



Defense Information Systems Agency

Department of Defense

Forecast to Industry Program Executive Office – Information Assurance/NetOps

Mr. Mark Orndorff
Director, Program Executive Office – IA/NetOps
8 August 2008

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 08 AUG 2008		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Information Assurance (IA) and Network Operations (NETOPS)				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) US Army PEO Enterprise Information System				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES Briefings presented at the DISA Forecast to Industry 2008 on August 8, 2008 at the FDIC Training Center in Arlington, VA, The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 14	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Who Are We?

We are the Program Managers for DoD Information Assurance (IA) and Network Operations (NETOPS) capabilities that provide responsive, secure, and interoperable net-centric solutions necessary to secure and operate the Global Information Grid (GIG) in support of the Secretary of Defense, Combatant Commanders, Joint/combined task forces, Services, and Agencies.



What Do We Do?

- **We ensure effective and efficient application, planning, programming, budgeting, and execution of IA resources**
- **We develop, acquire, and implement enterprise wide Computer Network Defense (CND) and IA security products and solutions that identify threats to the GIG, sense network and host-based attacks, develop/disseminate countermeasures and provide situational awareness for GIG NetOps personnel.**
- **We provide secure and reliable identity management services for DoD applications and systems.**
- **We provide cross-domain information sharing solutions for users anywhere on the GIG.**

