Missile Defense Agency

Office of Small Business Programs

Quarterly Newsletter | January 2016

Volume 18 - Issue 1

IN THIS ISSUE

2 Message from the Deputy

3 Safeguarding MDA Information

4 3 MDA Mentor-Protégé's Win Prestigious Nunn-Perry Award

6 MiDAESS (Full and Open)

7 MiDAESS (Small Business Set-Aside)

8 MDA Celebrates 5 New Mentor-Protégé Relationships

10 Outreach Efforts to Provide Small Business Commmunity with Cybersecurity

- How do the New DoD Cybersecurity Requirements Affect MDA's Future Market Research
- Cybersecurity and Mentor-Protégé Program

11 eSBIE Registration

12 Outreach Calendar

NEXT ISSUE

April 2016

Message from the Director,

Lee Rosenberg

As you are probably aware, cybersecurity is a big deal these days. Just look at the news and you will find all kinds of horror stories regarding sensitive information obtained through hacking of both Government and Civilian information systems. If you have been a victim, as have I and millions of other Government employees, you know that sinking feeling that you get knowing that your personally identifiable information is floating around out in cyber space, possibly in the hands of some who would do us harm by using that data. Now, look at a much bigger picture and think about the defense of our nation and the manner in which we go about provisioning ourselves for that defense. There is no doubt that all who are involved in that process are heavily dependent on the use of computers and electronic data to accomplish their work. As we transition to that cyber space to conduct business and to pass information, we bring with us unique security issues, which didn't exist 20 years ago. The Department of Defense (DoD) is beginning to realize the extent of our vulnerabilities in this cyber world, and is taking steps to protect our information from bad actors around the world, who would steal that data to increase their military capabilities while doing harm to ours. A lot of the data that needs protecting is not necessarily classified data. For classified data, we already have fairly robust systems to protect its unauthorized disclosure. The Department is now realizing that there is a plethora of data that is not classified, but that can provide potential adversaries with a wealth of information about our operations and systems. That brings me to the theme of this newsletter, and the information that you need to be aware of moving forward as a Defense contractor.

In August 2015, the DoD issued an interim ruling revising DFAR 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting and introduced two new mandatory clauses: 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls; and 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information. MDA has begun implementing these on all new solicitations. These clauses will have significant impact on you as an MDA contractor or subcontractor. DFARS 252.204-7009 and DFARS 252.204-7012 are required to flow down by the prime through all tiers of subcontracting. That means if you are a lower tier subcontractor, you are just as affected by the clauses as the prime contractor.

So, what do these clauses do? DFARS 252-204-7012 requires Contractors (and Subcontractors due to the flow down requirements) to protect any DoD information provided to the contractor or collected, developed, received, transmitted, used, or stored by or on behalf of the Contractor in support of performance of a Government contract. It now includes commercial goods as well. Protected information falls into one of the following categories:

(a) *Controlled technical information.*

(b) *Critical information* (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively, so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(c) *Export control.* Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(d) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies (e.g., privacy, proprietary business information).

These clauses also contain cyber incident reporting requirements, with which you must comply, and

Continued on Page 2

New Cybersecurity Regulations

Genna Wooten

The Department of Defense (DoD) decided to implement new cybersecurity regulations back in August of 2015, following the Office of Personnel Management's (OPM) breach of Data that impacted the Personal Identifiable Information (PII) of over 21 million government employees and contractors. The DoD stated that it decided to implement these rules because of the urgent need to guard information, understand the scope of cyber-attacks against contractors, and reduce the vulnerability of cloud computing attacks.

The new regulations require, among other things, that prime contractors and their subs employ "Adequate Security" and implement the security controls based on the National Institute of Standards Special Publication, titled "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations". Contractors are obligated to report, within 72 hours of discovery, any cyber incident that affects the covered contractor's information system. The DoD understands that this can be a significant cost to Small Businesses, so we have published a list of resources on our website at **www.mda.mil**.

Outside of the new DoD Cybersecurity requirements, here are 9 Cyber Security Tips for Small Businesses to help keep your data safe from cyber criminals:

1. Use the FCC's Small Biz Cyber Planner to create a cybersecurity plan.

The Small Business Cyber Planner, by the FCC (**https://www.fcc.gov/general/cybersecurity-small-business**), is valuable for businesses that lack the resources to hire a dedicated staff member to protect themselves from cyber threats. The tool walks users through a series of questions, to determine which cybersecurity strategies should be included in the planning guide, and generates a customized PDF that serves as a cybersecurity strategy template.

2. Establish cybersecurity rules for your employees.

Establish rules of behavior describing how to handle and protect personally identifiable information, and clearly details the penalties for violating cybersecurity policies.

3. Protect against viruses, spyware, and other malicious code.

Install, use, and regularly update antivirus and antispyware software on every computer used in your business. Such software is readily available online from a variety of vendors.

