Mark S. Orndorff

Director, Mission Assurance and NetOps

DISA

DISA MISSION PARTNER CONFERENCE 2012

Sustaining US Global Leadership: Priorities for 21st Century Defense

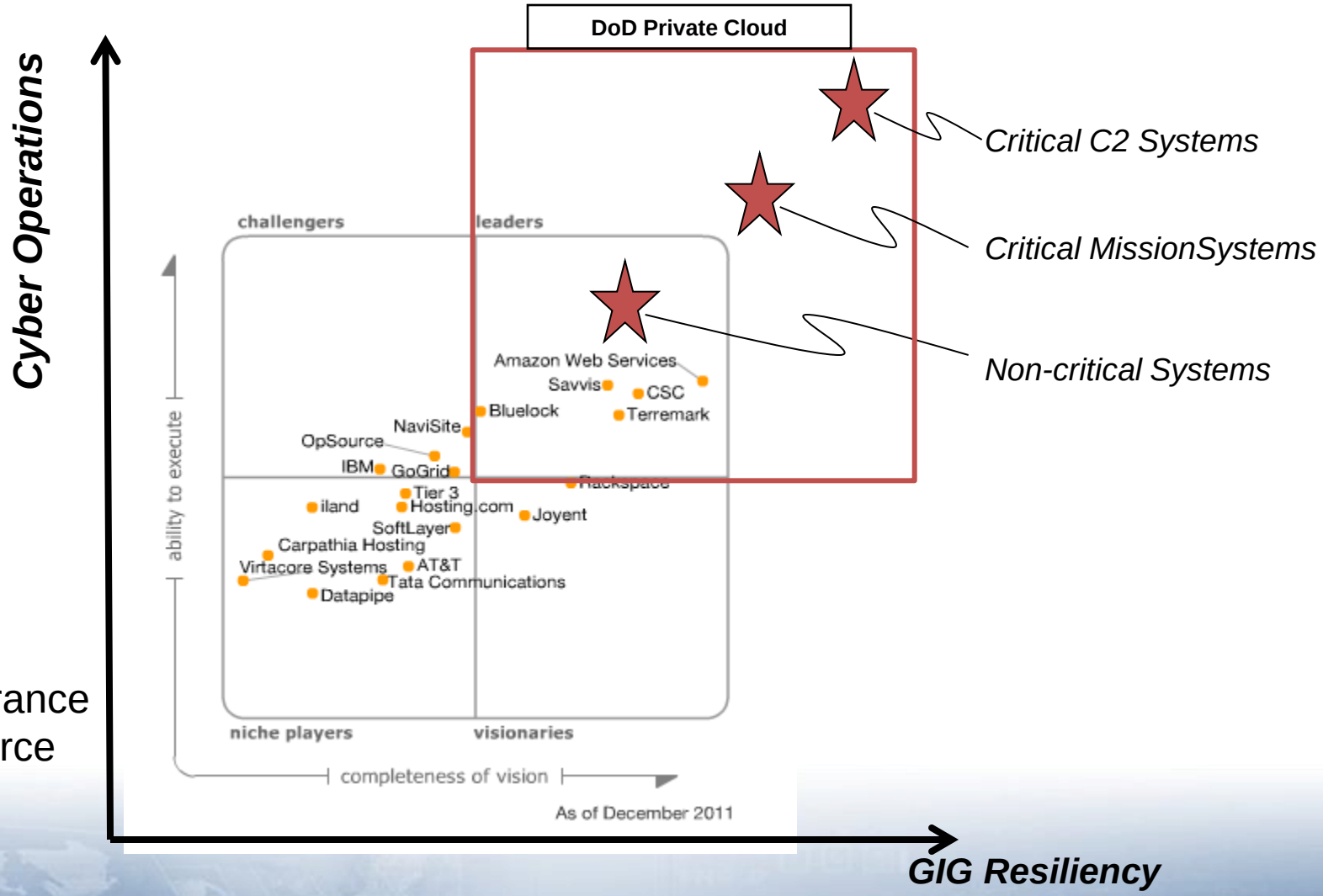
"Both state and non-state actors possess the capability and intent to conduct cyber espionage and, potentially, cyber attacks on the United States, with possible severe effects on both our military operations and our homeland."

"Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space. Today space systems and their supporting infrastructure face a range of threats that may degrade, disrupt, or destroy assets. *Accordingly, DoD will continue to work with domestic and international allies and partners and invest in advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace and space*."

Approach

- Defendable GIG
  - Configure securely, automatically
  - Enhance perimeter defenses – defense in depth
  - Drive out anonymity
  - Improved cyber readiness
- Improve Cyber C2
  - Improved situational awareness
  - Cyber attack detection, diagnosis, reaction at network speed
- Improve Safe Sharing
  - Cross domain flows as an enterprise service
  - Evolve directory, identity, and access control

Magic Quadrant for Cloud Infrastructure as a Service



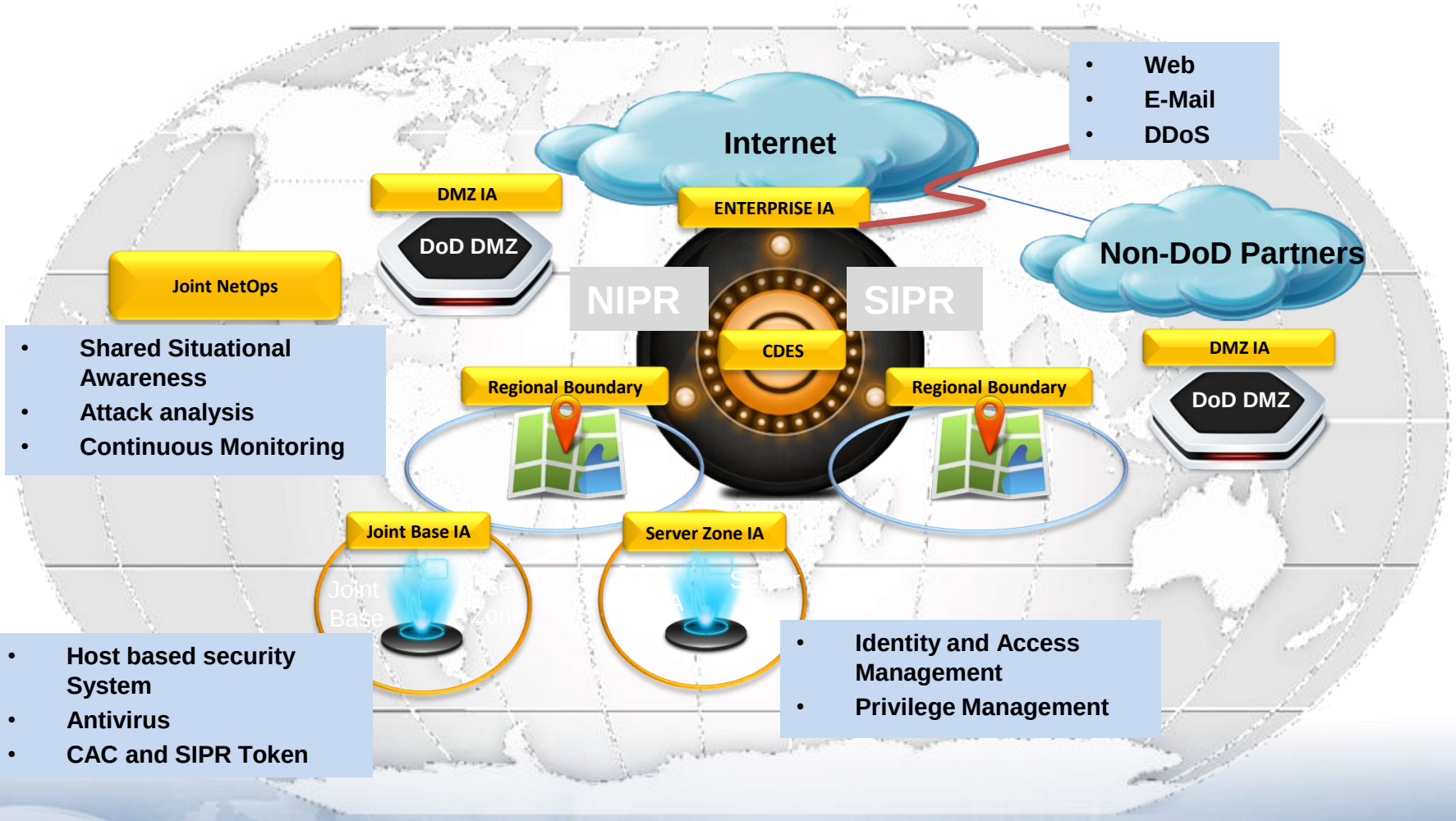
Key Enablers

- Intelligence
- Cyber COP
- CND RA
- Mission Assurance
- Cyber Workforce

Magic Quadrant for Public Cloud Infrastructure as a Service

Source: Gartner (December 2011)

