

**Engagement Guide
Department of Defense
Federally Funded Research and Development Centers
(FFRDCs)**

April 2013



OSD Studies and FFRDC Management Office

4800 Mark Center Drive
Suite 14G14
Alexandria, VA 22350
(571) 372-6206

Defense Laboratories Office

4800 Mark Center Drive
Suite 17C08
Alexandria, VA 22350
(571) 372-6376

Contents

Purpose.....	2
Points of contact for DoD FFRDCs and for Defense Laboratories.....	2
Overview of FFRDCs	3
Overview of DoD-sponsored FFRDCs	5
DoD Component Use of DoD-Sponsored FFRDCs	7
DoD Component Use of DOE-Sponsored FFRDCs	7
APPENDIX A: DoD-sponsored FFRDC Web Sites and POCs	8
APPENDIX B: DoD-sponsored FFRDC Core Competencies	9
APPENDIX C: DOE-sponsored FFRDCs and POCs.....	23

Purpose

The purpose of this Engagement Guide is to inform members of the Department of Defense (DoD) community about the 10 DoD-sponsored Federally Funded Research and Development Centers (FFRDCs) that provide research, analyses, science, technology, and engineering support for their DoD sponsors. This Guide provides information about the capabilities of the DoD FFRDCs and points of contact to facilitate communication about exploring the potential for leveraging the capabilities of these valuable resources.

The Engagement Guide also addresses Department of Energy (DOE) FFRDCs because they also perform a critical role in defense and national security research and development and offer unique resources and capabilities that are available for use by DoD on a work-for-hire basis. DOE has 18 FFRDCs that provide a broad spectrum of cutting edge research capabilities.

Points of contact for DoD FFRDCs and for Defense Laboratories

The Deputy Director, OSD Studies and FFRDC Management, Office of the Director, Acquisition Resources Analysis, Office of the Under Secretary of Defense (Acquisition, Technology and Logistics) (OUSD(AT&L)) is responsible for DoD policy on FFRDCs. Questions concerning this Engagement Guide can be directed to Dr. Mona Lush, Deputy Director, OSD Studies and FFRDC Management at mona.lush@osd.mil.

The Director, Defense Laboratories, Office of the Assistant Secretary of Defense (Research and Engineering) (OASD(R&E)) (OUSD(AT&L)) is responsible for DoD policy on DoD laboratories. Questions concerning DoD laboratories or engaging DOE FFRDCs (National laboratories) can be directed to Dr. John Fischer, Director, Defense Laboratories at john.fischer@osd.mil.

Appendix A contains the web site address for each DoD FFRDC, as well as a point of contact for each FFRDC and its DoD sponsor. Appendix B contains a list of the core competencies for each DoD FFRDC. Appendix C contains a list of the 18 DOE-sponsored FFRDCs and points of contact for each.

Overview of FFRDCs

FFRDCs are not-for-profit entities sponsored and funded primarily by the United States government to address research and development, engineering, and analytic needs that cannot be met as effectively by existing government or other contractor resources. FFRDCs are intentionally located outside the Government to provide a long-term strategic relationship and management flexibility to attract and retain high-quality scientists and engineers. The government establishes a long-term, strategic relationship with each FFRDC to establish and maintain research, development, or engineering capabilities critical to the mission of the sponsoring government organization.

Federal policy regarding FFRDCs is set in the Federal Acquisition Regulation (FAR) Section 35.017, which was updated in February 2010, as follows:

- An FFRDC meets some special long-term research or development need which cannot be met as effectively by existing in-house or contractor resources. FFRDCs enable agencies to use private sector resources to accomplish tasks that are integral to the mission and operation of the sponsoring agency. An FFRDC, in order to discharge its responsibilities to the sponsoring agency, has access, beyond that which is common to the normal contractual relationship, to Government and supplier data, including sensitive and proprietary data. The FFRDC is required to conduct its business in a manner befitting its special relationship with the Government, to operate in the public interest with objectivity and independence, to be free from organizational conflicts of interest, and to have full disclosure of its affairs to the sponsoring agency. It is not the Government's intent that an FFRDC use its privileged information or access to installations, equipment, and real property to compete with the private sector. However, an FFRDC may perform work for other than the sponsoring agency under the Economy Act, or other applicable legislation, when the work is not otherwise available from the private sector.
- FFRDCs are operated, managed, and/or administered by a university or consortium of universities, other not-for-profit or nonprofit organization, or an industrial firm, as an autonomous organization or as an identifiable separate operating unit of a parent organization.
- Long-term relationships between the Government and FFRDCs are encouraged in order to provide the continuity that will attract high-quality personnel to the FFRDC. This relationship should be of a type to encourage the FFRDC to maintain currency in its

field(s) of expertise, maintain its objectivity and independence, preserve its familiarity with the needs of its sponsor(s), and provide a quick response capability.

The National Science Foundation maintains a comprehensive list of FFRDCs sponsored by Federal Departments and agencies at www.nsf.gov/statistics/ffrdclist.