4. Educate employees about safe social media practices.

Depending on what your business does, employees might be introducing competitors to sensitive details about your firm's internal business. Employees should be taught how to post online in a way that does not reveal any trade secrets to the public or competing businesses. This type of safe social networking can help avoid serious risks to your business.

5. Manage and assess risk.

Ask yourself, "What do we have to protect? And, what would impact our business the most?" Cyber-criminals often use lesser-protected, small businesses as a bridge to attack larger firms with which they have a relationship. This can make unprepared small firms a less attractive business partner in the future, blocking potentially lucrative business deals.

6. Download and install software updates when they are available.

All software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install such updates automatically.

7. Make backup copies of important business data and information.

Regularly backup the data on every computer used in your business. Critical data includes word processing documents, spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files; also, backup data automatically, if possible, or at least weekly.

8. Control physical access to computers and network components.

Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft, so make sure they are stored and locked up when unattended.

9. Secure Wi-Fi networks.

If you have a Wi-Fi network for your home business, make sure it is secure and hidden. To hide your Wi-Fi network, configure your wireless access point, or router, so that it does not broadcast the network name, known as the Service Set Identifier (SSID). In addition, make sure that passwords are required for access. It is also critical to change the administrative password that was on the device when it was first purchased.

Continued from Page 1...

which may include reporting on compromises of proprietary data.

DFARS 252.204-7008 requires Contractors to comply with the security controls outlined in National Institute of Standards and Technology (NIST) Special Publication 800-171. You should be aware that there are new requirements in this publication that may cause additional capital investment in your information technology systems, and new training requirements to comply with the new requirements. There is a provision in the clause for you to put forward alternate methods for complying, but those must be approved by the DoD Chief Information Officer (CIO).

DFARS 252.204-7009 requires the protection of the cyber incident information that is disclosed and speaks to the obligations for non-disclosure of the information by third-parties, along with the possible civil and criminal penalties associated with the unauthorized disclosure. All in all, these new cybersecurity requirements may have a significant impact on you both financially, and in your business operations. You should become very familiar with all requirements. Now is the time to assess your operations and information technology infrastructure, to insure they comply with the new requirements. Now is also the time to implement the changes necessary to bring your business into compliance, if you plan to stay in the DoD marketplace.

As I mentioned earlier, cybersecurity is a big deal with the DoD. We are seeing that importance across all DoD operations, now including the procurement of goods and services to support our warfighters. In this edition of our newsletter, you will find helpful advice and information to assist you in your efforts. I urge you not to wait until the last minute to get your businesses into compliance, but assess your situation, now. Take those measures necessary to protect our valuable defense information from falling into the wrong hands.

Safeguarding MDA Information

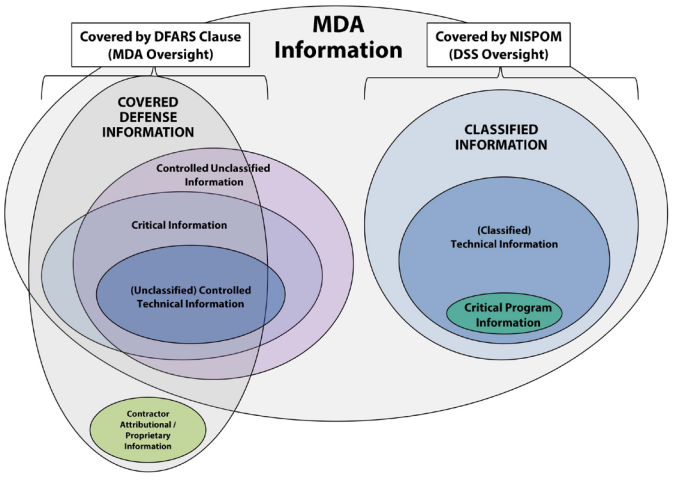
Jerrol Sullivan

Small businesses currently performing on MDA contracts as prime or subcontractors, and those seeking to do business with MDA in the future, must be aware of the implications of the August 26th, 2015 DoD interim ruling which revised DFARS 252.204.7012 to establish guidance for safeguarding unclassified DoD information. This interim rule is effective immediately, and is becoming increasing more prevalent in Missile Defense Agency (MDA) solicitations. This article intends to clarify the changes to this clause, and highlight MDA's oversight of the types of information handled by MDA contractors and requires protection. The following are highlights of the DFARS 252.204.7012 clause and the update:

- **DFARS Clause 252.204-7012, "Safeguarding Unclassified Controlled Technical Information", Published November 18, 2013**
  - Affects all contracts that contain, or will contain unclassified controlled technical information (UCTI)
  - Does not cover all Controlled Unclassified Information (CUI)…e.g., FOUO
- **DFARS Clause 252.204-7012: "Safeguarding Covered Defense Information and Cyber Incident Reporting", 26 Aug 2015 (updated)**
  - Covers all defense Information to include Controlled Unclassified Information (CUI)…e.g., FOUO
  - Focuses more on technical controls (for industry as) established in National Institute of Standards and Technology (NIST) standard publication NIST SP 800-171
  - Flows to all subcontractors and suppliers, regardless of size, and to all tiers of the supply chain
  - Requires that all Cyber incidents be reported via the DoD Defense Industrial Base (DIB) Cybersecurity Program portal (**http://dibnet.dod.mil**) within 72 hours of detection
  - Requires that contractors support DoD damage assessments
  - Requires contractors to identify deviations from NIST implementation guidance during contract proposals (DFARS provision 252.204-7008)

