Collateral, SCI, and SAP Information Systems in accordance with AFI 17-101.

2.10.8. Work with Space Systems Command (SSC) to ensure USSF equities are included.

2.11. All MAJCOMs and Field Commands.

2.11.1. Will provide input for cyberspace range investment and equipment requirements to ACC.

2.11.2. Review and forward requests for non-Tiered and T-0 waivers to this manual to AF/A3TI.

2.11.3. Serve as the T-2 waiver authority or delegate this authority to the appropriate MAJCOM and Field Command Director.

2.11.4. Contract for services to support execution of range missions in accordance with AFI 63-138, *Acquisition of Services*, and AFI 63-101/20-101, *Integrated Life Cycle Management.* Ensure RMF requirements, such as having an information system security officer, are implemented at each cyberspace range in a standardized manner. When practical, partner with other MAJCOMs and Field Commands to achieve economies of scale.

2.11.5. Ensure range scheduling and utilization data is standardized across the Department of the Air Force, recorded, reported, and archived in CSE.

2.11.6. Coordinate with other public and private interests and agencies as required to support MAJCOM range requirements.

2.11.7. Air Force Materiel Command (AFMC) only. Sponsor the PEM for the Cyber T&E investment PEs.

2.11.8. Identify primary and alternate POC’s to represent MAJCOM and Field Command equities at the Air Force Cyberspace Range Steering Group (O-6) and Air Force Cyber Range Working Group (O-4/5).

2.11.9. Provide quarterly feedback to Headquarters Air Force on cyberspace range capabilities and status. Status reports will come in the form of a report card formatted to mirror the Threat Matrix Framework (TMF). The TMF scores range capabilities against intelligence requirements outlined in the most current adversary assessment to ensure competitive advantage and exercises tactics, techniques and procedures (TTP) commensurate with near-peer threats estimates. TMF grading criteria are aligned to the National Defense Strategy and Congressional mandates for cyber readiness.

2.12. Air Force Agency for Modeling and Simulation.

2.12.1. Will provide guidance on standards, architectures, and future design of cyberspace ranges as it relates to modeling and simulation (M&S).

2.12.2. Provide guidance on backward compatibility with legacy ranges to the maximum extent possible as it relates to M&S.

2.12.3. Develop documented DAF and joint cyber M&S training requirements across the MAJCOM and Field Command enterprise and provide guidance and advocacy for solutions.

2.12.4. Develop documented joint interoperability challenges of OTTI requirements and provide advocacy and guidance for solutions across the MAJCOM and Field Command enterprise.

2.13. Program Management Offices.

2.13.1. Will integrate weapon system capabilities for integration into cyberspace ranges. **(T-1)**

2.13.2. Develop validated Lead MAJCOM and Field Command requirements for weapon-system related cyberspace range capabilities. **(T-1)**

2.14. Cyberspace Range Operating Authority. The cyberspace range Commanders are designated as the Range Operating Authority for their respective cyberspace test and training ranges.

2.14.1. Cyberspace Range Operating Authorities will:

2.14.1.1. Ensure compliance with this manual. **(T-1)** Cyberspace Range Operating Authority may delegate in writing, the daily scheduling, operation, maintenance, and management of the range to a subordinate unit.

2.14.1.2. Appoint a Cyberspace Range Operations Officer, in writing, to supervise range operations, management, planning, and maintenance. **(T-1)** The Cyberspace Range Operations Officer will be a military officer or DoD civilian employee. **(T-1) Note:** Cyberspace Range Operating Authorities must ensure requests for waivers forwarded to the MAJCOM and Field Commands are reviewed by the lead agency Office of the Staff Judge Advocate and manpower offices for compliance with applicable law and DoDI 1100.22, *Policy and Procedures for Determining Workforce Mix.* **(T-1)**

2.14.1.3. Ensure customer requirements are met. **(T-2)**

2.14.1.4. Manage Interconnection Security Agreements and maintain connectivity over a variety of means (e.g., local, JIOR, JMETC, JMN, PCTE, and commercial Internet).

2.14.1.5. Ensure the cyberspace range systems adhere to cybersecurity risk management framework requirements in accordance with AFI 17-101. **(T-2)**

2.14.1.6. Determine daily execution range priorities of test and training resources based on mission requirements, MAJCOM, Field Command, ACC and/or senior leader inputs. **(T-2)**

2.14.1.7. Execute cyberspace range events in accordance with guidance and priorities. **(T-2)**

2.14.1.8. Appoint a Cyberspace Range Safety Officer to assist with independent risk assessments. **(T-2)**

2.14.2. Cyberspace Range Operations Officer. The Cyberspace Range Operations Officer has responsibility over all cyberspace range activities and serves as the Cyberspace Range Operating Authority's primary point of contact for cyberspace range issues. **(T-2)** The Cyberspace Range Operations Officer will:

2.14.2.1. Develop cyberspace range procedures, and interface with support agencies and operational units related to range operations, management, planning, and maintenance. **(T-1)**

2.14.2.2. Work with the T&E organization, cybersecurity dedicated professionals, cyberspace range staffs and exercise community to ensure cyberspace ranges provide capabilities and environments that can be integrated at the appropriate classification levels to conduct training, joint exercises, mission rehearsals, experimentation, and testing of military capabilities within a cyberspace environment. **(T-2)**

2.14.2.3. Identify threats, potential risk, and impact analysis, in conjunction with the range safety officer, so the Authorizing Official can make an informed risk decision for on-going range operations.

2.14.2.4. Develop content to be used for all levels of cyber training, test, and mission rehearsals. **(T-2)** Cyberspace Range Operating Authority will oversee contracts established to develop training and/or testing events and will manage and maintain the content. **(T-2)** Any developed training content should also be focused on integration into PCTE for use by other services.

2.14.2.5. Participate in Cyber Test review, and T&E Master Plan (TEMP) or test strategies development in accordance with AFI 99-103, *Capabilities-Based Test and Evaluation,* by assessing test project plans, ensuring that they identify and mitigate cyber security system limitations. **(T-1)**

2.14.2.6. Provide information and assistance to test planners regarding cyberspace range costs, availability, and priorities for training and testing requirements, as requested.

2.14.2.7. Obtain MAJCOM and Field Command approval of test architectures prior to authorizing test events on a primary training range and primary cyberspace ranges.

2.14.2.8. Enter into written agreements in coordination with the MAJCOM/Field Command and in accordance with **paragraph 4.2.1** and AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures.* **(T-1)**

2.14.2.9. Develop and maintain a cyberspace range supplement to this manual. **(T-1)**

2.14.2.9.1. Must submit the range supplement to the parent MAJCOM or Field Command for review and coordination prior to publication. **(T-1)** When supplements require update due to a significant change in range operations, submit an updated supplement to the MAJCOM or Field Command within 120 calendar days. **(T-1)**

2.14.2.9.2. Ensure the supplement includes: Cyberspace Range Squadron description; general primary cyberspace range descriptions; services and capabilities available; hours of operation; cyberspace range diagrams; cyberspace range scheduling procedures; joint operating procedures (to include PCTE integration); crew training facility requirements, alignment of cyber operations forces to assigned cyberspace ranges; and establishment of persistent connections to cyberspace ranges. **(T-2)**

2.14.2.10. Maintain scheduling control over virtual environments, tools, training spaces, connectivity and equipment using CSE and document scheduling procedures in a letter of agreement or the range supplement. **(T-1)**

2.14.2.11. Post on CSE applicable cyberspace range information, points of contact, updated procedures, access to the local supplement to this manual, scheduling information, and links to other large reference sources, stored outside of CSE. **(T-1)**

2.14.2.12. Complete annual plans to ensure availability of necessary funding for personnel, contracts, equipment, facilities, and other resources. Submit updates to the parent MAJCOM, Field Command and ACC. **(T-1)**

2.14.3. Primary Range Providers will:

2.14.3.1. Serve as conduit for assigned users' requirements in support of Central Authority. **(T-2)**

2.14.3.2. Support Central Authority in evaluating cyberspace range requirements against current and projected capabilities to identify shortfalls and guide sustainable cyberspace range development. **(T-2)**

2.14.3.3. Plan, build, and execute range connectivity requirements, environments, scenarios, and events in support of assigned units' test, development, training, exercise, and/or mission rehearsal requirements which include relevant intelligence and user validated technical requirements. **(T-2)**

2.14.3.4. Serve as liaison with other Department of the Air Force and joint cyberspace ranges to leverage their capabilities to meet assigned units' cyberspace training range needs. **(T-2)**

2.14.3.5. Operate, manage, and maintain capabilities to provide high fidelity, operationally realistic cyber environments, to include physical hardware and software of DAF cyber systems, cyber weapon systems & networks, internet grey space, threat representative networks, and controlled environments on which malicious code can be deployed. **(T-2)**

2.14.3.6. Develop, manage, and integrate M&S capabilities to include live, virtual, constructive (LVC) models into test, development, training, exercise, and mission rehearsal events. **(T-2)**

2.14.3.7. Ensure all systems and services hosted on the range remain in compliance with Department of the Air Force information assurance standards. **(T-2)**

2.14.3.8. Operate, manage, and maintain event execution infrastructure that is adequately resourced and staffed to handle up to large scale, Department of the Air Force and combatant command level exercises. **(T-2)**

2.14.3.9. Provide crew training facilities capable of providing simultaneous support to multiple cyber operations teams including opposing forces. **(T-2)**

Chapter 3

CYBERSPACE RANGE PLANNING

3.1. Comprehensive Cyberspace Range Planning.

3.1.1. The DAF accomplishes comprehensive cyberspace range planning to ensure exercises, training, mission rehearsals, and testing requirements are met. This process evaluates cyberspace range requirements against current and projected capabilities to identify shortfalls. It also guides sustainable cyberspace range development to mitigate shortfalls. This manual, along with a hierarchy of plans, provide the guidance that documents the current sustainment and future cyberspace range development.

