

Home	Getting Started	General Info	Opportunities	Agencies	Privacy
------	-----------------	--------------	---------------	----------	---------

Buyers: [Login](#) | [Register](#) Vendors: [Login](#) | [Register](#) [Accessibility](#)



CYBERCOM

Solicitation Number: CYBERCOM

Agency: Other Defense Agencies

Office: Virginia Contracting Activity

Location: Virginia Contracting Activity (ZD50)

Notice Details

Packages

Print

Link

Complete View

[Original Synopsis](#)

Combined

Synopsis/Solicitation

Aug 02, 2010

4:23 pm

[Changed](#)

Aug 03, 2010

10:18 am

[Changed](#)

Aug 03, 2010

11:40 am

[Changed](#)

Aug 04, 2010

11:09 am

[Changed](#)

Aug 04, 2010

4:30 pm

[Changed](#)

Aug 10, 2010

5:00 pm

[Changed](#)

Aug 13, 2010

7:35 am

[Return To Opportunities List](#)

[Watch This Opportunity](#)

Solicitation Number:

CYBERCOM

Notice Type:

Combined Synopsis/Solicitation

ALL FILES

[SOW](#)

Aug 02, 2010

[CYBERCOM SOW.doc](#)

[Industry Day Attendees](#)

[List](#)

Aug 10, 2010

[Industry Day Attende...](#)

GENERAL INFORMATION

Notice Type:

Combined

Synopsis/Solicitation

Original Posted Date:

August 2, 2010

Posted Date:

August 13, 2010

Response Date:

-

Original Response Date:

-

Archiving Policy:

Manual Archive

Original Archive Date:

-

Archive Date:

-

Original Set Aside:

Total Small Business

Set Aside:

Total Small Business

Classification Code:

D -- Information technology

Synopsis:

Added: Aug 02, 2010 4:23 pm Modified: Aug 10, 2010
4:58 pm [Track Changes](#)

Due to popular request, this amendment posts the attendance list consisting of vendors who participated in the August 6, 2010 Industry day.

DIA anticipates awarding a contract to provide services in support of senior level organizations in the planning and execution of major initiatives, programs and projects across the agencies.

Only companies with facilities clearance can participate.

The Base period of performance is one year from the date of award with options to renew for three 12-month periods.

Place of Performance: Fort Meade,
Maryland

This will be the last posting on FBO. From hereonin, vendors must watch e-Buy on GSA Advantage for further information related to this upcoming solicitation. That is, pursuant to FAR Subpart 8.002(a)(1)(vii), "Priorities for use of Government Supply Sources, Optional use of Schedules, and FAR Subpart 7.105(B) (4)(ii)(b) wherein an agency can accomplish its mission more efficiently and effectively through the use of Schedules.

According to the FAR, GSA Schedules are the preferred method of acquisition. Teaming and partnering will be encouraged.

Multiple schedules will be included as follows: [Schedule 70 \(General Purpose Commercial Information](#)

services, including
telecommunications services

NAICS Code:

541 -- Professional,
Scientific, and Technical
Services/541519 -- Other
Computer Related Services

Please consult the list of [document viewers](#) if you cannot open a file.

SOW

Type: Other (Draft RFPs/RFIs, Responses to Questions, etc..)

Posted Date: August 2, 2010

[CYBERCOM SOW.doc](#) (74.00 Kb)

Description: SOW

Industry Day Attendees List

Type: Other (Draft RFPs/RFIs, Responses to Questions, etc..)

Posted Date: August 10, 2010

[Industry Day Attendees.pdf](#) (580.52 Kb)

Description: List of Attendees who participated in Industry Day conducted at Bolling AFB on August 6, 2010

Contracting Office Address:

200 MacDill Boulevard
Post Office Box 46563
Washington, District of Columbia 20035-6563

Place of Performance:

Fort Meade
Fort Meade, Maryland
United States

Primary Point of Contact:

Holly T Carr
holly.carr@dia.mil
Phone: 202-231-4597
Fax: 202-231-6179

[Return To Opportunities List](#)

[Watch This Opportunity](#)

Statement of Work
United States Cyber Command
Cyber Analytical Support
Date: 02 July 2010

1.0 BACKGROUND

The Department of Defense (DOD) is quickly and continuously transforming to achieve the objectives of Joint Vision 2020 (JV2020). A key enabler for transforming the operational capabilities is information superiority; the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Achieving information superiority requires a net-centric operations (NCO) environment -- a global information grid (GIG) that provides an end-to-end set of information services, associated processes, and people to manage and provide the right information to the right user at the right time with appropriate protection across all DOD war fighting, intelligence and business domains.