In summary, protection of MDA information is critical to preserving the intellectual property and competitive capabilities of the MDA industrial base, and the technological superiority of fielded Ballistic Missile Defense Systems (BMDS). MDA contractors and subcontractors, regardless of size or tier, within the BMDS supply chain, must provide adequate safeguards for MDA information by actively managing the Cybersecurity posture of their people, systems, and networks. Prime Contractors are responsible to report Cybersecurity incidents involving MDA information, both directly to MDA and via Defense Industrial Base Network (DIBNet), then work with MDA to assess any damage.

Types of Information for MDA Contractors



* Handled as CUI within DoD Defense Security Service (DSS) National Industrial Security Program Operating Manual (NISPOM) (DoD. 5220.22-M)

3 MDA Mentor-Protégé's Win Prestigious Nunn-Perry Award

Ruth Dailey

Several Missile Defense Agency (MDA) teams with Huntsville ties were recently named recipients of the Nunn-Perry Award, for their involvement in the U.S. Department of Defense's Mentor-Protégé Program. The Nunn-Perry Award was first awarded in 1995, and is named in honor of former Senator Sam Nunn and former Secretary of Defense William Perry. The award is given to recognize outstanding mentor-protégé teams formed under the auspices of the DoD Mentor-Protégé Program.

Announced by the DoD's Office of Small Business Programs, the winning Mentor-Protégé teams for 2015 are the teams of Northrop Grumman of Huntsville, Alabama, and Davidson Technologies, Inc. of Huntsville, Alabama; Raytheon Missile Systems of Tucson, Arizona, and Mentis Sciences of Manchester, New Hampshire; and Orbital ATK of Tucson, Arizona and Martinez and Turek, Inc. of Rialto, California.

The winners will be honored in the Spring of 2016. A total of 10 U.S. teams will receive the award, which honors companies that excel in commitment, technical assistance, quality, and economic development of small businesses.

Davidson Technologies, Inc. (DTI), a Woman-Owned Small Business, has made a strong commitment to the Department of Defense (DoD) Mentor-Protégé program by investing $171,571 in direct and indirect labor costs. DTI has gained more visibility from industry partners after Northrup Grumman Corporation's (NGC) guidance on marketing efforts. NGC has compiled strategic analysis of DTI's current capabilities and technical involvements, yielding focused capture plans. To date, DTI, jointly with NGC, is awaiting the award of four (4) programs. More importantly, DTI now has the technical, management, and information technology (IT) infrastructure in place to better support prime contract acquisitions. DTI has also bolstered success in some related areas, through investment of its own discretionary funds in innovative Cyber and IT solutions. In addition to DTI's commitments to grow, collaborate, and innovate in related areas, the success of the DoD Mentor-Protégé agreement can also be attributed to NGC's support and the breadth of contribution from across the company. Agreement accomplishments include the following:

- Subcontract of over $42(M) to DTI with long-term agreements to continue this work
- Successful implementation of DTI's IT infrastructure with innovative cybersecurity platforms
- Strategic planning, value proposition, and market analysis to solidify focused path for continued growth
- Successful ISO 9001:2008 certification as an added strength to DTI's low risk small business credentials
- Successful review of corporate policies and human resources procedures and policies
- Provision of support letters to DTI for two (2) Missile Defense Agency Small Business Innovation Research (SBIR) proposals which contributed to two (2) Phase I awards

The Mentis Sciences (MSI), Raytheon (RTN), and Bethune–Cookman University (B-CU) are teamed in an active and innovative MP agreement and opportunity. Mentis Sciences, Inc. is a small HUBZone engineering firm, located in the heart of Manchester's historic mill district. Since inception, Mentis has grown from 2 employees to some 35 employees, and is developing unique composite materials and applications for missile interceptor radomes, nose cones, windows, prosthetics, lightweight UAV's, and other diverse composite applications for the DoD and Aerospace Industries. Mentis is known for the use of textile braiding for production of radomes, with much of this technology development funded through SBIRs and research activities for the various DoD customers. Using SBIR funding, Mentis has developed unique composite material formulations, applicable for applications in high stress, high temperature environments that can transition to DoD products.

RTN and MSI have established a general understanding and collaborative working relationship that centered on process improvement, strategic growth, and enhancement of their diverse capabilities in the aerospace and defense space and commercial industries. The team's initial accomplishments are the result of the use of a thorough needs assessment and strategic planning session (with MSI leadership, RTN business leaders and B-CU). To this end, Mentis is transitioning into a more agile production facility, flawlessly achieving AS9100 Rev C. Quality Certification, and are installing and integrating the production enterprise requirements closed loop system into their company business infrastructure. Agreement accomplishments include the following:

Continued from Page 4...

