

ACTION MEMO

PDUSD(P) BM OCT - 5 2015

FOR: DEPUTY SECRETARY OF DEFENSE

FROM: Tom Atkin, Acting Principal Cyber Advisor

SUBJECT: Designation of Executive Agents for Cyber Training Ranges and Cyber Test Ranges

- This memo recommends that you: 1) sign the memorandum at TAB A designating the Secretary of the Army as the DoD Executive Agent (EA) for Cyber Training Ranges and the Director, Test Resource Management Center (TRMC) as the DoD EA for Cyber Test Ranges; and 2) approve the EAs' Roles and Responsibilities document at TAB B, which subsequently will be developed into a DoD Directive.
 - The Secretary of the Army should serve as the DoD EA for Cyber Training Ranges due to the Army's extensive cyber range assets as well as operational training culture, the Secretary of the Army's experience serving effectively as EA in other capacities, and the Secretary's expressed interest in serving as the EA. Additionally, the Under Secretary for Personnel and Readiness should serve as the Principal Staff Assistant (PSA) for the DoD EA for Cyber Training Ranges due to his oversight role for training.
- The Director, TRMC should serve as the DoD EA for Cyber Test Ranges due to TRMC's existing, similar role for the overall test range complex. Additionally, the Under Secretary of Defense for Acquisition, Technology, and Logistics should serve as the PSA for the DoD EA for Cyber Test Ranges due to his oversight role for testing.
- Designation of the EAs, and their accompanying roles and responsibilities, was reviewed by the Joint Chiefs of Staff Operations Deputies (OPSDEPs), the Cyber Investment Management Board (CIMB), and staffed across the DoD.

- All comments have been reconciled through adjudication, except for the Director, Operational Test & Evaluation's non-concur requiring one EA to service both communities. While we agree that the designation of a single Cyber Range EA would appear to be a simple and elegant solution, previous extensive discussions across the Department, including a March 2015 OPSDEPs, recommended that two separate EAs be established due to inherent expertise by TRMC and a Service in the cyber test and training arenas. Designating a single Cyber Range EA would result in the designated organization having to assume oversight of an area outside of its core expertise, potentially forcing the single Cyber Range EA to grow its organization in order to adequately oversee its new and unfamiliar mission. Two separate EAs are also consistent with the statutory provision requiring designation of these EAs (10 USC 392). In addition, the Cyber EAs' Roles and Responsibilities document (TAB B) acknowledges

SD CA	DSD SA	
SD SMA	DSD SMA	2/11/15
SD MA	DSD MA	2/11/15
TSA	DSD CA	
SA YB DB		
ES	ESR RW	
ESR	ESD	



DOT&E's concerns by establishing a structure that ensures collaboration and conflict resolution between the EAs.

- Key roles, responsibilities, and core functions of both DoD EAs include:
 - Review and certify the budgets of the four Defense Enterprise Cyber Range Environment (DECRE) ranges, to ensure unity of effort across the cyber range enterprise. This responsibility is consistent with Director, TRMC's current authorities.
 - Set priorities for those ranges and allocate their capacity to ensure that the ranges are fulfilling USCYBERCOM's Cyber Mission Force training requirements and the Department's test and evaluation requirements.
 - Consistent with the legislation, develop a Biennial Integrated Cyber Test and Training Range Plan.
 - Coordinate and deconflict range issues by leveraging existing forums, including an expanded DECRE for working level and technical issues, as well as the CIMB and Deputy's Management Action Group for senior-level decisions.
- These designations are mandated by Section 1633 of the National Defense Authorization Act for Fiscal Year 2015 (codified at 10 USC 392) (TAB C). The legislation also required the prescription of roles, responsibilities and authorities of those executive agents.
 - In the legislation's joint explanatory statement, the Armed Services Committees expressed concerns about the management of cyber range resources, observing that a lack of coordination among range owners has impeded the ability of cyber operators to train like they fight.

RECOMMENDATION: Sign the designation memorandum at TAB A and approve the EAs' Roles and Responsibilities document at TAB B.