To accomplish the centralized command and control and security of the GIG, United States Department of Defense (DoD) has established the United States Cyber Command (USCYBERCOM). USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to direct the operations and defense of specified Department of Defense information networks and prepare to, when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains and ensure United States / Allied freedom of action in cyberspace and deny the same to our adversaries. USCYBERCOM will command and control the operation and defense of the GIG in support of the President, Secretary of Defense, Joint Staff, Combatant Commanders, military Services and Defense Agencies. USCYBERCOM will collaboratively conduct operations through a tiered construct of Network Operations Centers. USCYBERCOM will lead and direct continuous GIG Enterprise Management, GIG Network Defense, and GIG Content Management throughout the GIG, maintaining near real time Situational Awareness (SA), end to end management, and dynamic DOD network defense, assuring Global Decision Superiority.

The full-spectrum of Computer Network Operations encompasses three domains: Computer Network Attack (CNA), Computer Network Exploitation (CNE) and Computer Network Defense (CND). CND includes actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions and other unauthorized actions that would compromise or cripple defense information systems and networks.

USCYBERCOM will conduct operational and tactical level planning and day-to-day employments of assigned and attached CNA forces, integration of CNA forces with CND forces and planning and coordination of network attack capabilities that have trans-regional effects or that directly support national objectives. This includes CAN in support of all assigned missions, and CAN planning and integration in support of other combatant commanders, as directed.

In defense of the GIG, the USCYBERCOM will, in conjunction with other Combatant Commands, military Services, and Agencies, be responsible for coordinating and directing the defense of GIG. This mission includes the coordination of DOD defensive/offensive actions with non-DOD government agencies and appropriate private and international organizations.

2.0 SCOPE

The contractor shall provide a broad range of cyber and NetOps analysis for USCYBERCOM. The VENDOR shall create cyber-intelligence products, recommend actions to affect the security of the networks, provide intelligence for Course-of-Action development for offensive operations and perform Cyber analysis necessary to increase informational understanding of nation states, criminal elements, and terrorist entities' computer network operations

programs and capabilities. Analysis will also be necessary to ensure the GIG is sufficiently controlled to provide situational awareness of network devices, applications, services, and conduits. This effort will help to ensure information is correctly protected and shared within the DoD, federal, state, and local government counterparts, and our coalition partners and allies.

3.0 SPECIFIC TASKS

3.1 Cyber Analysis Support

The contractor shall provide assistance in developing processes and procedures designed to facilitate CNO criminal and counterintelligence media and technical information analysis support to USCYBERCOM components, the USCYBERCOM staff and Commander. The contractor personnel will analyze ongoing Information Assurance/Computer Network Defense related activities and make recommendations from an LE/CI perspective for Commander, USCYBERCOM to protect the DOD GIG. The Contractor shall maintain visibility of non-DoD cyber events occurring both within U.S. government systems and internationally to identify possible relationships to current and available intelligence. The Contractor shall provide criminal and counterintelligence media analysis assessments and computer threat analysis from an LE/CI perspective. The Contractor shall provide CI requirements management expertise to facilitate the acquisition and dissemination of information required to formulate CI analysis, and assist in LE/CI and USCYBERCOM operations. At the direction of USCYBERCOM-, the Contractor shall maintain communications with Law Enforcement Counterintelligence (LE/CI) representatives at USCYBERCOM Service components, Combatant Commands, Military Services, parent headquarters, Dept of Homeland Security/National Infrastructure Protection Center (NIPC), NSA, CIA, and DIA/J2/JCS to identify changes in the cyber environment. The Contractor shall produce special reports and assessments related to specific cyber incidents and trends as required. The Contractor shall maintain cognizance of overall LE/CI trends, analysis and operations related to computer network defense within the DoD and national level communities of