Overview of DoD-sponsored FFRDCs

DoD has established 10 FFRDCs, each of which falls into one of three categories defined by the National Science Foundation as shown below. Table 1 lists the 10 DoD FFRDCs. These 10 FFRDCs are composed of:

- Research and Development (R&D) Laboratories (3)
- Systems Engineering and Integration Centers (2)
- Study and Analysis Centers (5)

DoD FFRDCs are operated by universities or privately organized, not-for-profit corporations through long-term Government contracts under the authority of 10 U.S.C. 2304(c)(3)(B).

FFRDC	Primary Sponsor	Parent Organization	Location
<i>R&D Laboratories</i>			
Lincoln Laboratory	Air Force (SAF/AQ)	Massachusetts Institute of Technology (MIT)	Lexington, MA
Software Engineering Institute	ASD(R&E)	Carnegie Mellon University (CMU)	Pittsburgh, PA
Institute for Defense Analyses (IDA) Communications & Computing (C&C) Center	National Security Agency (NSA)	Institute for Defense Analyses Corporation	Alexandria, VA
<i>Systems Engineering and Integration Centers</i>			
Aerospace	Air Force (SAF/AQ)	Aerospace Corporation	El Segundo, CA
MITRE National Security Engineering Center (NSEC)	DASD(SE)	MITRE Corporation	McLean, VA and Bedford, MA
<i>Study and Analysis Centers</i>			
Center for Naval Analyses (CNA)	Navy (ASN(RDA))	CNA Corporation	Alexandria, VA
Institute for Defense Analyses (IDA)	USD(AT&L)	Institute for Defense Analyses Corporation	Alexandria, VA
RAND Arroyo Center	Army Staff/PA&E	RAND Corporation	Santa Monica, CA
RAND National Defense Research Institute (NDRI)	USD(AT&L)	RAND Corporation	Santa Monica, CA
RAND Project Air Force (PAF)	Air Force (SAF/AQ)	RAND Corporation	Santa Monica, CA

Table 1: DoD FFRDCs, Sponsors and Locations

Each DoD FFRDC has a specific DoD official that is designated as its Primary Sponsor, responsible for implementing FFRDC management policies and procedures. The Primary Sponsor is responsible for maintaining a DoD Sponsoring Agreement with the FFRDC, defining

the core competencies or capabilities that the FFRDC must maintain, and ensuring that all work performed by the FFRDC is consistent with its core competencies. The Sponsoring Agreement lists the operational restrictions that the FFRDC must follow befitting its special relationship with the government, including operating in the public interest with objectivity and independence, being free from real or perceived organizational and personal conflicts of interest, and having full disclosure of its affairs to its Primary Sponsor.

The nature of their mission requires that DoD FFRDCs operate in a strategic relationship with their sponsors and users. FFRDCs and sponsors commit to a stable and long-term relationship. FFRDCs are responsive to evolving sponsor's needs, with a broad comprehensive knowledge of sponsor's requirements and problems. FFRDCs accept stringent restrictions on their scope, methods of operations and the kinds of efforts they can undertake in order to avoid actual or perceived conflicts of interest.

DoD FFRDCs perform work that: (1) is consistent with their mission, purpose, and capabilities; (2) is consistent with DoD's needs as reflected in their core competencies; (3) is consistent with the strategic relationship with their primary sponsor; and (4) cannot be performed as effectively by existing in-house or contractor resources. These FFRDCs may perform work only for DoD, other Government entities, and not-for-profit activities. FFRDCs are restricted from performing commercial work. The Primary Sponsor must approve all work.

As a result of its agreement to operate within these restrictions, maintain its objectivity and independence, and be free from conflicts of interests, FFRDCs have access—beyond that which is common to the normal contractual relationship—to Government and contractor information, including sensitive and proprietary information, and to employees and facilities.

DoD FFRDC work programs are strictly constrained by Congress each fiscal year. The annual DoD Appropriations Act sets a ceiling on the total number of staff years of work that may be put on DoD FFRDC contracts during that fiscal year. The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics controls and allocates the ceiling among the DoD FFRDCs. Congress sets separate staff year ceilings for the Military Intelligence Program and the National Intelligence Program, which are not discussed in this document.

DoD Component Use of DoD-Sponsored FFRDCs

If a DoD component is interested in examining the capabilities of a DoD-sponsored FFRDC, it should review the core competencies of the FFRDCs of interest. The component could also contact the FFRDC and/or DoD point of contact for the DoD FFRDC to determine if it can provide the research or analytic support and if there are resources available within the strict limits imposed on DoD FFRDC work programs for each fiscal year.

Appendix A contains the web site address for each DoD FFRDC, as well as a point of contact for each FFRDC and its DoD sponsor. Appendix B contains a list of the core competencies for each DoD FFRDC.