Approve:  Disapprove: _____ Other: _____

COORDINATION:  TAB D

Attachments:
As stated



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 8 2016

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF OF THE NATIONAL GUARD BUREAU
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Designation of Executive Agents for Cyber Training Ranges and Cyber Test Ranges

In accordance with DoD Directive 5101.1, *DoD Executive Agent*, September 3, 2002, and pursuant to title 10, U.S.C., section 392, I designate the Secretary of the Army as the Department of Defense Executive Agent (DoD EA) for Cyber Training Ranges and the Director, Test Resource Management Center as the DoD EA for Cyber Test Ranges. The Under Secretary for Personnel and Readiness (USD(P&R)) shall serve as the Principal Staff Assistant (PSA) for the DoD EA for Cyber Training Ranges. The Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) shall serve as the PSA for the DoD EA for Cyber Test Ranges. The roles and responsibilities of the two DoD EAs are attached.

The USD(P&R) and USD(AT&L), in coordination with the Principal Cyber Advisor and the Deputy Chief Management Officer, will further develop and refine the roles and responsibilities document and develop a Department of Defense Directive to be issued not later than one year from the date of this memorandum.

Attachment:
As stated



Roles, Responsibilities and Authorities for the Department of Defense Executive Agents for Cyber Test Ranges and Cyber Training Ranges

Overview

This document outlines the governance, scope, roles, responsibilities, and authorities for the Department of Defense Executive Agents (DoD EA) for Cyber Test Ranges and Cyber Training Ranges, pursuant to section 392 of Title 10, United States Code. Section 392 requires EA designations for both Cyber Test Ranges and Cyber Training Ranges in order to:

- Improve coordination of cyber test and training range capabilities.
- Train, certify, qualify, and sustain mission ready cyber mission forces and the cyber workforce.
- Standardize test, training, and operational tools.

The roles, responsibilities, and authorities for the DoD EAs do not supersede the responsibilities of DoD Principal Staff Assistants (PSAs), or the Title 10 authorities of the Chairman of the Joint Chiefs of Staff. The Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) will serve as the OSD PSA for the DoD EA for Cyber Test Ranges and the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) will serve as the PSA for the DoD EA Cyber Training Ranges.

I. Definitions

For the purposes of this document:

Cyber Ranges are defined as an environment that supports cyber effects on information technology (IT) and other network-enabled technologies for the purpose of experimentation, testing, training, and/or exercising on a real or simulated network. It can also support the development of new cyber technology.

Designated Cyber Test and Training Ranges refers to cyber test and training range assets and infrastructure, including the National Cyber Range, the Joint Information Operations Range, the Defense Cyber Security Range, and the C4 (Command, Control, Communications, and Computers) Assessments Division, and Cyber C2 (Command and Control) Laboratory of the Joint Staff.

II. Governance

The DoD EAs for Cyber Test and Training Ranges will oversee, coordinate, and adjudicate all designated cyber range issues. They will work closely together to resolve any issues. Should issues persist that cannot be resolved between the two DoD EAs they will be forwarded to the PSAs. The PSAs will execute the responsibilities outlined in DoD Directive 5101.1, DoD Executive Agent, September 3, 2002 to assess DoD EA activities. Issues that cannot be resolved between two PSAs will be forwarded to the Cyber Investment and Management Board (CIMB) or other senior-level decision-making forum for resolution. If necessary, issues may be elevated to the Deputy's Management Action Group (DMAG) for resolution.

The DoD EAs for Cyber Test and Training Ranges will follow standard Department processes and provide regular updates on the execution of the biennial plan to the CIMB, and DMAG as appropriate.

For the activities of the Designated Cyber Training Ranges conducted to fulfill the Chairman's responsibilities per Title 10 U.S. Code and Joint Staff Manual 5100.01E and DoDD 5101.1, the Chairman will continue to leverage the range assets to fulfill specific requirements. Cyber Test and Training Range EAs shall be responsive to the Chairman to address these requirements.

The EAs will work with existing working groups and develop appropriate sub-working groups, as necessary, to inform the decision making processes, comprised of membership from all the Services, and other appropriate agencies, to address plans, architecture, standards, and other subjects as required.

