ANNOUNCEMENT
San Diego Advanced Defense Technologies Cluster

Background

On September 20, 2010 the U.S. Small Business Administration (SBA) announced the award of $600,000 to fund the San Diego Advanced Defense Technologies (SDADT) Cluster Initiative to advance the competitiveness of the San Diego defense industry. San Diego State University Research Foundation (SDSURF) is the recipient of SBA award and program manager. The goal of this ambitious program is to create new opportunities for local small businesses engaged in research and development for cyber security, autonomous systems and advanced defense systems. The SDADT team will provide customized professional business support and services to help small innovative companies expand their business into the defense marketplace.

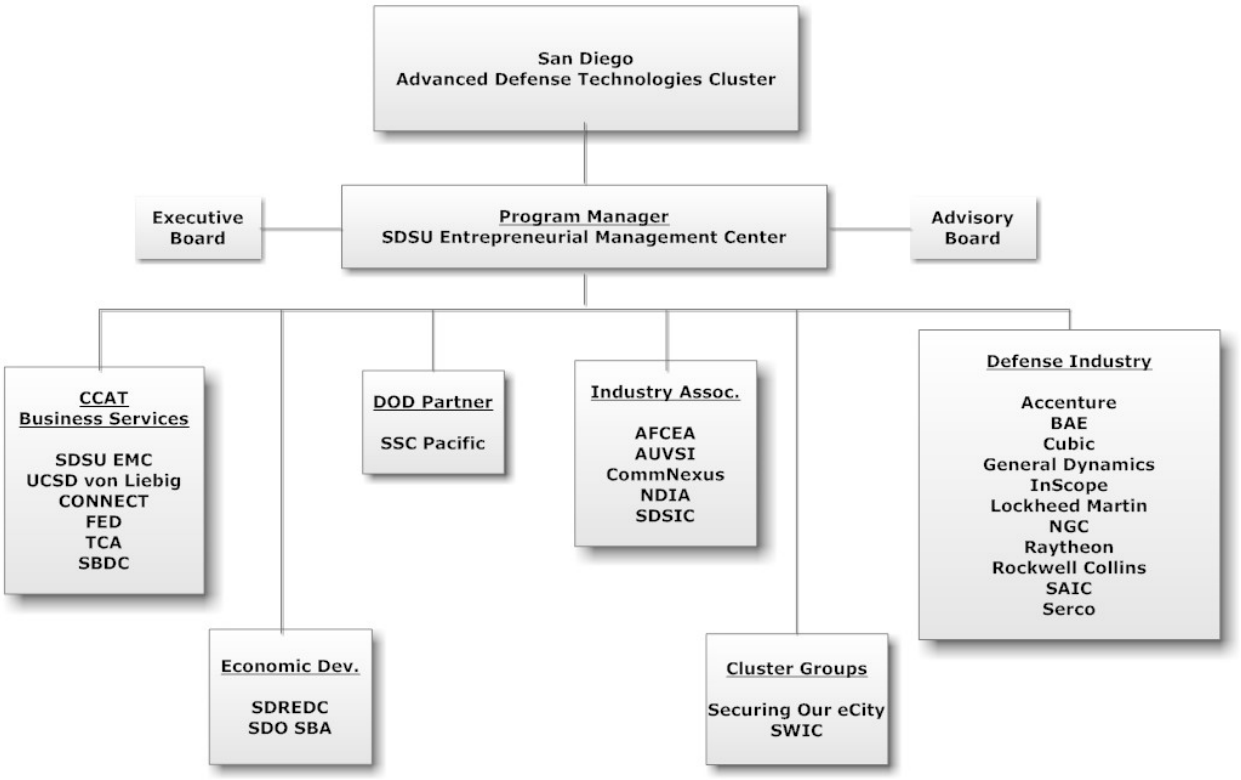
SDSURF was one of ten organizations throughout the nation to receive funding for regional economic development and job creation efforts. Only three of these awards, including the one issued to SDSURF, were for Advanced Defense Technologies. It is the intent of this new initiative to assist qualified small companies based in the San Diego region to become more competitive and to help bring their technologies to the defense marketplace.

Organization

The SDADT was created from the bottom-up and brings together a public-private partnership of major regional institutions and industry to assist small companies in matching innovative technologies to defense needs while creating new job growth and regional economic benefits.

