# *Risky Cyber Security: '7012' Regulations*

## *Federally-driven inhibitor to resilience within the defense industrial base*
## *A Position Paper*

Larisa Breton
FullCircle Communications, LLC
Troy, MI USA

***Abstract* – U.S. Department of Defense regulations intended to improve cybersecurity within the Defense Industrial Base may cause degradation of critical defense infrastructure. Four impediments to 'clean' compliance, environmental and internal, are detailed. Inability to functionally comply, or to correctly insure, will impact the DIB's cybersecurity decision-making at the enterprise level. Economic impact to the DIB may drive withdrawal and attrition from the sector, or aversion to R&D, which negatively affects mission resilience with concomitant capability loss to the DoD.**

***Keywords – Cybersecurity, resilience, R&D, DoD, economics, defense industrial base***

## I. INTRODUCTION

The United States' Defense Industrial Base (DIB) is a critical enabler to American national security due to the comprehensive support it provides to the U.S. Department of Defense (DoD), with 'procurement' and 'RDT&E' forming substantial categories within overall Defense budget allocations each year [1]. This support takes the form of direct contracting, professional services, and research and development (R&D) across all DoD-related verticals. The DIB also provides related support to defense-related Federal agencies such as those concerned with intelligence; homeland security; nuclear energy; public health; and financial systems.

When examining cybersecurity in national defense, typical foci are the attacker/adversary and the institutional defender [2]. Evaluations and ongoing research treating the defense complex include defining asymmetric imbalance in cybersecurity involving velocity of targeted attack versus institutional response; low cost-of-entry in a quiescent actor versus high cost of defense in a formal entity; and asymmetric operational speed of informal versus formal operating procedures [3]. Within the context of those evaluations, this paper examines an asymmetry occurring within, and driving impact to, the institutional side of the defense complex. This asymmetry is the declining relationship between security and resiliency in the DIB as it prepares to comply with the Defense Federal Acquisition Regulation 252.204-7012, more commonly referred to as the 7012 regulations, which were proposed in 2013, modified twice in 2015, and enacted in October 2016.

The 7012 regulations require all Federal contractors, of any size, to secure the networks carrying Covered Defense Information (CDI) as-designated by the DoD. The regulations direct all contractors to comply with the National Institute of Standards and Technology's Special Publication 800.171's (SP 800.171) technical rubric. Further, while the regulations originally required notifications of events both up, and down, the subcontracting chain, with notification triggers and attendant evidence-storage requirements [4], interim guidance and amendments in 2015 and final 2016 rule now permit verbatim subcontracting flowdowns only to those subcontractors expected to also require covered systems (CFR §48, 252.204-7012 as-amended).

In subsequent sections, this paper describes impediments to 7012 compliance within the DIB that will inhibit both the DIB's ability to accurately assess performance risk; and to price-tag true costs of compliance. These unpredictable, yet serious, economic impacts occur before and during contract performance. Illustrative scenarios, incorporating these impediments as drivers to outcomes, are presented. Attendant capability impacts to DoD caused by degradation to the DIB are then inferred.

## II. FOUR TYPES OF IMPEDIMENTS

Impediments to understanding and implementing comprehensive business-risk assessment and mitigation surrounding the 7012 regulations, as well as costs, are environmental and internal. In the American DIB, they include:

### *A. Regulatory Impediments.*

- Lack of brightline guidance from DoD itself about how DoD will interpret due care when evaluating contractors' planning for, and responding to, events.
- Diversity of systems covered under the regulatory architecture. For example, Tactics, Tools and Procedures (TTPs) to be issued by

DoD in a forthcoming memo of instruction setting out DoD ownership of, and components' internal responsibilities for, physical IT systems (PIT)[1] call on system owners to self-identify attack surfaces. This then drives the DoD PIT system owner to identify, and negotiate, potential vulnerabilities at axil points inside the PIT system which may include — but are not limited to — contracting, software licensing agreements, real property governance issues, vendor-maintained sub-systems, and operational interdependencies in mobile, but physical, IT-dependent systems. Any of the preceding five dependencies will involve DoD contractors who are engaged in everything from program management to logistics to mobile hospitals to parts manufacture.

- Potentially conflicting regulatory schema between Federal (NIST), and international (ISO) guidance.

*B. Judicial Impediments.*

- Until precedential, unclassified and public decisions are meted out in Federal courts, a body of case law pertaining directly to the regulation that would reduce ambiguity about liability is not available. Litigated commercial-insurance analogues, particularly as they pertain to indirect liability, may or may not be apt.
- More narrowly, it is yet to be seen whether Federal benches will approach interpreting events involving contractor due care and compliance arising from 7012-related events via the lens of formalist jurisprudence, in which an absolute legal principle will be applied; or via the lens of legal realist jurisprudence, in which judges solve complex legal situations by balancing the legal interests of the parties [5].

