



## DIUx Reports First Quarterly Results

### *DIUx Background*

In April 2015, Secretary of Defense Ash Carter announced the creation of Defense Innovation Unit Experimental (DIUx), a signature part of the Department of Defense's (DoD's) outreach to America's innovative technology companies. DIUx is a first-of-its-kind unit for DoD, staffed by civilian, active duty, reserve and contractor personnel with the ultimate goal of accelerating innovation to our men and women in uniform.

With offices in the heart of Silicon Valley and Boston, and a presence in Austin, DIUx serves as a bridge between those in the U.S. military executing on some of our nation's toughest security challenges and companies operating at the cutting edge of technology.

### *Innovating and Iterating*

On May 11, 2016, Secretary Carter announced important enhancements to DIUx that included a consolidated reporting structure, with DIUx reporting directly to the Office of the Secretary, and a leadership team comprised of partners with experience in technology, strategy, business, and management.

In an effort to build on a nationwide strategy of engaging innovators across the U.S., DIUx opened a presence in Austin this September, which consists primarily of personnel from the DIUx Joint Reserve Component. Reservists, who often serve as tech industry leaders and entrepreneurs in their civilian lives, will help DIUx access leading technologies and the entrepreneurs behind them across the country.

The primary focus for DIUx's outreach activities is to identify and introduce commercial technologists to national security challenges for potential military application. In June 2016, DIUx developed and launched a streamlined contracting mechanism, the Commercial Solutions Opening (CSO), to more easily do business with commercially-focused companies. The statutory authority behind the CSO allows DIUx to mirror the contracting practices that commercial companies normally use, enabling DIUx to design projects, and negotiate payment milestones, terms and conditions, and intellectual property rights - all within 60 days.

### *DIUx Impact to Date*

DIUx is tackling some of our nation's toughest defense challenges and the team is seeking solutions in a variety of technological areas -- from autonomy, artificial intelligence and machine learning to cybersecurity and analytics -- from Silicon Valley, Boston, and across the country.

DIUx awarded 12 agreements in the fourth quarter of fiscal year 2016 (for the period ending on September 30th), for a total of \$36.3M. DIUx accounts for \$8.3M of this spend, with the remainder coming from other DoD components. For every dollar DIUx invested in these projects, other DoD

customers contributed an additional \$3. On average, DIUx awarded these agreements within 60 days of receiving a company's solution brief.

**Executed (\$36.3M; \$8.3M DIUx, \$28M DoD Customers)**

*Endpoint Querying Solution (\$12.736M). Customer: DoD CIO/Army. Company: Tanium (Emeryville, CA).* The DoD owns and operates one of the world's largest legacy enterprise networks. The challenge of maintaining current situational awareness of all machines on the network to include patching levels, configurations, and the ability to modify them directly impacts the department's ability to reduce the computer network attack surface presented to adversaries. DIUx is working with Tanium to provide near real-time visibility and control of network endpoints that scales to support the size and complexity of DoD networks. The end result will provide our cyber defense operators the ability to monitor and react to the rapidly changing threats with confidence and speed.

*High Speed Drone Aircraft (\$12.623M). Customer: STRATCOM and Strategic Capabilities Office. Company: Composite Engineering (Roseville, CA)/Kratos (San Diego, CA) and three other companies.* DoD is exploring the use of high speed drones in either fully autonomous or semi-autonomous roles to support fourth and fifth generation fighter aircraft. To enable this concept development, the DoD needs to rapidly integrate and test both DoD and commercial capabilities onto a high-speed drone testbed. DIUx, in coordination with other service and joint organizations, will work with commercial drone vendors to ensure that a high speed drone can be used "as a service" for testing and experimentation.

*Game Theoretic Sandbox (\$5.8M). Customer: DoD CIO. Company: Improbable (London, UK).* DoD traditionally uses war games to map, plan and execute dynamic scenarios to inform plans. Through Improbable, complex simulations can be built and run on thousands of virtual machines to leverage massive amounts of data. DoD is interested in prototyping these commercial technologies and data applications to build a scalable simulation sandbox for real-world event modeling and planning. This technology can provide finely detailed re-creation of events

*Unmanned Maritime Surface Vehicle (\$1.515M). Customer: DoD. Company: Saildrone (Alameda, CA).* Collecting scientific data and maritime information at sea is expensive and challenging in many areas of the world. Manned vessels are expensive and often cannot be in enough places at once or cannot reach certain areas because of hazards and threats. DIUx is investing in wind powered autonomous sailing platforms that operate on the ocean's surface, provide persistent maritime surveillance and reconnaissance for the Navy, and navigate the ocean autonomously without the need for manned crews and human pilots.

*Autonomous Indoor Tactical Drone (\$1M). Customer: DoD. Company: Shield AI (San Diego, CA/Boston, MA).* US forces are required to fight adversaries in tight, dangerous quarters like caves, tunnel complexes, ships under way, and enemy strongholds. These environments are often owned by the enemy, and our soldiers are often forced to enter these structures without a complete picture of the lethal threats. DIUx is investing in small tactical handheld quadcopters to solve this problem. These unmanned aerial vehicles (UAVs), designed specifically to fly indoors rather than out, can autonomously speed through built and natural structures, mapping out their interiors and identifying threats without the need for a human pilot or a global positioning system (GPS).

