Information Assurance: Impacts on Army Target Programs

Barry Hatchett
Lead Project Director
Targets Management Office (TMO)
COM 256-842-6797,
DSN 788-6797
Barry.Hatchett@us.army.mil
Outline

• What is DOD Information Assurance Certification and Accreditation Process (DIACAP)?
• Why do Information Assurance?
• Process for DIACAP Compliance
• What impacts does DIACAP have on target programs
What is DIACAP?

It is the process by which information systems are *certified* for compliance with DoD security requirements and *accredited* for operation by a designated official. It is the standard process under which all DoD information systems will achieve and maintain their Authority To Operate (ATO).
Why do Information Assurance?

It is the Law! –
Clinger-Cohen Act, 1996
Federal Information Security Management Act (FISMA), 2002

DODI 5000.02 – “Operation of the Defense Acquisition System”

DODI 8580.1 – “IA in the Defense Acquisition System”

AR 25-2 – “Information Assurance”

*Military, Federal Civilian & Contractor* personnel may be subject to administrative &/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage or place Army information systems at risk by not ensuring implementation of DOD & Army policies & procedures.
Process for DIACAP Compliance

- Material Solution Analysis
- Technology Development
- Engineering and Manufacturing Development
- Production & Deployment
- Operations & Support

Pre-System Acquisition
- Program Initiation
- CCA Compliance
- Material Development Decision

System Acquisition
- Critical Design Review
- Develop IA Strategy
- Contract Award
- Develop RFP

Sustainment
- IOC
- FRP Decision Review
- Update

Disposal
- FOC
- Update

- Execute DIP
- Develop Artifacts
- Conduct DIP Review
- Develop DIP

- Conduct CT&E
- Make CD
- Grant ATO

Annual Security Reviews
- IAVA Management

IA Milestone Schedule

ACRONYM
- ATO: Authority To Operate
- CGA: Clinger-Cohen Act
- CD: Certification Determination
- CT&E: Certification, Testing and Evaluation
- DIACAP: DoD Information Assurance Certification and Accreditation Process
- DIP: DIACAP Implementation Plan
- FRP: Full Rate Production
- IA: Information Assurance
- IA VM: Information Assurance Vulnerability Management
- RFP: Request for Proposal
- SRR: System Registration Review

21 October 2010
Target Control System (TCS)

- The Army’s primary Subscale and Rotary Wing aerial target control system
- Current TCS began development in 2001
- System Configurations: Fixed Site, S280 Shelter, Portable
Targets Management Office

TTCS-U
Engineering Flight Test
20 May 2010
IA Issues with TCS

- Legacy System
  - Some IA controls cannot be implemented
  - Hardware could not support IA tools
- Certain IA controls could add risk to mission
- Funding to support DIACAP
- Each computer in the system must be configured separately
- Overall process is time consuming as it is manually intensive
Impacts to TCS

- Additional training is required for operators
- Manuals need to be updated
- Increases sustainment cost
- Increase time of regression testing
- Additional personnel needed to support IA needs
  - Review and storage of audit records
  - Updating DIACAP documentation and yearly IA recertifying scans
**TCS Open Vulnerabilities**

<table>
<thead>
<tr>
<th></th>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsystem Control Console</td>
<td>339</td>
<td>114</td>
</tr>
<tr>
<td>Command Telemetry Subsystem</td>
<td>338</td>
<td>119</td>
</tr>
<tr>
<td>Position Display Subsystem</td>
<td>338</td>
<td>124</td>
</tr>
<tr>
<td>STEALTH</td>
<td>356</td>
<td>135</td>
</tr>
</tbody>
</table>

* Windows XP Service Pack 3 accounts for ~ 90% of remaining Vulnerabilities
Aerial Weapon Scoring System (AWSS)

- An integrated group of computer-controlled sensors used to score live-fire helicopter gunnery exercises at designated gunnery ranges
IA Issues with AWSS

- Separate scan required for each computer hardware configuration
- Full licensed version of Retina required to resolve vulnerabilities
- AWSS is not connected to internet to receive security updates
- Overall process is time consuming as it is manually intensive
Impacts to AWSS

• Virtual Network Connection not authorized thus preventing communication from tower
• User login with password protection (14 characters)
• System response performance was degraded
AWSS Open Vulnerabilities

<table>
<thead>
<tr>
<th></th>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold Disk</td>
<td>732</td>
<td>3</td>
</tr>
<tr>
<td>Retina</td>
<td>43</td>
<td>34</td>
</tr>
</tbody>
</table>

- 3 Open Vulnerabilities with Gold Disk were considered acceptable for accreditation
- Most Open Vulnerabilities with Retina were low risk
Summary

• IA is law and here to stay
• Plan and prepare early in the acquisition of system
• Continue to support mission requirements