- 50% increase in square feet of manufacturing space with added agile aspects for growth in production
- Over 1000% increase from baseline for total performed on Prime contracts supporting DoD
- Over 2000% increase from baseline for total performed on DoD subcontracts
- AS9100 2009 Rev. C Certification (achieved with no negative findings)
- Team collaboration with other small businesses and MDA for production and SBIR development
- Enterprise Requirements Planning Implementation
- Extensive community service activity through High School Intern Program and STEM Program

The Martinez and Turek (M&T) and Orbital ATK are teamed in an active and state-of-the-art MP agreement and opportunity. The Mentor Orbital ATK has a proven history of providing high-tech defense, flight, and space systems. The Protégé has earned the reputation as a quality design and manufacturing service for multiple industries. In 2011, Orbital ATK developed a close working relationship with M&T, when the protégé provided the design and build of the transporter, erector, and launch ground support system for the Antares space vehicle. The year ending September 30, 2015 the focus of the Mentor and Protégé was to improve the manufacturing processes through improvements using three key parameter indicators (KPI): Cost of Poor Quality, On Time Delivery, and Baseline vs. Actual Cost. The following technical innovation was used to facilitate the transition:

- Use, Define, Measure, Analyze, Improve, and Control principals to shift Protégé's current paradigms
- Benchmark high performance companies to determine what has allowed them to be industry leaders
- Evaluate the results, identify key differentiators observed, and define the gaps in the Protégé's use of technologies to support improvement in performance
- Use value stream mapping to determine an implementation path for applicable technologies at the Protégé through benchmarking, the Mentor and Protégé observed high performing companies were planning all aspects of the work before it was released and scheduled in manufacturing. This change gave the Protégé the ability to do the following:
  - Provide work instruction to workforce, without the need for a supervisor to micro-manage all current work
  - Provide real-time data to manage throughput and elevate bottle necks, before they occur
  - Improve information flow to the customer base

The Protégé has seen 100% growth in invoiced dollars directly from DoD, and 49% growth in DoD subcontracts over this period of performance. The Protégé accomplished this during a period of less contract and subcontract opportunities from DoD, and showed productivity gains by performing the increased workload with a slightly reduced head count.

The purpose of the Mentor-Protégé Program is to provide incentives for DoD contractors to assist small businesses in enhancing their capabilities, and to increase participation of such firms in Government and commercial contracts.

"The DoD Mentor-Protégé Program benefits the Missile Defense Agency, by fostering lasting partnerships between large business prime contractors who support the Agency and small innovative businesses that have capabilities we can use," said Rosenberg. Mentors are prime contractors who agree to promote and develop small businesses, by providing developmental assistance, designed to amplify the business success of the protégé. The Mentor-Protégé Program is designed to encourage the mentor to provide beneficial developmental assistance to the protégé.

The Mentor-Protégé Program strengthens subcontracting opportunities for small businesses and enhances contracting goal achievements for MDA. When looking at proposed Mentor-Protégé Agreements to approve, Rosenberg (MDA OSBP Director) says he is always looking for the 'Win-Win-Win.' "The wins for the large and small businesses involved are inherent to the agreement. That third win is the payoff for the Agency, based on the terms of the agreement," he said. "This return on our investment in DoD dollars is the growth in the small business industrial base supporting MDA."

Congratulations to all awardees.

MiDAESS Awards

Full and Open

Blue text indicates IDIQ Awards
Red text indicates Task Order Awards
Recompeted/Recently Awarded

Acquisition Support (Capability Group 2)

IDIQ Contract Award Date: 9/8/2010

Booz Allen Hamilton	HQ0147-10-D-0018-0003	DOB-02	1/26/15	Strategic Planning and Financial Management Support
Computer Sciences Corporation	HQ0147-10-D-0019-0004	DP-01	1/19/2013	Integration Synchronization
	HQ0147-10-D-0019-0005	DOB-03	7/25/2013	Budget Execution/Funds Control
Paradigm Technologies, Inc.	HQ0147-10-D-0020-0004	DOB-07	2/27/2013	Financial Systems Support & Integration
Odyssey Systems Consulting Group	HQ0147-10-D-0021			

Engineering Support (Capability Group 3)

IDIQ Contract Award Date: 8/30/2010

ERC, Inc.	HQ0147-10-D-0006			
Madison Research Corporation	HQ0147-10-D-0007			
Computer Sciences Corporation	HQ0147-10-D-0008-0005	DE-05	2/10/2014	Sensor Engineering
General Dynamics IT	HQ0147-10-D-0009			
Parsons	HQ0147-10-D-0010-0012	DT-02	9/26/2013	Ground Test Support
	HQ0147-10-D-0010-0016	DE-01	4/9/2015	System Engineering Integration
	HQ0147-10-D-0010-0017	DE-03	7/16/2015	Weapons and Missile Systems
	HQ0147-10-D-0010-0010	DE-07	5/30/2013	Space Portfolio Engineering
	HQ0147-10-D-0010-0013	DE-08	3/20/2014	C3BM
	HQ0147-10-D-0010-0006	DE-10	9/24/2014	M&S Engineering
	HQ0147-10-D-0010-0011	DE-11	7/16/2013	Laser (Directed Energy) System Engineering
	HQ0147-10-D-0010-0014	DT-01	5/02/2014	Flight Component and General Test Support