3.1.2. The *Operational Training Infrastructure Flight Plan*. AF/A3TI drafts and publishes the *Operational Training Infrastructure Flight Plan* for the DAF. Since cyberspace ranges are part of the Air Force's OTTI, the OTTI Flight Plan provides the long-term strategic vision and direction for Air Force cyberspace ranges. The plan establishes a vision of a realistic, integrated training environment that allows forces to train in mission relevant employment schemes to achieve and sustain full-spectrum readiness. It also describes the long-term OTTI requirements to achieve the vision set forth in the 2015 Strategic Master Plan and Air Force Future Operating Concept.

3.1.2.1. Enterprise Range Plan Cyber Annex. ACC, as the lead MAJCOM, will produce an Enterprise Range Plan Cyber Annex and coordinate it with AF/A3TI and AF/TE prior to publication. **(T-1)** The plan should have a 10-year planning horizon and support achievement of the vision established in the *Operational Training Infrastructure Flight Plan*.

3.1.2.2. ACC will ensure the Enterprise Range Plan Cyber Annex identifies the current mission of each cyberspace range and the range requirements. **(T-1)** This includes detailing necessary test and training capabilities as well as specifying training requirements for assigned users. It should compare current and known future requirements against the current cyberspace range capabilities to identify shortfalls and describe investment actions.

3.1.2.3. Enterprise Range Plan Cyber Annex development provides an opportunity for all Combatant Commands, MAJCOM organizations and staff to provide input, coordinate actions within the command and across MAJCOMs. ACC will coordinate the plan with all MAJCOMs and Field Commands to ensure their needs and concerns are addressed. **(T-1)**

3.1.3. Department of the Air Force Cyber Training Requirements. Cyberspace range training support requirements are based on the USCYBERCOM Training and Readiness Manual, Combatant Command requirements, and Cyber Weapon System training events of the assigned units. As Cyber Weapon Systems, mission types, training events, and/or tactics, techniques, and procedures change to meet emerging threats and technologies, the MAJCOM Realistic Training Review Boards are instituted to maximize the quality of unit training and convene (usually annually) to update training events, frequency and standards. MAJCOM Realistic Training Review Boards will also publish requirements to AF/A3TI and AF/TE for review and funding advocacy and will comply with AFI 16-1007, *Management of Air Force Operational Training Systems*. **(T-1)**

3.1.3.1. At a minimum, MAJCOMs and Field Commands shall bi-annually review applicable portions of the Combat Air Forces Realistic Training Review Board, Cyberspace Range Steering Group, Offensive/Defensive Cyber Operations Steering Group, joint range user assignments, the range-supported Major Weapon System events, AFI 16-1007, and other applicable training requirements documents. **(T-1)** Following the review, the MAJCOMs, and Field Commands through ACC as the lead MAJCOM, will provide AF/A3TI and AF/TE with inputs on recommended changes to Attachments **2 and 3**. **(T-1)**

3.1.3.1.1. The bi-annual review should ensure specific cyberspace ranges have been tasked to support each specific training event and that the ranges have the required capability to do so. MAJCOMs and Field Commands must support shortfalls necessitating a change to assigned users, or capability and infrastructure investments based on the published data.

3.1.3.1.2. User-event assignments should consider connectivity requirements, scheduling, cyberspace range capabilities, joint interoperability requirements, crew training facilities, external cyberspace range support requirements, as well as the scope and attributes required for the assigned event. Units can be assigned to more than one range for the same training event.

3.1.3.1.3. When a MAJCOM or Field Command does not have an adequate cyberspace range to support one of its units, the lead MAJCOM will engage other cyberspace range-owning MAJCOMs, Field Commands, service(s) and DoD organizations for support and assignment of their units. **(T-1)** If the shortfall cannot be serviced, the Cyberspace Range Squadron will submit a Test/Training Space Needs Statement (T/TSNS) to the Central Authority for resolution. **(T-1)**

3.1.3.1.4. During the bi-annual review, MAJCOMs and Field Commands should review test and training requirements to determine the adequate mixture of threat representative cyber environments and multi-domain integrative capability to include: M&S; LVC; space training range integration; and, if necessary, changes to cyberspace range requirements. This drives a continuous modernization process that meets test objectives, increases combat realism, aids tactics development, enhances day-to-day training, and moves toward a balanced and appropriate live, cyber and synthetic mix.

3.1.3.2. Priority at primary cyberspace ranges. The Lead MAJCOM and the Cyberspace Range Operating Authority determines priority. The cyberspace range-operating Wing and individual ranges should schedule adequately to support each assigned user in the assigned event. The central authority for the ANG Cyber Range Squadron is NGB/A2/3/6/10CR, ANG Cyber Training, Range, and Exercises Branch.

3.1.3.3. Training Priority at Major Range and Test Facility Base (MRTFB) funded cyberspace ranges in accordance with DoDD 3200.11, *Major Range and Test Facility Base (MRTFB),* scheduling of the MRTFB is based upon a priority system that considers all DoD Components and accommodates DoD acquisition program priorities. The Test Resource Management Center implements the composition, sizing and usage for the MRTFB.

3.1.3.4. Cyberspace Range Test-Support Requirements. Test requirements are based on the characteristics and attributes of the specific test and are governed by departmental and service-level directives and instructions. MAJCOMs, Field Commands, Systems Program Office, Program Management Office, SAF/AQ, SAF/CN and AF/TE collaboratively define the test requirements and the resources necessary to support them.

3.1.4. Training and Test Resource Programs. Training and test requirements are funded through a combination of institutional funds and reimbursements and/or customer fees. Training and test resource funding is managed through Air Force and other DoD unique PEs. Execution is accomplished by various Air Force training and test activities. AF/TE provides T&E resource oversight and guidance to the AF MRTFB-funded range capabilities through the parent MAJCOM or Field Command. AF/A3T provides training resource oversight and guidance for all cyberspace ranges.

3.1.4.1. Aligning and Deconflicting Training and Test Requirements. Within the Department of the Air Force, the investments needed for training requirements may also be required for testing, and vice versa. MRTFB infrastructure investments are planned and allocated through different processes, PEs and special access programs. It is imperative to avoid redundancy and gain synergy by closely aligning and deconflicting test and training requirements; however, consideration must be made to adequately prioritize and adhere to the existing cyberspace range providers' business models for MRTFB funded cyberspace range assets.

3.1.4.1.1. Training O&M. ACC programs the funding of the Cyberspace Training PE (84762F) and the Support to Information Operations Capabilities PE (33166F). ACC will transition appropriate cyberspace range training funding and allocate the appropriate cyberspace range program codes in conjunction with the Operational Training Infrastructure Funding Strategy. **(T-1)** NGB A2/3/6/10 programs the funding of the ANG Cyber Range capability PE (53056F / 53151F).

3.1.4.1.2. Program Element 84762F funds the O&M and procurement budgets for the 318th Range Squadron's (RANS) Cyber Test and Training Range and Distributed Mission Operations Center (DMOC) Cyber (DMOC-C) and the 39th Information Operations Squadron's Initial Qualification Training (IQT) Training Range. These budgets support cyberspace range contracts, certain cyberspace range personnel, and O&M of cyberspace range capabilities. It also funds technical and service contracts to maintain operating hours and the basic infrastructure for environment development and design, technical management, data collection and analysis activities, threat and debrief systems, connectivity, data link capabilities and other cyberspace range services as determined by the cyberspace range governance boards and steering groups. Individual MAJCOMs execute funding in the PEs for their assigned ranges.

3.1.4.1.3. Program Element 33166F funds the O&M and procurement budgets for the JIOR. These budgets support cyberspace range contracts, certain cyberspace range personnel, and O&M of cyberspace range capabilities. Specifically, funding supports technical and service contracts to maintain 24/7/365 operations of Unclassified through Top Secret-Sensitive Compartment Information in a MILS transport network to conduct mission rehearsal, training, testing, concept development and experimentation in support of Information Operations, Electromagnetic Spectrum Warfare, Offensive

Cyber Operations, Defensive Cyber Operations, Space Operations, and Special Operations Forces mission areas in a realistic threat representative environment.

3.1.4.1.4. Program Element 53056F and PE 53151 fund the O&M and procurement budgets for the ANG Cyber Range Squadron. The program funds cyberspace range contracts, certain cyberspace range personnel, and O&M of cyberspace range capabilities. It also funds technical and service contracts to maintain basic infrastructure, threat systems, training content, connectivity and other range services.

3.1.4.2. Cyber Training and Test Environments. Training and test environment attributes accommodate missions based on tactics, techniques, and procedures and event requirements. When Cyberspace Range Operating Authorities/MAJCOMs/Field Commands project a unit readiness decline due to a deficiency or gap in cyberspace range capabilities, MAJCOMs and Field Commands should first attempt to shift the unit assignment to a cyberspace range with the required capability, or submit a T/TSNS to lead Command to document and address the shortfall.

