

CONFIDENTIAL

**Monitoring Report – February, 2007**  
J. Markowitz, Consultants  
Program C: Government Projects and Biometrics Initiatives

This report is confidential and intended for registered JMC clients only

**Biometric Initiatives and Projects**

**North America**

**Government Security News Releases List of Top 100 DHS Contractors for 2006**

*Government Security News* (GSN), a publication for IT defense contractors and government agencies, published its annual “top ten Department of Homeland Security (DHS) Contractors” for 2006. The list contains 100 companies who received the largest value of total contracts awarded by DHS between Oct. 1, 2005 and Sept. 30, 2006.

POTENTIAL IMPACT: Only one biometrics contractor was listed: No 19, Northrop Grumman Information Technology (a multi-year \$357 million contract with the U.S. Citizenship and Immigration Services to provide biometric capture services in support of citizenship applications and green card renewals) but IBM and L-3 services (#9) have SIV technology and UNISYS has partnerships in the biometrics industry. The absence of biometric suppliers is an opportunity for SIV and other biometric technology and solutions providers because the real value of this list is to provide names of companies tied into DHS that could become partners.

DETAILS: The list was compiled by GSN during the first week of December 2006, based on data provided by the Federal Procurement Data Center, a unit of the General Services Administration (GSA). Around a third of the companies that on the list are there because they are performing clean-up, construction, engineering or other work related to Hurricane Katrina. This is why construction and engineering firms (e.g., Fluor, Shaw Environmental and Bechtel) top the list instead of the systems integrators, technology companies and consulting firms more commonly associated with homeland security programs. The list includes a number of low-profile companies and organizations, such as J.H.M. Research and Development, of Silver Spring, MD (#10) and Cooperative Personnel Services, of Sacramento, CA (#18).

The top ten companies are

<b>Company</b>	<b>Description</b>	<b>Total amount of DHS contracts</b>
<b>Fluor Corporation</b> Irving, TX 469-398-7000 <a href="http://www.fluor.com/">www.fluor.com/</a>	One of the world's largest engineering and construction companies. Provides disaster cleanup, damage assessment and other services for nine different FEMA regions.	\$1,504,817,784
<b>Shaw Environmental, Inc</b> Baton Rouge LA 225-932-2500 <a href="http://www.shawgrp.com/">www.shawgrp.com/</a>	It is a subsidiary of Shaw Group, Inc., of Baton Rouge, LA. and a major provider of environmental, infrastructure and emergency response services. It has a 10-year contract from the U.S. Air Force to provide maintenance, demolition, force protection and homeland security services.	\$852,205,338
<b>Bechtel National, Inc.</b> San Francisco, CA 415-768-1234	An engineering, construction and project management company. It has contracts with FEMA for Hurricane Katrina survivors	\$471,243,361

CONFIDENTIAL

<a href="http://www.bechtel.com/">www.bechtel.com/</a>	and the Dept of Energy as well as DHS.	
<b>CH2M Hill Constructors Inc.</b> Englewood, CO 720-286-2000 <a href="http://www.ch2m.com">www.ch2m.com</a>	A full service engineering, consulting, construction, operations management, and physical security company. Among other projects, it developed systems to secure nuclear material for the U.S. Government.	\$436,537,706
<b>IBM Corporation</b> Armonk, NY 914-499-1900 <a href="http://www.ibm.com/">www.ibm.com/</a>	IBM was selected last year as part of DHS's indefinite-delivery, indefinite-quantity contract to provide a range of services to the Enterprise Acquisitions Gateway for Leading Edge program.	\$413,342,747
<b>Unisys Corporation</b> Blue Bell, PA 215-986-4011 <a href="http://www.unisys.com/">www.unisys.com/</a>	Unisys holds a \$ 1 billion multi-year task order to build an advanced information technology infrastructure for the Transportation Security Administration. In addition, it markets a broad range of information security products to DHS and other government agencies.	\$362,832,751
<b>Integrated Coast Guard Systems</b> Washington, DC 202-267-2116 <a href="http://icgsdeepwater.com/">icgsdeepwater.com/</a>	ICGS is a joint venture of Lockheed Martin and Northrop Grumman. ICGS was awarded in June 2002 the Deepwater program to modernize and replace the Coast Guard's aging ships and aircraft.	\$325,635,240
<b>The American Red Cross</b> Washington, DC 800-733-2767 <a href="http://www.redcross.org/">www.redcross.org/</a>	In addition to its hands-on disaster work, the Red Cross helped draft the National Strategy for All Hazards Preparedness being developed by DHS and was involved in a <i>Together We Prepare</i> campaign to ready individuals, communities, workplaces and schools for potential disasters and emerging dangers.	\$285,007,831
<b>L-3 Communications Corp.</b> New York, NY 212-697-1111 <a href="http://www.l-3.com/">www.l-3.com/</a>	L-3 Communications supplies Intelligence, Surveillance and Reconnaissance (ISR) systems, satellites, and secure communications systems to the Department of Defense, DHS and government intelligence agencies. In November 2006, L-3 was selected by DHS to assess the agency's second generation Civil Aircraft Protection System (CAPS2), which is intended to detect man-portable air defense systems (MANPADS).	\$270,639,463
<b>J.H.M. Research &amp; Development</b> Silver Spring, MD 301-589-4000 <a href="http://www.jhmrads.com/">www.jhmrads.com/</a>	A supplier of facilities management, records management, document conversion and information technology services. J.H.M. Research & Development includes among its government customers the U.S. Citizenship and Immigration Services unit of DHS, the FBI and the U.S. Coast Guard.	\$250,169,552

