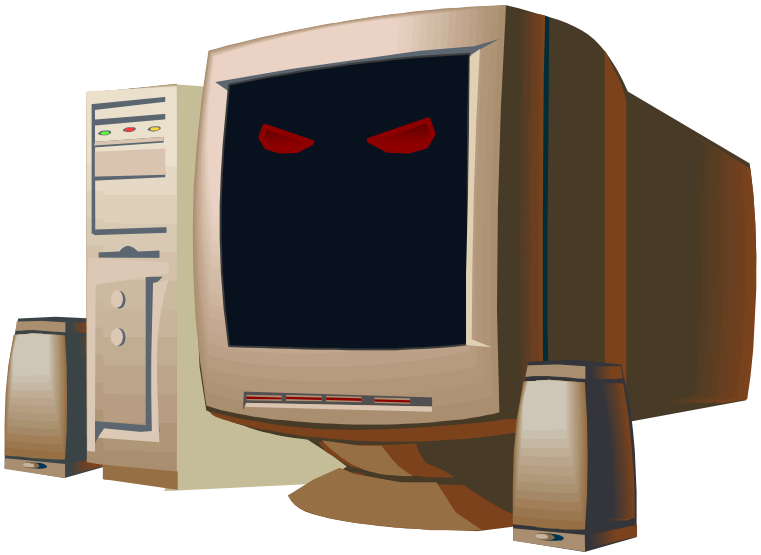
Cybersecurity & Fraud Testing



Exercise Assessments and Acquisition OT&E Cyber Issues

Brief for ITEA
March 2016

David J. Aland

Cyber OT&E Efforts

- Exercise Assessments
  - Fielded systems and networks,
  - Cybersecurity (CS) and interoperability (IOP)
  - Major exercises and real-world events
- Acquisition OT&E
  - Associated with Milestone C
  - Specific DOT&E procedures
  - Fraud testing where applicable
- Reporting
  - Annual Report to Congress (UNCLAS)
  - Annual Cybersecurity Assessment (SECRET//NOFORN)
  - OT&E reports
  - Finding Memoranda

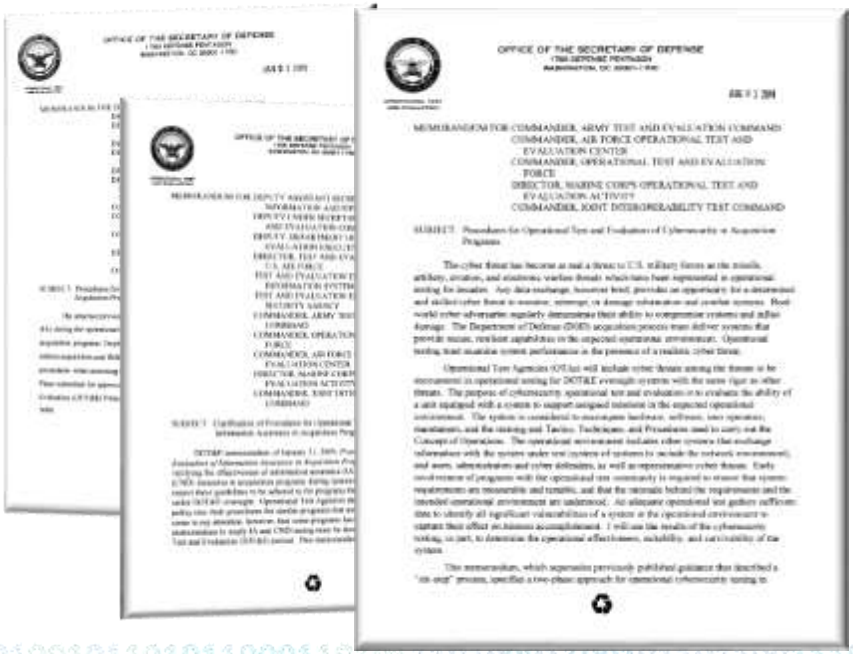
What you *got*, is what you *bought*…

- The top four classes of vulnerabilities found during cybersecurity acquisition testing in FY13-15:
  - Password/Credential exposure
  - Software not configured for security
  - Software out of date
  - Unnecessary network services in use
- The top four classes of vulnerabilities found during cybersecurity exercise testing in FY13-
  - Password/Credential exposure
  - Software not configured for security
  - Software out of date
  - Unnecessary network services in use

So… how do we "buy better"?

OT&E of Cybersecurity in Acquisition Systems

2009-2013: *Set basic processes and policies*



2014: *Revised and updated*

- Improve rigor for cyber testing
- Establish requirements for both oversight and other programs
- Synchronize with early design and developmental plans/tests
- Sets requirements for TEMPs/OTPs
- Provides specific metrics
- Reflects new certification processes
- Two OT phases:
  - Vulnerability & Penetration Tests
  - Adversarial Assessment

Some Acquisition Lessons Learned

- Planning for success
  - Planners established a safety board to avoid negative consequences
- Combining efforts
  - Scheduled cyber events to occur during other planned test events, or establishing equivalent environments
- Multi-system testing
  - One adversarial team, many programs, one environment
- Building the documentation
  - Early reviews of information architectures to identify and eliminate opportunities for cyber exploits
- Planning for too much
  - Effects or events that are not operationally safe or feasible
- Not considering resources
  - Too many test events in a constrained time or location, overwhelms the assessors
- Not considering all sources
  - Repeating tests that could have been captured elsewhere
- Basic ball-drops
  - Bringing the wrong equipment to the test, not understanding the representative environment