III. DoD Executive Agent for Cyber Test Ranges

Scope

The DoD EA for Cyber Test Ranges will develop, coordinate, and integrate plans to synchronize activities across the designated cyber test ranges and establish appropriate test infrastructure architectures and standards in order to provide a cohesive set of test and evaluation resources (e.g. facilities, capabilities, and workforce) needed to ensure that DoD has the capability to conduct experimentation, research and development, and test and evaluation in realistic, secure, and effective cyber-contested environments. The primary purpose of cyber test capabilities and ranges is to enable the development, acquisition, and sustainment of DoD resilient systems. A federated set of cyber test range capabilities that are developed, funded, owned and operated by DoD Components¹ is envisioned. The DoD EA will have appropriate authorities and resourcing to partner with DoD Components to evolve existing capabilities to achieve this cohesive vision. Ranges are dual purpose and serve a multitude of stakeholders; therefore, with respect to the National Cyber Range, the DoD EA for Cyber Test Ranges will coordinate and synchronize efforts with the DoD EA for Cyber Training Ranges. Recognizing in particular the criticality of the existing National Cyber Range to the establishment of a cyber training environment, the DoD EAs for Cyber Range Test and Training will develop a memorandum of agreement that ensures the apportionment of training assets, infrastructure, and range enhancements to meet Training requirements on the National Cyber Range.

Roles and Responsibilities

The DoD EA for Cyber Test Ranges will exercise DoD-wide responsibilities for planning and integrating activities across the cyber test infrastructure and oversee its strategic modernization in coordination with the Principal Staff Assistant (USD (AT&L)) and in collaboration with DoD

¹ IAW DoDD 5101.1, "DoD Executive Agent," September 3, 2002, DoD components are defined as the Office of the Secretary of Defense; the Military Departments; the Chairman of the Joint Chiefs of Staff; the Combatant Commands; the Office of the Inspector General, Department of Defense; the Defense Agencies; the DoD Field Activities; and all other organizational entities within the Department of Defense.

Components and the Principal Cyber Advisor to the Secretary of Defense. The DoD EA for Cyber Test Ranges will:

- 1) Together with the DoD EA for Cyber Training Ranges, develop and oversee execution of a *Biennial Integrated Plan* as specified in Section V of this document.
- 2) Facilitate, establish, maintain and oversee implementation of DoD-wide requirements and standards for the integration of the designated cyber test ranges consistent with the needs of the Services' acquisition communities (e.g. Service Acquisition Executives, Program Executive Officers, Program Managers, etc.). While the primary purpose of the cyber tests ranges are in support of acquisition, as an additional function, they need to be capable of augmenting training when called upon.
 - a) In collaboration with the DoD EA for Cyber Training Ranges, establish the architectures for designated cyber test ranges, with a focus on implementing and sustaining operationally representative environments capable of interoperating with other DoD test infrastructure (kinetic and non-kinetic) and appropriate training infrastructures. Architectures must allow for integrated closed-loop testing in a secure environment of cyber and electronic warfare capabilities.
 - b) In collaboration with the DoD Components and the DoD EA for Cyber Training Ranges, perform the systems engineering to develop cyber test and training infrastructure interface standards and other technical and operational standards as deemed necessary.
 - i) Establish, in coordination with the DoD Components and in consultation with the DoD CIO, a standard language (data exchange protocol) for representing and communicating cyber event and threat data during a cyber-range event. The language must be compatible (machine-readable) with the Joint Information Environment (JIE) and coordinated with the DoD CIO.
 - ii) Maintain and update the architectures and standards consistent with DoD CIO Information Enterprise Architecture Standards as required, and communicate requirements with the DoD Components. Also ensure the architectures and standards are made available to appropriate industry partners, academic institutions, allies and other mission partners. Coordinate, as needed, with these critical partners on cyber training and test range issues to accomplish DoD goals.
 - c) Monitor Component investments in designated cyber test ranges. Ensure investments in cyber range systems and capabilities are tracked and reported consistent with DoD IT investment requirements. For those investments determined not to be consistent with approved architectures and standards, coordinate with the responsible DoD Component, and the DoD CIO, on a mutually satisfactory set of corrective actions. DoD Executive Agent written approval of corrective actions is required before investments may proceed.
 - d) In collaboration with the DoD Components, maintain a current and comprehensive list of designated DoD Cyber government, and non-government test and training cyber ranges

based on the definition in the front matter of this document. Through continuous involvement at all levels, with programs, projects, and processes supporting defense acquisition, the DoD EA for Cyber Test Ranges will work directly with the Components to identify additions, deletions, and revisions to the DoD Designated Cyber Range inventory. DoD Component assets will not be added, removed, or revised without coordination from the range owner.