## CONFIDENTIAL

### **DHS to consolidate Centers of Excellence program**

The Department of Homeland Security (DHS) announced that it will merge three of its existing academic research centers and create four new centers, to study natural disasters, border security, explosives detection, and maritime security.

**POTENTIAL IMPACT:** The focus of the new centers will be closer to areas that involve biometric security and authentication but it is not yet clear whether biometrics or any other existing technologies will be subjects of investigation. The call for proposals could open the door to additional research on the use of biometrics for authentication in various contexts but it is likely to be a small, secondary function.

**DETAILS:** The centers that will be merged are the Center for Advancing Microbial Risk Assessment, the National Center for Foreign Animal and Zoonotic Disease Defense, and the National Center for Food Protection and Defense. All of them focus on chemical and biological weapons. The new centers will work on natural disasters, border security, explosives detection, and maritime security. The changes are expected to be completed by 2010.

The Centers of Excellence program came under scrutiny last year from Congress, which criticized the way that the DHS Science and Technology Directorate managed its entire research portfolio. To punish the directorate, legislators slashed \$12-million from the budget of the Office of University Programs and threatened to withhold \$50-million of its research budget in the 2007 fiscal year until they received a report describing the agency's efforts to "address financial-management deficiencies, improve its management controls, and implement performance measures and evaluations." They also demanded a briefing, within 60 days of when the bill was signed into law, on the department's goals and projected outcomes for its six Centers of Excellence. The DHS responded by conducting a review of its university-research program which led to the current proposal to merge three of the seven existing centers and create four new centers to conduct research in new areas. It also issued requests for proposals for the new centers earlier this month.

### **Raytheon Announces Self-Authenticating PASS Card for Western Hemisphere Travel Initiative (WHTI)**

Raytheon introduced the Personal Authentication Device (PAD) for WHTI. It allows passengers to authenticate their own fingerprints as they approach a checkpoint. The purpose is to save time while supporting the requirements of WHTI.

**POTENTIAL IMPACT:** The idea of using biometric authentication while a person is in motion and moving towards a security station is not new. In the 1990s, there was a multi-biometric initiative at Otay Mesa, California that included testing of in-car SIV of the driver and passenger as the car approached the port of entry to the US. The concept of authentication while in motion was difficult for many people to grasp so drivers would often stop their cars which defeated the goals of speed and efficiency that motivated both the Otay Mesa test and the Raytheon product. It may be that business travelers – who are the ones who have expressed great concern about delays that could be caused by WHTI authentication requirements – may be more sophisticated about biometrics in motion (sometimes called "flying biometrics").

**DETAILS:** Under the Western Hemisphere Travel Initiative (WHTI), those traveling by land or sea from Mexico or Canada to or from the United States will have to present either a passport or a special fingerprint biometric PASS Card. Many business people from all three countries worry about the cost and delays that these extra authentication requirements would create. The Personal Authentication Device (PAD) permits passengers to authenticate their own fingerprints as they approach a checkpoint, thereby saving time and increasing border efficiency. The Raytheon PAD card contains an enrolled fingerprint and an identification number. When the user approaches the border she/he presses a finger onto a small scanning screen on the card while at the same time using another finger to activate the card's internal power supply. If the scanned print matches that on file, an RFID signal is sent to border agents who can instantly access the

## CONFIDENTIAL

file and prepare for any required follow-up once the traveler reaches the checkpoint. The PAD system works at speeds of up to 60 miles per hour and the supply activation step is designed to prevent "digital pick pocketing" by limiting the time the card is active.

