Bloomberg BNA

Federal Contracts Report™

DOD

Convergence of Counterfeit and Cyber Threats: Understanding New Rules on Supply Chain Risk

BY ROBERT S. METZGER

Section 818 of the National Defense Authorization Act of 2012 (''NDAA 2012'') should be understood in the context that led to its enactment, and the harm that it sought to prevent. But as time has passed, since enactment of Section 818 late in 2011, the federal government's perception of the threat has changed and so too has the emphasis of policy and regulatory initiatives being taken in response. While DoD will continue to develop and implement rules to protect the military supply chain against counterfeit electronic parts that could cause premature system failure, the increasing emphasis of DoD and other federal agencies (including the GSA) will be on protection against those counterfeits that present cyber risks. The government's initiatives to protect the supply chain will naturally focus first on agencies responsible for critical infrastructure and those that perform national security functions. But measures to protect the supply chain against cyber threats will come to affect acquisition practices and contractor oversight for all federal agencies. This is because of the dependence of federal functions upon information and communications technology (ICT), the omnipresent use of electronic equipment that draws upon a global supply chain, and the vulnerability of that supply chain both to counterfeits and cyber attack.

Prudent federal contractors should assess how they can improve protection of their supply chain against counterfeits (and other nonconforming materiel) and what measures they can take now to reduce cyber vulnerability and improve cyber resilience. Improved supply chain security and reduced cyber vulnerability are important national objectives.[1] To secure these objectives, the government can and will use its control over acquisition practices and its oversight and compliance mechanisms. Some in industry object to greater government intercession in supply chain and cyber risk management, citing an absence of standards and concerns about industrial base impact and adverse effects upon traditional notions of ''open competition.'' Even though many such concerns have merit, industry should focus its attention on preparation for new rules and regula-

Robert S. Metzger, a shareholder with Rogers Joseph O'Donnell, P.C., has written or co-authored four previous articles in Federal Contracts Report on counterfeit parts prevention and supply chain security. *The author acknowledges with appreciation the assistance of Oliya S. Zamaray, an associate in the Washington, D.C. office of Rogers Joseph O'Donnell, in the preparation of this article.*

[1] Among U.S. national security leaders, cyberwarfare is considered the most serious threat facing the United States, according to a ''Leadership Poll'' conducted by *DefenseNews*. *See* Zachary Fryer-Biggs, *Poll: Cyberwarfare is Top Threat Facing US*, DefenseNews (Jan. 5, 2014) http://www.defensenews.com/article/20140105/DEFREG02/301050011.

 ISSN 0014-9063

tions, rather than objection and resistance. The national interest in achieving greater supply chain and cyber security is so compelling that, in the author's estimation, the federal government will act irrespective of industry's doubts. The pace of implementation of supply chain and cyber actions is likely to accelerate and the breadth of such actions likely will encompass most or all federal procurement functions. Companies that ignore or resist these trends do so at their business peril.

NDAA Section 818 Focuses on Counterfeit Electronic Parts. Between 2011 and 2012, the Senate Armed Services Committee (SASC) conducted a thorough investigation of counterfeit *electronic* parts. The Report on the SASC investigation was released on May 21, 2012. The investigation was a principal cause of the enactment of Section 818, the purpose of which was to avert the risk to military systems and military personnel that could result if counterfeit electronics caused defense equipment to fail. While it operates at many ''junctions'' of the supply chain, Section 818 addresses only electronic parts purchased for defense supplies. It does not deal with other forms of counterfeit materiel. And, while the law has generated considerable attention and some anxiety within the defense contracting community, its formal implementation has been delayed.[2] Moreover, as a matter of legislative construction, Section 818 may not now impose binding obligations upon any contractor, because there are no implementing regulations yet.[3] Once regulations are in place, the law applies directly only to ''covered contractors, i.e., those DoD suppliers who are subject to the Cost Accounting Standards.''[4]

Though implementation of Section 818 is incomplete and many particulars are unresolved, no responsible contractor should postpone taking action to reduce vulnerability to counterfeits or to enhance capability to detect and avoid counterfeits. Independent of the legal effect of Section 818, and its implementing regulations, solicitations already may include tougher anti-counterfeit measures and many companies that are or will be subject to Section 818 already have taken steps to improve their internal practices and to ''flow down'' to their vendors clauses that are derived from the expected requirements of Section 818.