DoD Component Use of DOE-Sponsored FFRDCs

Appendix C contains a list of the 18 DOE-sponsored FFRDCs and points of contact for each. DOE uses a Work-for-Others (WFO) process for reviewing, approving/accepting, and authorizing work for other Federal agencies. There are 6 stages to this process:

- Stage 1: Proposal development by the facility contractor
- Stage 2: DOE review and approval of the proposal
- Stage 3: Sponsor review of the proposal
- Stage 4: DOE acceptance of the interagency agreement
- Stage 5: Performance of the work by the facility contractor
- Stage 6: Project closeout

Prior to Stage 1, the contractor and work sponsor have preliminary proposal development discussions, focusing primarily on the needs of the potential sponsor and technical capabilities of the contractor. The intended purpose is to determine if the FFRDC can provide the needed expertise and facilities to meet the work sponsor's needs. Additional information regarding the DOE WFO program can be found in the DOE Work-For-Others Guide.¹

¹ <https://www.directives.doe.gov/directives/0481.1-EGuide-1/view>

APPENDIX A

DoD-sponsored FFRDC Web Sites and POCs

as of April 25, 2013

<i>FFRDC</i>	<i>Web Site</i>	<i>FFRDC POC</i>	<i>DoD Sponsor POC</i>
R&D Laboratories*			
Lincoln Laboratory (MIT)	www.ll.mit.edu	Mr. Marc Bernstein Assoc Director, MIT-LL 781-981-7030 mbernstein@ll.mit.edu	Mr. Bob Baker 703-695-9602 robert.baker@osd.mil
Software Engineering Institute (CMU)	www.sei.cmu.edu	Mr. John Bramer Dir, Prog Dev & Transition 703-908-8207 bramer@sei.cmu.edu	Dr. Michael May 571-372-6719 michael.may@osd.mil
Systems Engineering & Integration Centers			
Aerospace	www.aerospace.org	Mr. Rand Fisher Vice President 703-812-0604 Rand.H.Fisher@aero.org	Mr. James R. Horejsi 310-653-1807 james.Horejsi@losangeles.af.mil
MITRE National Security Engineering Center (NSEC)	www.mitre.org	Ms. Cindy Spaney Exec Dir, Strategy & Plans 781-271-7372 lts@mitre.org	Mr. Rick Bunn 703-692-1108 richard.bunn@osd.mil
Studies and Analyses Centers			
Center for Naval Analyses (CNA)	www.cna.org	Ms. Alison Basse 703-824-2657 BASSEA@cna.org	Ms. Kim Fagan (COR) 703-693-8725 kimberly.fagan@navy.mil
Institute for Defense Analyses (IDA)	www.ida.org	Mr. Phil Major Vice President, Programs 703-845-2201 pmajor@ida.org	Mr. Brad Oeth (COR) 571-372-6199 bradrack.oeth@osd.mil
RAND Arroyo Center	www.rand.org	Ms. Marcy Agmon Dir, Operations 310-393-0411 x6419 agmon@rand.org	Ms. Angela Parris (COR) 703-695-4634 Angela.Parris1@us.army.mil
RAND National Defense Research Institute (NDRI)	www.rand.org	Ms. Nancy Pollock Dir, Ops & Bus Strategy 412-683-2300 x4945 npollock@rand.org	Mr. Robert Flowe (COR) 571-372-6231 robert.flowe@osd.mil
RAND Project Air Force (PAF)	www.rand.org	Mr. Rich Moore Air Staff Liaison 703-413-1100 x5432 richmm@rand.org	Ms. Ericka Reynolds (COR) 703-692-9728 ericka.reynolds@pentagon.af.mil

* IDA Communications and Computing Center FFRDC only supports NSA and is not included in this listing.

APPENDIX B

DoD-sponsored FFRDC Core Competencies

as of April 25, 2013

Lincoln Laboratory (Massachusetts Institute of Technology) (MIT-LL)

- Lincoln Laboratory's core work is research and development across the entire range of electronic technologies, with particular emphasis on the application of these technologies to issues of national defense problems. Lincoln Laboratory's programs extend from fundamental investigations in science through the development of new, advanced technologies to the integration and demonstration of these technologies into new or existing systems, including technology transfer to industry. Technology areas include solid state electronics; radar, biological-chemical and optical sensors; signal processing; surveillance; communications; spacecraft; analog and digital integrated circuit technology; air traffic control; signal intercept technology; high-energy laser-beam control; laser devices; optics; antennas; electromagnetic propagation; and strategic and tactical systems and countermeasures.

In carrying out its core work, Lincoln Laboratory organizes its activities into different mission areas, which have evolved over time and which are expected to change in the future. The current Laboratory mission is aligned within these areas of focus:

1. Space Control: Combined efforts in detection, tracking, and identification of man-made satellites, utilizing space-based and ground-based sensors; satellite mission and payload assessments; and environmental monitoring.
2. Ballistic Missile Defense Technology: Working with the government, industry, and other laboratories to improve the integrated system for defense against short-, medium-, and long-range ballistic missiles.
3. Air Defense: Focusing on systems and system capabilities for theater and homeland air defense applications.
4. Communication Systems: Expanding the capabilities of U.S. global defense communication networks in the space, air, land, and sea domains.
5. Cyber Security and Information Sciences: Conducting research, development, evaluation, and deployment of prototype components and

Distribution Statement A: Approved for public release; distribution is unlimited

systems designed to improve the security of computer networks, hosts and applications.