Notional Security Architecture



- Shared Situational Awareness
- Attack analysis
- Continuous Monitoring

- Host based security System
- Antivirus
- CAC and SIPR Token

- Identity and Access Management
- Privilege Management

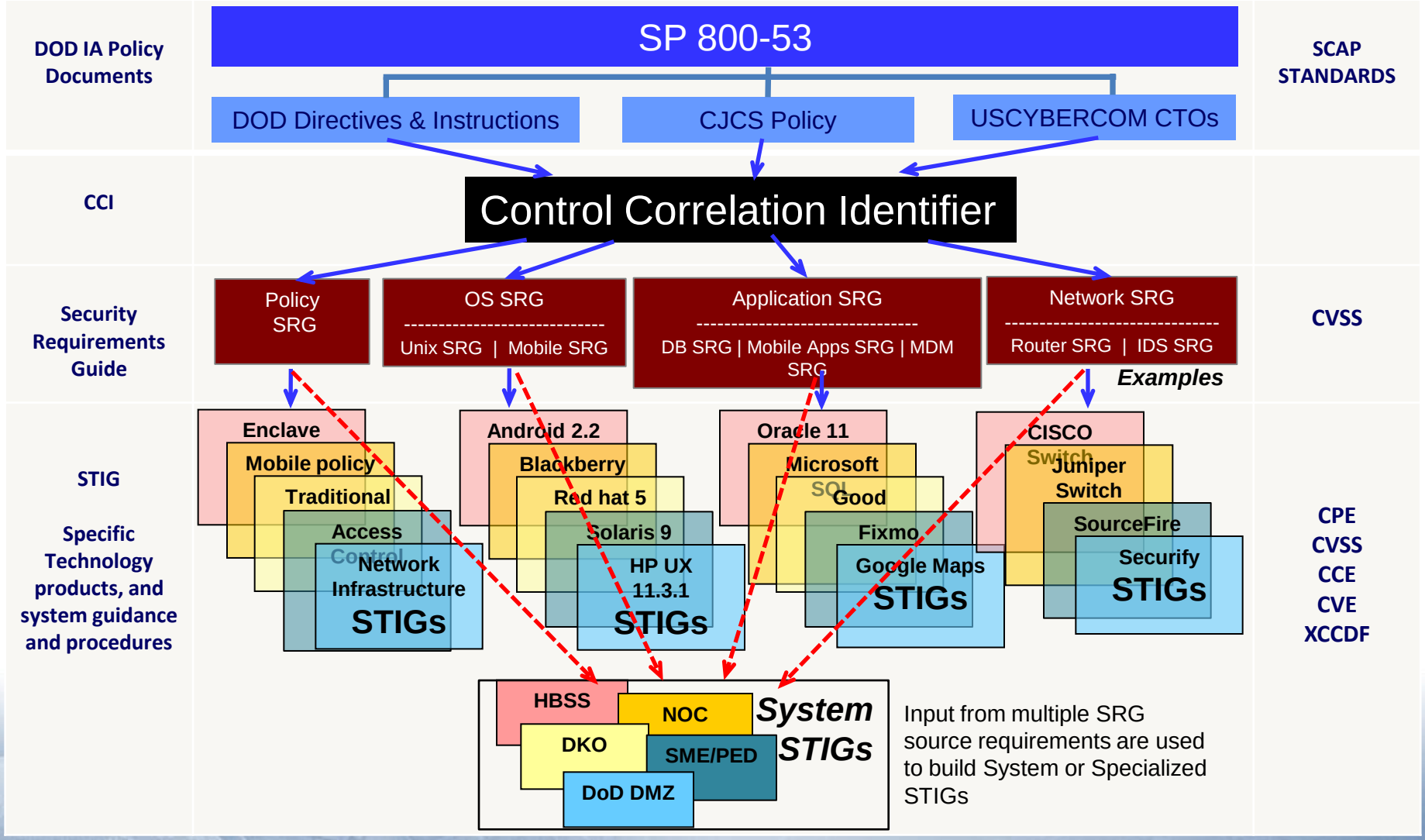
DISA
A Combat Support Agency

Security Guidance: Approach to Improve Agility

- Utilize a standards based approach to develop IA configuration guidance, publish IA guidance, assess assets, and report compliance
- Leverage Security Content Automation Protocol (SCAP)
  - Industry standard championed by NIST
  - Designed to provide a structured means to express security checks to any SCAP enabled tool and ensure consistent results
  - Benefits:
    - Enables vendor community to develop standardized guidance once for use by all communities
    - Allows commercial assessment tools to utilize DoD configuration guidance
- Produce "Security Requirements Guides (SRG)"
  - SRGs serve as the basis for requirements in developing a STIG
  - Benefits:
    - SRGs are non-vendor specific
    - Product vendors can use SRGs to develop product specific guidance or support validation of compliance in the C&A process

Mobile Devices will be key use-case to prove benefits of our new approach

Framework for the Future



PEO-MA Engineering Support Services

Project: PEO-MA Engineering Support Services

Anticipated Start Date: 4th Quarter, FY12

Predecessor Contracts: N/A

Anticipated Small Business Involvement: Small Business set-aside