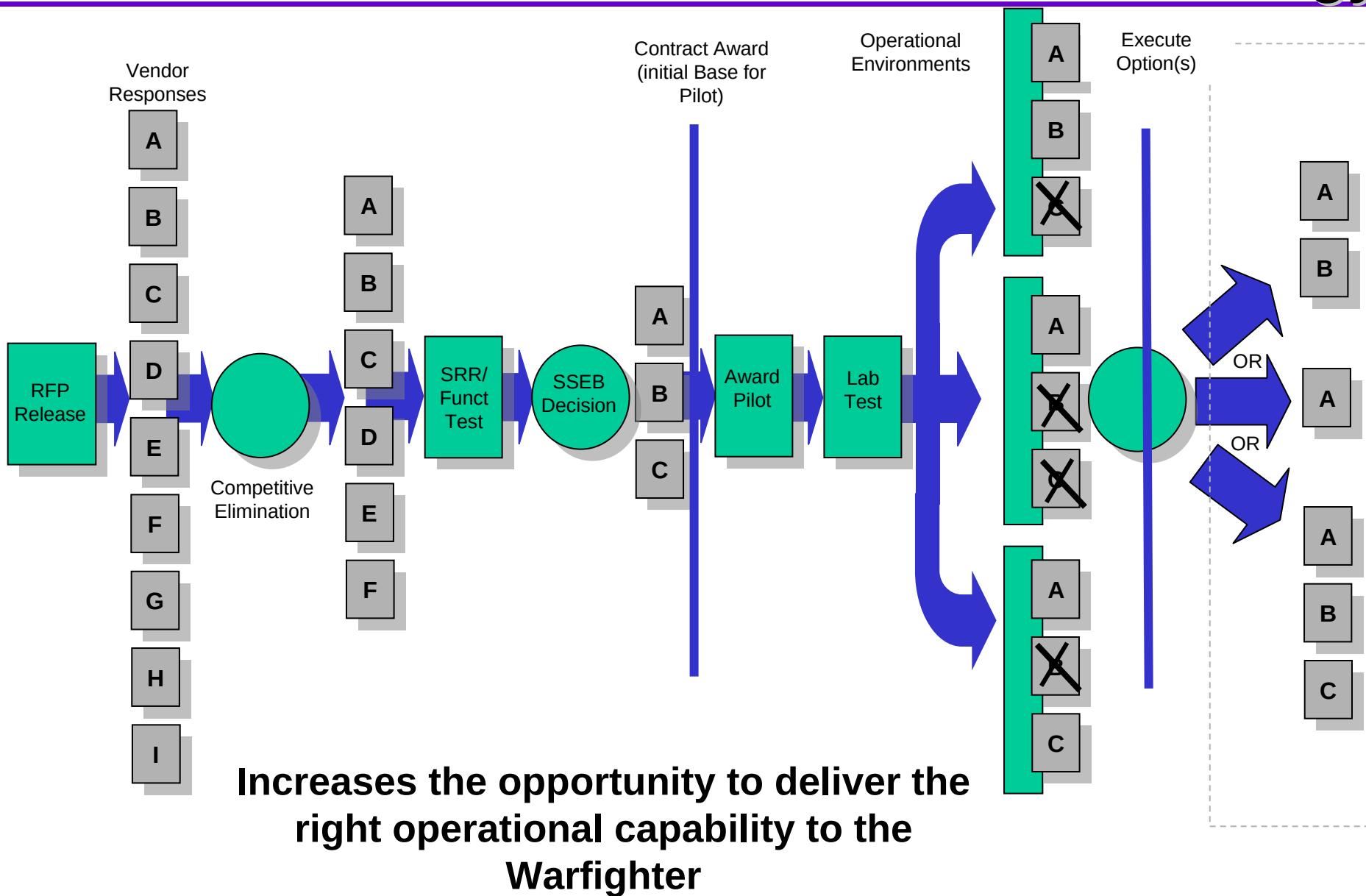


Contract Options

- **IASSURE Vehicle expired in Jan 08**
 - Need to recompetete over 200 Service Contracts in FY09/10
- **ENCORE II**
 - 26 Primes (Small and Large)
 - Performance Based Task Orders for Services and limited support related hardware and software
 - Just awarded for multiple option years
- **GSA**
 - Hardware/Software
 - Vendor needs to have a GSA Schedule to be eligible
- **Other potential options for Service, Hardware & Software**
 - NetCENTS, ITES 2S/H, NASA SEWP....
 - Small Business set asides



Possible Enterprise Acquisition Strategy





We Need Your Help

- **To acquire enterprise-level capabilities that are easier to implement across DoD**
- **To understand the market space and develop innovative ways to scope costs related to the actual usage**
- **To implement and operationalize the capabilities that we acquire**
- **To help us to come up with better ideas to integrate products into a DoD suite**
- **To create multiple opportunities and awards options**



DoD CND Enterprise-wide Solutions Available Now...

Antivirus Products



McAfee



Symantec

Scanning



eEye Retina

Remediation



Citadel Hercules

Wireless



Flying Squirrel

Host Security



McAfee



On-Going Projects

CND User Defined Operational Picture

- Provides network defenders a synchronized view of defensive information
- Development effort
- FY09 - No new acquisition activity

GIG Common Operational Picture

- Provides network operators situational awareness of the Global Information Grid
- Development effort
- FY09 - No new acquisition activity

Joint CERT, Joint Threat Incident, and DoD CERT Databases

- Provides centralized collectors and management databases
- Development effort
- FY09 - No new acquisition activity

Wireless

- Provides wireless (802.11) detection and location
- Currently a GOTS deployed solution
- FY09 – No new acquisition activity



On-Going Projects (cont)

Security Information Manager

- A system that collects, aggregates, and normalizes intrusion and defensive information
- FY09 – sustainment of services and licenses

Antivirus

- Capability and tools to protect computer from compromise, detect infected systems, clean infected systems, and prevent further contamination from those threats to DoD.
- FY09 – No new acquisitions

Demilitarized Zones

- Relocate publicly accessible servers to the NIPRNet edge in controlled DMZs
- FY09 – sustainment of services and licenses. Limited new expansion



New Acquisition Activities

Host Based Security System

- Deploys and manages host based intrusion sensors, defensive capabilities, and INFOCON actions
- FY09 - New capabilities: Asset, Configuration, and Vulnerability control and management. Look at follow-on capability. (Contract(s) TBD)

Insider Threat

- Detect potentially malicious activity by users within the DoD community.
- Fielding a current capability
- Analyzing the existing gap to determine future acquisitions
- FY09 – Market Research and requirements development

Technical Media Analysis Tool

- Forensics analysis tool to determine attack information
- Targeted DoD user group (LE/CI/Network Defenders)
- FY09 – Initial acquisition (ENCORE II Contract Vehicle)

Network Access Control

- Provides an enclave-level Network Access Control (NAC) system to restrict classified network access to known and securely configured devices
- FY09 acquisition (ENCORE II Contract Vehicle)

New Acquisition Activities (cont)

Enterprise Sensors

- Centralized buy of COTS sensors for DoD Combatant Commanders, Services, and Agencies
- FY09 - maintain previously purchased licenses and acquires new capability (Vehicle - GSA, Hardware/Software vehicles)

Secure Configuration Compliance Validation Initiative

- Scans and automatically identifies configuration vulnerabilities
- FY09 – Re compete for a follow-on capability (Vehicle TBD)

Web Content Filtering

- Capability to filter malicious/undesirable web traffic at the DoD NIPRNet to Internet interfaces
- FY09 – Limited Deployment and pilot activities (ENCORE II)



FY09 Acquisition Activities

	Oct 08	Nov 08	Dec 08	Jan 09	Feb 09	Mar 09	Apr 09	May 09	Jun 09	Jul 09	Aug 09	Sep 09	Oct 09
Host Based Security System	Acquisition (RFP and Source Selection) New Capability												
					Market Research/RFI Existing Capability								
Insider Threat	Market Research (RFI and Vendor Days)											Acquisition	
Technical Media Analysis Tool	Acquisition (RFP and Source Selection)												
Sensors		Acquisition											
Firewalls					Acquisition								
Web Content Filtering	Acquisition (RFP and Source Selection)												
Network Access Control	Acquisition (RFP and Source Selection)												
Secure Configuration Compliance Validation		Acquisition (RFP and Source Selection)											

- Increased vendor participation in Market Research and acquisitions (Vendor days and demonstrations)
- “Brainstorming” events to encourage both Government and industry innovation
- Emphasis on implementation of solutions – reduce the deployment time

Assured Mission Execution



www.disa.mil