6. Intelligence, Surveillance, and Reconnaissance (ISR) Systems and Technology: Providing improved ISR capabilities through research and development in advanced sensing, signal and image processing, automatic target classification, ISR processing, exploitation, and dissemination (PED) architectures and analytics, and unmanned vehicle systems.
7. Tactical Systems: Improving the development and employment of various weapon systems, particularly tactical air and counterterrorism systems.
8. Advanced Technology: Identifying new phenomenology that can be exploited in novel system applications, and by developing the revolutionary advances in subsystem and component technologies that allow key, new system capabilities.
9. Homeland Protection: Developing technology and systems to help prevent terrorist attacks within the United States and to minimize both vulnerability to and damage from such attacks, as well as from natural disasters, and attacks using biological and chemical weapons.
10. Air Traffic Control: Developing communication, navigation, surveillance, weather, and automation systems and technology to improve safety and efficiency of air transportation.
11. Engineering: Applying state-of-the-art design, fabrication, and rapid prototyping techniques to systems under development.

Software Engineering Institute (Carnegie Mellon University) (SEI)

- Architecture
- Planning
- Cost estimation
- Requirements
- Design
- Testing, verification, and validation
- Technical development process and software lifecycle
- Performance measurement
- Sustainment (post deployment software support or post production software support)
- Maintainability and changeability
- Producibility

Distribution Statement A: Approved for public release; distribution is unlimited

- Reliability
- Evolvability
- Technical risk analysis and mitigation
- Reengineering and reuse
- Coding
- Security, safety, survivability, and timing
- Cyber software assurance and forensics
- Embedded software

Aerospace

- **Launch Certification**: The Aerospace FFRDC provides an independent launch readiness verification of the launch system design, payload integration, launch system analyses, hardware qualification and acceptance testing, software development and final overall launch processing. Aerospace provides a formal launch readiness assessment input to the SMC/CC's launch certification process.
- **Systems of Systems Engineering**: The Aerospace FFRDC provides the architecture planning and development, internal and external interface analysis, modeling and simulation analysis, and independent testing necessary to support the development of space systems.
- **Systems Development and Acquisition**: The Aerospace FFRDC provides operational requirements analysis and evaluation, mission threat analysis, risk assessment, and technical performance analysis and assessment to support acquisition planning, program preparation and evaluation, test planning and evaluation, and program milestone and design reviews for all space systems.
- **Process Implementation**: The Aerospace FFRDC provides technical expertise to support acquisition reform initiatives such as military specifications and standards reform, development and evaluation of critical processes, as well as to support proof-of-concept prototyping in support of space systems.
- **Technology Application**: The Aerospace FFRDC provides state of the art assessments of technology opportunities, alternatives, and risks to support the application of new technology in current or developing space systems

MITRE National Security Engineering Center (NSEC)

- MITRE draws on global and national strategic vectors to project the implications for the NSEC FFRDC work program, and continually adjusts its particular competencies and their mix to respond to evolving customer needs;

Distribution Statement A: Approved for public release; distribution is unlimited

e.g., increased emphasis on a comprehensive understanding of government and commercial strategies and best practices for systems engineering and system-of-systems engineering of technology applications that enhance national security.

- The NSEC FFRDC possesses a broad and deep working knowledge and wide spectrum of skills in its evolving mission domain. In addition to its fundamental technical strengths, the competencies of the NSEC FFRDC encompass: (1) the areas of knowledge management and enterprise systems engineering and architecting related to DoD business and health systems, as well as complex command and control, intelligence, surveillance, reconnaissance, weapon, cyber and other national security capabilities; (2) the processes of engineering, integration, change management, cost-effective acquisition, and advanced manufacturing; (3) the wide and growing range of technologies that underpin realization of the objectives for rapid integration, interoperability, and information sharing. The resulting NSEC capabilities rest upon:

1. *Widespread and substantial involvement with the organizations that develop, acquire, field, and utilize complex national security systems and enterprise infrastructures in support of joint service and inter/intra-agency missions and operations.* This experience leads to an understanding of: (a) the requirements for effective, integrated mission command and unity of effort for successful outcomes of complex missions involving many government, non-government agency, and coalition partners; (b) the intelligence cycle: requirements generation, collection, exploitation, analysis, and dissemination; (c) operations, from the perspective of the mission organization; (d) information technology embedded in mission operations systems; (e) information operations; as well as familiarity with emerging business models and processes and their implications for DoD and its national security partners; and it underpins the FFRDC's ability to define and engineer the specific interoperating and secure capabilities most required by the warfighters against current and near-peer threats, within the constraints of limited resources.
2. *Detailed knowledge of a broad array of national security systems.* Such knowledge is critical to successfully addressing issues of interoperability, enterprise integration, security, sustainability and modernization across the DoD, the IC and their national security mission and inter-agency partners. Support to preparation for multi-

agency operations also requires knowledge of mission partners' systems, including foreign systems.