3.2. GIG Threat and Intrusion Intelligence Analysis Support

The contractor shall provide assistance in developing processes and procedures designed to facilitate all-source intelligence analysis of the foreign threat picture in support of USCYBERCOM- components, the USCYBERCOM staff and Commander. The Contractor shall assist in analyzing ongoing threat related activities and information targeting the GIG. The contractor personnel will assist in analyzing Information Assurance/Computer Network Defense activities on DoD systems and make recommendations for USCYBERCOM action to protect the DoD GIG. Analysis will evaluate operational information, intelligence assessments and reports, Computer Emergency Response Team, LE/CI, allied/coalition, and open-source information to assess potential impacts on the GIG and alert the USCYBERCOM and parent command structure. At the direction of USCYBERCOM-GNO leadership, the Contractor shall maintain communications with the USCYBERCOM service components, other combatant commands, parent command, Department of Homeland Security/NCSD, other CERTS and Information Assurance Centers to identify changes in the environment. The Contractor shall maintain visibility of events occurring both within the U.S. government systems and internationally as directed to identify possible relationships to current and databased intelligence. The contractor shall continue to execute tasking with J2 guidance.

- The Contractor shall produce special reports and assessments related to specific incidents and trends concerning threats to the GIG as required.
- The Contractor shall conduct Indications and Warning (I&W) analysis to assist in predicting potential against the DOD GIG.
- The contractor shall respond to the J2 for threat identification of activity directed against DoD systems.
- The Contractor shall evaluate international events, all-source and open-source intelligence, and operational information to assist in the assessment of potential impacts to the DOD GIG and alert the USCYBERCOM and parent command structure to potential network exploitation or attacks. Using these techniques and taking advantage of web-based research tools, the contractor shall match potential threat candidates with the J3 identified activity, produce reports and/or briefs, and make intelligence-derived recommendations to the J2/J3 for the defense of the affected network.
- The Contractor shall assist in editing all reports and report formats for content and clarity as needed in support of J2, USCYBERCOM-GNO Phase I and II intelligence reporting.

- The contractor may develop and present in-depth intelligence briefings and presentations concerning nation-state and non-state actor capabilities and activities, specific actor profiles, and incidents affecting DoD communications networks.
- The contractor shall assist in the management of daily intelligence reports and bulletins and web sites on the classified networks.
- The Contractor shall maintain communications as directed with intelligence representatives at USCYBERCOM Service components, other Combatant Commands, parent command, Department of Homeland Security, National Infrastructure Protection Center (NIPC), NSA, CIA, DIA, Joint Staff J2/JCS, and other organizations as designated.

3.3 Intelligence Watch Officer Support

The Contractor shall man a 24 x 7, 365 day-a-year Intelligence Watch Officer position in support of J2 surge operations as needed. As the J2 representative to the Joint Operation Center (JOC), the Contractor shall assist the Command Duty Officer (CDO) understand, manage, and mitigate incidents on the DoD GIG. The Contractor shall maintain 24 x 7 communications with the analytical divisions and J2 leadership. The contractor shall assist in the development and management of daily intelligence reports and briefings. The Contractor shall update and maintain USCYBERCOM /J2 websites on the NIPRNET, SIPRNET, JWICS, NSANet and Stone Ghost systems. The contractor shall supply administrative assistance to the J2 directorate as required. The contractor shall continue to execute tasking with J2 guidance.

3.4 Intelligence Mission Management Collection and Requirement Analysis Support

The contractor shall provide assistance in the creation of collection strategies, postures, and plans in order to meet USCYBERCON Intelligence and information gaps. Contractor personnel will assist in the validating, coordinating, drafting, submitting, and maintain of formal USCYBERCOM Intelligence requirements and requests to the IC through USSSTRATCOM. Contractor personnel will participate in strategic working groups in order to effectively assist in the planning of long range collection efforts, deconflict and coordinate Intelligence and information needs and requirements that cross organizational boundaries, and facilitate joint collection efforts at the strategic level. Contractor personnel will also assist in the deconfliction of time sensitive requirements among JIATF-CYBER partners with assistance of designated members of the J2X and other CYBERCOM J2 personnel as needed. Contractor personnel will assist in the planning and management of organic collection assets through the Intelligence, Surveillance, and Reconnaissance planning process. Contractor personnel will assist in the coordination of non-organic collection activities supporting USCYBERCOM missions and goals. Contractor personnel will assist in the validation, deconfliction, and consolidation of assigned/attached service J2 elements Intelligence requirements. Contractor personnel will assist in the development, revision, and maintenance of the Command Priority Intelligence Requirements as well as support the collection planning of Operational Planning Teams and other working groups operating within the command.