While the purposes and principles of Section 818 are commendable and draw little industry opposition, effective and practical implementation is challenging because of the breadth and depth of the electronics supply chain. Prime contractors and higher tier subcontractors, where they are ''CAS-covered,'' will be subject to the compliance and contract clause requirements of Section 818 when the regulations emerge. We can expect the regulations to ''require'' flow-down by ''covered contractors'' to their subcontractors. The conundrum is that the law itself, by its terms, does not appear to apply directly to anyone other than the large, ''covered contractors.'' This implies that those companies that must comply will not have a legal basis to insist upon adherence on the part of their suppliers who are not ''covered'' and who do not choose to agree to accept the requirements. This asymmetry is a source of great concern to the larger contractors, who know that the law and regulation *will* apply to them, but who have no assurance they *can* satisfy supply chain needs with vendors who will also accept similar compliance obligations or liability risks. These considerations contribute to the continuing efforts of larger defense contractors to change Section 818 to expand the boundaries of the very narrow ''safe harbor'' that is now present.[5] While these efforts have generated some support in the House, the Senate Armed Services Committee has consistently rebuffed attempts to give greater protection or relief to industry. This likely reflects what the Committee cited as ''Conclusion 5'' when it issued its final Report on counterfeits: ''Permitting contractors to recover costs incurred as a result of their own failure to detect counterfeit electronic parts does not encourage the adoption of aggressive counterfeit avoidance and detection programs.''[6] While the Committee may be persuaded by examples of unfairness or hardship actually experienced, it is very unlikely to be moved by speculative scenarios of potential harm.

Rulemaking to Implement Section 818 is an Iterative Process. DoD recently acknowledged that rule-making to implement Section 818 has followed an ''iterative'' process, including two DFARS cases and two FAR cases.[7]

- The most attention, so far, has been upon DFARS Case 2012-D055, ''Detection and Avoidance of Counterfeit Electronic Parts.'' The proposed rule that DoD re-

[2] The implementing regulations for Section 818 originally were due on September 26, 2012. *See* Section 818(c)(1). That the regulations are so late reflects the complexity of the area, at the implementation level, and (in the author's opinion) DoD's recognition that it should proceed carefully, so as not to issue prescriptive rules that would have dysfunctional consequences or impose costs disproportionate to benefits.

[3] NDAA Section 818 is not a ''self-executing'' statute. From the plain language of Section 818, Congress expressly instructed DoD to ''revise the DFARS'' and thus it appears to be a ''wholly-enabling'' statutory provision that lacks legal effect without the enactment of a regulation.

[4] At Section 818(c)(2), ''covered contractors'' are responsible for detecting and avoiding the use of counterfeit electronic parts and for any rework or corrective action. The statute defines ''covered contractors'' by reference to Section 893(f)(2) of the FY 2011 NDAA, which in turn provides that ''covered contractor'' is one that is subject to the Cost Accounting Standards. Section 818(c)(2)(A) makes ''covered contractors'' responsible for detecting and avoiding the use of counterfeit electronic parts and Section 818(c)(2)(B) makes unallowable the costs of any counterfeit part and of rework or corrective action. The specifics of implementation of the disallowance are presently unknown, but the direct effect likely will be limited to contracts that are subject to the Cost Principles at FAR Part 31.

[5] Section 833 of the FY 2013 NDAA provides relief from the potential disallowance of costs of replacement of a counterfeit part and of remedial costs where a company has an operational and approved system of counterfeit avoidance, promptly notified the government of the discovery of a counterfeit or suspect counterfeit part, *and* where the bad part came from DoD as government-furnished property.

[6] ''Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts'' (May 21, 2012), http://www.levin.senate.gov/newsroom/press/release/senate-armed-services-committee-releases-report_on-counterfeit-electronic-parts#sthash.p4JNsra2.dpuf.