3. *Detailed understanding of scientific, technical and process issues.* The NSEC FFRDC must understand the scientific and specific technical solutions that may be required to solve problems or to adapt existing systems to meet new requirements, as well as understand in detail the acquisition process and the systems engineering and testing processes necessary to implement secure solutions at an affordable cost.
4. *Broad and deep working knowledge of existing and emerging underlying science and technologies.* As national security becomes increasingly reliant upon technologies originally developed for commercial purposes, it is necessary that the NSEC FFRDC understand in detail the science, along with government and commercial technologies that underpin: (a) sensor systems of all types; (b) communications of all types; (c) geospatial location, navigation, timing; (d) cyber security; (e) decision-support technologies and theory; (f) collaborative technologies and behaviors; (g) business process engineering; (h) all phases of the intelligence cycle; (i) cognitive and complexity sciences; (j) health and life sciences; (k) human enabling technologies; (l) security and information operations; (m) networking and distributed systems of all kinds; (n) data fusion technologies, analytics, visualization, and enterprise data integration; (o) enterprise service building blocks; (p) biometrics; (q) microelectronics; (r) nanotechnology; and (s) advanced manufacturing. This detailed knowledge must encompass the capabilities of the technology and systems, as well as the vulnerabilities within the technology and integrated system, with a deep understanding of advanced and persistent threats.
5. *Extensive application and advancement of enterprise-level tools.* Effectively supporting the transformational goal of leveraging information technology to provide joint national security and enterprise capabilities means that the NSEC FFRDC must possess expert level skills in applying knowledge management and techniques for integrating, fusing and making sense of information from a multitude of sources and sensors. In addition, the FFRDC must understand the theory and practice of implementing change management and human factors solutions necessary to assist organizations throughout the national security community in integrating and enhancing their operations.

6. *Underlying infrastructure of laboratories, information systems, telecommunications and network services.* To be effective, the NSEC FFRDC relies upon a network of processors, tools and laboratory facilities. They support the FFRDC's capabilities and strengthen the veracity of its independent technical analyses and evidence-based recommendations. They also enable collaboration with peers and cost-effective experimentation with government and industry partners in research, development and evaluation of technology applications; tactics, techniques and procedures; and concepts of operation.

Center for Naval Analyses (CNA)

- CNA's strength is its ability to plan and execute the integrated network of research activities mandated by its mission. Recently, non-DoN, DoD activities have sponsored a larger percentage of CNA's work. DoD's need for analytical support from CNA led to the establishment of five core areas of research, all of which are essential to DoD's missions and successful development and application. The sum of CNA's core competencies is the integration of all five areas of research in a single organization coupled with a strategic relationship that is unique to CNA. Topical areas within these research areas are: Research, Development and Acquisition (RDA); Manpower/Personnel, Medical and Training (MMT) (N1); Intelligence, Information and Networks (IIN) (N2/N6); Plans, Policy and Operations (PAO) (N3/N5); Infrastructure and Readiness (IAR) (N4); Resources, Programs and Assessments (RPA) (N8); Capability Integration (CI) (N81); and Marine Corps Programs (MCP).
 1. Analysis of Defense, National Security, and Maritime Operations: CNA's ability to support operating forces with theoretical and empirical analysis is their most important core competency. In order to do any of their work effectively, CNA continually updates their methods and models to faithfully capture all essential features to realistically replicate the problems facing the operating military forces.
 2. Analysis of Defense, National Security, and Maritime System Requirements and Acquisition: CNA's long-standing involvement with military operations is relevant to almost everything they do—but from it spring other capabilities. For example, to develop or improve tactics, it is necessary to understand the systems that will be used to execute those tactics. In addition, from a solid understanding of the characteristics and shortcomings of fielded equipment, it is often only a short step to a thorough appraisal of the operational requirements for future systems. Thus, for nearly 70 years CNA and its predecessor organizations have helped the

DoD formulate and implement plans for the development and acquisition of new platforms and systems. As a result, CNA has a broad capability that allows DoD decision-makers to think through system related consequences of new missions, theaters, and warfighting concepts.