4.0 DELIVERABLES Indicate the deliverables and when they are due. Tie them into the tasks.

Task #	Deliverable Title	Format	Quantity	Calendar Days to Start
All	Monthly Status Report	Government-derived	Two (2) copies to COR; Two (2) copies to Division Chief; One copy to Contracting Officer	Monthly, on the 15 th workday
All	COAs, Reports, Plans and Studies	Standardized Format	One (1) copy to COR, One (1) copy to Division Chief ; One(1) copy distributed to Division staff via electronic mail.	Within five (5) business days of event.
All	After action reports and meeting	Standardized Format	One (1) copy to COR,	Within three

	minutes		One (1) copy to Division Chief ; One(1) copy distributed to Division staff via electronic mail.	(3) business days of event.
All	Special studies and reports	Standardized Format	One (1) copy to COR, One (1) copy to Division Chief ; One(1) copy distributed to Division staff via electronic mail.	Within ten (10) business days of event.
All	Mission enhancement reports	Standardized Format	One (1) copy to COR, One (1) copy to Division Chief ; One(1) copy distributed to Division staff via electronic mail.	Within five (5) business days of event.
All	Evolving IO Policy Trends and Issues and Reports	Standardized Format	One (1) copy to COR, One (1) copy to Division Chief ; One(1) copy distributed to Division staff via electronic mail.	Within ten (10) business days of event.
All	Survey and Analysis of Requirements Reports	Standardized Format	One (1) copy to COR, One (1) copy to Division Chief ; One(1) copy distributed to Division staff via electronic mail.	Within ten (10) business days of event.
All	Plans and Reports for an Enhanced Requirements Handling Process	Standardized Format	One (1) copy to COR, One (1) copy to Division Chief ; One(1) copy distributed to Division staff via electronic mail.	Within five (5) business days of event.

Task Order Management. Prepare a Task Order Management Plan describing the technical approach, organizational resources and management controls to be employed to meet the cost, performance and schedule requirements throughout TO execution. Provide a monthly status report monitoring the quality assurance, progress/status reporting and program reviews applied to the TO.

- Contractor management personnel will meet weekly with the government task monitor to discuss activities, identify resource issues, and clarify priorities.
- The contractor shall coordinate with the government and plan 2 Configuration control boards at locations TBD.
- The contractor will provide a monthly status report monitoring the quality assurance, progress/status reporting and program reviews applied to the TO. Within the monthly status report, the contractor shall provide the following information: sub-tasks worked, hours expended by labor category and costs by labor category. The contractor will document its accounting procedures for tracking labor hours.
- The contractor and the government will meet to discuss follow-on efforts within 15 days after contract award for the purpose of reviewing requirements and establishing firm dates for the Contract Deliverable Requirements List.

- The contractor shall prepare a Plan of Accomplishment (POA) that will address any changes made at the time and serve as the vehicle for establishing firm dates for incremental deliverables.
- The contractor will deliver quarterly progress reviews, which will include expected tasks for the next quarter.

5.0 PERIOD OF PERFORMANCE Base period of one year (12) months with three option periods of 12 months each.

6.0 PLACE OF PERFORMANCE Work shall be performed at the Government site located in the vicinity of Fort Meade, Maryland.

7.0 TRAVEL Travel may be required, however, specific durations and locations cannot be specified at this time. All Contractor travel shall be coordinated and approved in advance by Contracting Officer's Representative and Program Manager.

8.0 CLASSIFICATION/SECURITY Vendor shall possess a TS/SCI security clearance with requirement to complete Counterintelligence polygraph. The contractor shall comply with the provisions of the DoD Industrial Security Manual for handling classified material and producing deliverables. ADP Level I is required for all levels of information classification. Unclassified reports prepared under this task order shall be marked For Official Use Only (FOUO) unless otherwise stated by the Contracting Officer's Representative. The contractor shall be responsible for safeguarding all government property and information provided for contractor use. At the close of each work period, government facilities, equipment and materials shall be secured. The contractor will provide to the government the safeguard measures used to protect information when it is stored off-site. The contractor will provide these safeguard measures at the Contract Deliverable Requirements List Meeting.