Infrastructure and Deployment Support (Capability Group 4)

IDIQ Contract Award Date: 6/23/2010

Computer Sciences Corporation	HQ0147-10-D-0022-0007	DPF-01	5/8/2014	Facility, Logistics, and Space Management
	HQ0147-10-D-0022-0006	DPF-03	6/3/2013	Environmental Management
General Dynamics IT	HQ0147-10-D-0023			
Parsons	HQ0147-10-D-0024-0004	DDW-01	2/15/2013	Warfighter Strategic Integration
	HQ0147-10-D-0024-0005	DDW-02	10/23/2013	Operations Support
	HQ0147-10-D-0024-0006	DPF-02	2/20/2014	Facilities Life-Cycle Management Site Activation Planning, Deployment, and Integration
	HQ0147-10-D-0024-0007	DT-08	5/8/2014	Warfighter Operational Support

Agency Operations Support (Capability Group 5)

IDIQ Contract Award Date: 6/17/2010

ALATEC, Inc.	HQ0147-10-D-0002-0003	DS-01	10/26/2012	Functional Management and Non-Matrix Admin. Support
Computer Sciences Corporation	HQ0147-10-D-0003			
EMC, Inc.	HQ0147-10-D-0004			

Security and Intelligence Support (Capability Group 6)

IDIQ Contract Award Date: 8/30/2010

Booz Allen Hamilton, Inc.	HQ0147-10-D-0011-0006	DEI-02	6/18/2013	Declassification
	HQ0147-10-D-0011-0008	IC-03	6/26/2014	BMDS Information Assurance/Computer Network Defense
	HQ0147-10-D-0011-0005	DEI-03	5/1/2012	Intelligence
	HQ0147-10-D-0011-0007	DEI-06	3/7/2014	Cyber Security and Engineering
Lockheed Martin, Inc.	HQ0147-10-D-0012			
ManTech International Corporation	HQ0147-10-D-0013-0005	DEI-01	3/7/2014	Security and Program Protection
	HQ0147-10-D-0013-0004	DEI-05	6/6/2013	Counterintelligence

Agency Advisory Analytical Support (Capability Group 7)

IDIQ Contract Award Date: 2/14/2011

Booz Allen Hamilton, Inc.	HQ0147-11-D-0001			
MacAulay-Brown, Inc.	HQ0147-11-D-0002-0003	A3-01	3/26/2013	Engineering & Technical Advisory & Analytical Support
	HQ0147-11-D-0002-0004	A3-02	3/21/2014	Test
SAIC	HQ0147-11-D-0003-0002	A3-03	3/26/2013	Executive Programmatic Advisory & Analytical Support
TASC	HQ0147-11-D-0004			

All information valid as of 1 October 2015

MiDAESS Awards

Small Business Set-Aside

Blue text indicates IDIQ Awards
Red text indicates Task Order Awards
Recompeted/RecentlyAwared

Quality, Safety, and Mission Assurance (Capability Group 1)

IDIQ Contract Award Date: 1/21/2010

a.i. Solutions	HQ0147-10-D-0027-0003	QS-03	5/24/2013	Quality Assurance
	HQ0147-10-D-0027-0004	QS-02	11/07/2013	Mission Assurance
A-P-T Research, Inc.	HQ0147-10-D-0028-0004	QS-01	12/01/2012	System Safety & Safety Occupational Health
Bastion Technologies, Inc.	HQ0147-10-D-0029			

Acquisition Support (Capability Group 2)

IDIQ Contract Award Date: 7/21/2010

Acquisition Services Corporation	HQ0147-10-D-0035			
BCF Solutions, Inc.	HQ0147-10-D-0036-0005	DO-04	5/01/2013	Cost Estimating and Analysis
	HQ0147-10-D-0036-0006	DO-06	4/29/2013	EVMS
Quantech Services, Inc.	HQ0147-10-D-0037	DA-01	4/01/2014	Acquisition & Program Management Support
	HQ0147-10-D-0037-0007	DPL-01	3/27/2013	Logistics Management
	HQ0147-10-D-0037-0006	DA-02	3/27/2013	Acquisition Executive Support
	HQ0147-10-D-0037-0010	DI-01	3/10/2014	International Affairs
	HQ0147-10-D-0037-0008	DI-02	9/20/2013	Aegis BMD FMS and International Support
	HQ0147-10-D-0037-0011	DOB-05	7/23/2012	Accounting

Engineering Support (Capability Group 3)

