



ANPR: Safeguarding Unclassified Information

(DFARS Case 2008-D028)

- **Scope – too broad in some places and too specific in others**
- **Definitions - ambiguous**
- **Reporting – concerns about provision, use and protection of data**
- **Implementation – Compliance, subcontractor concerns**

Note: Best Practices responses to all questions will be submitted in writing no later than May 3, 2010.

- **Safeguarding/marketing requirement to address “all DoD information” is too broad to execute successfully – need to be put in contract specifics.**
- **Technical standards too specific – “anti-virus”; “anti-spyware”; “patches”; “service-packs”; “hot fixes”**
- **ANPR requirements are not risk based—need a risk based assessment to reduce personnel and resources costs.**
- **ANPR requires “best level of security available”—will be costly to implement and will impact smaller companies.**
 - **Need to address small subcontractors without IT capability to protect information at the ANPR required level.**
- **Cyber security is a national priority and is a concern to all federal agencies, not only DoD.**

- **As a general rule, terms, clauses, terminology must be clearer to ensure effective implementation.**

- **Examples:**
 - **“Adequate security” needs citation for standardized implementation**
 - **“Encrypted wireless security” is addressed but not wired connections.**
 - **Terms such as “regularly updated” “appropriate”, “adequate”, “prompt”.**

- **How are the existing Company's Voluntary Framework Agreements impacted by this ANPR?**
 - **Need to transition requirements with the mandatory contract requirements in the ANPR.**
- **How will mandatory reported intrusions be addressed in Past Performance evaluations?**
- **Reported intrusions have the potential to disrupt business continuity**
 - **Seizure of computers or servers for forensic analysis could require costly redundant systems for continued business operations.**
 - **Unrealistic reporting response requirement (72) has the potential to be administratively burdensome**
- **What assurance does industry have that the data the government collects is secure?**
- **How will the government assure protection of companies' proprietary information and report contents?**
- **Final FAR Rule should provide protection of companies' information involved in cybersecurity incidents (e.g., privileged information, information protected by agreements with third parties, etc.)**

- **What is the Government's standard for industry compliance with this ANPR, e.g. NIST 800-53 or ISO 27000 series?**
 - **Who determines company compliance?**
 - **Will there be a recognized certification that will reduce the proliferation of subcontractor audits by primes/government?**

- **Meeting compliance requirements does not guarantee complete protection of DoD's information from compromise.**
 - **How will the Government treat "compliant organizations" that suffer a breach?**

- **Subcontractor Concerns- Is there a risk based approach to assure proper flowdown?**
 - **Are contracts/orders for "nuts and bolts" treated equally as contracts/ subcontracts for major systems?**
 - **Are primes liable for subcontractor compromises of DoD's information**
 - **Primes cannot accept responsibility for subcontractor's overall control environment.**