9. GOVERNMENT FURNISHED PROPERTY The Government will provide workspace, computers, connectivity and other resources required to accomplish the tasks outlined in this Statement of Work. The Government will provide access to non-procurement sensitive documentation, information on various weapon systems, program process and schedules as well as intelligence and information pertaining to cyber activities in support of military information operations, related activities and associated follow-on tasks to enable contractors to complete their assigned tasks. Information will include reports, briefings and other related reference material. Government furnished equipment related to this task may be provided. The Government will provide the contractor with the timely information, to include access to both unclassified and classified government information networks, required for the completion of this effort and facilitate contractor personnel interfaces with other Department of defense staff, service staff, national agency offices, as required to complete this effort.

10. PAYMENT SCHEDULE The contractor shall bill monthly.

11. NON-PERSONAL SERVICES STATEMENT

Contractor employees performing services under this order will be controlled, directed, and supervised at all times by management personnel of the contractor. Contractor management will ensure that employees properly comply with the performance work standards outlined in the statement of work. Contractor employees will perform their duties independent of, and without the supervision of, any Government official or other Defense Contractor. The tasks, duties, and responsibilities set forth in the task order may not be interpreted or implemented in any manner that results in any contractor employee creating or modifying Federal policy, obligating the appropriated funds of the United States Government, overseeing the work of Federal employees, providing direct personal services to any

Federal employee, or otherwise violating the prohibitions set forth in Parts 7.5 and 37.1 of the Federal Acquisition Regulation (FAR). The Government will control access to the facility and will perform the inspection and acceptance of the completed work

SB Sign In Roster

6 August 2010

Name	Company	Telephone #	E-mail
Josh Kinley	PCI	410.967.0335	josh.kinley@pci-sm.com
Jacky Kimmed	ITK	410-782-4862	Jacky@Infotekcorp.com
Courtney Matson	ITK	410.782.4862	courtney.matson@infotekcorp.com
Don Whiffeld	PCI	443-538-6445	don.whiffeld@pci-sm.com
Jonathan Sutton	Radius Technology Group	301 865 3400	jsutton@radius360.net
David Wheeler	Tsource, LLC	301-502-2072	dwheeler@tsource.com
Michael Lynott	Evergreen ITS	571 435 6835	mlycott@evergreenits.com
JOHN SELVA	Fedconcepts	202 680 4980	JOHNSELVA@FEDCONCEPTS.COM
ERIK HALVERSON	FEDCONCEPTS	202 510 6517	erik.halverson@fedconcepts.com
JUSTIN KEES	CYBERSPACE Sol	703.798.7920	JKEES@CSPACESOL.COM
PAUL SULLIVAN	CYBERSPACE Sol		SULLY@CSPACESOL.COM
TODD VAN HAAREN	AKG	703 919 3145	trvanhaaren@akgroup.com
MICHAEL PAIT	DASTON	703 314 8287	mike.pait@daston.com
Melanie Newton	Daston Corp.	703-962-8083	melanie.newton@daston.com
John A. Sanders	Global Resource Solutions	571 257-5155 571 329-0987	jsanders@grsco.com
Gerhard Tieferbrunn	IKM	703.362.9727	tieferbrunn@interf. w
Ben Edson	Varig	202-210-6051	ben.edson@varig.com
ERIC KREBS	Blue Glacier	703-961-5555	eric.krebs@BlueGlacier.com
DAN LOOPER	TMR	703-431-1697	dan.looper@TMRHQ2.com
Jason Port	Harnessed Electrom	610 613 9204	jason.port@us.army.mil

Michael Savaiides Pillar Systems 703-548-4800 #1009 mdsavaiides@PillarSystems.com

6 August 2010

6 August 2010

[illegible]