3.1.4.3. Cyberspace Range Equipment, Personnel, and Infrastructure. Cyberspace range equipment and infrastructure provide numerous functions, including T&E, readiness training, tactics development and evaluation, command and control, and mission rehearsals. Ideally, these systems provide precise monitoring and reconstruction, and facilitate post-mission debriefing of cyberspace range and multi-domain audiences for various missions. The requirement for continuous modernization of these systems drives investments in this area.

3.1.4.4. Crew Training Space. The Cyberspace Range Operating Authority will provide a common use crew training facility for its assigned range. **(T-1)** The Operating Authority will manage common use crew training facilities at primary cyberspace ranges. **(T-2)** Cyberspace Operation Squadron will provide a crew training space that is connected to the Cyber Operations Squadron assigned range. **(T-2)** These will not be the exclusive crew training facilities. **(T-2)**

3.1.4.5. Test Equipment and Infrastructure. The Test Investment Planning and Programming Process (TIPP) provides the venue for investing in test infrastructure. Air Force Test Center, within AFMC, manages the AF TIPP process to identify test resource investments needed to support military systems testing. Investments that have possible multi-service applicability may be referred to the Central T&E Investment Program for funding.

Chapter 4

CYBERSPACE RANGE OPERATIONS AND CONNECTIVITY

4.1. Cyberspace Range Operations.

4.1.1. Cyberspace Range Operating Authority will ensure that range operations are conducted in accordance with this manual, DoDD 5101.19E, DoDI 8510.01, and DoDI 8540.01, *Cross Domain (CD) Policy*. **(T-0)**

4.2. Written Agreements.

4.2.1. AFI 25-201 details the required procedures for entering into written agreements. Range Operating Authorities should closely coordinate with ACC any time the range is agreeing to provide support to an unassigned range user and a written agreement is required. DoDD 3200.11 and AFI 99-103 address the written agreements and documentation for test support. Range Operating Authority will ensure that all written agreements are maintained in accordance with AFI 33-322. **(T-1)** Subject to classification restrictions, all agreements pertinent to their range should be readily available to range personnel and users.

4.2.1.1. Support Agreements. In accordance with AFI 25-201, Cyberspace Range Operating Authority must use the DD Form 1144, *Support Agreement*, to document recurring reimbursable support when the Air Force is the supplier or recipient, and the support exceeds the funded requirement. **(T-0)** The Range Operating Authority, in coordination with the lead agency, shall complete an inter-service support agreement when providing training support to any other DoD component, and interconnection security agreement and environment agreement as necessary. **(T-1)**

4.2.1.2. Cyberspace Range Operating Authority may entertain requests and discuss user requirements with any non-Air Force user, but the Range Operating Authority will coordinate and receive coordination from MAJCOMs prior to entering into any agreement for support of non-Air Force training events that require commitment of additional resources by range owner. **(T-2)**

4.2.1.3. Written support agreements are recommended, but not required for occasional or limited use or during Air Force-sponsored exercises, deployments, evaluations, or inspections. **(T-0)**

4.2.1.4. Memorandum of Understanding. Ensure memorandums of understanding involving other nations are reviewed by the lead agency Office of the Staff Judge Advocate and the State Department mission in the host country for legal implications. **(T-0)** See DoDI 5530.03, *International Agreements* and AFI 51-403, *International Agreements*, for agreement procedures, content, and format requirements.

4.2.1.5. Memorandum of Agreement. Ensure the lead agency Office of the Staff Judge Advocate and Financial Management, and the State Department Mission in the host country for legal and financial implications review memorandums of agreement involving other nations. **(T-0)** See DoDI 5530.03 and AFI 51-403, for agreement procedures, content, and format requirements.

4.2.1.6. Written Agreements for T&E Activities. AFI 99-103 details the processes required for T&E activities. Ranges may enter into written agreements via formal documentation and coordination at the Range Operating Authority level.

4.2.2. Foreign User Training Support Agreements. Allies will submit written requests for cyberspace range support through the Cyberspace Range Operating Authority to appropriate country offices within SAF/IA to AF/A3TI. **(T-1)** AF/A3TI will coordinate with the appropriate range squadron to determine the level of support and to integrate the support requirement into the cyberspace range mission. The lead agency will then task the Cyberspace Range Operating Authority to develop the agreement resulting in a memorandum of understanding or memorandum of agreement between the cyberspace range and appropriate foreign authority.

4.2.2.1. These agreements may also include specific letters of agreement, Host-Tenant Support Agreements, and other support agreements. Each signatory ensures that these agreements meet the needs of the organization without compromising the mission and obligating the organization beyond its intent or authority and are consistent with any applicable international agreements with the host nation. Cyberspace Range Operating Authorities will coordinate the draft agreement with the lead agency Office of the Staff Judge Advocate. **(T-1)**

4.2.2.2. If a conflict arises regarding one of these agreements, the Cyberspace Range Operating Authority should resolve the issue at the appropriate level.

4.3. Connectivity.

4.3.1. Distributed operations should be used to maximize value to the cyber test and training audience.

4.3.2. Cyberspace ranges require access to a variety of connectivity methods to enable integration with complimentary capabilities and services, such as PCTE and access to other cyberspace range providers to support operations and user requirements. Connectivity methods include, but are not limited to, JIOR, JMN, Defense Research and Engineering Network, and commercial Internet.

4.3.3. Cyberspace ranges that require connectivity via a commercial Internet Service Provider (ISP) must first submit an ISP waiver request and brief to Defense Information Systems Network Services utilizing the on-line Systems / Networks Approval Process (SNAP) Database at **https://snap.dod.mil**. **(T-0)** The Defense Security/Cybersecurity Authorization Working Group, Defense Information Systems Agency Service Manager and the Office of the Secretary of Defense Global Information Grid Waiver Panel will review the waiver request package prior to granting a decision. The nominating point of contact will be responsible for submitting the package via SNAP and attending any follow-on Panel meetings as the package is being coordinated. **(T-0)**

4.3.4. Cyberspace ranges should have the ability to utilize a cross domain solution that aligns with Air Force, joint policy, and service-level established security classification guidance. The cross-domain solution should provide the ability to test and train across weapons systems, domains, and services. The solution should also pass unchanged data, protect data from compromise, as well as maintain performance, capability, and additional critical elements required to foster integrated testing and training.

Chapter 5

JOINT REQUIREMENTS

5.1. Joint Cyberspace Range Environment.

5.1.1. Cyberspace is inherently a joint effort and requires joint and/or interagency coordination and integrated capabilities to enable training across a full range of military operations. *The Joint Training Technical Interoperability Strategy* promotes a collaborative coordination effort among stakeholders. The Strategy is intended to achieve a technical interoperability standard to prepare forces for Globally Integrated Operations. Joint Staff J7 is the OPR for the strategy and a full report can be obtained on the Defense Technical Information Center website at **https://apps.dtic.mil/dtic/tr/fulltext/u2/1057364.pdf**

5.1.1.1. DoD Executive Agents for the Cyber Test and Training Ranges. DoDD 5101.19E designated the DoD Executive Agents for the Cyber Test and Training Ranges. Each organization is designated DoD-wide responsibilities for planning, integrating activities and establishing joint and common requirements across the designated cyberspace test and training ranges in addition to the aligned capability infrastructures. DoDD 5101.19E designates the following:

5.1.1.2. Director, TRMC as the DoD Executive Agent (EA) for Cyber Test Ranges.

5.1.1.3. Secretary of the Army as the DoD Executive Agent for Cyber Training Ranges.

5.1.2. PCTE. Secretary of the Army is tasked to develop a material solution in support of USCYBERCOM.

5.1.2.1. The Secretary of the Army has established the governance structure outlined in the PCTE Executive Board (EB) Charter and echoed in this section. The AF supports this governance model. The governance construct consists of the following DoD-level PCTE forums.

5.1.2.1.1. The PCTE EB is a 3-Star General Officer (GO)/Flag Officer (FO)/ Senior Executive Service (SES) decision group. The meetings are scheduled as directed by the PCTE EB or requested by the PCTE General Officer Steering Committee (GOSC) co-chairs. AF/A3 represents the DAF [in coordination with the Air Force Reserve (AFRES) and Air National Guard (ANG)] and 16th Air Force/Air Forces Cyber (16 AF/AFCYBER) represents the Service Cyber Component (SCC).

5.1.2.1.2. The PCTE GOSC is a 1-2 Star GO/FO/SES decision and information meeting that convenes the last month of each quarter or as directed by co-chairs. AF/A3T represents the DAF (in coordination with the AFRES and ANG) and 16 AF/AFCYBER represents the SCC.

5.1.2.1.3. The PCTE Council of Colonels (CoC) is an O6/GS-15 decision and informational meeting that convenes the second Wednesday of each month or as directed by co-chairs. AF/A3TI represents the DAF (in coordination with the AFRES and ANG) and 16 AF/AFCYBER represents the SCC.

5.1.2.1.4. AF/A3TI, ACC/A326K, and 16 AF/J37/8 will charter and co-chair a DAF-level action officer working group to analyze and coordinate DAF equities in PCTE,

develop DAF requirements (features and capabilities) and solutions for PCTE, as well as advise the DAF principal representatives on DAF requirements and related matters prior to scheduled and unscheduled PCTE EB, GOSC, and CoC meetings.

5.1.2.1.5. Roles and Responsibilities. DAF and SCC representatives and action officers will support the PCTE GOSC, CoC, and other related activities IAW the roles and responsibilities laid out in the current PCTE EB Charter.