Anticipated Contract Type: Multiple-Award BPA

RFP to be released: May/June 2012

This acquisition will provide a full range of engineering support services in support of IA2, IA3, IA4 and IA5 missions. All missions supported will require IA and CND expertise. The Government's intention is to set up a Blanket Purchase Agreement (BPA) with one or more contractors to provide the support described in the Performance Work Statement (PWS), with delivery orders specifying which task and sub-task areas will be completed at that time.

DDoS-MS

Project: Distributed Denial of Service – Mitigation Solution (DDoS-MS)

Anticipated Start Date: 3rd Quarter, FY13

Predecessor Contracts: Distributed Denial of Service-Tech Refresh (DDoS-TR), NNG07DA21B/HC102810F2699

Anticipated Small Business Involvement: TBD

Anticipated Contract Type: TBD

RFI released: September 2011

PEO-MA requires a Distributed Denial of Service-Mitigation Solution (DDoS-MS), to be integrated with Distributed Denial of Service-Tech Refresh (DDoS-TR) program, which will monitor network traffic traversing the internet/NIPRNET border and protect DoD assets. The DDoS-MS solution must enhance the current DDoS-TR system by providing packet scrubbing. The current DDoS-TR system uses Arbor Peakflow to perform DDoS detection and mitigate attacks with Remote Triggered Black Hole (RTBH) and BGP Flow-Spec. The government is interested in solutions that provide other mitigation techniques.