SB Sign In Roster

6 August 2010

Name	Company	Telephone #	E-mail
Sean Battle	PCI Strategic Managers	410 312 0885	sean.battle@pci-sm.com
Andy Baratta	Wius	301 356 0754	andybaratta@wiusnetworks.com
RON DABIZIERI	BCT	703-582-6777	r.dabizieri@bct-llc.com
STEPHEN TATE	BCT	(240) 315-3043	s.tate@bct-llc.com
Craig Parisot	Inventix	703-513-2154	cparisot@inventix.com
Vince Jones	SGIS	571 277 3541	VJones@SGIS.com
Mark Thomas	IP Network Solutions	703 340 6025	MThomas@iwnsinc.com
Karen Sobieski	NMR Consulting	410-573-0080	ksobieski@NMRConsulting.com
William DeVault	IP Network Solutions	703-787-0095	wdevault@ipnwsinc.com
PATRICK BURNS	GS Advisors	703 582 1418	PAT@GSadvisorsCorp.com
Shawn Broughton	Mass3I	202 270 4044	Sbroughton@mass3i.com
Mike Leishman	ADVANTAGE SOLUTIONS	301-875-8888	Mike@ADVANTAGESOLUTIONS.com
Ash Halim	Xpect Solutions	571-233-5880	ahalim@xpectsolutions.com
JOHN GOULDMAN	XPECT SOLUTIONS	540-374-0989	JOHN.GOULDMAN@XPECTSOLUTIONS.COM
Ken Spedden	DATA	703 309 8875	KSPEDDEN@DATA-INC.COM
GREG FURST	IOMAXIS	703 455 2555	GFURST@IOMAXIS.COM
CHRIS WALTERS	TRI-COR	301 731 6140	C.WALTERS@TRICORIND.COM
Helen Elwood	Phacil Inc	703-564-2424	Helwood@phacil.com
James Hooper	IFM	703 227 8432	hooper@interf.com
JACK WARD	VPSI	571-766-3506	jack.ward@wvps.com

Marshall Hawkins SHC 571-323-6565 m.hawkins@systemshigh.com
 NICHOLAS KLEIN OPTIMUS TECHNOLOGY 443.684.2121 NICHOLAS.KLEIN@OPTIMUSTECHINC.COM

SB Sign In Roster

6 August 2010

Name	Company	Telephone #	E-mail
KEN SWELTZ	CTC	814-241-4576	KWS@CTC.COM
Thaddaus Shaw	Analyst Warehouse	443-562-3431	tshaw@analystwarehouse.com
DAVID CRAY	VEXITSS	703.391.9270	DAVID.CRAY@VEXITSS.COM
JOHN ANDERSON	TANGLER	571-225-4700	JANDERSON@TANGLER.NET
J.D. McFALLS	POINT ONE, Inc	443-538-6745	jmcfalls@pointoneinc.com
Joe Parker	Delphi Prime	410-774-5887	jparker@delphi.prime.com
Michael Islek	Phacil TOXICITY	516-713-4895	mislek@phacil.com
Mark Hall	ESS	202-604-0514	mhall@essworld.net
DOUG HARLOW	GD AIS	703 227 1406	douglas.harlow@gais.com
Bob Thompson	VPSI	574 766-3507	Bob.Thompson@myvpsi.com
Omee Dauplaise	AZ-Tech Intl	301-471-0373	jd@AZ-TechINTL.COM
DENTON BIRGEL	GENERAL DYNAMICS	410-684-3760 x225	DENTON.BIRGEL@GDI.COM
ANTHONY MANICILLAS	OLGOMK GLOBAL SECURITY	703 265 0208	amanicillas@olgonk.com
RAY FIELDS	UMISYS	443-690-8058	RAY.Fields@umsys.com
JASON BRUDZINSKI	CSC	571 217 8667	jbrudzinski@csc.com
JIM KOSHAR	SAVA	703.597.8625	JAMES.KOSHAR@SAVASolutions.ca
RANDALL COLEMAN	RED FIVE SECURITY	703 855 6513	KRIS@REDFIVESECURITY.COM
Michael Mock	Dependable Global Solutions	371-594-4466	mike.mock@us-dgs.com
GEORGE ROMAS	THERMOPYLAE	301-641-2656	gromas@t-sciences.com
Calvin Rhodes	IPPLUS Consulting	443 629 7838	calvin.rhodes@ipplusinc.com
Shawn Elliott	IPKEYS	540 657 4117	sellott@ipkeys.com