5.1.3. In order to adequately account for emerging joint requirements, all cyberspace ranges will provide the following:

5.1.3.1. Integration into Joint cyberspace range operations. **(T-1)**

5.1.3.2. Support content creation for Cyber Mission Forces. **(T-2)**

5.1.3.3. Content metadata based on joint standards at all classifications of content. **(T-2)**

5.1.3.4. Centralized management of locally developed content. **(T-2)**

5.1.3.5. Support to USCYBERCOM's PCTE and JCTE. **(T-1)**

Chapter 6

GOVERNANCE

6.1. Cyberspace Range Governance.

6.1.1. The Operational Training and Test Infrastructure (OTTI) Cross-functional Team (CFT) is an AF/A3T-led group consisted of Headquarters Air Force, MAJCOM staffs, and select subordinate organizations to explore and provide solutions to the Air Force's toughest OTTI problems and bring those solutions to bear. The purpose of the CFT is to affect the policy, strategy, capability planning, programming, sustainment and resourcing of cyberspace OTTI. The OTTI CFT will:

6.1.2. Develop overall cyberspace OTTI strategy/concept and component concepts.

6.1.3. Develop the Cyberspace OTTI Capability and Systems Development Plans (CDP/SDP) to enable senior leaders to make informed and effective policy, strategic or resourcing decisions in support of cyberspace ranges.

6.1.4. Execute approved CDPs and SDPs by engaging external elements to pursue corporate funding and required acquisition efforts and documentation (Capability-based Assessments, Analyses of Alternatives, etc.).

6.2. ACC.

6.2.1. ACC, in coordination with their respective program offices and other MAJCOMs, will establish standards management processes for the cyberspace ranges. **(T-1)** This includes establishing governance bodies that will interface with the enterprise level governance structure. The Cyberspace Range Steering Group will:

6.2.2. Establish an OTTI and Test Enterprise Working Group composed of AF/A3T, AF/TE, MAJCOM and program office representatives from the Cyberspace Range Steering Group. **(T-2)**

6.2.3. Establish a governance body and create a charter that includes cyberspace range stakeholders. **(T-1)**

6.2.4. Provide the forum to address cyberspace range issues. **(T-2)**

6.2.5. Create and manage processes for identification of test and training requirements. **(T-1)**

6.2.6. Determine and manage resourcing of test and training range requirements. **(T-1)**

6.2.7. Provide cyberspace range requirements to the OTTI CFT. **(T-1)**

Chapter 7

CYBERSPACE RANGE MULTI-DOMAIN INTEGRATION

7.1. Training System Multi-domain Integration.

7.1.1. The Air Force Future Operating Concept describes an environment in 2035 in which "integrated multi-domain operations will encompass full interoperability among air, space, and cyberspace capabilities." If the ability to act in one domain becomes limited, Air Force and joint forces will outpace the enemy by rapidly shifting to operations in other domains to accomplish the required tasks and objectives.

7.1.2. ACC and cyberspace ranges will work with the DMOC-C and the Air National Guard Cyberspace Range Squadron to develop LVC cyberspace range and simulator capability to enable full-spectrum battlespace in Service, Joint, and coalition operations. **(T-1)**

7.1.3. ACC will resource and prioritize multi-domain training system integration efforts with live and synthetic training systems such as, but not limited to, the Virtual Test and Training Center, Nevada Test and Training Range, Live Mission Operations Capability, Joint Pacific Alaska Range Complex and DMOC-Space (Reference **Figure A8.1**). **(T-1)**

7.2. DMOC-C.

7.2.1. Provides LVC environments for mission rehearsal, concept exploration, and capability assessments. The DMOC-C is officially designated to support major exercises with M&S tools for realistic training to satisfy operational learning objectives.

7.2.2. DMOC-C will quickly adapt to the various changes in policy, guidance, operational environmental changes with minimal cost as it incorporates Government off the Shelf products with existing contractors. Additionally, it will make extensive use of JIOR nodes worldwide. **(T-2)**

7.2.3. The DMOC-C currently consists of the Operational Level Constructive Environment, the Tactical Level AFNet and Exercise Operations Environments, control system capabilities with hardware-in-the-loop, Integrated Air Defense simulated and constructive injects and two anechoic chambers for radio frequency integration. (Reference **Figure A8.2** DMOC-C Multi-domain Training System Integration.)

7.3. ANG Cyber Range Squadron (RANS). The ANG Cyber RANS will provide the cyber component with persistent Distributed Mission Operations (DMO) capability and expertise in support of realistic, relevant training opportunities for Cyber Mission Forces (CMF) in a networked environment. **(T-2)** The ANG Cyber RANS will integrate the distributed ANG Virtual Integrated Training Environment (VITE) capabilities, cyber ranges and simulators into a regional data control center which will provide centralized management capabilities, system standardization, and a common architecture. At the same time, the center will maintain decentralized operational capability needed to cater to the unique scheduling constraints of the Reserve force (48 regularly scheduled drills/rescheduled drills and 15 annual training days).

The ANG Cyber RANS will utilize the Joint Information Operations Range (JIOR), commercial internet, and/or DoD Information Network (DoDIN) networks to provide access to directed cyber training platforms and_environments that meet Combat Mission Ready (CMR) requirements for the Reserve Component's Cyber Warfighter. (Reference **Figure A8.3**) **(T-2)**

JOSEPH T. GUASTELLA, Lt Gen, USAF
Deputy Chief of Staff for Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 10 United States Code (USC), Section 392, *Executive agents for cyber test and training ranges*

DoDD 5101.19E, *DoD Executive Agents for the Cyber Test and Cyber Training Ranges,* 24 August 2018

DoDD 3200.11, *Major Range and Test Facility Base (MRTFB),* 27 December 2007

DoDI 5530.03, *International Agreements,* 4 December 2019

DoDI 1100.22, *Policy and Procedures for Determining Workforce Mix,* 12 April 2010

DoDI 8500.01, *Cybersecurity,* 14 March 2014

DoDI 8540.01, *Cross Domain (CD) Policy,* 8 May 2015

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT),* 12 March 2014

AFPD 13-2, *Air Traffic, Airfield, Airspace, and Range Management,* 3 January 2019

AFPD 16-7, *Special Access Programs,* 21 November 2017

AFPD 16-10, *Modeling and Simulation,* 23 January 2015

AFI 16-701, *Management, Administration, and Oversight of Special Access Programs,* 18 February 2014

AFI 16-1007, *Management of Air Force Operational Training Systems,* 1 October 2019

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT),* 6 February 2020

AFI 17-130, *Cybersecurity Program Management,* 13 February 2020

AFI 17-220, *Spectrum Management,* 16 March 2017

AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures,* 18 October 2013

AFI 33-360, *Publications and Forms Management,* 1 December 2015

AFI 38-101, *Air Force Organization,* 29 August 2019

AFI 51-403, *International Agreements,* 8 February 2019

AFI 63-101/20-101, *Integrated Life Cycle Management,* 30 June 2020

AFI 99-103, *Capabilities-Based Test and Evaluation,* 17 December 2020

AFI 33-322, *Records Management and Information Governance Program,* 23 March 2020

DAFI 33-360, Publication and Forms Management, 7 Aug 20

HAFMD 1-54, *Deputy Chief of Staff, Operations, Plans & Requirements,* 8 September 2015

Department of the Air Force Strategic Plan for Control Systems, March 2021

ACC Enterprise Range Plan, 15 August 2017

https://usaf.dps.mil/sites/ACC-A3/A3A/A3AR

Joint Training Technical Interoperability Strategy, 27 July 2018
https://apps.dtic.mil/dtic/tr/fulltext/u2/1057364.pdf

Operational Training Infrastructure Flight Plan, 5 September 2017
https://org2.eis.af.mil/sites/12594/A3T/I/SharedDocuments/Forms/AllItems.aspx

USAF Strategic Master Plan, May 2015
https://www.af.mil/Portals/1/documents/Force%20Management/Strategic_Master_Plan.pdf

Prescribed Forms

None

Adopted Forms

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

AF Form 847, Recommendation for Change of Publication

DD Form 1144, Support Agreement

Abbreviations and Acronyms

ACC—Air Combat Command

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

ANG—Air National Guard

CDP—Capability Development Plan

CFT—Cross-functional Team

CSE—Center Scheduling Enterprise

DAF—Department of the Air Force

DMOC—Distributed Missions Operation Center

DMOC-C—Distributed Mission Operations Center-Cyber

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DT—Distributed Training

DTC—Distributed Training Center

IOS—Information Operations Squadron

ISP—Internet Service Provider

IT—Information Technology

JCTE—Joint Cyber Training Enterprise

JIOR—Joint Information Operations Range

JMETC—Joint Mission Environment Test Capability

JMN—Joint Mission Environment Test Capability (JMETC) MILS Network

LVC—Live, Virtual, and Constructive

M&S—Modeling and Simulation

MAJCOM—Major Command

MILS—Multiple Independent Levels of Security

MRTFB—Major Range and Test Facility Base

O&M—Operation and Maintenance

OPR—Office of Primary Responsibility

OTTI—Operational Training and Test Infrastructure

PCTE—Persistent Cyber Training Environment

PE—Program Element

PEM—Program Element Monitor

RANS—Range Squadron

RMF—Risk Management Framework

SNAP—Systems / Networks Approval Process

T&E—Test and Evaluation

T/TSNS—Test/Training Space Needs Statement

TEMP—Test and Evaluation Master Plan

TRMC—Test Resource Management Center

TS—Test Squadron

USCYBERCOM—United States Cyber Command

Terms

Aligned capability infrastructure—Cyberspace ranges, test facilities, test beds, and other means of testing, training, and developing DoD and non-DoD software, personnel, and tools. Aligned

capabilities are those in which the DoD EA for Cyber Test Ranges has invested or which are compliant with the EAs' established architectures and standards.