*Knowledge Management (\$500K). Customer: DoD. Company: Zeuss (San Francisco, CA)* DoD organizations and military units are overwhelmed with the incredible pace that data is being generated internally along with constant staff turnover. DIUx is prototyping a Silicon Valley startup's knowledge management and enterprise search platform. Zeuss aggregates communications and disparate data from across the organization, illuminates key relationships and allows people to find what they are looking for by presenting data in a way that people natively understand it.

*Network Change Detection and Processing (\$500K). Customer: DISA. Company: Qadium (San Francisco, CA).* DoD networks are constantly probed by both adversary militaries and foreign intelligence services. DoD must understand how our networks look to adversaries, how DoD network assets can potentially be exploited by adversaries, and how we can automatically detect vulnerabilities and confirm their remediation. DIUx is working with Qadium, which continually indexes all devices connected to the public Internet, enabling organizations to understand their networks and how they relate to the broader world. This will allow DoD to detect and manage these vulnerabilities, addressing previously unseen security risks by developing comprehensive network footprints of their organizations.

*Problem Curation, Translation, and Research (\$500K). Customer: DIUx and DIA. Company: BMNT Partners (HQ in Palo Alto and an office in LA).* DoD personnel often lack the tools and processes to adequately understand rapidly evolving problems. DIUx is developing a new mechanism to refine and validate problems before engaging the traditional acquisition process. DIUx will translate these problems into commercial language, situations, and applications. By bridging the language gap, DIUx dramatically expands the number of non-traditional companies who are aware of opportunities to bring their innovative solutions to bear on DoD problems.

*Endpoint Security (\$441K; all DIUx). Customer: DOD. Company: Bromium (Cupertino, CA).* The DoD requires an end-point security solution capable of protecting individual endpoints from known and unknown malware threats that are delivered across the network, with minimal impact to a user and the end-point's system performance. DIUx is piloting Bromium's technology, which uses micro-virtualization to hardware-isolate untrusted user-initiated tasks and to protect critical OS services.

*Automated Textual Analysis and Content Curation (\$357K). Customer: Army, SOCOM. Company: Quid (San Francisco, CA).* The DoD lacks the ability to rapidly analyze, visualize, and derive insight from news sources, blogs, social media, patent databases, scientific/academic publications, and other large volumes of text-based content on mission critical intelligence, operational, and national security topics. DIUx is working with Quid to leverage an algorithmic approach to expand a user's ability to comprehend massive amounts of information on any given topic. Interactive visual maps depicting this information make it easier to navigate and determine relationships through the world's open-source and proprietary intelligence.

*Wireless, Hands-Free, Ears-Free, Communicator (\$210K). Customer: Air National Guard. Company: Sonitus (San Mateo, California).* Operators across DoD frequently need to communicate with each other in the midst of operations while maintaining situational awareness. Existing communication tools - either through traditional radios or headsets - add weight to a warfighter's load, occupy their hands, or restrict visibility. DIUx is adapting commercially available hands-free, ears-free, two-way removable communications devices placed in the mouth that integrate wirelessly to radios and offer clear communications in high noise environments.

*Strength and Skill Training Enhancement (\$153K). Customer: DoD. Company: Halo Neuroscience (San Francisco, CA).* Warfighters constantly train to improve their skills. DIUx awarded its first contract to Halo Neuroscience in just 31 days. Halo Sport is a head-worn stimulation system, similar to a pair of headphones, that increases the brain's natural ability to adapt to training. Halo Sport headsets will be used by special ops teams, who will work with Halo to assess the effects of this neurostimulation and evaluate improvements in tactical motor skills, such as marksmanship, close-quarters-combat, and overall strength training.

## **Project Pipeline**

Below is a selection of additional DIUx projects in progress.

*Multifactor Authentication.* The DoD's complex data access environment and the evolving threat landscape requires device-agnostic agility, with strong identification and authentication, even when devices or credentials are lost. DIUx will invest in one or more multi-factor authentication technologies to prototype solutions to this problem. Industry has recognized many of the challenges associated with legacy, single-factor authentication and identification systems, and a number of commercial solutions exist to reduce the risk of unauthorized data access and loss while increasing agility and integration.

*Persistent Heavy Lift Drone.* DoD spends millions of dollars on contractors to build facilities and conduct logistics operations in high threat environments. Today, building Forward Operating Bases and other secure sites require large amounts of transportation, coordination, security, contracting, and other efforts to build bases in austere and dangerous environments. DIUx is exploring the use of drones with heavy lifting capabilities that will move and emplace large equipment and material that currently require manned construction vehicles and heavy machines on the ground.

*Cyber Protection Toolkits.* DoD cyber incident response teams conduct tactical network analysis in all environments across the world. DoD is seeking software solutions for a deployable cyber incident response tool kit that offer the following capabilities: discovery, identification, containment, eradication, recovery, information sharing, and capturing lessons learned. This evaluation will nest within a larger hardware and infrastructure evaluation being conducted by CYBERCOM in fiscal year 2017.

*Micro-satellite and Advanced Analytics.* A growing number of firms in the U.S. ingest large volumes of satellite images and convert these datasets into insights through the use of advanced analytics and machine learning. DoD is considering leveraging commercial-based, micro-satellite technology capable of observing during the day, night, and all-weather conditions, such as synthetic aperture radar satellite technology, to complement existing capabilities. Resulting imagery produced from the micro-satellite payload would be ingested into a cloud-based computing architecture for subsequent machine learning and object detection analysis.