SB Sign In Roster

6 August 2010

Name	Company	Telephone #	E-mail
Mark Clark	Bridges	301-974-6233	Mark.Clark@Bridges-inc.com
Daniel Peterman	New World Solutions	703 413 3703	daniel.peterman@nws-us.com
Joe Halfon	Ida	301 675 3719	jo.halfon@ida-ss.com
Paul Rosenbloom	SATC	443 367 7755	paul.rosenbloom@satc.com
Rick Barton	SPT	301-854-2215	RichardB@spt-inc.com
CHAD SUMPTER	Roz Allen	703 855 6239	sumpter_chad@694.com
Cynthia Viola	ITT	313 601 7743	cynthia.viola@itt.com
Tom Loney	Evolver	703-742-4090	tloney@evolverinc.com
Mike O'Kane	Evolver	703-742-4090	mokane@evolverinc.com
DAN Lundien	CTP	410-290-3280	dan.lundien@ctp-web.com
Chris Archer	Radius Technology Corp	301 565 3400	carcher@radius360.net
JUAN SEBASTIAN	ABSC	703-437-3000	Juan.Sebastian@ABSC-us.com
DAVID CARDONE	ABSC	703-437-3000	DAVID.CARDONE@ABSC-us.com
Priscilla Charles	STI	301-352-9048	pcharles@stihp.com
Ed Stoker	Bluemont Technology	703-608 5087	ed@bluemonttechnology.com
Tim Hatcher	LONGVIEW	540-636-7930	thatcher@longview-inc.com
Greg Gurnu	OKS	703-462,693	ggurnu@ok6000.com
Ted DiBenedetto	TJ Westlake, LLC	703 597 6714	Ted@tjwestlake.com
Ted Tzavellas	S4 Inc.	703-418-0040	ttzavellas@s4inc.com
Reggie Ragland	Paul Prutz Solutions	410-703-0689	rragland@paulprutzsolutionsinc.com
DAREN MAGRUDER, CLEARSHARK 910.528.2850 daren@clearshark.com			

SB Sign In Roster

6 August 2010

Name	Company	Telephone #	E-mail
ROMAN NOWAKOWSKI	QUALTECH INC	571-236-7635	ROMAN@QUALTECHINC.NET
LAMART BAZUE	QUALTECH INC	301-351-4197	lamart.bazue@QUALTECHINC.NET
Glen Adams	Cogent Solutions	542-872-7707	gadam511@Cogent-7003.com
Norman P Byers	Analyse Warehouse	703 644 2794	nbyers@STRATIVES.COM
MARK GREER	CENTAURI Solution	703 308 4876	MARK.GREER@CENTAURI-SOLUTION.COM
Mark Szanca	Szanca Solutions	301-785-1605	mark@szanca.com
BOB BEITER	SZANCA SOLUTION	814 624 0123	bbeiter@SZANCA.COM
Ron Sinek	Point One	703 414-5440	rsinek@pointoneinc.com
Steve Frenz	SAIC	443-621-0822	sfrenz@saic.com
MARTY LESHIN	VAREN	410-290-8008	leshinm@varentech.com
Tom Nugen	Booz Allen	(703) 439-4057	nugen-tom@bah.com
Paul Kim	Booz Allen	713-377-7145	kim-paul@bah.com
GREG FURST	10MAXIS	703 455 2555	GFURST@10MAXIS.COM
BRUCE BELT	10MAXIS	703 455 2555	BBELT@10MAXIS.COM
STEVE WALKER	NET CENTRICS	703 714 7345	SWALKER@NETCENTRICS.COM
ANTHONY BARGAR	ESS	571-366-7492 703-644-1444	ABARGAR@ESSWORLD.NET
MATTHEW MILLER	BLUE CANOPY	571 275 2842	mmiller@bluecanopy.com
C.J. Heatley	Ashlar	703-627-1748	heatley@cmcast.net
John Meincke	LIS/SENSEX	703 585-7124	jmeincke@lisworld.net
Brian Oliver	TRUSTLARK	703-543-2003	Brian.Oliver@TRUSTLARK.COM
MATT TIRMAN	Strategic Social	571-338-7015	Matt.tirman@strategicsocial.com
Latoya Jones	GWA Innovative Technology, Inc.	703-364-6324	latoya@gwainneter.com