3. Analysis of Defense, National Security, and Maritime Resources: Resource analysis can be viewed as comprising the following areas of research: Workforce management, sustainment, medical, readiness and logistics, and installations and infrastructure. All have in common the need for estimating both costs and benefits of alternative ways of allocating DoD resources. Moreover, all tend to include more than their share of highly controversial studies for decision-makers who have to be sensitive to a variety of business, political, and societal concerns as well as mission and operational concerns. In the highly charged atmosphere characteristics of such studies, CNA's objectivity, independence, and privileged access to information can be critical.
4. Defense, National Security, and Maritime Program Planning: CNA's ability to help support program planning is a natural consequence of their long-term involvement with operations analysis, systems requirements, and resource analysis. Because CNA thoroughly understands the fundamentals, it is well equipped to assist in formulating coherent and executable long-term plans covering everything from the evolution of military missions to the optimal size and shape of future forces. Program planning constitutes one of the broadest and most complex of CNA's research pillars. It includes, but is not limited to, the following types of effort: Broad futuristic studies; Reviews of military missions; Force structure studies, ranging from the very broad to the quite specific; Assistance in formal program-development processes.
5. Analysis of Defense, National Security, and Maritime Policies, Strategies, and Doctrines: With the rapid changes attendant upon the end of the Cold War, and with a new emphasis with the Department of Defense on jointness, CNA's policy, strategy, and doctrine pillar has taken on a new importance. CNA is well placed to fuse policy, deterrence, operational, and technical considerations to assist the armed forces in anticipating and adapting to whatever future missions the nation may call upon them to undertake. CNA has a cadre of international affairs specialists, from both academia and government, who bring knowledge of history and a sensitivity to the politics and cultures of other countries to bear on DoD concerns. CNA field representatives augment that knowledge with their understanding of actual operations.

Institute for Defense Analyses (IDA)

- Systems and Capabilities Evaluations. IDA's evaluations of national security systems and capabilities will support decisions on acquisition and program planning, and involve assessments of military worth, performance, technological risks, costs, and joint and allied interoperability. Mission and functional area assessments, analyses of program portfolios, architecture studies, and concept analyses will be conducted as well, along with detailed evaluations of technology and integration issues related to sub-components of major systems and the information environment. Because DoD missions increasingly require integration of capabilities provided by various other federal government and non-federal organizations, IDA will maintain expertise in systems and capabilities provided by all DoD components and relevant non-DoD organizations. This will include strategic systems and missile defenses; tactical systems and capabilities for land, naval, and air warfare, including irregular warfare and homeland security / defense capabilities; mobility systems; command, control, communications, intelligence, surveillance, and reconnaissance systems; space systems; and information and computing environments. IDA will also assess potential threats and countermeasures to these capabilities. The evaluations will cover systems and information environments at all stages of development and deployment, including test and evaluation. IDA's test and evaluation work will involve reviewing and assessing operational and developmental test plans and methods, monitoring operational and developmental tests, and analyzing test results. IDA will also provide assessments of live fire test plans and results, assist in structuring and evaluating joint tests, and examine test-related infrastructure and other issues.
- Technology Assessments. IDA will provide scientific, technical and analytical support related to identifying, evaluating, developing and using advanced technologies for national security systems and capabilities, as employed by the United States and by others. This work will involve assessments of technology feasibility, readiness, performance, producibility, demonstrations, and development risks. Areas in which IDA will maintain special expertise include materials; sensor, surveillance, and target acquisition; simulation, training, and human factors; aerospace and weapons technologies; chemical, biological, radiological, and nuclear sciences and related national security technologies; manufacturing and test processes; and information and computing. In this latter area, IDA will assess processes, methods and tools for developing information and communications systems; examine architectures and methodologies for information sharing; assess means for enhancing cyber security and cyber operations; and evaluate emerging information technologies, including those used to analyze large quantities of data. IDA will develop and apply advanced simulation and modeling techniques, including examining, evaluating, and demonstrating new

simulation technologies. IDA will also assist its sponsors in developing technology strategies, plans, standards, and investment priorities; and in assessing the domestic and international implications of trade and technology cooperation, plans, and controls.

- Force and Strategy Assessments. IDA will conduct assessments relating systems; operational performance; command relationships; force structure; and national security plans, policies and strategies. Analyses will examine ongoing and past contingency operations, joint exercises, and peacetime operations to identify lessons learned and to determine the implications for national security planning. A principal focus will be on joint and combined contingency force planning, including assessments of possible scenarios at home and abroad, operational concepts, force readiness, logistic support, weapons effectiveness, and force-on-force capabilities assessments. IDA analyses also will address defense against chemical or biological attacks, cyber operations including policy and governance challenges, counter-terrorism, irregular warfare operations, and homeland security / defense operations. In addition, IDA will help develop joint operating concepts, propose and conduct joint experiments, and serve as a catalyst for innovation and transformation. Applying its technical and analytic expertise, IDA will also assist its sponsors in examining broad security topics such as organizational issues, management processes, analyses, and plans related to intelligence; countering proliferation of nuclear, chemical, and biological weapons; regional political, economic, and military trends; international military cooperation; and arms control. As in other areas, models and simulations will be developed and maintained to carry out this work.
- Resource and Support Analyses. IDA will develop methods and models for estimating the resources to develop, procure, test, operate, and support defense forces, national security systems and capabilities, information environments, cyber defenses, and intelligence capacities. IDA will apply these techniques to evaluate the implications of policy, planning, programming, and acquisition decisions. This work will identify and assess the resource implications of pending decisions and the root causes of observed changes in resource demands. IDA will propose and assess ways to mitigate resource uncertainties and risks, and to promote efficient operations. IDA's work typically will involve sensitive information on the government's future plans, as well as proprietary data from industry. IDA will also examine organizational issues, policies, and management processes, including those used to assess capability needs and identify gaps, to establish requirements, to acquire systems and capabilities, and to manage resources and budgets. Additionally, IDA will examine infrastructure and support activities, including issues related to acquisition and research and development planning; advanced manufacturing practices; the national security and commercial industrial and technology bases; mobilization and stockpiling of critical materials; the training establishment; readiness, personnel, and medical issues; total force