IDIQ Contract Award Date: 3/10/2011

COLSA Corporation	HQ0147-11-D-0005-0002	IC-01	9/12/2014	Information Technology Management and Analysis
ERC, Inc.	HQ0147-11-D-0006			
MEI Corporation	HQ0147-11-D-0007-0009	DE-12	6/12/2014	Specialty Engineering / International Engineering
	HQ0147-11-D-0007-0008	DE-09	5/05/2014	Speciality C3BM
	HQ0147-11-D-0007-0007	DE-13	3/21/2014	Risk and Lethality Engineering
	HQ0147-11-D-0007-0011	DT-06	6/24/2014	Ground Test Provisioning Support
	HQ0147-11-D-0007-0010	DT-07	6/24/2014	Test Infrastructure Support
	HQ0147-11-D-0007-0006	DE-04	3/27/2013	Threat Engineering
Torch Technologies, Inc.	HQ0147-11-D-0008-0002	IC-02	9/24/2014	Cybersecurity & Risk Management
	HQ0147-11-D-0008-0007	DE-02	6/06/2014	Test Analysis & Reporting
	HQ0147-11-D-0008-0008	DT-05	7/25/2014	Flight Test Provisioning Support
DCS Corporation	HQ0147-11-D-0009			

Agency Operations Support (Capability Group 5)

IDIQ Contract Award Date: 8/20/2010

Harlan Lee & Assosciates	HQ0147-10-D-0030-0007	DS-04	3/18/2013	Strategic Planning & Communication
	HQ0147-10-D-0030-0008	DS-05	4/17/2014	VIPC
	HQ0147-10-D-0030-0006	PA-01	1/28/2013	Public Information Support
PeopleTec, Inc.	HQ0147-10-D-0031-0007	DS-02	5/17/2013	Executive Admin. & Action Officer Support
	HQ0147-10-D-0031-0008	DS-03	4/17//2014	Protocol & Event Management
	HQ0147-10-D-0031-0005	DOH-01	11/30/2012	Human Resources
	HQ0147-10-D-0031-0006	DOH-02	1/04/2013	Training and Development
Total Solutions, Inc.	HQ0147-10-D-0032			

All information valid as of 1 October 2015

MDA Celebrates Five New Mentor-Protégé Relationships!

Ruth Dailey

MDA is proud to announce a new Mentor-Protégé Agreement between Lockheed Martin and Accurate Machine and Tool Corp (AMT). AMT is a Woman-Owned SB in Madison, Alabama, just minutes from Huntsville International Airport, Redstone Arsenal, and Cummings Research Park. AMT operates in a modern, climate-controlled, 36,000-square-foot facility, designed to support efficient workflow. In addition, AMT has 5,000-square-feet of additional enclosed space suitable for office space, storage, and temporary/long-term warehousing. AMT also has an AS-9100C & ISO-9001:2008 certified Quality Management System (QMS). AMT has been conducting business for close to 33 years. AMT's history of repeat business, and growing list of satisfied customers, is a testament to the dedication of the AMT team, and its commitment to quality and outstanding customer service on every task, every time. AMT has recently enjoyed a tremendous growth in revenue over the last 2 years. Their accomplishments in support of the THAAD program for LMC, and development of complex chassis manufacturing in support of the rotary wing industry, has fueled much of this growth.

We are also pleased to announce a new Mentor-Protégé Agreement between Parsons Government Services and Mobius Consulting, LLC. Mobius Consulting, LLC. ("Mobius") is a SBA certified Historically Underutilized Business Zone (HUBZone SB) Small Business, Woman-Owned Small Business (WOSB), and Economically Disadvantaged Woman-Owned Small Business (EDWOSB) headquartered in Alexandria, VA; with staff located in Washington, DC, Virginia, Alabama, Florida, Colorado, and California. Mobius began operating in May 2011, and has an average growth rate of over 50%, year-over-year, since inception. They currently employ 37 engineers, scientists, analysts, and administrative professionals with a retention rate of 95%. Their goal is to provide a world-class lifecycle, engineering solutions to customers facing issues of national and global significance. They strive to be admired for excellent people, fair and honest partnership, innovative problem solving, and exceptional performance. Mobius Consulting currently provides systems engineering, technical analysis, and program management solutions to federal and commercial customers. Mobius' specialized expertise in Weapons and Missile Systems, Space Systems, and Intelligence, has been proven through several successful programs with the Missile Defense Agency, Navy, and other government agencies. Their engineers, analysts, and program management professionals, provide clients actionable solutions to current and emerging challenges. Their experience encompasses the end-to-end systems engineering lifecycle – from concept definition to system disposal. They bring a team with extensive experience, implementing best practices and proven processes that result in increased system effectiveness, while meeting critical program schedule milestones and cost targets. Mobius has special expertise in space vehicle design and development, infrared sensor evaluation, radar system performance evaluation, optical sensor system design, hardware and software development, custom modeling and simulation, resource management, and risk analysis, mitigation, and tracking.

Lastly, we are delighted to announce three (3) new Mentor-Protégé Agreements with the Raytheon Company.