The cluster leverages many of the existing industry associations, which in effect are mini-clusters that exist to promote objectives of interest to its membership. Across all of these, however, are several common objectives, not the least of which is development and sustainment of a vibrant economy in the San Diego region. Joining this group are the regions academic institutions, local government agencies, and federal agencies including representative organizations from the Department of Defense and Small Business Administration. Equally important to the success of the cluster initiative are the representatives from entrepreneurship organizations, economic development councils, and defense industry prime contractors. Together, these organizations help the SDADT to bring unprecedented new opportunities for the region's small companies engaged in defense technologies research and development.

The chart on the next page is the organizational representation of the SDADT included in the proposal to the SBA. It identifies the key participants representing both public and private organizations, institutions, and industries, as well as SPAWAR Systems Center Pacific as the lead Department of Defense organization.



Services

The SDADT Custer management team and its partners and stakeholders, collectively, have established training, education, consulting, and other key business development resources and relationships with additional regional organizations (law firms, federal agencies, etc.) to meet the needs of the small businesses in the Cluster. All are prepared and committed to provide key services to support the development and growth of small businesses in the SDADT Cluster region. For example, the following represent the types of services, not all inclusive, which will be offered to small businesses:

- Business Training/Counseling/Mentoring: Based on assessment of a small company's business plan, model, strategy, and management team, business development training, counseling, mentoring, and other services will be provided by the SDSU Entrepreneurial Management Center (EMC) with support from CONNECT, Tech Coast Angels, Small Business Development Centers, and other Cluster resources.
- Technology Commercialization Support: These services include market research studies and strategic planning, including technology transfer (licensing support). SDSU EMC, Foundation for Enterprise Development (FED), and CONNECT are lead providers: for example, Market Studies to identify viable markets; market characteristics and trends, potential risks and barriers to entry will be overseen by SDSU EMC using teams of faculty/entrepreneurs and graduate students. FED will provide workshops for marketing in DoD, CONNECT will provide entrepreneurs-in-residence as technical and business advisors. Industry primes and others will provide support.

- Venture Funding: Identification of capital requirements and exposure to investment opportunities will be provided by CONNECT and Tech Coast Angels. SDSU EMC in addition to the CCAT network of angel and venture capital organizations are resources that will be used to meet this small business need.
- Intellectual Property and Export Assistance: Training programs and seminars will be provided to help small companies in the development of Intellectual Property protection strategies, licensing and partnership agreements. SDSU Research Foundation with its Tech Transfer Office and CONNECT will assist in providing or arranging for IP and Export training from Department of Commerce, local law firms, and other providers.
- Entrepreneurs-in-Residence/Mentors: Experienced business professionals will help take the small business through the transition and commercialization process. CONNECT, Tech Coast Angels, and SDSU Entrepreneurial Management Center have extensive resources to draw from as needed to help cluster small businesses.
- Springboards: Small businesses will be selected for participation in "SpringBoards" through the CONNECT organization which prepares the companies for presentations to investment groups and potential strategic partners.
- Special Workshops: Working in the Department of Defense arena is a challenge for even the most experienced company. The Foundation for Enterprise Development offers a series of half-day workshops for companies seeking information on how to partner with DoD primes, contract and procurement in the DoD sector, and DoD R&D Transition Support.

Application (Request for Information)

Working with SSC Pacific, prime contractors, and other members of the SDADT Cluster, the project team reviewed DoD requirements documents and other sources to define a set of priority technology requirements in the focus areas of autonomous systems and cyber security. This priority list of needs will be used in this "Open" Application opportunity (Request for Information), the objectives of which are to: 1) identify and select viable technologies (components, products or systems) in small businesses within the Cluster region that meet one or more of these priority requirements, and 2) define a set of customized business development services for these small businesses to facilitate advancement of the technology to the defense marketplace.

Technology Requirements

1. Cyber Security

The purpose of this topic is to facilitate the discovery and deployment of advances in technology that address DoD requirements to provide more secure cyber systems through the introduction of new technologies that help in the move from **reactive** to **predictive** to **adaptive** and assist in providing **persistent situation awareness** that facilitate self-protections through:

- Monitoring systems and automatically improving system defense,
- Using sensor technologies to anticipate problems before they occur, and

- Identifying cyber issues as they occur and taking steps to avoid them or reduce their consequences

Specific topics include:

(a) Enhance Cyber Security Attack Protection, Prevention, and Preemption
Includes: providing system wide capabilities to intercept malicious attacks and systems that will have the capability to identify and preempt unknown and novel attacks

(b) Enhance Cyber Security Situational Awareness
Includes autonomous systems that can help visualize and understand the current state of the IT infrastructure as well as the defensive posture of the IT environment

(c) Enhance Automated Attack Detection, Warning and Response
Includes autonomous responses to elicit warnings and defensive actions at the time of attack; provide autonomous system countermeasures; and provide autonomous systems that are preemptive rather than reactive

(d) Enhance Recover and Reconstitution
Includes autonomous systems that in the aftermath of a cyber attack can restore the functionality and availability of network, systems, and data; self healing and self restoring systems; damage assessment tools; modeling, simulation and visualization of the future network environment; computer and network forensic capabilities.

