

April 20, 2010

To: Julian Thrash  
From: Jeff Reich, Director of Operations for the Institute for Cyber Security  
Subject: Remarks from Jeff Reich for the Public Meeting DFARS Case 2008-D028

Good morning and thank you for the opportunity to provide comments, from a research perspective, on the proposed changes to the Defense Federal Acquisition Regulation Supplement (DFARS) which addresses requirements for the safeguarding of unclassified information.

My role at the Institute for Cyber Security is Director of Operations. The Institute is part of the University of Texas at San Antonio, which is a university focused on research and located in a city surrounded by military installations and activities. Cyber security research at the Institute encompasses **four major thrust areas** with mutual synergy covering **basic research and applied research**.

- **Application-Centric:** Theory and practice of security for new and emerging application domains. Current projects include:
  - Secure Information Sharing
  - Social Networking/Computing Security
  - Infrastructure Assurance
- **Technology-Centric:** Theory and practice of security in context of specific technologies which present novel challenges due to the intrinsic nature of the technology. Current projects include:
  - Trustworthy Cloud Computing
  - Secure SOA (Service Oriented Architecture)
- **Attack-Centric:** Theory and practice of malware analysis and detection. Current projects include:
  - Botnet Analysis and Defense
- **Special Projects:** Projects which do not align precisely with the above thrusts.

We collaborate with at least 11 other higher education institutions.

In prior positions, I have served as Chief Security Officer at a number of technology and financial services organizations. My experience of over 30 years in cyber security has taught me that it always makes sense to take appropriate security measures to protect information that is critical to an organization's function. Without question, the rules and procedures presently in place for classified data are appropriate. That being said, however, unclassified data are just that, unclassified. These unclassified data are the lifeblood for researchers who need to use and to share this type of data in their collaborations, publications and efforts to protect resulting intellectual property.



The two types of research typically produced at the Institute are Academic Research and Applied Research. Effective academic research thrives when collaboration and peer review help to develop and hone the research. Therefore, the goal of academic research is to advance the state of knowledge in that field through publications and professional presentations and to have your findings used by subsequent researchers. Any restrictions placed on the exchange of academic research will greatly slow our progress in cyber security and thereby increase our vulnerability to attack and exploitation. Academic research often forms the foundation for applied research. Applied research focuses on the development of innovative intellectual property, which often results in patent applications and the direct improvement of our cyber security posture.

Today I am letting you know that, generally speaking, many of the DFAR changes being considered would have adverse effects on both academic and applied research. Without question, the rules and procedures in place for classified data are appropriate. Unclassified data are just that, unclassified. Here are some specific concerns:

First, 204.7402 (b) requires that Contractors must report to the Government certain cyber intrusion events that affect DoD information resident or transiting on contractor unclassified information systems. Detailed reporting criteria and requirements are set forth in the clause at 252.204-7YYY. This section could be considered ambiguous and places an undue burden on cyber security research facilities. It is fact backed by empirical evidence that different levels of attacks occur on a near-continuous basis on many computer systems. Adding reporting requirements to these conditions when dealing with unclassified data would slow research activities to a near standstill. The proposed constraints stand to prevent collaboration and publication of associated information. These conditions would force cyber security academic researchers to seek other disciplines for their research and greatly reduce the amount of academic research in cyber security. As to applied research, protection of intellectual property through patents and deployment of associated innovations could be delayed significantly and, again, drive innovative researchers to seek other fields. The bottom line is that we will lose significant defensive capability against cyber attacks.

Secondly, because most, if not all, cyber security research could result in DoD information, 204.7403 Contract clauses could apply to every cyber security research project. This places an onerous burden on all research contracts and opens the possibility for the imposition of indefinite delays added to projects.

Additionally, I interpret [252.204-7YYY Enhanced Safeguarding and Cyber Intrusion Reporting of Unclassified DoD Information Within Industry as required encryption of all data associated with a given project and preventing any release or sharing of that data unless that release had been cleared in accordance with DoD Directive 5230.09, Clearance of DoD Information for Public Release] as added expense and administrative overhead that provides little if any value.



For the record, I want to re-state that classified data should be treated with enhanced protection measures commensurate with the sensitivity of the data. Unclassified data, by definition, has lower security needs and basic measures should apply. When dealing with academic research the amount of time, effort and funding to be invested should relate to the proportional output at the end of the research cycle. Many times, such output comes in the form of publications, citations and follow-on research. The more those constraints put that output at risk, the less you will see successful research.

In the long run, these additional constraints will have a larger detrimental affect on applied research. As I stated, academic research often forms the foundation for applied research. If that base were to shrink and the additional disclosure constraints were to inhibit patent protection of intellectual property applied research will slow down, if not dry up.

Once again, thank you for the opportunity to address you and I look forward to more opportunities to work with you in creating appropriate controls over properly identified data.

Respectfully Submitted,

Jeffrey N. Reich  
Director of Operations  
Institute for Cyber Security