### **Bioscrypt Selected for Canadian airport I.D. authentication system**

Bioscrypt, a Canada-based supplier of biometric access-control systems, was selected by The by Labcal Technologies as part of the latter company's contract with the Canadian Air Transport Security Authority (CATSA). The project is to provide authentication on airport employees' Restricted Area Identification (RAIC) Cards. The solution will be deployed at twenty-nine airports throughout the country.

POTENTIAL IMPACT: Unlike TWIC, Canada's CATSA is focused solely on air travel and, therefore, has not faced the kind of opposition that TWIC has endured with regard to ports. A smooth implementation of biometric access security control at airports will facilitate the deployment of similar systems in North America and elsewhere. It could also lead to use of other biometrics, including SIV, for other kinds of authentication in airports.

DETAILS. CATSA's RAIC program is similar to the U.S.-based Transportation Worker Identification Credential (TWIC) program. One of its features is that it allows airport authorities to immediately adjust the level of security at any access point or in large areas such as the tarmac. The Canadian Air Transport Security Authority (CATSA) selected Labcal's Be.U Mobile handheld device for RAIC which includes Bioscrypt's fingerprint matching algorithm and a fingerprint reader. The solution will be deployed at 29 airports throughout the country

### **GSA to Stop Paying Vendors to Test Products for HSPD-12 Compliance**

The US General Services Administration (GSA) has announced that it will stop paying vendors to test their products and services as HSPD-12-compliant.

POTENTIAL IMPACT: The move to pay vendors to test compliance was designed to help move the HSPD-12 back on deadline. Now that the program has begun moving forward at a faster pace the GSA is terminating the free-testing incentive. This program tests biometric products as well as other security technologies. If, as the GSA claims, the cost of compliance testing will not be high the elimination of free testing should not significantly slow the flow of products into testing facilities.

DETAILS: In May 2006, the GSA installed a free testing lab in order to help companies move forward on the much-delayed HSPD-12 mandate. It has since spent \$725,000 on equipment and supplies to support the program. GSA will continue to certify independent testing labs but starting April 23, 2007 the cost of HSPD-12 testing will be borne by the suppliers who will pay the testing labs directly. GSA has tested products or services in twenty-two categories and approved 166 products from seventy-five different vendors. Thirty service vendors were approved, as were an additional five to provide public-key infrastructure digital certificates. According to the GSA now that testing is better understood and more efficient the costs should not be as high as they were initially.

## **US State and Local**

### **Iris Scanning for Finding Missing Persons**

Galveston County in Texas developing an iris database to help find missing children and senior citizens. This project is part of the Children's Identification and Location Database (CHILD) Project

POTENTIAL IMPACT: This is not the first use of biometrics for programs related to missing children. We included one in our January, 2007 report. The Galveston deployment is typical in that it requires prior enrollment of a child in order to assist in the location of the child (or in the identification of

## CONFIDENTIAL

that child's remains). These programs are becoming more popular and are contributing to increased acceptance of biometrics but they are unlikely to involve SIV.

DETAILS: CHILD works in conjunction with the Nation's Missing Children Organization and the National Center for Missing Adults. Iris biometrics will initially be used in conjunction with the fingerprinting and photo identification kits the County already employs. The Galveston County Sheriff's Office purchased two of iris scanning sensors from Massachusetts based Biometric Intelligence and Identification Technologies. The company also supplies law enforcement agencies with biometric identification systems for use in jail systems and recently launched a similar program to help identify kids and seniors. The county plans to make the iris sensors available at safety fairs, church meetings, school meetings and the other public events so that it can quickly build a local database. The system eventually will be used to maintain a database of people who have been arrested as well as those who are missing.

### **Hand Scanning New York City Employees– Follow-up**

After months of protest and legal sword-rattling by employees and employee union Local 375 (which represents city employees), the Bloomberg administration decided to leave the decision about the use of hand scanning to each department.

