Mission Assurance

2014 Forecast to Industry

Mr. Mark S. Orndorff
Mission Assurance Executive
20 August 2014
The Problem

Problem Statement: Neither the DoD nor the combatant commanders can adequately see, control, or defend their networks. We can’t meet the urgent and immediate cyber threat, defend the current infrastructure or reduce network vulnerabilities.

Capability Gaps

- Lack of Enterprise-level view and standardized security topology
- Too many avenues of attack
- Heavy reliance on independent delivery of security services
- Inability to apply advanced threat analysis
- Lack of Enterprise responsiveness in assessing, detecting, responding to threats
- Lack of [unity of effort] in operating and managing cyberspace operations
- Segmented approach to networks creates seams and creates difficulty in information sharing, thus complicating protection of forces

High Level Objectives (HLOs)

- HLO 1: Operate, defend, manage, and maintain the JIE (DoDIN)
- HLO 2: Enable and protect critical warfighting information and information exchange through various capabilities and services
- HLO 3: Ensure critical warfighter information, capabilities and services are available in a degraded cyber condition

Gaps and HLOs Identified in Authoritative Sources (paraphrased)

Authoritative Sources:
- JIE ICD v 3.1.1, GIG 2.0 ICD and Cyber SA ICD
- JIE OPS CONOPS and Chairman’s White Paper
Mission Assurance (Cybersecurity and NetOps)

Internet Access Points
- Sensors (ECOS)
- Web Content Filtering
- Demilitarized Zone (DMZ)
- Distributed Denial of Service Mitigations
- Enterprise Email Security Gateway
- Domain Name System (DNS) Hardening

Regional Security
- Joint Regional Security Stacks
- Perimeter Zero Day Network Defense
- Cross Domain Enterprise Services
- Filter List Manager

Commercial Cloud (Levels 3-5)

Foundational
- Cyber Workforce Development
- Cyber Readiness Assessments

Enclave and Endpoint Security
- Public Key Infrastructure
- Host Based Security System
- Enterprise Anti-Virus/Anti-Spyware
- Assured Compliance Assessment Solution
- Bootable Media
- Rogue Wireless Detection

Cyber SA/NetOps
- Cyber SA Analytic Cloud (CSAAC)
- Secure Configuration Management
- Continuous Monitoring Risk Scoring
- Enterprise Mission Assurance Support Service (eMASS)
- Insider Threat Analytics
- Security Information /Event Manager
- Joint Incident Management

Projected contract actions:
- Service Contract
- New Solution
Cyber Situational Awareness Analytic Cloud

Enterprise Operations Center

Components
COTS:
- ArcSight
- Splunk
- Sensage
- Etc

GOTS:
- “Big Data Analytics”
- Insider Threat
- Fight by Indicator
- CMRS

Structured Databases:
- MADSS
- JIMS
- eMASS

Single Security Architecture

Enterprise Service Status
Alert Correlation
Risk Scoring
Mission Mapping

CYBER Operators & Cyber Protection Teams

Data Ingest Service
API

CDCs
IAPs & DISN
JRSS
Enclaves and End Points
Acquisition Point of Contact

Charles S. Hamilton
Charles.S.Hamilton1.civ@mail.mil
(301) 225-8598

Vendor Coordinator

Mark D. Hamilton
DISA.Meade.ma.mbx.dcto-ma@mail.mil
(301) 225-8583