HSSCMR

Project: Hardened System Secure Configuration Management and Reporting (HSSCMR)

Anticipated Start Date: 2nd Quarter, FY13

Predecessor Contracts: None

Anticipated Small Business Involvement: TBD

Anticipated Contract Type: TBD

RFI released: September 2011

The goal of HSSCMR is to improve configuration management practices by increasing awareness of security weaknesses through the identification and analysis of host configuration states using operational context. HSSCMR is a DoD Enterprise-wide capability envisioned to provide visibility and awareness of the security posture of every network-connected host in DoD. HSSCMR provides visibility of DoD host operating systems and application inventories, system and environmental attributes, and technical and non-technical security guidance and security patch compliance measurements. The HSSCMR capability is enabled by the use of standardized configuration assessment and reporting data specifications and is architected as a service oriented architecture (SOA).

HBSS Phase II

Project: Host Based Security System (HBSS) Phase II

Anticipated Start Date: 1st Quarter, FY14

Predecessor Contracts: HBSS Phase I, HC1028-08-D-2023/0056

Anticipated Small Business Involvement: TBD

Anticipated Contract Type: TBD

RFI released: December 2011 (Central Management Framework and Host-Based Security Modules)

The Host Based Security System (HBSS) solution suite is an enterprise-wide automated, standardized tool that provides host-based security, against both insider threats and external threats. DISA, at the request USSTRATCOM and in support of National Security goals established by the President; purchased from industry, a capability that will develop and deploy an automated HBSS solution. HBSS supports the “Defense-in-Depth” initiative by providing network administrators and security personnel with mechanisms to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DoD networks and information systems throughout the DoD Enterprise.

DIBNet Development

Project: Defense Industrial Base Network (DIBNet) Development
Anticipated Start Date: 4th Quarter, FY12
Predecessor Contracts: IATAC, SPO70098D4002/0334
Anticipated Small Business Involvement: TBD
Anticipated Contract Type: TBD

The purpose of DIBNet is to develop and deploy DIBNet-U and DIBNet-S to facilitate the collaboration between DoD and Defense Industrial Base (DIB) partners to protect Sensitive DoD data residing in commercial space. DIBNet-U and DIBNet-S capabilities facilitate the sharing, analysis, integration, and visualization of network attacks, to include a publicly available registration site that is a critical capability in opening the DIB Cyber Security/Information Assurance (CS/IA) Program to all qualified cleared defense contractors (CDCs).

The DIB CS/IA program is focused on helping Cleared Defense Contractors (CDCs) protect DoD information resident on DIB unclassified networks that is not publicly releasable. To be successful the DoD and DIB require a secure environment for cyber threat information sharing and collaboration between the DoD and DIB. The DIB CS/IA Program is critical to assisting the DoD community that includes the DIB, in securing DoD program information on DIB unclassified networks that are threatened daily, mitigating attacks when they occur, and enabling the DIB Partners to protect against future attacks. This multi-phased project will facilitate the sharing, analysis, integration, and visualization of network attacks, and is a critical milestone in opening the DIB CS/IA Program to all qualified CDCs.

Improve Cyber C2

IA Audit Management

Project: Information Assurance (IA) Audit Management

Anticipated Start Date: 3rd Quarter, FY13

Predecessor Contracts: Centaur Support, HC1028-10-C-2015/0000

Anticipated Small Business Involvement: TBD

Anticipated Contract Type: TBD

RFI to be released: TBD

This effort will provide follow-on support for the development and support of the implementation of an IA Audit Management operational pilot focused on web, firewall and other application logs. This includes researching, developing, testing, and providing IA Web Audit Management tool(s) , and tactics, techniques and procedures (TTPs) to the Government to support DOD Computer Network Defense (CND) analytics performed at the operational level.