Architecture—The reference structure of operational training components, their relationships, and the principles and guidelines governing their design and evolution over time.

Authoritative Data Source—The point at which information is first captured as data. The most current, reliable, highest-quality data that captures the information. The authoritative data source is designated by the owner of the subject information. A recognized or official data production source with a designated mission statement or source/product to publish reliable and accurate data for subsequent use by customers. An authoritative data source may be the functional combination of multiple, separate data sources.

Capability—A specific resource, such as hardware, software, instrumentation, infrastructure elements, tools, processes, facilities, and workforces that can be integrated with other capabilities to constitute an event environment.

Central Authority—Office within the lead MAJCOM that collects requirements, advocates for funding at higher headquarters, and monitors usage and availability of all DAF cyberspace ranges.

Crew Training—Those activities which ensure all cybercrew members obtain and maintain the certification/qualification and proficiency needed to effectively perform their unit's mission

Constructive environment—Computer generated entities, weapons, systems used to enhance the live or virtual training environment.

Cyberspace range—An event environment that supports cyber effects on information technology; weapons; command, control, communications, computers, intelligence, surveillance, and reconnaissance; and other network-enabled technologies for the purpose of experimentation, testing, training, or exercising on a real or simulated network. It includes hardware, software, and connectivity; test facilities; test beds; tailored scenarios; other means and resources for testing, training, and developing software; personnel; and tools for accommodating the DoD. A range can be a single facility or a federation of capabilities that provides a complete, realistic mission environment for the system under test or to meet the training objectives. A range is designed to be persistent and support various events over its lifetime. Cyberspace ranges can also support the development of new cyber technology. "Cyberspace range" is synonymous with the term "cyber and information technology range" as used in 10 USC § 392.

Cyber Testing—The testing of systems and sub-systems that operate in the cyberspace domain, and the access pathways to such systems that are part of DoD weapon systems. Cyber testing includes cybersecurity testing (with associated RMF processes) and cyber resiliency testing.

Cybersecurity—Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (DoDI 8500.01, *Cybersecurity*).

Cybersecurity Testing—The testing of the systems' and sub-systems' ability to protect or defend against a cyber attack. Cybersecurity testing focuses on identifying and eliminating or mitigating system cyber vulnerabilities. It is scoped through assessing a system's cyber boundary and risk to mission assurance. Risk analysis, at a minimum, should consider the threat and threat severity,

the likelihood of attack, and system vulnerabilities. Cybersecurity is evaluated based on the Security Assessment Plan, Program Protection Plan, Information Support Plan, and RMF artifacts.

Distributed Training (DT)—DT is shared training that includes LVC simulations. DT allows warfighters to train individually or collectively at all levels of war. This combination of live, virtual, and constructive environments provides on-demand, realistic training opportunities for warfighters by overcoming many current constraints that limit training effectiveness.

Event—A planned, controlled, and scheduled set of activities conducted on a cyberspace range to meet specific goals, objectives, or requirements. Events include, but are not limited to, experimentation; T&E science and technology, research and development, developmental T&E, and operational T&E); tactics, techniques, and procedures development; concept of operations development; demonstration; exercise; training; or mission rehearsal.

Event environment—The combination of representative operational environment elements, including systems under test, emulations and simulations, and related tools that satisfy the requirements of a specific event.

Infrastructure—The facilities, ranges, and all other physical assets used to support cyber events.

Interconnection Security Agreement—A detailed security document that defines the protocols, timing, and responsibilities of connecting a cyberspace range, a sponsor network, other ranges, or commercial entities to identify and mitigate any risks associated with an environment.

Interoperability—The ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces, and to use the data, information, materiel, and services exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with cybersecurity (formerly Information Assurance).

Lead Major Command—As defined in AFI 38-101, *Air Force Organization*, a lead MAJCOM consolidates responsibilities for a particular function in a single MAJCOM, supporting the entire Department of the Air Force as applicable.

Modeling and Simulation (M&S)—The use of models, including emulators, prototypes, simulators, and stimulators, either statically or over time, to develop data as a basis for making managerial or technical decisions. The terms "modeling" and "simulation" are often used interchangeably.

Operational Training Infrastructure (OTI)—The framework and resources essential to accomplishing Air Force Operational Training objectives.

Operator—Refers to the operating command which is the primary command operating a system, subsystem, or item of equipment. Generally applies to those operational commands or organizations designated by Headquarters, US Air Force to conduct or participate in operations or operational testing, interchangeable with the term "using command" or “user.” In other forums the term “warfighter” or “customer” is often used. “User” is the preferred term in this manual.

Oversight—Senior executive-level monitoring and review of programs to ensure compliance with policy and attainment of broad program goals.

Primary Range Providers—Cyberspace range organizations designated to create synergy between cyberspace operational unit test and training requirements with cyberspace range resources to accommodate training and/or test activities.

Resources—A collective term that encompasses the infrastructure, workforce, and funding resulting in a capability.

Simulator—A training device that permits development and practice of the necessary skills for accomplishing operational tasks, to a prescribed standard of competency, in a specific prime mission system and duty position. A simulator can be connected to a cyberspace range to provide test and training.

Standards—Authoritative data sources and enterprise technical standards increase efficiency and enable improved integration of various systems during operational training events.

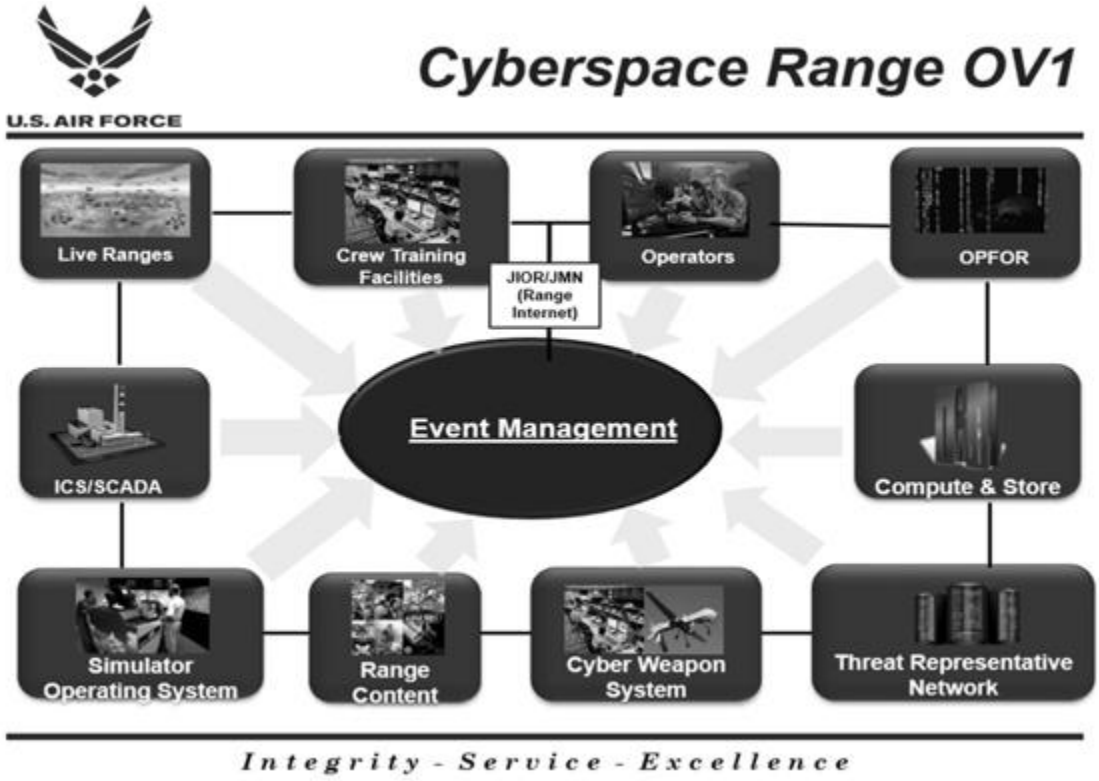
Synthetic environment—The integrated set of data elements that define the environment within which a given simulation application operates. The data elements include information about the initial and subsequent states of the terrain including cultural features, and atmospheric and oceanographic environments throughout an exercise. The data elements include databases of externally observable information about instantiable entities, and are adequately correlated for the type of exercise to be performed.

Virtual environment—The infrastructure in which real assets and/or operators interact with simulated or emulated systems of any kind.

Attachment 2

CYBERSPACE RANGE OVERVIEW

Figure A2.1. Cyberspace Range Overview.



Attachment 3

AIR FORCE PRIMARY CYBERSAPCE RANGES OPERATED AND GOVERNED BY THIS MANUAL

Description: The "Owner" column in the tables contained in this attachment is intended to reflect the entity with real property accountability for the cyberspace range infrastructure.

Table A3.1. Air Force Primary Cyberspace Range Providers.