POTENTIAL IMPACT: To a great extent this is an example of what can happen when there is no communication with users. Had the Bloomberg administration gone to the union beforehand with the plan and armed with their reasons for using the technology and with proof that the system cannot track an employee's movements or expose personal information they might have had a chance. Local 375 officials said they were also concerned about other biometrics, such as using SIV to track staffers out in the field as well as other kinds of monitoring, such as global positioning systems built into city employees' cars or cell phones.

DETAILS: Six months ago, New York City announced that it would require many of its 345,000 employees to use hand scanners instead of standard punch clocks to punch in and out. Both employees and unions protested claiming, among other things, that the technology was an invasion of privacy and could be used to track employees. Last week the head of the city department where objections were strongest told his staff that use of controversial "hand geometry" devices will become voluntary.

The use of hand geometry was selected to computerize the time-and-attendance system which would make it faster and more accurate. Employees began to object to the plan when it was announced in 2006. Employee unions participated in a city council meeting that discussed the topic. Not long afterwards, since the city's Office of Labor Relations (OLR) announced that use of the new Hand Punch 4000 units will be at the discretion of each city agency's chief. For those agencies that do not use the hand scanners it is not clear what tools and procedures will be used. .

## **Global**

### **Mobile Biometrics in Iraq**

The Automated Biometric Identification System (ABIS) project is a fully-funded project to implement mobile biometric system intended for use in tracking down insurgents and other Iraqi criminals. It was on hold until this month when L-1 Identity Solutions joined the project.

POTENTIAL IMPACT: The addition of L-1 has kick-started the project which needs the breadth of technology that L-1 can provide. This project does not include voice but it could conceivably be linked to voice surveillance that is being done in the Middle East.

DETAILS: This project is being led by Northrop Grumman. It is a mobile, networked, biometric, identity-verification project that is expected to support up to 2.4 million finger, face, palm, and iris records, and a lesser number of unsolved latent fingerprints. L-1 will supply its Identix's ABIS

## CONFIDENTIAL

System, which is based upon its underlying Facelt facial recognition and BioEngine fingerprint technologies. L-1 will also provide a suite of professional services, including legacy data conversion and rationalization, as well as system architecture, design, implementation, and ongoing support. Other additional products provided by L-1 include workstations for ten print and latent fingerprint examiners, as well as forensic face matching. Other team members on the DoD ABIS contract include Arlington, Virginia-based Ideal Innovations and Fairmont, West Virginia-based NEW-BOLD Enterprises.

### **Biometric Testing in Thailand and Malaysia for Dual Citizenship**

Malaysia and Thailand will each select 500 residents living along their mutual border for testing under the biometric system to determine if they have dual Malaysia-Thai citizenship.

POTENTIAL IMPACT: This is an interesting wrinkle in the use of biometrics and other identification technologies that could not have been done before the deployment of e-passports and other biometric identity documents. We should expect to see more such uses, especially outside of North America and Western Europe.

DETAILS: Both governments agreed to perform the testing using automated biometric thumbprint technology that was adopted by both Malaysia and Thailand to keep an electronic databank of their citizens. Thai's border with Peninsular Malaysia stretches from Perlis to Kelantan, some 1,500km of rugged terrain including mountains and rivers. Thai media reports estimate there were between 50,000 to 100,000 border residents with dual nationality. Malaysia does not allow dual citizenship

### **TOPIC: Passports and National IDs**

The push to deploy biometric e-passports is global. In a growing number of cases countries has spawned national ID programs across the globe. Some programs are using passports as the starting point while others are simply getting their e-passport projects started.

### **Azerbaijan National ID Program**

Azerbaijani president Ilham Aliyev issued an executive order establishing a biometric identification. President Aliyev formally issued an executive order approving the 2007-2012 State Program and charged the Cabinet of Ministers with controlling the implementation of the order, organizing the project and taking necessary measures for financing the program. The Cabinet of Ministers is also requested to evaluate the progress of the State Program as it proceeds and to update the President every six month on the status of implemented measures.

### **Brunei to Implement Biometric Passports**

Brunei's Immigration and National Registration Department will become the third Asean country to implement biometric features in travel documents. Biometric features will be in accord with the standards issued by the International Civil Aviation Organization (ICAO). Giesecke & Devrient will provide the technology to produce the e-Passport. The project will cost BND\$7,148,885.20, and includes supply, delivery, installation, testing, commissioning and maintenance.