SB Sign In Roster

6 August 2010

Name	Company	Telephone #	E-mail
John Reinemann	Inventix	703 813 2115	jreinemann@inventix.com
Steve Willett	Inventix	703 882 8741	swillett@inventix.com
Rick Shaffer	MorganFranklin	703 895 9797	rick.shaffer@morganfranklin.com
CYRUS NELSON	Fullcast	410-799-4119	CYNELSON@STARPOWER.NET
KYLE VON BUCHOLZ	FEDERATED IT	202 434 8959	KVONBUCHOLZ@FEDERATEDIT.COM
WILLIAM RING	FOURCAST	410 799-4119	WILLIAM.RING@FOURCASTUSA.COM
MATT BUCHOLZ	FEDERATED IT	202 434 8959	MBUCHOLZ@FEDERATEDIT.COM
Tom Stauber	Axiologic Solutions	571 252 9461	Tom.Stauber@axiologic.com
Michael Chavira	Axiologic Solutions	202-374-6453	michael.chavira@axiologic.com
Andre Long	EAEG LLC	301-237-2197	AndreLong@eaeg.com
Ernest Hampson	Battelle	571-227-6331	hampson@battelle.org
Brian Snyder	ISW	703 222 7015	brian.snyder@iswcorp.com
JAMES STEPHENS	RED ARCH	703 343 6680	JAMES.STEPHENS@REDARCHSOLUTIONS.COM
Joshua Segroves	ISW	281-660-8666	joshua@iswcorp.com
Heather Hoyer	Red Arch	443-539-0615	heather.hoyer@redarch.com
Charles Trinker	ETG	203-298-4484	ctrinker@etg.com
John R. Clark	Battelle	571-227-6353	clarkjr@battelle.org
Jerome Newsome	PTS	(703) 682-4144	jerome.newsome@enterpts.com
Robert Cairne	HP	703-229-4324	Robert.cairne@HP.com
Cindy Furbush	QualTech	703 772 1032	cindy.furbush@qualtech.com
Andrew Dumas	Vet's Group	703-428-4394	adumas@vetsgroup.com

SB Sign In Roster

6 August 2010

Name	Company	Telephone #	E-mail
Paul Debow	Varen	416-290-8008	weidowp@varentech.com
Stan Nolan	Varen	"	nolans@varentech.com
Dee Cutter	Sterling Regency	410 977 9989	dee.cutter@sterlingcomputers.com
JOE GAWLIK	FGM	703-885-1039	jog@FGM.COM
Lillian Heizer	TMC	571-521-9566	lillian.heizer@tmrhy2.com
Paul Strasser	DRC	571-226-8650	pstrasser@drc.com
Paul Mullis	Ashlar	703 870 4740	pmullis@ashlar-Tech.com
Brian Barrett	Ideogenics	202 904-2495	bbarrett@ideogenics.com
JAY MARLEY	ACCESSDATE	202-573-2679	JMARLEY@ACCESSDATE.COM
Bill Young	Imprimis	703-217-3076	WAYIIE3@Verizon.net
Hector Marquez	SSG	703-582-8388	hmarquez@SecuredSciences.com
Noah Leask	ISHPI	843 329 4100	Noah.Leask@ishpi.net
Matt Letnaunchyn	Veris Group	571-722-1725	mletnaunchyn@verisgroup.com
ROBERT MANNING	3IT CONSULTING, LLC	210-887-9857	RNMANNING@3ITCONSULTING.COM
LEWIS RADER	ZEL TECHNOLOGIES	757-325-1381	LOU.RADER@ZELTECH.COM
Harvey Davis	Overwatch Sys	703-945-3062	HDAVIS@OVERWATCH.TECHN.COM
ANTONIOS HATZIGEORGALIS	ITK (INFOTEK)	410-782-4862	TONY@Infotekcorp.com
ERIN HORTON	ITK (INFOTEK)	410-782-4862	ERIN.HORTON@Infotekcorp.com
DOUGLAS HARLOW	GENERAL DYNAMICS - AES	703 277 1406	DOUGLAS.HARLOW@GD-AES.COM

6 August 2010

[illegible]