

ANPR DFAR 252.204-7000
Disclosure of Information 73
FR 9563

Presentation by
Ron Hutchins, PhD
CTO, Georgia Institute of Technology
Atlanta GA

Management of DoD Data Today

- Non-Classified Data
 - Treated as business sensitive by Institute
 - Standard Campus Security
 - Network/Host firewalls, antivirus, patching,
- Classified data
 - Additional requirements on where data is stored/processed, and who has access,
 - Strict reporting requirement for breeches,
 - Separate services such as email, storage
 - Professional management of workstations and laptops required.
 - Separate network with Network Access Control recommended.

Reaction to Proposed Changes

- New restrictions for Non-classified Data (Basic Security)
 - Expectations are somewhat vague, advising users to use the “best level of security available.”
 - How is compliance measured and assessed?
 - Will data be monitored, or will new controls be mandated with new reporting rules?
 - Additional costs will be incurred for the new “Basic” category.
 - Education
 - Administration
 - Compliance

Impact

- Limited number of faculty researchers working with DoD-Classified Data today.
- Many more faculty, graduate students and research scientists working with non-classified Data on DoD contracts.
- Potential Immediate Costs to Georgia Tech:
 - Education of all faculty researchers working with ANY DoD Data.
 - Moving faculty to NAC controlled network
 - Consolidated management of workstations and laptops
 - Self-assessments for compliance
 - Personnel time required to implement these processes for all DoD data, not just classified data.