The Integrated Defense Systems Division is mentoring New England Die Cutting (NEDC) and TRM Microwave (TRM).
NEDC was founded in 1982, by James C. Abare. Always the entrepreneur, James owned and operated several businesses and soon had son, David, running NEDC, and transferred majority ownership to David, in 1999. David's passion for the technical and engineering aspects of the product is key to his interests and skills. In 2005, David handed the reins and the majority ownership over to his business partner and spouse, Kimberly, whose passion for management and growing the company both matched and complimented David's technical fervor. This was the real turning point for NEDC. Over the following 23 years, NEDC has grown to over $5M per year in sales and now has 36 dedicated employees. NEDC has been successfully certified to Military Standard MIL-DTL-83528E by the Defense Logistics Agency. NEDC Sealing Solutions and American EMI Solutions, a Division of NEDC, has been a top manufacturer of gaskets, seals, insulators, o-rings, and EMI shielding for over 30 years. Specializing in die cutting, waterjet cutting, and laser cutting, they work with their customers to help find solutions to best fit their needs. Because they make their own conductive elastomers in-house, they can customize

Continued from Page 8...

their products to fit a wide range of different designs.

TRM Microwave was founded in 1970, by founder and now CTO Anthony Tirollo with a single-minded goal: To design and manufacture innovative products at a reasonable cost. In 1994, Wendy Tirollo joined the company as CFO, and this year took controlling interest of the company. As CEO, Wendy now leads a dynamic woman-owned small business, providing engineering leadership and creativity to the development of new products for the telecommunications, medical, aerospace, industrial and military Markets. The company's products are globally promoted through a dedicated, experienced, and knowledgeable team of independent field sales representatives.

The TRM portfolio includes a wide range of passive and active control components and integrated assemblies operating in the range of DC-40GHz. These innovative standard and custom developed units have contributed to the success of numerous system architectures through a global base of customers.

The Raytheon Missile Systems division is mentoring Fifth Gait Technologies Inc (FGT). Fifth Gait is a minority-woman-owned small business, founded in 2007. FGT leadership consists of engineers and scientists who are directly involved in the development of most Missile Defense concepts and systems over the last 30+ years. FGT investigators were principal developers of many concepts and ideas for the Strategic Defense Initiative, under multiple contracts to Lawrence Livermore National Laboratory (LLNL), Defense Threat Reduction Agency (DTRA) and Strategic Missile Defense (SMD). FGT's experience and pedigree can be traced to a long tenure at Mission Research Corporation, a well-established radiation environment, and effects think tank that was sold in 2007 to ATK/Orbital. Following the sale, many of the principals dispersed to other companies and jobs, and in some cases retired. This led to significant technical knowledge loss, as well as, loss of critical mass in a single company. FGT assembles some of the remaining experts in MDA survivability and operability. Fifth Gait believes that it is their responsibility to ensure that a new generation of experts is mentored and trained to provide the services FGT currently provide.

We are proud of all of our mentors and protégés, and past experience has shown how successful this program can be in growing the small business industrial base for the BMDS. For information relating to the MDA Mentor-Protégé Program, please contact Ms. Ruth Dailey at ruth.dailey@mda.mil.

Outreach Efforts to Provide Small Business Community with Cybersecurity

ALL defense contractors and subcontractors, including small businesses, must protect their networks and data, as required by certain clauses within the Department of Defense (DoD) contracts. As outlined in the U.S. Government Accountability Office's report (GAO-15-777) on Defense Security, "Small businesses, including those that conduct business with DoD, are vulnerable to cyber threats and may have fewer resources, such as robust cybersecurity systems, than larger businesses to counter cyber threats". Knowledge is empowering. To better position defense small businesses in protecting information and networks from cyber threats, the Missile Defense Agency (MDA) Office of Small Business Programs (OSBP) has compiled a listing of Cybersecurity Resources.

For a complete listing of the Cybersecurity Resources compiled by the MDA OSBP, please go to http://www.mda.mil/business/smallbus_programs.html

Laura Anderson

How do the New DoD Cybersecurity Requirements Affect MDA's Future Market Research

The Department of Defense (DoD) has initiated new mandatory cybersecurity requirements for all DoD procurements. These new cybersecurity requirements will affect all areas of contracting within the DoD. Here we are going to discuss how it will affect future market research. In concert with other data that MDA reviews during market research, cybersecurity requirements will now be a critical part of determining a small businesses' ability to perform all of MDA's requirements. MDA will need to be confident that SBs will be able to comply with the cybersecurity requirements, as well as other technical capabilities. It will also be critical that SBs are able to communicate these new cybersecurity requirements with their subcontractors. For additional information on the new cybersecurity requirements, please visit www.sba.gov/tools/sba-learning-center/training/cybersecruity-small-businesses.