Range	Provider	Location(s)	Owner
Cyber Test and Training Range	318th Range Squadron (RANS)	Joint Base San Antonio - Lackland, Texas	ACC
Distributed Mission Operations Center (DMOC) - Cyber	318 RANS	Joint Base San Antonio - Lackland, Texas	ACC
Joint Information Operations Range	318th Cyberspace Operations Group, Operating Location B	Naval Station Norfolk, Virginia	ACC
ANG Cyber Range	ANG Cyber RANS	Des Moines ANGB, Iowa	ANG
Cyber Training Range Environment	39th Information Operations Squadron	Hurlburt Field, Florida and Joint Base San Antonio - Lackland, Texas	ACC
***** Cyberspace Test Range	47th Cyber Test Squadron	Joint Base San Antonio - Lackland, Texas,	AFMC
Note: The Cyberspace Test range located at Lackland AFB Texas, is a Development Test and Evaluation Range (DT&E). As such, when conducting these DT&E activities, will follow procedures outlined in paragraph 2.10 of this DAFMAN as well as AFMC supplements and local procedures as prescribed.			

Attachment 4

JOINT CYBERSPACE RANGE CAPABILITIES

Table A4.1. Air Force Cyberspace Range Capability Matrix.

		AIR FORCE CYBERSPACE RANGES																			
Owner																					
Air Force	Cyber Test Training Range	L-V-Lg	V - Lg	L-V-Lg	V-M		V-M	V-M		X	X	U-SAR	X			X	X		La-BP-S		X	318th Range Squadron San Antonio, TX
Air Force	Cyber Test Range						V-M	V-M		X	X	TS-SAR/SCI	X			X		X	La-BP	X	X	47th Cyberspace Test Squadron San Antonio, TX
ANG	ANG Cyber RANS	L-V-Sm-Pt	L-V-Sm-Pt	L-V-Sm-Pt	V-Sm				X	X									X	X	X	168 Cyberspace Operations Squadron 3100 McKinley Ave, Des Moines, Iowa 50321
Air Force	Distributed Mission Ops Center - Cyber	L-V-C		L-V		L-V-C	L-V-C	Pt	Pt	X		S-SCI			X			X	La-BP			318th Range Squadron San Antonio, TX
Air Force	Cyber Training Range Environment	L-V-C Lg	L-V-C Lg	V-M						X		U (S-TS/SCI Future)	X					X	X		X	39th Information Operations Squadron Hurlburt Field, FL; San Antonio, TX; Keesler AFB, MS
Air Force	Joint Information Operations Range									X		TS-SAR/SCI	X			X						Naval Station Norfolk, VA + Global

L = Live	Sm = Small (< 500 devices)
V = Virtual	M = Medium (501-3000 devices)
C = Constructive	Lg = Large (> 3000 devices)
SAR = Special Access Rqd	Pt = Partial Capability
La = Lariat	BP = Breaking Point
S = Spirent	

Table A4.2. Air Force Multi-Domain Range Capability Matrix.

		Capability Providers	Blue General Purpose	Red General Purpose	Gray General Purpose	Control Systems	Blue Battlefield Systems	Red Battlefield Systems	Telephony/ Commercial	Mobile	OPFOR	JCOR Connectivity	JMN Connectivity	Class. Level - SAR Environ.	Environment Planning/Integration	CNAP	Cyber Mission Event C2 & Mgmt	Instrumentation	Automated Configuration/Reconfiguration	Traffic Gen/Injection	Analysis Support	Archival/Playback	Location
		AIR FORCE CYBERSPACE RANGES																					
Owner																							
Air Force	AF CRC		L-V-M	L-V-M			X	X				S-SAR					X		BP				
Air Force	AF Cap Int. Environ																						
Air Force	AF Cyb Exp Environ	V-SM	V-SM									S, TS					X	X	La	X		525 Brooks Road, Rome, NY 13441
Air Force	AF Nellis Test Training Range					X	X	X		X		U-SAR										P.O Box 871 Tonapah, NV 89049
Space Force	USSF Space Test and Training Range									X		U-SAR										Schriever AFB, CO
Air Force	AF Distributed Mission Operations Center									X												4500 Aberdeen Dr. SE, Kirtland AFB, NM,

L = Live	Sm = Small (< 500 devices)
V = Virtual	M = Medium (501-3000 devices)
C = Constructive	Lg = Large (> 3000 devices)
SAR = Special Access Rqd	Pt = Partial Capability
La = Lariat	BP = Breaking Point
S = Spirent	

Table A4.3. Joint Cyberspace Range Capability Matrix.

Owner	Capability Providers	Blue General Purpose	Red General Purpose	Gray General Purpose	Control Systems	Blue Battlefield Systems	Red Battlefield Systems	Telephony/Commercial Mobile	OPFOR	JEOR Connectivity	JMN Connectivity	Class. Level - SAR Environ.	Environment Planning/ Integration	CIKR	Cyber Mod & Sim	Event C2 & Mgmt	Instrumentation	Automated Configuration/Restoration	Traffic Gen/ Injection	Analysis Support Archival/Retrieval	Location
		JOINT RANGES																			
Joint	CS Assessment Division					V-M	V-M		X	X	U-S	X			X		X	La-BP	X	X	Joint Staff, Suffolk, VA
DoD	National Cyber Range (NCR)	V-Lg	V-Lg	V-Lg			Pt		X		S-SAR	X			X	X	Pt	La-BP	X	X	Orlando, FL
Army	Army EPG									X											
Army	Army Cyber BL								IP												Ft. Gordon
Army	Army I2WD		L-V-Lg	L-V-Lg				L-V-M	X		U-SAR				X	X	X	La-BP	Pt		
Army	Army CTSF									X											53rd St, Fort Hood, TX 76544
Army	BMC NIEs (Ft Bliss)	L-S		L-S		L-Pt	L-Pt*		Pt *	X	U-SCI	X			X				X		fort Bliss, TX
Navy	PACOM CWIC								X				X								Camp Smith, HI
Army	Army TSMO APTN																				Redstone Arsenal, AL
Navy	NCWDG ITF DART																				Suitland, MD
Navy	NCDOC HBSS																				Suffolk, VA
Navy	SPAWAR-PAC								X	X			X								
Navy	USS Secure				V-Pt				X												
Marines	AZ Cyber Warfare	V-M																			5115 N 27th Ave, Building 66, Phoenix, AZ 85017
Army	MI Cyber Range	V-M																			1000 Oakbrook Drive, Suite 200, Ann Arbor, Michigan 48104

L = Live	Sm = Small (< 500 devices)
V = Virtual	M = Medium (501-3000 devices)
C = Constructive	Lg = Large (> 3000 devices)
SAR = Special Access Rqd	Pt = Partial Capability
La = Lariat	BP = Breaking Point
S = Spirent	

Table A4.4. Industry Range Capability Matrix.

Owner	Capability Providers	Blue General Purpose	Red General Purpose	Gray General Purpose	Control Systems	Blue Battlefield Systems	Red Battlefield Systems	Telephony/Commercial Mobile	OPFOR	JEOR Connectivity	JMN Connectivity	Class. Level - SAR Environ.	Environment Planning/ Integration	CIKR	Cyber Mod & Sim	Event C2 & Mgmt	Instrumentation	Automated Configuration/Restoration	Traffic Gen/ Injection	Analysis Support Archival/Retrieval	Location
		INDUSTRY RANGES																			
Industry	SANS Institute	V-M			LC						U		X								600 E. Market Street San Antonio, TX 78205/ Bethesda, Md
Industry	FireEye Partners	V-M																			
Industry	Idaho NL				L-V			L-V		X			X		X	X		X	X		2525 Fremont Ave, Idaho Falls, ID 83402
Industry	Pacific NW NL				V				Pt	X	U-SCI		X					X			902 Battelle Blvd, Richland, WA 99354
Industry	Sandia NL	V-M	V-M	V-M	V			V	Pt	X	U-SCI		X	X		X		La	X	X	1515 Eubank Blvd SE, Albuquerque, NM 87123
Industry	Sandia NL																				7011 East Ave, Livermore, CA 94550
Industry	MIT/LL	V-M		V-M		V-Pt				X								La			244 Wood St, Lexington, MA 02421
Industry	JHU/APL									X						X				X	11100 Johns Hopkins Road, Laurel, Maryland 20723
Industry	GTRI		V-S						X		X			X							400 10th St NW, Atlanta, GA 30318
Industry	New Mexico Tech - Playas Training and Research Center									X		X			X	X					801 Leroy Pl. Socorro, NM 87801
Industry	Cybertropolis				L-Pt*																4230 E Administration Dr, Butlerville, IN 47223

L = Live	Sm = Small (< 500 devices)
V = Virtual	M = Medium (501-3000 devices)
C = Constructive	Lg = Large (> 3000 devices)
SAR = Special Access Rqd	Pt = Partial Capability
La = Lariat	BP = Breaking Point
S = Spirent	

Table A4.5. Other Cyberspace Range and Transport Capability Matrix.

Owner	Capability Providers	Blue General Purpose	Red General Purpose	Gray General Purpose	Control Systems	Blue Battlefield Systems	Red Battlefield Systems	Telephony/Commercial Mobile	OPFOR	JIOR Connectivity	JMN Connectivity	Class. Level - SAR Environ.	Environment Planning/ Integration	CIXR	Cyber Mod & Sim	Event C2 & Mgmt	Instrumentation	Automated Configuration/Restoration	Traffic Gen/ Injection	Analysis Support	Archival/Retrieval	Location
OTHER CONNECTED RANGES AND TRANSPORT																						
Joint	JMETC MILS Network									X	S											Worlwide JMETC SECRET Network (JSN)
Industry	Hanscom Collab & Innovation Ctr																					Hanscom AFB MA
Air Force	412 TENG/ENI																					Edwards AFB
	Port Hueneme																					Port Hueneme
Air Force	CYBERCOM STEP	V-Lg	V-Lg	V-Lg					X													

L = Live	Sm = Small (< 500 devices)
V = Virtual	M = Medium (501-3000 devices)
C = Constructive	Lg = Large (> 3000 devices)
SAR = Special Access Rqd	Pt = Partial Capability
La = Lariat	BP = Breaking Point
S = Spirent	

Table A4.6. DOD Cyber Red Team Capability Matrix.