management; industrially-funded activities; logistics needs; operational energy; and environmental technologies and planning.

RAND Arroyo Center

- The Arroyo Center’s work spans the breadth of US Army policy. It is focused on the most critical and difficult concerns of high-level policymakers and their staffs, especially those requiring independent research and analysis. In line with these concerns, the scope of Arroyo’s work is categorized into five areas: (1) Military Logistics; (2) Strategy, Doctrine, and Resources; (3) Force Development and Technology; (4) Manpower and Training; and Military Health. The core competencies within the research areas include:

Military Logistics

- Supply chain management
- Fleet management and modernization
- Logistics force development
- Infrastructure management

Strategy, Doctrine, & Resources

- Assessing evolving operating environment
- Developing capabilities to face new challenges
- Developing partner capabilities
- Improving capabilities for stability operations
- Improving resource management
- Learning from past and present operations
- Supporting Army war games and analysis

Force Development and Technology

- Systems and technology analysis
- Networks and C4ISR
- Modeling and simulation
- Force and organizational development
- Acquisition policy
- Assessment of tactics, techniques and procedures

Manpower and Training

- Recruiting and personnel fill requirements
- Reserve Component readiness

- Leader development
- Training (Major Combat Operations and stability operations skills)
- Distance learning, sim training development/application, training support systems
- Retention (Active Component and Reserve Component)
- Officer career fields, selection, assignment sequencing
- Soldier and Family support

Military Health

- Enhancing health promotion and health care provision
- Assessing health related issues associated with deployment
- Measuring appropriateness and quality of health care
- Reducing health care costs and improving productivity
- Improving medical readiness
- Preparing medical personnel for the full spectrum of future demands

RAND National Defense Research Institute (NDRI)

- Regional security, spanning Europe, Russia, the Middle East, Asia, and Latin America as well as expertise in international security structures, such as treaty regimes and institutions like NATO.
- Defense doctrine, military concepts of operation and force employment, as well as knowledge of broader issues of defense strategy, including net assessment and deterrence theory.
- Threats to national security which span the spectrum from traditional military threats to those from terrorists and non-governmental organizations, whether they target U.S. interests abroad or in the U.S. homeland. This expertise involves special technical and policy knowledge about weapons of mass destruction, weapons proliferation, and arms control and includes particular competence in understanding non-military instruments of power such as economic instruments.
- DoD personnel requirements including skills and performance, recruiting, demographics as it relates to recruiting, retention, separation and retirement, education and training, and other special issues associated with military and civilian personnel management. NDRI's expertise in education and training covers both theory and application in traditional military as well as non-military settings.
- DoD health issues, crossing military and civilian health care systems and spanning the range of health issues, including quality of care, benefit design and cost, and the

medical support of military operations, including the identification and treatment of physical and mental health consequences.

- Other factors affecting the well-being of those in government service, including compensation, career opportunities, deployment, and various aspects of individual and family support, including resilience to stress.
- Budget analysis and resource management, including special expertise in analyzing and developing the models and systems needed to match resources to requirements and activities and to determine the most cost-effective source for each activity.
- Logistics and military infrastructures, focusing on operational logistics issues such as equipment and supply prepositioning, strategic airlift and sealift, and in-theater distribution; materiel management issues such as distribution, inventory management, maintenance, and transportation; and military infrastructure issues such as the impact of environmental policy, ensuring the adequacy of training space, and the efficiency of maintaining and operating installations.
- Weapons technologies, information technologies, and other critical technologies, focusing on how to assess the value (or potential threat) of those technologies in a military or national security context—in regional conflict, force projection, or homeland defense scenarios—and the non-defense implications associated with the technologies.
- Modernization of U.S. military forces, focusing on methods to achieve enhanced capabilities and protect critical national infrastructure against all classes of threats, from nation-states to non-governmental organizations and individuals, whether they target U.S. interests abroad or the U.S. homeland; this includes the comparative analysis of the costs, performance, and design and construction schedules of alternative platforms, particularly in the maritime domain.
- Modeling and simulation, including expertise in the feasibility of modeling approaches, modeling theory, and validation, verification, and accreditation issues. This expertise spans the range of modeling and simulation applications, from high-level strategic modeling (as exemplified by the Joint Integrated Contingency Model developed and maintained within NDRI) to detailed simulation of weapon system performance.
- The science and technology base and the defense production base, focusing on analysis of the absolute size and relative efficiency of these structures, together with the labor mixes and other resources required in design and production, particularly for naval systems, as well as the application of organizational theory to improve acquisition policy.
- Cost analysis, focused on the changing trends in the costs of weapon systems and the sources of cost growth in acquisition programs.

