TechAmerica Comments on DFAR Case 2008-D028

Safeguarding Unclassified Information

TechAmerica

- TechAmerica is the largest trade association for the technology and IT sector, representing over 1200 companies from all areas of the tech sector.
- Today's comment touch upon some high level concerns and will be augmented by our formal written comments to be submitted by the May 3, 2010 deadline.

TechAmerica

- **DoD must align this activity with the broader government initiative regarding critical unclassified information (CUI).** Failure to do so risks creating multiple, possibly conflicting requirements regarding the handling of unclassified information by contractors.
- **DoD must share the risk and responsibility with industry to better protect unclassified information**. This proposal contemplates mechanisms that places the burden solely on the contractor and does little to incentivize and encouraging better practices around protecting unclassified data.

- **There has been little discussion with existing members of the DIB IA initiative to assess successes or shortcomings in the existing frameworks and no discussion with them regarding the proposals in this DFAR.** TechAmerica recommends that DoD take advantage of the knowledge already developed within the framework of the DIB IA Initiative to assess what has worked and what has not and apply those lessons here.

TechAmerica

- **DoD has to date focused the efforts of the existing DIB IA initiative on traditional manufacturers in the defense industrial base** and intentionally avoided discussions with the tech sector during the development and implementation of the existing DIB IA frameworks. TechAmerica would like to reinforce that such a lack of dialogue with the broader tech sector has been detrimental to understanding the threats and identifying the solutions industry can bring to help address those threats. Until full industry engagement occurs, DoD will continue to be engaged in an incomplete dialogue with industry and experience only partial success in this effort.

- **Responsibilities that would fall to the contractor should be an extension of protections that the Government had already placed upon information** that was being shared with vendors-not a new responsibility once the data had transferred to contractors. If DoD did not exercise equivalent protections on the data before being transferred to contractors, no new requirements should be attached to the data. A model for this concept can be found in the Digital Millennium Copyright Act, whose definition of effective technologic protection at 17 USC 1201 would seem to offer a possible option to achieve the goals of this ANPR.

- **Static standards, like NIST 800-53, are unlikely to be able to be reviewed and updated at the pace of innovation**, so reliance upon them may actually restrict the adoption of technology at the Department. If reliance on a standard is necessary, TechAmerica is concerned that 800-53 may not be the best option because there is currently no mechanism to certify, accredit or audit compliance. It would also unnecessarily restrict options for the establishment of adequate controls by the contractor.

- **Better definitions and requirements regarding reporting "incidents" are necessary.** The requirement presumes a full-time monitoring capability, which is less and less likely as you move down the spectrum from large to mid to small companies. The shear volume of "incidents" on government networks would be dwarfed by the number of incidents occurring across the entire defense industrial base and even if all such incidents could be clearly identified, the Department would be unable to manage the volume of information for processing and threat detection in a timely fashion.

TechAmerica

- **Existing industry protections around financial and B & P activities could be used as models** for a proposal in order to avoid creating processes or procedures that would be different from currently robust information protections.
- **Commercial company business models and rules may not enable adherence to government unique requirements.** Such companies would have to assess the impact of these proposals to their global business model.

- **The requirements that this DFAR propose will create substantial burdens, both administrative and financial, on any company that wants to contract –** directly or as a sub – with DoD. Such burdens are certain to be a barrier to market entry for many mid – to – small companies. This will reduce competition, limit access to the full range of innovation developed in the commercial marketplace (a barrier our adversaries do not have) and make achieving socio-economic goals more difficult.

Unanswered Questions

- **TechAmerica is concerned about the one-size-fits-all approach of the ANPR in regards to different forms of unclassified data.** There is an intentional mixing of the formats of data, which from the perspective of the compliance could require significantly different approaches to secure. For example, a lost or stolen laptop with encryption is a different issue from a lost or stolen paper file. Another example is that if the Department physically handed a vendor a document or shared information orally, it would not be DoD information as defined in the proposed DFAR, but would be subject to the relevant classification category. If the Department sent the information electronically, however, as written, the broad definition would impose an obligation on the vendor to treat the information differently.

TechAmerica

- **It is unclear if companies can use the latest innovations, like cloud computing, to comply with this DFAR.** Would companies be able to use cloud computing to meet requirements or would that raise additional security and other government-specific concerns?
- Would vulnerabilities that are identified in the normal **lifecycle of COTS or commercial software** that operate corporate networks be subject to the requirements in this DFAR?

- **The proposal is very DoD-centric and does not include protections for other unclassified but sensitive data** that the Department may possess regarding a program. There are significant differences between DoD classification and Commercial Business Classification in regards to protecting commercial vendor's Intellectual Property. The latter seems to be ignored in this proposal, but should share in the protections it purports to create.

- **It is unclear if the Department intends to apply the restrictions this DFAR would create prospectively or retroactively.** If applied retroactively, it would place a significant financial burden on the contractor to reengineer their services to meet the requirements, may require modification to service delivery and may result in an increase in price to the customer.

Trey Hodgkins
Vice-President for National Security & Procurement Policy
Public Sector
TechAmerica
703-284-5310
thodgkins@techamerica.org

TechAmerica