*C. Legal and commercial practice- issues Impediments.*

- The risk driven to contractors by their own advisory law firms that, themselves, do not understand the holistic nature of cyber threat which occurs outside of network perimeters; and/or have not yet instituted robust IT hygiene practice in their workforces. Advisory professional service providers, themselves, may be a physical network attack vector. They also may be a vector for a sneaker-netted entry or some other soft entry, such as blackmail, due to their access to comprehensive information about the contractor's business and its personnel [6].
- Skills gap between the DIB and the legal advice they may receive, including the potential involvement of state (tort) law when physical damages have occurred as a result of an event. The contractor, itself, may possess more technical acumen than the advisory professional; and it may already have more robust defenses and operating procedures in place than the advisor. However, unless specifically focused in cybersecurity, or large enough to afford coordinated internal legal and IT expertise, the contractor may be less likely to understand the potential legal impacts to its business. For example, the contractor may trip itself up on chain of custody or other forensic issues.
- The current and future lack of judicial guidance occurring from confidential settlements arising from notable security that otherwise could be considered precedential examples of acceptable, or unacceptable, incident response.
- The inability of the wider DIB or its advisory services to learn from the mitigations or impacts of events that occur within classified programs. This may include how the DoD views spillage, which may be a useful corollary to 'contained' CDI breaches within the rubric of the regulations.
- More narrowly, the portion of the DIB that handles classified information has, in practice, a greater conceptual understanding of the meaning of and how to segregate information, practices and personnel to reduce attack surface. But the un-cleared portion of the DIB has little experience on which to draw. It also has little/no access to the DoD's Defense Security Service-provided training and guidance that is available to cleared contractors.

*D. Dynamism Impediments.*

[1] The unclassified memo, in draft as of this writing, is iterative to the current Department of Defense Instruction 8500.01 issued March 14, 2014 (DoDI 8500.01).

- Dynamism in pricing. Contractors who bid and perform on "indefinite delivery indefinite quantity" (IDIQ)-type contracts for DoD are subject to forward-pricing constraints, in which their pricing models can be acceptable to the government at the time of bid submission, but subject to real-time (usually downward) adjustment as programs evolve and overhead structures change.
- Dynamism of threats and ongoing defensive response to threats. This dynamism is well-examined and requires no additional elaboration here.
- Dynamism of insurance market pertaining to required coverage. Insurers wish to capitalize on rapid market growth; yet they themselves incur additional risk in doing so [7].
- Dynamism of contractor maturity-in-practice at any business size. This maturity-in-practice covers all aspects of business operations, from the C-suite (risk management, continuity planning) to the front desk (networks, hygiene, physical access). Large contractors with well-defined practices may experience an event due to entropic adherence to these practices. Small contractors with good regimens may fall out of compliance due to insufficient formal management structures and products.
- Dynamism of impacts from events in other parts of the contractor's DoD business chain. These could include:
    - Direct or indirect liability for insurance claims
    - Direct or indirect liability for legal claims
    - Inability to fulfill contracts due to sub-contractor nonperformance
    - Cancellation of sub-contracts by prime contractors
    - Cancellation of prime contracts by DoD

## III. NOTIONAL SCENARIOS DEVELOPED USING IMPEDIMENTS

In this section, each developed scenario utilizes an impediment as-described in the previous section. Each scenario contains a brief précis statement that articulates whether the scenario-driver is an environmental or internal impediment.

*Scenario 1.*
*Scenario-driver: External impediment*
*Impacts: Contractor revenue shortfall. DoD loses commercial capability*

A small commercial engineering firm that started in a University incubator, SafeCo, has earned multiple software patents in pattern detection, and is awarded a sole-source contract from the Air Force to help develop a network surveillance tool. As part of their diligence to comply with prime contract provisions, SafeCo applies for additional general liability insurance with a rider for breach recovery that includes legal defense fees. Their application is denied by every insurance firm who quotes them because SafeCo works "in cybersecurity," and is thus deemed too high-risk by underwriters to insure. SafeCo weighs the costs of legal defense in the event of a breach; and weighs the reputational damage that would occur to them if they take on a prime contract that is rescinded. Regretfully, they turn the contract back to the Air Force.