[7] Letter from Richard Ginman, Director, Defense Procurement and Acquisition Policy, to Scott Bouson, TechAmerica, dated January 17, 2014 (available from author upon request).

  FCR ISSN 0014-9063

leased for comment, on May 16, 2013, 78 Fed. Reg. 28780, produced over 200 public comments.[8]

■ FAR Case 2012-032, ''Higher Level Contract Quality Requirements,'' was published on December 3, 2013, 78 Fed. Reg. 72620, and comments on this proposed rule were due on February 3, 2014.

■ Industry also awaits the outcome of FAR Case 2013-002, ''Expanded Reporting of Nonconforming Supplies,'' which is expected to address reporting of counterfeit and suspect counterfeit items (possibly extending beyond electronic parts). This proposed rule is under review at OMB.[9]

■ DoD has just opened a new DFARS case, 2014-D005, ''Detection and Implementation of Counterfeit Electronic Parts – Further Implementation,'' about which no particulars are presently known.[10]

Of the four rulemaking cases that DoD acknowledges are intended to implement Section 818, two are pointed towards new DFARS, applicable only to defense procurement, while two extend beyond defense procurement to the FAR generally. This is an important signal that the counterfeit prevention measures, propelled by Section 818 and targeted initially upon large defense suppliers and electronic parts, will extend to reach other sectors of federal systems acquisition. Just as counterfeit parts can cause a defense system to fail, the introduction of counterfeits into other systems purchased or used for the federal government can have similar, undesirable effects.

'Malicious' Counterfeit Parts May Harbor Cyber Threats. The threat posed by ''counterfeits'' now is understood to be broader than the immediate focus of the SASC investigation – and more pernicious. Independent of the various rule-making actions to implement Section 818, the federal government has taken a number of important initiatives in recent months that address *supply-chainsecurity* with objectives that encompass, and enlarge, efforts to detect and avoid counterfeit electronic parts. These actions reflect the intersection of *supply-chain* and *cybersecurity*.

Specifically, it is now evident that the government is directing special attention to avoidance of parts which harbor malicious code and which, if installed in military equipment, in a secure network, or in a key system used for information processing or telecommunications, for example, could have disabling effects upon such ''trusted systems and networks'' and other ''critical functions'' of government. Parts that carry a cyber threat are ''counterfeit,'' in the sense that they are not what they purport to be, and have been modified or subjected to ''tampering'' without authorization. The threat of such ''tainted'' parts is distinct and potentially more severe than that posed by ''ordinary'' counterfeits. Initially, the sources of such ''malicious'' counterfeits are likely to be even more sophisticated than the suppliers of counterfeit parts (where ''greed'' is the dominant motive). Sources of malicious counterfeits may be state sponsored or even state actors who pursue adversarial objectives against the interest of the U.S. and our allies. Even the very best testing and inspection techniques, which ordinarily will serve to flush out counterfeits that are ''fakes,'' may not succeed with ''malicious'' parts that mimic expected operational functionality but also carry hidden, hazardous code.

The threat of ''malicious'' counterfeits is very real and the potential harm to the national interest is very great. Examples have been found of sophisticated ''clones'' of current production electronic parts, made by unauthorized sources. These may seemingly possess ''correct'' electrical functionality. Through such ''clones'' or other means, a hostile entity could introduce code for such purposes as exfiltration of sensitive data, theft of technology and private intellectual property, to disable or alter intended functionality or to create ''backdoors'' through which other cyber threats could be communicated. Detecting hostile code or unexpected features can be extraordinarily difficult even with the most sophisticated of techniques. This is one reason that supply chain security measures exclude sources of parts where the maker or place of origin of the part can be associated with hostile actors or known cyber risk.

The nexus between counterfeit parts and cyber risk has recently been recognized in a Joint Report, ''Improving Cybersecurity and Resilience through Acquisitions,'' issued by the Department of Defense and the General Services Administration on January 23, 2014. This report implements Section 8(e) of Executive Order (EO) 13656.[11] The Joint Report observes that counterfeit components can be introduced during both initial acquisition and sustainment, and that such nonconforming parts create vulnerabilities that include prema-

[8] Public comments are available through the Defense Procurement and Acquisition Policy (DPAP) web page, at http://www.acq.osd.mil/dpap/dars/counterfeit_electronic_parts.html. The author's statement on the proposed rule is available at http://www.acq.osd.mil/dpap/dars/publicmeeting/presentations/Robert_Metzger_Statement.pdf.