### **Estonian Biometric ID System**

The Estonian Ministry of Internal Affairs, Citizenship and Migration Board is starting a program to create a massive ID Management system. Although the project will include use of biometrics in passports and other travel documents, the main goal of the new system is to establish effective and objective criteria for person identification as well as the detection of misused identities. The system will use biometric facial recognition from European face-recognition vendor Cognitec. The primary contractor is IBM Estonia.

### **Portugal Developing National ID Card**

Portugal's Imprensa Nacional-Casa da Moeda (INCM), the Portuguese Mint and National Printing Office began a pilot project to establish a national e-ID card containing biometric fingerprint

## CONFIDENTIAL

technology on a smart card. The pilot began in Portugal's Acores region. The "Citizen Card" will include several ID numbers such as civil identification, taxpayer, social security and health and will also replace, in the future, the elector card. A variety of e-government services will be available through the electronic identification provided by the new Citizen Card. The cardholder has a secret pin code to identify and authenticate himself/herself, and the card generates a, legally-binding digital signature for secure declarations and administrative procedures. This application will provide the required cryptographic means for secure access to e-government services portal and digital signature for electronic exchanges. Another application, which access to is electronically restricted to forensic and police authorities, will perform the identity verification through fingerprint check.

### **UK National ID Program**

This program has gone in the opposite direction from the ones described above. Poor media relations, cost overruns, delays, and anti-project leaks were all fodder for the growing national opposition to the program. This month, British Prime Minister Tony Blair, the leading proponent of the National ID project, sent personal email messages to approximately 28,000 people who had signed a petition opposing the introduction of identity cards. He also stated he would continue to work to convince civil liberties groups of the program's value.

The petition called for Blair to drop the plan saying it would not prevent terrorism or crime and would be "yet another tax on all law-abiding citizens." Countering those claims, Blair's message focused on the "important contribution" the ID cards would make to counter fraud, international crime, illegal immigration, and terrorism. Saying, "I recognize that these arguments will not convince those who oppose a National Identity Scheme on civil liberty grounds," Blair asserted that it would be "foolish" not to take the opportunity to use biometric data like fingerprints to secure a person's identity and disputed "exaggerated" claims about the cost of the scheme.

## **Solicitations, RFIs, and RFPs**

### **The Space and Naval Warfare Systems Center, Charleston**

#### **RFI: Biometric Devices for Facility Access Control (No. DON SNOTE 070221-001)**

Posted February 21 Due March 9

Point of contact and non-technical questions to the Contract Specialist paula.somers@navy.mil .  
Technical point of contact is Kelly Williams, 843-218-4823

DETAILS: Code 741 (Advanced Law Enforcement Technology Branch). Seeking information on Biometric Devices for Facility Access Control. The DHS Authorized Equipment List (AEL) item number for this equipment is 14.1.1.4. The target audience for this information is the emergency responder community and all submittals should be suited to their specific needs. Information sought should be relevant to biometric devices that provide for biometric controlled access to emergency responder facilities. Review of this information is being performed for DHS, Preparedness Directorate, Office of Grants and Training (G&T). G&T established the System Assessment and Validation for Emergency Responders (SAVER) Program to conduct comparative assessments and validation activities that provide the emergency responder community with information on important products and services. Visit the SAVER Program Web site at <http://www.dhs-saver.info> for more information on the SAVER Program. All information received will be treated as public knowledge and may be used in SAVER Program documentation; therefore, vendors should not submit proprietary information in response to this RFI. Specific information sought includes: 1. Company information, including name, address, URL, revenue, and number of employees. 2. Whether the company is a manufacturer or distributor. 3. A point of contact for follow-up information, and the point of contact's phone number and e-mail address. 4. Product name, price, and a brief description (75 words or less). The submitted information will be evaluated for inclusion in SAVER projects and reports. Determination as to an individual product's suitability will be made by SPAWARSSYSCEN Charleston based on the objectives of this request. Vendors may be contacted following submission to requested more detailed product information. Vendor provided information may

## CONFIDENTIAL

be reformatted for publication in SAVER Program documents. Submittals: Respondents are required to complete the attached product summary questionnaire (Product\_Summary\_FAC.xls) for each product and submit the questionnaires via e-mail to [kelly.h.williams@navy.mil](mailto:kelly.h.williams@navy.mil) with email subject

This RFI is for information gathering and planning purposes only, and should not be construed as a Request for Proposal (RFP) or solicitation of an offer. The Government does not intend to award a contract on the basis of this RFI or otherwise pay for the information solicited. Submission of vendor information constitutes consent to publication of that information in SAVER Program documentation.

