Information Assurance

Marine Corps Information Assurance Assessment Team

IA for Acquisition Programs of Record

Independent Verification & Validation

Expeditionary Support (IA & IOP)

Support to other Services & DoD OTAs (IA & IOP)

IA Assessments during Exercises (DOT&E)

Interoperability Assessments during Exercises (DOT&E)
IA Opportunities

• IA for Acquisition
• Independent Verification and Validation for Acquisition
• Exercise/Service IA Assessments
• Blue Team Assessments
• Green Team Assistance
• Interoperability Assessments
• Expeditionary Support
• IA Range
IA for Acquisition

• Focus: USMC Programs of Record (POR)
  – DOT&E Oversight List
  – Major Defense Acquisition Programs/Major Automated Information Systems

• Support for Programs of Record (POR)
  – Review IA requirements for POR with PMO stakeholders
  – Review and update IA for POR TEMP and JCIDS
  – Support IA control determination
  – Review POR DIACAP Implementation Plan (DIP)
  – Witness and review IA results for DT
  – Perform IA Operational Assessment
    • IA Control Compliance
    • Evaluate Protect, Detect, Respond, Restore
IV&V for Acquisition

- Conduct Independent Verification & Validation
  - IV&V is the last major step in DIACAP prior to IATO/ATO
  - IATO is required to proceed to OT&E
- DIACAP requires third party performance of IV&V
  - Supports accreditation decision
- Ensure IA controls have been effectively implemented to support survivability for the system under test
  - Confidentiality, Integrity, Availability
  - Protect, Detect, Respond, Restore
  - Less disruptive during DT
- Conducting IV&V creates efficiencies in the OT by drastically reducing OT IA assessments
Exercise/Service IA Assessments

- **Support to the DOT&E IA&I Program**
  - Congressionally mandated and funded Information Assurance and Interoperability (IA&I) assessments since 2003
  - OTAs, IWCs and NSA will assess the IA and Interoperability posture of *fielded systems* (network enclaves and information systems) and through annual exercises and assessments at each COCOM and Service
    - Vigilant Shield (NORTHCOM), Fuertes Defensas (SOUTHCOM), Turbo Distribution (TRANSCOM), Global Thunder (STRATCOM), Terminal Fury (PACOM), United Endeavor (JFCOM), and others
    - Support to MEFs and MARFORs
  - Feedback provided to the COCOM exercise authority, Service operational commanders, program partners (DOT&E, ASD[NII], and Joint Staff) and Congress
  - Results shared with USSTRATCOM, DISA, NSA, and DOT&E
  - MCOTEA leads Marine Corps participation
Blue Team Assessments

- Conduct non-technical and technical assessments of DoD networks and information systems to meet periodic independent assessment requirements
  - Operational support provided to MEFs & MARFORs and other agencies as requested
- Conduct non-technical and technical assessments in support of DIACAP accreditation decisions for DoD (DoD 8500 series) and intelligence systems (DCID 6/3)
  - IO Range

<table>
<thead>
<tr>
<th>Non-Technical</th>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review key IA documentation to determine its completeness and relevancy</td>
<td>Conduct baseline security configuration scans</td>
</tr>
<tr>
<td>Determine the application and enforcement of policy</td>
<td>Conduct vulnerability scans</td>
</tr>
<tr>
<td>Conduct interviews with key IA personnel</td>
<td>Review perimeter defense configurations</td>
</tr>
<tr>
<td>Verification and Validation of documented procedures</td>
<td>Conduct wireless detection scans</td>
</tr>
<tr>
<td></td>
<td>Conduct password compliancy scans</td>
</tr>
</tbody>
</table>
Green Team Assistance

- Training/Mentoring of IA Community
  - Blue Team Methodology Course
    - Provide adaptable methodology to conduct self-assessments
    - Attended by DOT&E, Systems Command, SPAWAR, and Service IA personnel
    - Taught annually at the Marine Corps IA Conference and at MCOTEA
    - Taught on site by request of the Marine Corps at home or abroad
  - For the assessed organization
    - Provide remediation and education of vulnerabilities discovered
    - Develop COA to mitigate risk for vulnerabilities
    - Provide instruction on proper procedures to build security into architecture
    - Provide functional guidance and training on DISA and NSA sponsored enterprise IA tools
Expeditionary Support

- Assessment support to deployed forces during or after Relief in Place/Transfer of Authority (RIP/TOA)
  - II MEF in Iraq, March - April 2009
- Marine Expeditionary Forces ‘Assistance’ Visits
  - Baseline network scan for vulnerabilities
  - Provide recommended COA’s and POA&M for remediation of discovered vulnerabilities
- Purpose
  - Provide the incoming Commander with a snapshot of the network security posture
  - Provide mentoring/assistance to improve the IA posture of the network
  - Provide training in self-assessments to maintain a high level of security
  - Support the Commander as needed
IA Range

• Mission
  – Provide a persistent environment to support Test and Evaluation, Exercise Support, and Training and Education
  – Allows for continuous self-assessment for POR in addition to training IA professionals

• Objective
  – Build an operational IA/Computer Network Defense architecture in a network operations configuration to test and train in which is identical to the one we defend

• Stakeholders
  – DoD CIO, USSTRATCOM, USJFCOM, Joint Staff, Services, NSA, DISA
Questions