Owner	Capability Providers	Blue General Purpose	Red General Purpose	Gray General Purpose	Control Systems	Blue Battlefield Systems	Red Battlefield Systems	Telephony/Commercial Mobile	OPFOR	JIOR Connectivity	JMN Connectivity	Class. Level - SAR Environ.	Environment Planning/ Integration	CIXR	Cyber Mod & Sim	Event C2 & Mgmt	Instrumentation	Automated Configuration/Restoration	Traffic Gen/ Injection	Analysis Support	Archival/Retrieval	Location
DOD CYBER RED TEAMS																						
Marines	TRMC RSDPs	V-Lg	V-Lg																			
Joint	DISA Red Team		L					X														
Army	TSMO Red Team		L					X	X													Redstone Arsenal, AL
Marines	USMC IA Red Team		L					X														Code Talkers Hall, 27410 Hot Patch Rd, Quantico, VA 22134
Navy	Navy Red Team		L					X														
Navy	SPAWAR Red Team		L					X														4301 Pacific Highway, San Diego, CA 92110
Army	1st IO Command		L					X	X													8825 Beulah Street,Fort Belvoir, VA
Air Force	57 IAS		L					X	X													Nellis AFB, NV
ANG	177 IAS		L					X	X													McConnell AFB, KS
Joint	NSA Red Team		L					X	X													NSA, Fort Meade, MD

L = Live	Sm = Small (< 500 devices)
V = Virtual	M = Medium (501-3000 devices)
C = Constructive	Lg = Large (> 3000 devices)
SAR = Special Access Rqd	Pt = Partial Capability
La = Lariat	BP = Breaking Point
S = Spirent	

Attachment 5

UNIT TRAINING RANGE ASSIGNMENTS

Table A5.1. Assigned Training Range Users.

Cyber Range Assignments			
WG	Unit	Location	Cyber Primary Range Provider (PRP)
Regular Air Force			
67 CW	39 IOS	Florida	39 IOS
67 CW	DCO FTU	Florida	
67 CW	CS&D FTU	Mississippi	
67 CW	39 IOS (Det 1)	Texas	
67 CW	DCO FTU	Texas	
67 CW	833 COS	Texas	318 RANS
67 CW	834 COS	Texas	
67 CW	835 COS	Illinois	
67 CW	836 COS	Texas	
67 CW	837 COS	Illinois	
67 CW	91 COS	Texas	
67 CW	92 COS	Texas	
67 CW	390 COS	Texas	
67 CW	90 COS	Texas	
67 CW	352 COS	Hawaii	
67 CW	315 COS	Maryland	
67 CW	315 COS (Det 3)	Georgia	
67 CW	318 COG (Det 1)	Maryland	
67 CW	318 COG (Det 2)	Nevada	
67 CW	67 OSS	Texas	
688 CW	688 OSS	Texas	
688 CW	26 NOS	Texas	
688 CW	33 NWS	Texas	
688 CW	68 NWS	Texas	
688 CW	690 NSS	Texas	
688 CW	83 NOS	Virginia	
688 CW	561 NOS	Colorado	
688 CW	690 COS	Hawaii	
688 CW	691 COS	Germany	
688 CW	38 OSS	Oklahoma	
688 CW	38 ES	Oklahoma	
688 CW	38 CONS	Oklahoma	
688 CW	38 CyRS	Illinois	
688 CW	85 EIS	Mississippi	
688 CW	5 CBCSS	Georgia	
688 CW	51 CBCS	Georgia	
688 CW	52 CBCS	Georgia	

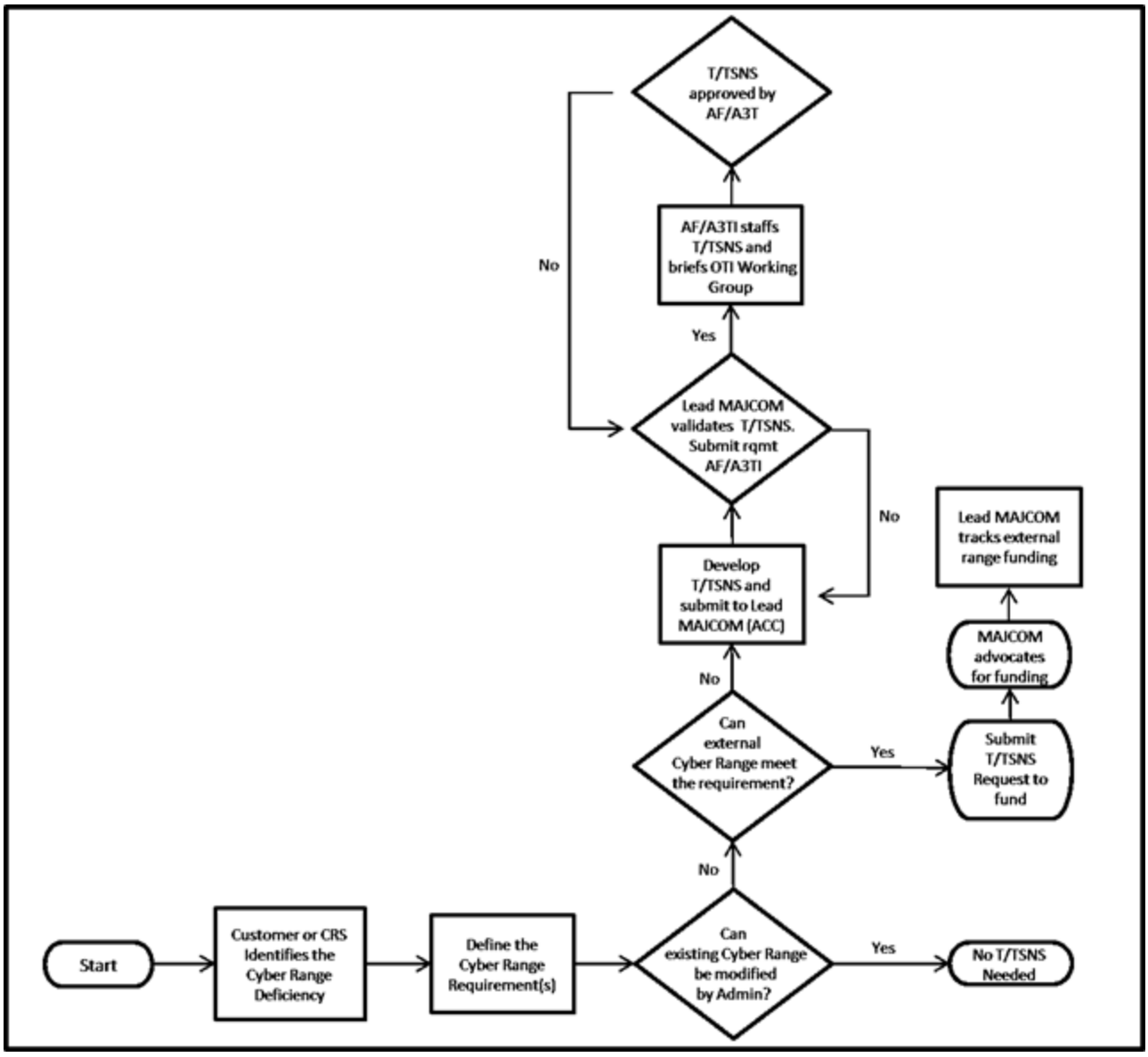
Cyber Range Assignments			
WG	Unit	Location	Cyber Primary Range Provider (PRP)
Air Force Reserve			
960 CW	717 IOS	Florida	39 IOS
960 CW	689 NOS	Alabama	318 RANS
960 CW	42 COS	Illinois	
960 CW	52 NWS	Nebraska	
960 CW	51 NOS	Virginia	
960 CW	53 NOS	Colorado	
960 CW	710 NOS	Georgia	
960 CW	426 NWS	Texas	
960 CW	50 NWS	Texas	
960 CW	854 COS	Texas	
Air National Guard			
134 ARW	119 COS	Tennessee	ANG-RANS
189 AW	223 COS	Arkansas	
175 WG	175 COS	Maryland	
175 WG	275 COS	Maryland	
175 WG	276 COS	Maryland	
166 AW	166 COS	Delaware	
194 WG	262 COS	Washington	
194 WG	143 COS	Washington	
132 WG	168 COS	Iowa	
149 FW	273 COS	Texas	
110 AW	272 COS	Michigan	
124 FW	224 COS	Idaho	
195 WG	261 COS	California	
184 IW	127 COS	Kansas	
	177 IAS	Kansas	
108 WG	140 COS	New Jersey	
111 WG	112 COS	Pennsylvania	
192 FW	185 COS	Virginia	
143 AW	102 ACD	Rhode Island	
	AATC	Arizona	
158 FW	229 COS	Vermont	

Attachment 6

TEST/TRAINING SPACE NEEDS STATEMENT (T/TSNS)

Description: Examples of actions requiring a T/TSNS include, but are not limited to: acquiring a new cyberspace range distributed location; fielding a new capability with a recurring sustainment cost; and moving or establishing a new cyberspace range. Equipment replacement governed by a program office does not require a T/TSNS.