### **Non-Biometric, Related Initiatives and Projects**

The following projects are not directly related to biometrics or SIV but they could represent opportunities for work in those areas.

#### **FEMA seeks applicants for National Advisory Council**

[NOTE: This item was included because FEMA does need to have effective communications and to verify the identities of individuals in the field. Having a representative on this new National Advisory Council could enhance its understanding of speech and speaker recognition.]

The DHS's Federal Emergency Management Agency (FEMA) is looking for knowledgeable individuals to apply to sit on its National Advisory Council. The Council is being created as an advisory role to the FEMA Administrator to help ensure effective and ongoing coordination of the federal preparedness, protection, response, recovery and mitigation for natural disasters, acts of terrorism, and other man-made disasters. Individuals seeking to be considered for an appointment on the council should submit a resume by 9 March detailing their experience in the arena of emergency management.

The creation of a FEMA is mandated by the Post-Katrina Emergency Management Reform Act of 2006. As its name suggests, Its role is advise the FEMA administrator. It will focus attention on the development and revision of the following:

- National preparedness goal
- National preparedness system
- National Incident Management System
- National Response Plan

and other related plans and strategies. Interested individuals should submit a resume detailing their experience in the arena of emergency management and related fields. The resumes must be received by FEMA by March 9, 2007. Resumes are to be sent

by email: [john.sharetts-sullivan@dhs.gov](mailto:john.sharetts-sullivan@dhs.gov)

or mailed to: FEMA  
Attention: John Sharetts-Sullivan  
500 C Street, SW  
Room 316  
Washington, DC 20472

#### **NATO and the US Department of Defense to sign cybersecurity pact**

The North Atlantic Treaty Organization (NATO) and the US Department of Defense (DoD) worked out the final points of an agreement to share IT incident and threat information

## CONFIDENTIAL

POTENTIAL IMPACT: Planning for the agreement has been going on for some time even though the announcement of its finalization came immediately after revelations that a hacker attempted to bring down three Internet mil root servers and two other servers. This kind of agreement is of interest to SIV because it is an example of the internationalization of security – including cybersecurity.

DETAILS: The agreement will involve the sharing of incident and threat information. The organizations involved are NATO's Computer Emergency Response Team (CERT) and the DoD's International Information Assurance Program National Cyber Response Coordination Group (NCRCG). There are 26 NATO countries and the organization's CERT center is connected to all of those nations' networks. By crafting an agreement with CERT, the NCRCG eliminates the need to deal with 26 individual nations. The NCRCG is the US Federal incident response coordinator. The group guides federal agencies and works with the private sector, state governments and other nations to defend U.S. cyberspace.

According to a DoD spokesperson CERT played in assessing the effect of the Feb. 6 cyberattack on three Domain Name System root servers, the Internet's backbone. U.S. CERT worked with owners of critical infrastructure and other Internet organization to minimize the attack, Hackers appeared to have launched botnets of zombie PCs against three root servers. The servers attacked included the G, which host .mil web sites, the L and M. The DNS servers were able to withstand the attack. There was no impact on server operations and no Internet users were affected, Witt said.

### **ManTech Wins DoD Anti-Terrorism Contract**

ManTech International Corp. received a \$89.9 million contract from a Department of Defense group to support its interagency anti-terrorism missions, including research and development. ManTech International Corp. is a supplier of technologies and solutions focused on mission-critical national security programs for the intelligence community, the DoD, DHS, and other agencies of the US federal government. ManTech has provided support services, management oversight, and technical solutions to DoD since 1999. The new contract provides an opportunity for significant expansion of DoD work. ManTech's teammates include Science Applications International Corporation and Battelle Memorial Institute.

Contact information; ManTech International Corporation, Fairfax

Mark Root, 703-218-8397

Cell: 571-259-1169

[mark.root@mantech.com](mailto:mark.root@mantech.com)

or

Joseph Cormier, 703-218-8258

[joe.cormier@mantech.com](mailto:joe.cormier@mantech.com)