Working with the DoD Cyber Science and Technology Community

15 March 2010

Steven E. King, Ph.D.
Deputy Director for Cyber Security Technology
Office of the Assistant Secretary of Defense for Research and Engineering
Outline

- DoD Cyber S&T
- SBIR Workshop
- IA Connect
- DeVenCI
- IATAC → CSIAC
- CERT/SEI
Cyber S&T Receives Focused Support from DoD Leadership

• **DepSecDef, Hon. William J. Lynn, III**
  – The Defense Department has formally recognized cyberspace for what it is – a domain similar to land, sea, air, and space; a domain that we depend upon and must protect

• **ASD(R&E), Hon. Zachary J. Lemnios**
  – The problem is complex and asymmetric – attackers often need to find just one vulnerability while defenders must currently defend everywhere with multiple approaches
  – In order to meet the challenge of defending against and defeating the threat, new thinking and new research ideas are needed to build a more resilient and trustworthy cyberspace
DoD IA Research Community

- DoD IA Research: $222.3M in FY11
  - Coordinated by Cyber S&T Steering Council
- SBIRs are funded by ASD(R&E), DARPA, the Services and Agencies
Annual ASD(R&E)
Cyber Security SBIR Workshop

• **Goals**
  – Showcase the latest Cyber Security SBIR-related research, technology, and products
  – Provide networking opportunities for Government customers, Phase II SBIR contractors, DoD primes/integrators to identify technology transfer and commercialization opportunities
  – Capture metrics demonstrating SBIR technology transfer effectiveness

• **Format consists of these major elements**
  – Briefings (rapid fire – 12 minutes – non-proprietary)
  – Private meetings – one-on-one break-outs to discuss opportunities
  – Poster session – networking opportunity and social
  – Featured speakers – timely topics or areas of special interest
DoD/DHS Annual SBIR Workshop

- **Information Assurance, Software Protection, Anti-Tamper**
  - More than 120 participants at 2010 workshop

- **Briefings:**
  - 32 small businesses
  - 11 primes/integrators
  - 4 government
  - 6 featured speakers

- **Metrics data collection:**
  - New relationships: 131 reported company-to-company contacts
  - One-on-one meetings: 85 private discussions between small businesses and primes
  - Planned follow-ups: 167 reported
  - Deals made on-site: 21 reported
  - Overall satisfaction: 4.7/5.0 (48% response rate)

- **Fifth annual SBIR Workshop will take place on 12-14 July 2011 in McLean, VA**
  - Register online: https://register.mitre.org/sbir/

- **For more SBIR/STTR information:**
  - [http://www.dodsbir.net/](http://www.dodsbir.net/)
2010 OSD SBIR/STTR Projects

- **OSD10-IA1** Countermeasures to Malicious Hardware to Improve Software Protection Systems
- **OSD10-IA2** Effective Portable Data Content Inspection and Sanitization
- **OSD10-IA3** Robust and Effective Anti-Phishing Techniques
- **OSD10-IA4** Preventing Sensitive Information and Malicious Traffic from Leaving Computers
- **OSD10-IA5** Biometric-based Computer Authentication during Mission-Oriented Protective Posture Scenarios

- **Approximately $10M annually**
  - 2009: 25 new Phase I, 32 active Phase II contracts
  - 2007-present: 123 Phase I, 67 Phase II awards
IA Connect

- IA Connect provides a single interface within the Office of the DoD Chief Information Officer (CIO) to facilitate initial interactions and conduct research on commercial IA vendors

- IA Connect breaks down barriers of information sharing between the IA commercial community and potential DoD customers by serving as one focal point for vendor research, communication, and coordination

- In turn, DoD gains valuable insights into IA market trends and a history of vendor interactions between the community and specific IA companies

- The research functionality of IA Connect supplies DoD with market insights and a view of commercial IA vendors, improving "matchmaking," and increasing knowledge of valuable IA commercial technologies

- IA Connect will provide such relevant information as: company and product background, previous contacts with other DoD entities, competitors, and other useful market information

http://iac.dtic.mil/iatac/IA_connect.html
Defense Venture Catalyst Initiative (DeVenCI)

- Supports DoD and other government agencies, including the Intelligence Community, in discovering promising technology products from non-traditional commercial markets that meet stated operational needs
- Leverages volunteer Venture Capitalists as the “search engine” to identify emerging commercial products
- DeVenCI is an AT&L/ASD(R&E)/Rapid Fielding program using an OGC approved business plan