*Scenario 2.*
*Scenario-driver: Internal impediment*
*Impacts: DoD program capability shortfall. Operant knowledge loss inside contractor. Operant knowledge loss inside DoD program.*

BICKERSON, a large services-aggregator, is engaged in negotiations for an IDIQ contract extension with the Navy to provide hardware and software engineering and program management support services. Just as BICKERSON was ready to submit its DCAA-compliant forward pricing rates, its IT department socialized revised department costs that reflected a 247% increase in order to hire internal cybersecurity personnel, harden its unclassified network, re-train personnel, and hire two full-time administrators to ensure 7012 compliance in its subcontracting chain. Reviewing this, BICKERSON finds its proposed labor costs will not bear the additional overheads, and its functional profit margin (fee) would go from four percent to break-even on the contract. BICKERSON is unable to provide cost-of-living increases to its full-time staff, and discontinues subcontracts with its smaller vendors. In frustration, the Program Manager and senior developers find jobs on other projects, taking a combined 25 years of institutional memory out of the program. As a result, technical event milestones are missed.

*Scenario 3.*
*Scenario-driver: External impediment*
*Impacts: Mass casualties. Civil liability for negligence. Negative public sentiment to DoD agency. Environmental cleanup drives $2.7 million into DoD program costs.*

Dandelion Trucking, famous for its bright-yellow vehicles and funding college scholarships, has performed flawlessly on a Veterans Administration contract for years, to haul and store hazardous waste from VA hospitals in Virginia. Dandelion's management hired an outside consultancy to bring them into compliance with the 7012 regs and to shore up cybersecurity. The outside consultancy committed Dandelion to a server backup company which suffered a catastrophic breach. Information was exfiltrated and bought on the darkweb by a hacktivist collective, which used the information to enter Dandelion's network and disable sensor controls and alarms. As a result, toxic fumes were released from a Dandelion storage facility and sickened hundreds in a residential neighborhood. A court granted class-action status to the victims. At trial, the court found that the software licensing agreement between Dandelion and the server backup company expressly indemnified the server company from any-and-all liability — and that the consultancy, acting on Dandelion's behalf, had done insufficient diligence. Dandelion goes under. The VA now bears environmental remediation costs and is embroiled with Dandelion's landlord and the EPA about the contaminated waste site.

## IV. SUMMARY: ECONOMIC IMPACT-DRIVERS AND CAPABILITY LOSS TO DoD

This paper sets-out four types of critical upstream impediments faced by the U.S. DIB as it is poised at the leading edge of what will be, to all but the most sophisticated contractors, an onerous and confusing requirements-set to comply with the 7012 regs. Unfortunately, on-paper compliance with the NIST 800.171 does not ensure that contractors will, in fact, have secured their systems, not does it completely insulate them from culpability to the DoD or from outside liability with insurers and courts.

Cyber-events, themselves, are asymmetric to the DIB because a 'small' checklist issue such as an unattended terminal can hamstring a large program; and the smallest businesses driving high-impact intellectual capital into the defense complex can run into the ground with 'large' legal issues pertaining to administering Federal work. These compliance-related issues are economic drivers that cause a larger asymmetry within the defense complex itself by degrading DoD capability. Loss of access to leading commercial technologies, loss of institutional (operant) knowledge, loss of depth in research and development, and velocity loss / program disruptions are predictable capability gaps. All of these widen the attack surface for nefarious actors (offense side) wishing to discover and exploit weaknesses.

## BIBLIOGRAPHY


[1] N. D. Hensel, *The defense industrial base : strategies for a changing world*. Farnham, Surrey, England ; Burlington, VT: Ashgate, 2015, pp. x, 290 pages.

[2] J. Carr and C. Lotrionte, *ed, . Inside Cyber Warfare*. 2012.

[3] J. Bayuck, J. Healey, P. Rohmeyer, M. Sachs, J. Schmidt, and J. Weiss, *Cyber Security Policy Guidebook*. Hoboken, N.J.: Wiley, 2012.

[4] L. Breton. (2015, May 26, 2015). *7012 Regs and Cyber insurance on collision course with small business*. Available: https://ctovision.com/cyber-insurance-small-business/

[5] (April 25, 2017). *Jurisprudence*. Available: https://www.law.cornell.edu/wex/jurisprudence

[6] S. Randazzo, "Cyberattack Exposes Law Firms' Weak Spots," in *The Wall Street Journal*, ed. Online Edition, 2016. Available: https://www.wsj.com/articles/cyber-hack-exposes-law-firms-weak-spots-1482965375

[7] M. Grey. (2015) Cyber poses credit risk to insurers who offer it. *Insurance Business Magazine Online Edition*. Available: http://www.insurancebusinessmag.com/au/news/breaking-news/cyber-poses-credit-risk-to-insurers-who-offer-it-56303.aspx



*Author acknowledgement*. L.C.B. wishes to acknowledge Leonard F. Charla, J.D., L.L.M..