Becky Martin

Cybersecurity and Mentor-Protégé Program

The Mentor-Protégé program is also working to comply with the Implementation of DFARS Rule 2013-D018. For any new Mentor-Protégé agreement, we have added a new task that all mentors need to implement. "Security - Computing, Facility and Cyber: Protégé requires the security of its employees and its assets (tangible and intangible) to be of primary importance of its continued growth, profitability and success. The continued strengthening of security controls and procedures is essential for the protection of employees, the preservation of assets, and the effective enforcement of rules and regulations.

Protégé wishes to enhance its proactive security program, by establishing a robust and secure computing capability, to minimize security risks and business losses, and to comply with all regulatory requirements. This will present additional growth opportunities for growing small businesses. Mentor will provide training and guidance to help Protégé develop and address growing vulnerabilities to computer systems. This will support future contracting efforts with Department of Defense (DoD) and prime customers for classified and unclassified operations and requirements."

As we move forward, we need to be diligent on cybersecurity requirements of DoD information on contractor systems and help the DoD to mitigate the risks related to compromised information, as well as, gather information for future improvements in cybersecurity policy by training small businesses on the importance of safeguarding DoD information.

Ruth Dailey

eSBIE Registration Steps

Have the following information ready:

1. 9-digit DUNS number
2. Company contact information
3. Company socio-economic categories
4. Up to 10 VALID 2012 NAICS codes
5. Company facility clearance
6. Two points of contact

How to Register:

1. Go to http://www.mda.mil/business/smallbus_programs.html
2. Click on the 'OSBP Directory' button on the right side of the page
3. Click on the 'Register' button at the top of the page and enter the information you collected earlier
4. Click on the 'Submit' button and stand by while we review your application for authenticity

Having issues? Have questions?
Please contact **Outreach@mda.mil**

Missile Defense Agency (MDA) How to do business with MDA?

- Send the MDA Office of Small Business Programs (OSBP) an email requesting a meeting or teleconference) to: nancy.hamilton.ctr@mda.mil
- Attach your company capability statement, briefing or overview with your initial request. You will be sent a reply with several dates and times that are available on the OSBP Directors calendar and the option to choose one that will work with your schedule.
- For face-to-face meetings our office can provide access to Redstone Arsenal by way of a visitor pass. You will be provided with directions and a map to our location in Von Braun III, Bldg. 5224.
- For teleconferences our office can provide multiple call-in lines if required.
- All small business capability briefings are scheduled for one hour in duration.

Having issues? Have questions?
Please contact **Outreach@mda.mil**

2016 Calendar of Events

- **January 12-14, Surface Navy Symposium, Crystal City, VA**
- **February 1-2, Gulf Coast Procurement Matchmaker, Mobile, AL**
- **February 8-10, Aerodef Manufacturing Conference Exposition, Long Beach, CA**
- **February 9-10, National 8(a) Conference, Orlando, FL**
- **February 17-19, US NAVY Institute WEST 2016 Annual Conference, San Diego, CA**
- **February 18, Chamber of Commerce Matchmaking Event, Reston, VA**
- **March 14, SBDC Opportunities, Asheville, NC**
- **March 14, Team Redstone SB Industry Outreach 2016, Huntsville, AL**
- **March 15-17, AUSA Winter, Huntsville, AL**
- **March 21-25, TechNet Air, San Antonio, TX**
- **April 6, OSDBU, Washington, DC**
- **April 6, AL PTAC 5th Annual Matchmaker, Pelham, AL**

Save the Date

- **April 17-22, The 2016 Mentor-Protégé Conference / Nunn-Perry Awards Ceremony Houston, TX**

OSBP Staff

Lee Rosenberg, *Director*
Genna Wooten, *Deputy Director*
Jerrol Sullivan, *Subcontracting Program Manager*
Laura Anderson, *Outreach Program Manager*
Becky Martin, *eSRS Manager*
Ruth Dailey, *Mentor-Protégé Manager*
Nancy Hamilton, *Sr. Administrative Assistant - ALATEC*
Chad Rogers, *Sr. Analyst - ECS, Inc.*
Chrissy Bijold, *Acquisition Analyst - Quantech Services*

OSBP Main Office Numbers
P: (256) 450-2872
F: (256) 450-2506

OSBP Main Office Mailing Address
ATTN: MDA/SB
Building 5222, Martin Road
Redstone Arsenal, AL 35898

For additional information regarding Subcontracting activities at MDA, please email us at subcontracting-oversight@mda.mil.

For additional information regarding Outreach activities at MDA, please email us at outreach@mda.mil.

Websites of Interest

MDA Office of Small Business Programs
www.mda.mil

MDA Marketplaces and Directory
www.mda.mil/business/smallbus_programs.html

MDA Business Acquisition Center
www.mda.mil/business/acquisition_center.html

MDA SBIR/STTR Programs
www.mdasbir.com

Fed Biz Opps
www.fbo.gov

Electronic Subcontracting Reporting System (eSRS)
www.esrs.gov

MDA Small Business Advocacy Council
www.mda.mil/business/bus_mdasbac.html

MDA Unsolicited Proposal Guide
www.mda.mil/global/documents/pdf/MDA_Unsolicited_Proposal_Guide.pdf