Develop Needs
- Needs Workshop
- Create Needs Document

Product Nomination
- VCs Nominate Companies
- FedBizOpps self nominations

Product Presentations
- Sponsor selects Products
- Solution Workshop

Product Experimentation & Sponsor Acquisition

For more information: http://devenci.dtic.mil
Information Assurance Technology Analysis Center (IATAC)

• **Mission**
  – IATAC provides the DoD a central point of access for information on Information Assurance emerging technologies in system vulnerabilities, research and development, models, and analysis to support the development and implementation of effective defense against Information Warfare attacks

• **Current**
  – Maturing cloud computing capabilities at DISA
  – Performing IA/NETOPS Mission Assurance analysis for DISA
  – Developed SIPRNET architecture for USSTRATCOM Joint Cyber Operations Range (JCOR)
  – Provided analysis to JTF-GNO transition of CND capabilities to USCYBERCOM
  – **Spotlight**: Developed DoD IA Policy Chart for DoD CIO
  – IATAC State-of-the-Art Report - *Security in the IT Supply Chain* published October 2010 (Distribution C)

• **Future**
  – Providing cryptography analysis to USAF Cryptologic Systems Group for analysis of Key Management Infrastructure
  – **Spotlight**: Developing national cyber security curriculum for grades 4-12 for the National Science Center

http://iac.dtic.mil/iatac/index.jsp
Solicitation to Run the New CSIAC

• DoD Information Analysis Centers are going through several organizational changes

• IATAC will become part of the Cyber Security & Information Systems Information Analysis Center (CSIAC)
  – Technical Area Tasks (TATs) will include
    – Software Analysis
    – Information Assurance
    – Information Sharing
    – Knowledge Management
    – Modeling & Simulation

• The new CSIAC will be operated under one contract, with an expected award in December 2011

• See FedBizOpps Solicitation # FA1500-11-MKTRES
  – https://www.fbo.gov/
CERT @ SEI – Networked Survivable Systems

• **Code Construction and Analysis**
  – Develop tools and techniques that software developers and software development organizations require to eliminate vulnerabilities
    – Develop secure coding standards for C++ and Java
    – Introduce and promote secure coding standards in international bodies
    – Provide proof-of-concept demonstration of compilers and code analysis tools that verify conformity with secure programming standards

• **Insider Threat Modeling and Analysis**
  – Create empirically based models of insider threat and espionage
    – Develop system dynamics models of insider threat based on findings from the analysis of actual cases
    – Research, identify, and validate a means for organizations to measure insider threat risk

• **Resiliency Measurement and Analysis**
  – Measure security and resiliency in complex systems and critical information infrastructures and develop models for implementing, operating, and sustaining resilient architectures
    – Research and develop objectives for identifying and measuring resiliency attributes for processes and technologies
CERT @ SEI – Networked Survivable Systems

• **Acquisition and Development Practices and Metrics**
  – Prepare acquirers, developers, and operators of large-scale, complex, networked systems to address security and survivability throughout the life cycle
    – Enhance SQUARE requirements engineering approach for privacy; automate SQUARE for acquisition and privacy
    – Develop and pilot a prototype of the Secure Mission Assurance Diagnostic
    – Develop and pilot a prototype software security measures identification method

• **Advancing the Practice of Secure Software Engineering & Technology**
  – Address the technical behaviors required to enable government organizations to make measured improvements in their security and survivability practices
    – Research individual and team technical practices and identify performance measures that correlate to improved mission outcomes

• **Next Generation Security Mechanisms**
  – Leverage emerging software and hardware-based approaches for establishing trusted transactions, even in environments assumed to include malicious agents
    – Conduct trusted computing workshop in Q1FY11
    – Provide proof-of concept demonstration of trusted applications in a known compromised environment
DoD Cyber S&T
- Looking Ahead -

• Cyber domain is a dynamic and complex operational environment
  – Man-made
  – Intelligent adversaries
  – Requires technical solutions in addition to doctrine, planning, and training

• Coordinated S&T activities position DoD to achieve full spectrum operations in the cyber domain

• DoD S&T will accelerate the innovation cycle through:
  – Defense S&T community
  – Federal partners
  – Industry
  – Academia
  – International partners

Achieving Safe and Secure Cyber Operations Requires Focused DoD S&T Investment
Steven E. King, Ph.D.

Deputy Director for Cyber Security Technology
Research Directorate, Information Systems & Cyber Security
Office of the Assistant Secretary of Defense for Research and Engineering