- e) Ensure access to and usage of the designated cyber test ranges are cost effective and efficient (prioritized when required).
 - f) Approve the addition, reduction, or deletion of programs, functions, and cyber test capabilities to and from the cyber test ranges in consultation with the DoD EA for Cyber Training Ranges as appropriate.
 - g) Utilize the existing Testing and Evaluation (T&E) Board of Directors as an Advisory Board for cyber and Information Technology (IT) test ranges.
 - h) Establish with the DoD Components (including the DoD EA for Cyber Training Ranges and its PSA) appropriate policies and memorandums of agreement (MOAs) to ensure efficiency in operating common usage cyber range assets. One of the developed policies/MOAs shall address range activity prioritization, apportionment, and arbitration to optimize the growth of the Cyber Mission Force and cybersecurity/cyber survivability testing activities through FY18.
- 3) Represent and advocate for DoD-wide cyber test range interests to ensure that they are adequately resourced to achieve DoD strategic goals, for science and technology (S&T), research and development (R&D), modeling and simulation, program acquisition, and test and evaluation (T&E).
- a) Participate in designated cyber test range planning, programming, budgeting, and execution (PPBE) activities by reviewing resource programs, requirements, and budget estimates, and by commenting on resource allocations proposed by the DoD Components.
 - b) Oversee existing program elements (PE) associated with designated cyber test ranges consistent with established goals/objectives, and periodically review operations of the cyber test infrastructure for effectiveness and efficiency in coordination with the DoD EA for Cyber Training Ranges. If transparency of resources is not sufficient, examine options to establish new PEs to improve transparency.
 - i) Identify, prioritize, and recommend new cyber test infrastructure requirements supporting the development and fielding of systems which are cyber resilient.
 - ii) Annually review each designated cyber test range proposed budget not later than 60 days prior to the official DoD budget submission, in accordance with Program/Budget Review guidance as it pertains to the specific budget year.

- iii) Annually certify that the designated cyber test ranges meet established standards, are adequately funded and capable, and have a workforce with appropriate expertise, prior to the official DoD budget submission, in accordance with Program/Budget Review guidance as it pertains to the specific budget year.
- iv) Develop and partner with DoD participants of the cyber test ranges in the development of common tools, instrumentation, applications, processes, procedures, services, common security, interoperability, compatibility, interfaces, and best practices throughout the cyber test infrastructure, the primary purpose of which is to increase availability of cyber infrastructure to the acquisition and sustainment of programs, with additional support to training and operations.

IV. DoD Executive Agent for Cyber Training Ranges

Scope

The DoD EA for Cyber Training Ranges will develop, coordinate, and integrate plans to synchronize activities across the designated cyber training ranges and establish appropriate training infrastructure architectures and standards in order to provide a cohesive set of training resources (e.g., facilities, capabilities, and workforce) needed to ensure that DoD has a realistic, scalable, and persistent cyber range architecture. This architecture will improve the readiness of the cyber workforce by providing the capability to train and mission-rehearse consistently. A federated set of cyber training range capabilities that are developed, funded, owned and operated by DoD Components is envisioned. The DoD EA will have appropriate authorities and resourcing to partner with DoD Components to evolve existing capabilities to achieve this cohesive vision. Ranges are dual-purpose and serve a multitude of stakeholders; therefore, the DoD EA for Cyber Training Ranges will coordinate and synchronize efforts with the DoD EA for Cyber Test Ranges, and with other DoD Components. Recognizing in particular the criticality of the existing DoD Cyber Ranges to the establishment of a cyber training environment, the DoD EAs for Cyber Range Test and Training will develop a memorandum of agreement that ensures the apportionment of training assets, infrastructure, and range enhancements to meet testing requirements on the designated cyber ranges.

