

Public Meeting for Advance Notice of Proposed Rulemaking (ANPR) on Safeguarding Unclassified Information (DFARS Case 2008-D028)



**Kristen Baldwin
Director, Systems Analysis
OUSD(AT&L)DDR&E/Systems Engineering**

April 22, 2010



Purpose of Potential DFARS Changes

- ❑ The purpose of the potential DFARS changes addressed in this ANPR is to-
 - Implement adequate security measures to safeguard DoD information on unclassified industry information systems from unauthorized access and disclosure; and
 - To prescribe reporting to the Government with regard to certain cyber intrusion events that affect DoD information resident or transiting on contractor unclassified information systems
- ❑ This ANPR does not address procedures for Government sharing of cyber security threat information with industry; this issue will be addressed separately through follow-on rulemaking procedures



Scope of ANPR

□ This ANPR Addresses:

- Basic safeguarding requirements that apply to any unclassified DoD information that has not been cleared for public release in accordance with DoD Directive 5230.9, Clearance of DoD Information for Public Release (consistent with national and commercial standards, e.g. NIST 800-53)
- Enhanced safeguarding requirements, including cyber incident reporting, that apply to information subject to Critical Program Information; export control under the ITAR and EAR; FOIA; controlled access and dissemination designations; limitations IAW DoD Directive 5230.24 and 5230.25; and PII
- Assessment of reported cyber incident to determine any technology and programmatic implications
- Federal coordination with NARA



Basic Safeguarding Clause

- Applies to any unclassified DoD information not cleared for public release
- Incorporates 8 basic safeguarding requirements (defined in clause)
- Applies to both prime contractors and subcontractors that have access to or generate DoD information



Enhanced Safeguarding and Cyber Intrusion Reporting Clause

- ❑ Applies to specific information types further defined within the proposed clause (e.g. CPI, ITAR)
- ❑ Enhanced Safeguarding Requirements
 - Encryption/Storage
 - Network intrusion protection
 - Recommended security controls for Federal Information Systems and organizations (NIST 800-53)
- ❑ Cyber Intrusion Reporting
 - Report cyber intrusion events that affect DoD information
 - Support forensic analysis and cyber intrusion damage assessment
- ❑ DoD will protect information reported in accordance with applicable statutes, regulations and policies (e.g. Privacy Act, HIPAA)



Objectives for Cyber Security

- ❑ Ensure no competitive advantage is created for any industry partners as Cyber Security policy evolves
- ❑ Establish a standard of adequate security for protecting DoD Unclassified Information to provide consistency throughout industry
- ❑ Create incident reporting standards for DoD
- ❑ Establish and implement cyber intrusion damage assessment processes to analyze programmatic and/or operational impact due to loss
- ❑ Establish liabilities and remedies following a cyber incident resulting in DoD information loss or compromise



Questions/Comments



Backup Slides



Important Case Information

- ❑ Presentations will be posted at <http://www.acq.osd.mil/dpap/ops/news/index.html>

- ❑ Submit ANPR comments no later than May 3, 2010, by any of the following means:
 - Post comments at <http://www.regulations.gov>.
 - E-mail: dfars@osd.mil. Include DFARS Case 2008-D028 in the subject line of the message.
 - Fax: 703-602-0350
 - Mail: Defense Acquisition Regulations System, Attn: Mr. Julian Thrash, OUSD(AT&L)DPAP(DARS), 3060 Defense Pentagon, Room 3B855, Washington, DC 20301-3060