Distribution Statement A: Approved for public release; distribution is unlimited

- Intelligence policy and intelligence analysis, including related C3I issues.
- Emerging technologies and methods for intelligence gathering, including remote sensing, foreign signals, and human intelligence.
- Analysis of risks and their management.
- Analyses of diverse key defense topics enabled by the application of advanced social-science methods and expertise not typically employed in defense studies.

RAND-Project AIR FORCE

- The Strategy and Doctrine Program provides research and analysis to help the U.S. Air Force understand new challenges in the areas of emerging or evolving threats; changes in the character, conduct, and modes of warfare; and new directions in the strategies and policies of the United States, its allies, and its potential adversaries. Studies in the program are conducted using an interdisciplinary mix of functional knowledge in strategy, force planning, joint operations, and regional expertise.
- The Force Modernization and Employment Program (formerly the Aerospace Force Development Program) conducts research to evaluate the capabilities of air, space and cyberspace forces to accomplish military tasks, and develops new concepts to enhance these capabilities. This research includes assessing alternative modernization strategies to provide the highest priority capabilities to the nation effectively and affordably. The overall focus of the program is to suggest modernization and organizational priorities for achieving an effective, flexible, and responsive force for the 21st century.
- The Manpower, Personnel, and Training Program's research scope includes all aspects of defining, developing, and sustaining military and civilian workforces in the active duty and reserve components. Studies aim to help the Air Force anticipate changes and create plans and programs that adapt to shifts in operational requirements, technologies, basing, demographics, and economic conditions. Research on requirements may address organizational design, peacetime and wartime requirements, occupational contents and boundaries, competencies, and composition of the workforce. Research may also identify and evaluate potential changes in policies and practices that govern workforce development, management, readiness through recruiting, education, training, assignment, retention, cross flows between occupations and components, deployment, career progression, promotion, and separation. Projects may also address compensation, culture, diversity, sustainment programs, and other related topics.
- The Resource Management Program analyzes policies and practices in the areas of combat support; wartime readiness; weapon system acquisition and cost estimating;

Distribution Statement A: Approved for public release; distribution is unlimited

planning, programming, and budgeting; outsourcing and contracting; the industrial base; infrastructure; and energy. The goal of this program is to maximize the Air Force's operational effectiveness in a resource-constrained environment. In seeking cost-effective solutions for the Air Force's use of scarce resources in carrying out its mission, the program seeks to develop methods, models, and analyses that link resources (inputs) to capabilities (outputs); identify tradeoffs among options; consider capital, labor, and process changes together; take a multi-year view of problems and solutions; and maintain a global perspective.

APPENDIX C

DOE-sponsored FFRDCs and POCs

DOE Laboratory	State	POC
Ames Laboratory	Iowa	Debra Covey (515) 294-1048 covey@ameslab.gov
Argonne National Laboratory	Illinois	Cindy Wlodarski (630) 252-7694 weso@anl.gov
Brookhaven National Laboratory	New York	Mike Furey (631) 344-2103
Fermi National Accelerator Laboratory	Illinois	Gary Leonard (630) 840-2719
Idaho National Laboratory	Idaho	Lance Lacroix (208) 526-9799 lacroill@id.doe.gov
Lawrence Berkeley National Laboratory	California	510-486-4000 -- front office
Lawrence Livermore National Laboratory (NNSA)	California	David Brown (925) 424-2550 brown247@llnl.gov
Los Alamos National Laboratory (NNSA)	New Mexico	http://www.lanl.gov
National Renewable Energy Laboratory	Colorado	Jennifer Schofield (303) 384-7424 jennifer.schofield@nrel.gov
Oak Ridge Institute for Science and Education	Tennessee	Richard Salkeld (865) 241-2680 Richard.Salkeld@orise.orau.gov
Oak Ridge National Laboratory	Tennessee	David W. Bradford (865) 574-9798 bradforddw@ornl.gov
Pacific Northwest National Laboratory	Washington	Genice Madera (509) 372-4010
Princeton Plasma Physics Laboratory	New Jersey	Ed Winkler (609) 243-2218 ewinkler@pppl.gov
Radiological and Environmental Sciences Laboratory	Idaho	http://www.inl.gov/res/
Sandia National Laboratories (NNSA)	New Mexico	(505)284-2001
Savannah River National Laboratory (NNSA)	South Carolina	Wendolyn Holland (803) 725-8087 wendolyn.holland@srnl.gov
SLAC National Accelerator Laboratory	California	(650) 926-3300
Thomas Jefferson National Accelerator Facility	Virginia	http://www.jlab.org/div_dept/admin/business/contact_list.html