Roles and Responsibilities

The DoD EA for Cyber Training Ranges will exercise DoD-wide responsibilities for planning and integrating activities and establish joint and common requirements across the cyber training infrastructure and oversee its strategic modernization in coordination with the Principal Staff Assistant (USD (P&R)), and in collaboration with DoD Components, including U.S. Cyber Command (USCYBERCOM), and the Principal Cyber Advisor to the Secretary of Defense. The DoD EA for Cyber Training Ranges will:

- 1) Together with the DoD EA for Cyber Test Ranges, develop and oversee execution of a *Biennial Integrated Plan* as specified in Section V of this document.

- 2) Facilitate, establish, maintain and oversee implementation of DoD-wide requirements and standards for the integration of the designated cyber training ranges.
 - a) In collaboration with the DoD EA for Cyber Test Ranges, establish the architectures for the designated cyber training ranges, with a focus on implementing and sustaining an available, realistic, scalable, and persistent cyber range architecture in order to train and mission-rehearse consistently. Architectures must allow for integrated closed-loop training in a secure and operationally realistic environment of cyber, electronic warfare, and traditional warfighting domain capabilities.
 - b) In collaboration with the DoD Components, and the DoD EA for Cyber Test Ranges, perform the systems engineering to develop cyber training and test infrastructure interface standards and other technical and operational standards as deemed necessary.
 - i) Establish, in coordination with the DoD Components and in consultation with the DoD CIO, a standard language (data exchange protocol) for representing and communicating cyber event and threat data during a cyber-range event. The language must be compatible (machine-readable) with the Joint Information Environment (JIE) and coordinated with the DoD CIO.
 - ii) Maintain and update the architectures and standards consistent with DoD CIO Information Enterprise Architecture Standards as required, and communicate requirements with the DoD Components. Also ensure the architectures and standards are made available to appropriate industry partners, academic institutions, allies, and other mission partners. Coordinate, as needed, with these critical partners on cyber test and training range issues to accomplish DoD goals.
 - c) Integrate the training needs and requirements of the DoD Components, including USCYBERCOM, into cyber range training standards.
 - d) Monitor Component investments in the designated cyber training ranges. Ensure investments in cyber range systems and capabilities are tracked and reported consistent with DoD IT investment requirements. For those investments determined not to be consistent with approved architectures and standards, coordinate with the responsible DoD Component on a mutually satisfactory set of corrective actions. DoD Executive Agent written approval of corrective actions is required before investments may proceed.
 - e) In collaboration with the DoD Components, maintain a current and comprehensive list of designated DoD Cyber government, and non-government test and training cyber ranges based on the definition in the front matter of this document. The DoD EA for Cyber Training Ranges will work directly with the Components to identify additions, deletions, and revisions to the DoD Designated Cyber Range inventory. DoD Component assets will not be added, removed, or revised without coordination from the Range Owner.
 - f) Approve the addition, reduction, or deletion of programs, functions, and cyber training capabilities to and from the cyber training ranges in consultation with the DoD EA for

Cyber Test Ranges as appropriate. This would include the development, review, and approval of new cyber training range requirements through the existing requirements processes.

- g) Ensure access to and usage of the designated cyber training ranges are cost effective and efficient (prioritized when required).
 - h) Establish with the DoD Components (including the DoD EA for Cyber Test Ranges and its PSA) appropriate policies and MOAs to ensure efficiency in operating common usage cyber range assets. One of the developed policies/MOAs shall address range activity prioritization, apportionment, and arbitration to optimize the growth of the Cyber Mission Force and cybersecurity/cyber survivability testing activities through FY18.
 - i) Provide standardized programmatic reporting guidance to designated cyber range owners in order for the DoD Cyber Training Range EA to review and certify the designated cyber range owners' fiscal year (FY) and future-years defense program as directed in Section VI, "Responsibilities of Designated Cyber Range Owners."
- 3) Represent and advocate for DoD-wide cyber training range interests to ensure that they are adequately resourced to achieve DoD strategic goals; in particular, to ensure that ranges fully support the fielding and sustainment of the DoD cyber forces, including the Cyber Mission Force, Cyber Enterprise Defense Force, and related Command and Control elements.
- a) Participate in designated cyber training range planning, programming, budgeting, and execution (PPBE) activities by reviewing resource programs, requirements, and budget estimates, and by commenting on resource allocations proposed by the DoD Components.
 - b) Oversee existing PEs associated with designated cyber training ranges consistent with established goals/objectives, and periodically review operations of the cyber training infrastructure for effectiveness and efficiency in coordination with the DoD EA for Cyber Test Ranges. If transparency of resources is not sufficient, examine options to establish new PEs to improve transparency.
 - i) Identify, prioritize, and recommend cyber training range infrastructure requirements.
 - ii) Annually review each designated cyber training range proposed budget not later than 60 days prior to the official DoD budget submission, in accordance with Program/Budget Review guidance as it pertains to the specific budget year.
 - iii) Annually certify that the designated cyber training ranges meet established standards, are adequately funded and capable, and have a workforce with appropriate expertise, prior to the official DoD budget submission, in accordance with Program/Budget Review guidance as it pertains to the specific budget year.