2. Autonomous Systems

The purpose of this topic is to provide capabilities for intelligent behavior that can perform complex missions in challenging environments with reduced need for human intervention, while promoting effective man-machine interaction.

Specific topics include:

(a) Improved Environmental Perception
Object/terrain and activity understanding including maneuvering systems in dynamic environments with wide range of sensing capabilities; assessing intent of other human machine agents; automated fusion and conversion of data into information, development of flexible, coherent and extensible architecture for representation of the environment by unmanned systems

(b) Human/Unmanned System Interaction and Collaboration
Includes more natural modes of interaction and cognitively compatible architectures, ability to understand intent and actions of human team members, adversaries, and bystanders, trading off levels of autonomy dynamically while ensuring appropriate levels of trust in the automation

(c) Scalable Teaming of Unmanned Systems
Includes scalable algorithms for heterogeneous teams, understanding capabilities and effects based on coordinated action of large numbers of entities and the benefits for the warfighter, airspace/waterspace/ground traffic management, learning and situational awareness in teams, coalitions, swarms, etc.

Application Process:

If your company is a small business (less than 499 employees) located in the County of San Diego and engaged in the research and development of advanced technology in the areas of cyber security and autonomous systems, we would like to invite you to apply for participation in this exciting new regional opportunity. Application information, instructions, and forms may be downloaded at www.ccatsandiego.org/SDADT_sol.html.

In particular, this Application (RFI) consists of three sections:

1. Company Profile: The intent of this section is to gather key publicly available and non-proprietary information about the company such as:
   - *Company Personnel:* Do the company's management and development teams have a proven track record in connection with the development of similar technologies? Have they worked together on the proposed technology solution or is the team newly formed?
   - *Transition Experience:* Has the company successfully brought one or more technology products to a market place? If so, did this include the defense marketplace?
   - *Business Model:* What is the company's business model? Is it an engineering/research firm or technology integrator? Does it have manufacturing and distribution capabilities?
   - *Resources:* Does the company have partnerships or collaborative agreements to be used in promoting this technology? Are these relationships formalized?
   - *Company Stats:* number of employees, annual revenues, number of products, etc.
2. Technology Profile: The intent here is to determine how the company's technology relates to one or more of the topic areas, its maturity, stage of development, intended application; for example:
   - *Technical Merit:* What is the stage of development (e.g., prototype, product, etc)? Has it been tested or used in a relevant application? Is the proposed technical application viable? Is the technology novel and non-trivial? What hurdles need to be overcome?
   - *Value Proposition:* To what degree does the technology demonstrate the potential for a superior solution to a significant problem? To what degree does the product/system represent at least an 80% solution to the overall capability gap?
   - *Transition Potential:* Has an appropriate DoD market been identified? Does the company have a plan to commercialize the technology into this market? What barriers exist commercialization?
   - *Market Cost:* What is the projected unit/service cost of the technology? Will the market accept this price?
   - *IP Protection:* Is there intellectual property? Is it adequate to sustain a competitive advantage? Is the technology protected under US or foreign patent law? If not, how is the technology protected from other competitors?

3. Commercialization Needs: The intent of this section is simply to have the company identify what it perceives to be its critical needs or short comings that limit or restrict the transition of its technology into the defense marketplace. These needs may include:
   - *Funding*: Is the company seeking additional R&D funds through government grants/contracts or private investment sources?
   - *Business*: Is the company seeking a partnership, licensee, etc? Do they need consulting support for business development?
   - *Marketing*: Does the company have a marketing or technology transition plan? Do they need marketing assistance?

The information provided via the application (RFI) process will help us understand your company, its technology, and what your interests and needs are. We intend to review your information to validate the relevance of your technology to one or more of the DoD defined requirements and ascertain how the SDADT program can best assist your company in moving this technology to the defense marketplace.

Next Steps

If you have a technology or technologies that address one or more of the topics listed above, please go to www.ccatsandiego.org/SDADT_sol.html to download the application instructions and forms. Applications are to be submitted electronically to the SDADT team via email at ccat@foundation.sdsu.edu.

For further information regarding this opportunity, you may contact Tom Sheffer, SDADT Program Coordinator via email at tsheffer@foundation.sdsu.edu.