Improve Cyber C2

PCAP Solution

Project: Packet Capture and Analysis Solution (PCAP)

Anticipated Start Date: TBD

Predecessor Contracts: None

Anticipated Small Business Involvement: TBD

Anticipated Contract Type: TBD

RFI released: March 2012

The Data Access and Long Term Storage (DALTS) initiative requires a Packet Capture and Data Retrieval System. For network security and situational awareness purposes, the DoD plans to collect the data traveling through the network infrastructure. The DoD is seeking a solution capable of providing full Packet Capture of the Enterprise GIG, to include long-term storage of that capture data, and allowing systems analysts to retrieve the data from the system. The needed solution will consist of three aspects: full packet capture, data storage, and query capability for analysis.

SIEM Solution

Project: Security Information and Event Management (SIEM) Solution

Anticipated Start Date: TBD

Predecessor Contracts: None

Anticipated Small Business Involvement: TBD

Anticipated Contract Type: TBD

RFI released: March 2012

PEO-MA needs a Security Information and Event Management (SIEM) solution with a data fusion and long-term storage capability. This SIEM solution will provide the collection, trending, reporting and analysis of log data from host systems and applications as well as network and security devices.

Improve Cyber C2

CDES – Operations & Integration Support

Project: Cross Domain Enterprise Service (CDES) – Operations and Integration Support

Anticipated Start Date: 1st Quarter, FY13

Predecessor Contracts: Cross Domain Solutions Implementation, Engineering and Documentation Support, HC1028-08-D-2025/0010

Anticipated Small Business Involvement: TBD

Anticipated Contract Type: TBD

RFI released: November 2011

The objective is to provide DISA and the Cross Domain Solutions Branch with software and systems engineering and information assurance services, i.e., high quality operational, integration and documentation support services at the lowest reasonable cost, in support of the Cross Domain Enterprise Service and Cross Domain Solutions Product Line.

PKI – Program Management, Technical and Engineering Support

Project: Public Key Infrastructure (PKI), Program Management, Technical and Engineering Support

Anticipated Start Date: 2nd Quarter, FY13

Predecessor Contracts: PKI PM Support, HC1028-08-D-2015/0014, PKI Engineering Support, HC1028-08-D-2015/0015

Anticipated Small Business Involvement: TBD

Anticipated Contract Type: TBD

RFI to be released: May 2012

PEO-MA has two goals for this effort: 1) The Contractor shall provide program management consultant services through subject matter experts on the configuration of PKI systems; and 2) The Contractor shall provide technical and engineering support services to execute the PKI program in accordance with the current DoD X.509 Certificate Policy and the appropriate DoD approved architectures, programs standards and guidelines such as DoDI 5000.2, Defense Information Infrastructure (DII), Defense Information Systems network (DISN), and Global Information Grid (GIG).

Cross Domain Enterprise Services

Project: Cross Domain Enterprise Service (CDES)

- Enterprise E-mail
- Web Services
- File Transfer

Anticipated Start Date: TBD

Predecessor Contracts: None

Anticipated Small Business Involvement: TBD

Anticipated Contract Type: TBD

RFI released: September 2011

The PEO-MA Cross Domain Solutions (CDS) Program implements the Cross Domain Enterprise Service (CDES), which provides hardware and software for the transfer of information between the DoD's classified and unclassified networks. This transfer of information between networks of different security domains is conducted using various cross domain guard technologies and accomplished with high assurance, speed, and integrity. This enterprise service is provided to combat commands, military services, and defense agencies. Aspects of the enterprise service are web services, e-mail, and file transfer across security domains. The CDS Program is seeking technologies that can serve the needs of the DoD enterprise for cross domain web services, e-mail, and file sharing, scale to support the DoD enterprise, operate within the enterprise environment, and realize cost efficiencies.

Improve Safe Sharing

DISA
A Combat Support Agency

Summary

- Defendable GIG
  - Building enterprise architecture consistent with CYBERCOM and DoD CIO vision. Significant capability available today.
- Improve Cyber C2
  - Basic capabilities in place with significant challenges ahead.
- Improve Safe Sharing
  - Robust foundation with actions underway to achieve near term successes.

The foundation of the Cyber program is a well trained and experienced workforce