Figure A6.1. T/TSNS Flowchart.



Test/Training Space Needs Statement (T/TSNS) Example

ACC 19-01
(MAJCOM Year/Numbered Submission (01 for first of the new calendar year))
346TH TEST SQUADRON
JOINT BASE SAN ANTONIO
SAN ANTONIO, TEXAS
MODIFICATION OF CYBER TEST AND TRAINING RANGE

Proponents' Names:
Commander Name, Unit
Deputy or Director of Operations Name, Unit
Proponent POC: Primary Contact

Unit
Address
Phone Number

Updated on 2 February 2019

Table of Contents
Page

1. Overview

1.1. Concept/Purpose. This T/TSNS addresses 346 TS requirement to provide an integrated, year-round, threat representative and realistic cyberspace training environment (cyberspace range, facilities, and equipment) for units to enhance their combat capability as outlined in (ex. DAFMAN 13-212v3) and the need to amend and establish virtual training environment to support Large Force Employment exercises. (Provide strategic and MAJCOM level policy, mission requirements or additional justifications for the amendment.)
1.1.1. This T/TSNS addresses recommendations made by the Cyberspace Range Steering Group (June 2008). That group, comprised of representatives from the Headquarters Air Force, ACC, and the Air National Guard, identified multiple shortfalls with the existing cyberspace range and made several recommendations to improve/optimize the environment to meet mission requirements.

1.1.2. Additional information as required.
1.2. **Existing and Concept/Proposed Architecture.**

Figure 1. Provide diagrams and brief description of existing infrastructure.

Figure 2. Provide diagrams and brief description of recommend changes to infrastructure.

2. Operational Requirements/Justification.

2.1. Unit and Mission. The Cyber Test and Training Range (CTTR), located Joint Base San Antonio, TX, is managed by the 346th Test Squadron (346 TS) and is operationally and organizationally tasked to provide an operationally relevant environment to support cyberspace test, training, exercises and mission rehearsals. This capability can be accessed remotely for initial qualification training, mission qualification training, continuation training, or tactics, techniques, and procedures development/validation. This 346 TS asset is scalable to support various levels of training and can provide access to the Joint Information Operations Range for large-scale exercises. This capability is a unique Air Force asset which requires targeted investment across the next two future years defense programs (FYDPs) to achieve its required capabilities.
2.2. Unit and Mission. Provide additional units and missions as necessary to encompass all impacted cyberspace ranges.
2.3. CTTR Shortfalls. Provide an overview of the shortfall:
2.3.1. Provide support factors justifying the shortfall.
2.3.2. Outline actions taken to remediate the shortfall internal to the organization.
2.3.3. Identify the impacts to the unit mission.

3. Concept/Proposed Actions: Provide specific details, descriptions and proposed actions.

4. Alternatives. Provide alternative action plans.
4.1. Provide description of impacts if shortfall cannot be remediated.
4.2. Provide alternative solutions.

Attachment 7

RISK MANAGEMENT FRAMEWORK CHART

Description: The RMF Chart identifies the recommended security control families for two different cyberspace range network focus areas, the Management and Threat network. The Management network is the underlying out-of-band network used to control configure and monitor the test and training network. The Threat network identifies the training network environment created for the test or training audience to participate.

Table A7.1. Cyberspace Ranges RMF Control Families.

RMF Control Families	Acronym	Management	Threat
Access Control	AC	X	
Audit and Accountability	AU	X	
Awareness and Training	AT	X	
Configuration Management	CM	X	X
Contingency Planning	CP	X	X
Identification and Authentication	IA	X	
Incident Response	IR	X	X
Maintenance	MA	X	X
Media Protection	MP	X	X
Personnel Security	PS	X	X
Physical and Environmental Protection	PE	X	X
Planning	PL	X	X
Program Management	PM	X	X
Risk Assessment	RA	X	
Security Assessment and Authorization	CA	X	X
System and Communications Protection	SC	X	
System and Information Integrity	SI	X	
System and Services Acquisition	SA	X	

Attachment 8

MULTI-DOMAIN INTEGRATION WITH TRAINING SYSTEMS

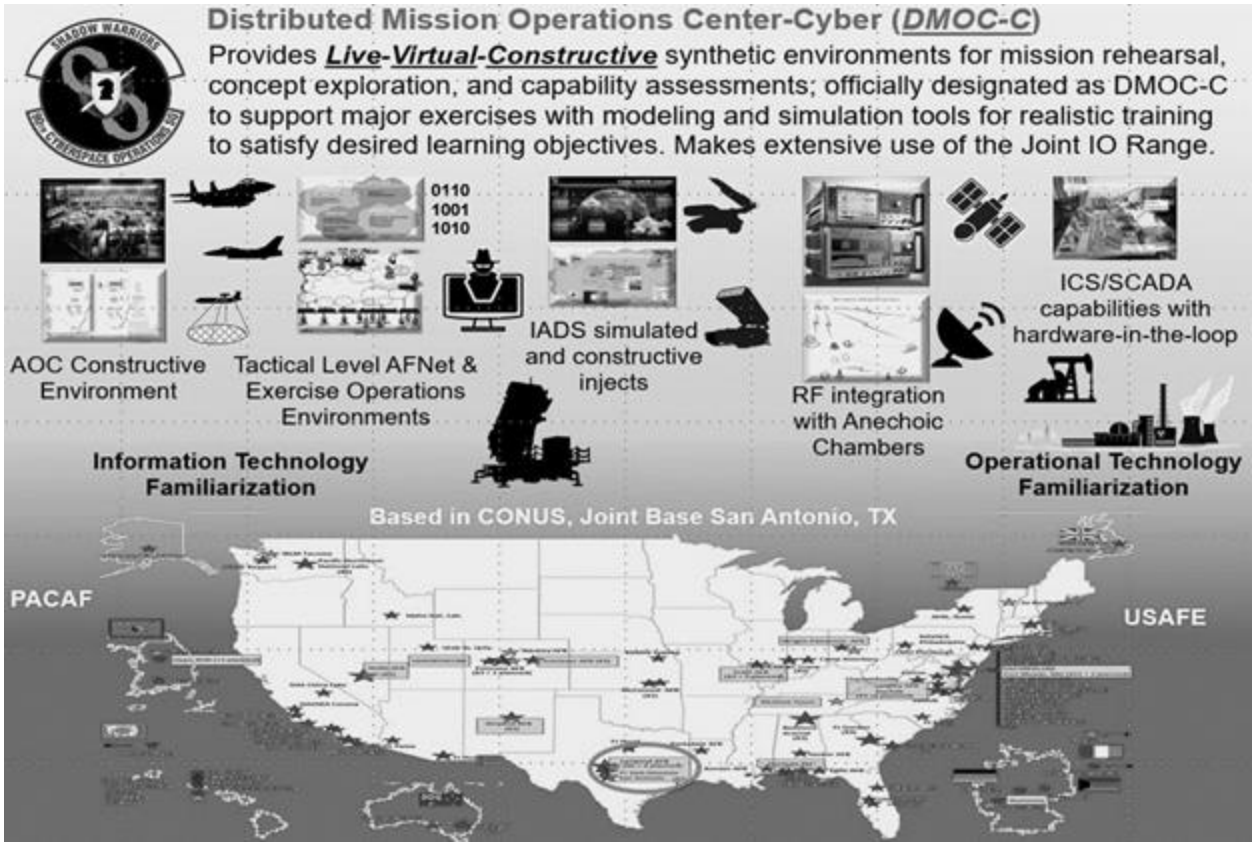
Description: The Air Force Future Operating Concept describes an environment in 2035 in which "integrated multi-domain operations will encompass full interoperability among air, space, and cyberspace capabilities." The below diagram is a pictorial representation of multi-domain integration.

Figure A8.1. Multi-Domain Training System Integration.

DMOC-C Multi-Domain Training System Integration.

Description: DMOC-C provide the synthetic environment for mission rehearsal, concept exploration, and capability assessments; officially designated as DMOC-C to support major exercises with M&S tools for realistic training to satisfy desired learning objectives. The below diagram is a pictorial representation of multi-domain integration.

Figure A8.2. DMOC – Cyber Multi-Domain Training System Integration.



DTC – Cyber Multi-domain Training System Integration

Description: The ANG Cyber Range Squadron (RANS) will provide a training and exercise environment for ANG Cyber Forces to "train as they fight" outside the operational network environment. The ANG Cyber RANS will enable planning, preparation, execution & assessment across the full spectrum of cyberspace operations (e.g. Scheduling/Deconfliction of Range, Mission Planning/Rehearsal, Infrastructure/Scenario Development, Standards/Evaluation of Cyber Forces, Opposing Forces or Red Team Injects, Joint and/or International Exercises, VITE/JIOR/PCTE/JCTE Interconnectivity, Individual/Crew Readiness Training, Multiple terrains, Range Maintenance/Compliance, Testing/Experimentation, Modeling/Simulation, Secure Transport, Remote/Onsite Support) needed to cater to the unique scheduling constraints, range and simulator availability, and training needs of the Reserve Component Warfighter.

Figure A8.3. DTC – Cyber Multi-Domain Training System Integration.