- iv) Develop and partner with DoD participants of the cyber training ranges in the development of common tools, instrumentation, applications, processes, procedures, services, common security, interoperability, compatibility, interfaces and best practices throughout the cyber training range infrastructure.

V. **Biennial Integrated Cyber Range Plan**

The DoD EAs for Cyber Test Ranges and for Cyber Training Ranges will develop a biennial integrated plan for cyber ranges to serve as a roadmap for cyber range use over a two-year period. The *Biennial Integrated Cyber Range Plan* will describe the previous usage, planned use, modernization, and sustainment of the cyber test and training infrastructure. The EAs will submit the Plan to their respective PSAs and the CIMB for resource considerations. The *Biennial Integrated Plans* are due to the CIMB on May 1, annually starting in 2016 to inform the annual Program/Budget Review process and will include:

- 1) A current and comprehensive list of government and non-government cyber ranges, based on the definition contained in the front matter, which is updated regularly.
- 2) Documented priorities for cyber ranges to meet Department goals.
- 3) A Service coordinated proposal for cyber test and training ranges that should be added to the designated ranges over which the DoD EAs have jurisdiction.
- 4) Appropriate architectures (e.g., “As Is,” “To Be,” secure, Electronic Warfare (EW) capabilities etc.) with a progress report across the cyber test and training infrastructure on implementing architectures and standards.
- 5) Organization and management of the ranges.
- 6) Recommendations regarding resources efficiencies and improvements, including:
 - a) Trends, strengths, weaknesses, and customer satisfaction.
 - b) Activities and accomplishments during the last two years.
 - c) Identified unwarranted duplication (when noted).
 - d) Identified opportunities for integration among the cyber ranges regarding test and training functions.
 - e) Identified opportunities for cost reduction, integration, consolidation, and coordination among other resources.
 - f) Identification of modernization investments required to keep pace with technology and expected demand, and to enhance the quality of the workforce through training and personnel policies.
- 7) Recommendations for USD(AT&L) of policies and projects that improve, streamline and strengthen DoD-wide cyber test infrastructure in support of science and technology (S&T), research and development (R&D), development test and evaluation (DT&E), and operational test and evaluation (OT&E) for acquisition programs.

- 8) Recommend policies and projects that improve, streamline and strengthen DoD-wide cyber training infrastructure.

VI. Responsibilities of Designated Cyber Range Owners

- 1) Each designated cyber test and training range owner will submit annually to the appointed DoD EAs the proposed fiscal year (FY) and future-years defense program budget for test and/or training activities in accordance with Program/Budget Review guidance as it pertains to the specific budget year, for review and certification.
- 2) Designated Cyber Test Ranges and Cyber Training Range owners will comply with the standards which are developed in conjunction with the Services per above Paragraph 2) b) of the Roles and Responsibility paragraph for each EA. Owners may not implement divestment, consolidation, or curtailment of activities, until the designated cyber test range or cyber training range owner gets approval of the appropriate DoD EA.

VII. Resources

- 1) The designated DoD EAs for Cyber Test Ranges and Cyber Training Ranges will conduct an assessment of the administrative costs and resources required to carry out assigned responsibilities, functions, and authorities. The DoD EAs will work through the normal PPBE processes (including the issue paper process) to ensure appropriate funding is available to perform EA roles and responsibilities for the ranges they have oversight for.
- 2) The DoD EAs for Cyber Test Ranges and Cyber Training Ranges will have full cognizance of designated cyber range budgets and spend plans, and will review and make recommendations as part of the Program/Budget Review process.