[9] Industry sources have expressed concern that the reporting obligations extend what is dictated by Section 818(c)(4) because coverage in the FAR would indicate applicability beyond counterfeit electronic parts to supplies purchased by DoD. The subject of reporting, like so many other aspects of the struggle to combat counterfeit materiel, is much more difficult than may first appear. There is a general consensus that both suppliers and customers have a need to know, promptly, the particulars of a counterfeit event. At the least, the desired information should include the nature of the event (the ''what''), the method or vector by which the event occurred (the ''how''), the origin of the suspect or known counterfeit part (the ''who'') as well as information on potentially affected parties, possible impacts, and recommended remedial actions. But putting these concepts into rules that are objective and reflect current technical best practices is very demanding. There is no industry consensus on which parties in the supply chain should have responsibility for reporting or on how to disseminate information once collected. Assuring fairness and due opportunity for correction or rebuttal also is very important and potentially a source of great contention.

[10] The new DFARS case, 2014-D005, appears to be a ''division'' of the original case, 2012-D055, suggesting that DoD intends to proceed to implement some aspects of what was initially proposed in D055 while reserving other issues for later consideration. This is a positive sign as many in industry have urged further consultation and coordination with stakeholders before the effective date of any Section 818 implementation rule.

[11] Executive Order 13636 (EO), released on February 12, 2013, sought to protect critical infrastructure against cybersecurity threats. Section 8(e) directed the Secretary of Defense and the GSA Administrator to make recommendations on the ''feasibility, security benefits, and relative merits'' of incorporating cybersecurity standards into acquisition planning and contract administration.

ture system failure and latent security gaps that could be exploited by an adversary.[12] The Joint Report contains six recommendations, one of which is to avoid the risk of counterfeit, inauthentic or otherwise nonconforming items by limiting sources to original equipment manufacturers (OEMs), their authorized resellers, or other trusted sources.[13] The Joint Report anticipates changes to federal acquisition practices – though they have not yet happened – that will emphasize use of trusted sources, require contractual ''guarantee'' of security and integrity of purchased items, and cause suppliers to be evaluated against criteria that include risk factors relevant to supply chain source.[14]

Supply Chain Risk Management Must Address the Cyber Threat. The seriousness of the cyber threat, as can be carried by malicious parts put into the supply chain, is discussed in a Defense Science Board (''DSB'') Report titled ''Resilient Military Systems and the Advanced Cyber Threat.''[15] The DSB Report states:

> Recent DoD and U.S. interest in counterfeit parts has resulted in the identification of widespread introduction of counterfeit parts into DoD systems through commercial supply chains. Since many systems use the same processors and those processors are typically built overseas in untrustworthy environments, the challenge to supply chain management in a cyber-contested environment is significant.
>
> . . . .
>
> DoD is in the process of institutionalizing a Supply Chain Risk Management (SCRM) strategy that prioritizes scarce security resources on critical mission systems and components, provides intelligence analysis to acquisition programs and incorporates vulnerability risk mitigation requirements into system design.[16]

The link between cyber security and supply chain risk management was emphasized recently in the confirmation hearings conducted by the Senate Armed Services Committee on January 16, 2014, including the confirmation of Dr. William LaPlante, nominated to serve as the Assistant Secretary of the Air Force (Acquisition). In response to a question from Sen. Joe Donnelly (D-Ind.), and comments from the Committee Chairman, Sen. Carl Levin (D-Mich.), Dr. LaPlante tied responses to the threat of counterfeit electronic parts into the broader issue of cyber security.[17] Dr. LaPlante endorsed further research into science and technology measures to implement non-invasive systems that enable surveillance of the composition and code of electronic parts, in order to detect anomalies and ''Trojan Horse'' viruses.[18]

Previous DoD Initiatives to Protect Critical Systems Against Malicious Parts Insertion. DoD has taken several important initiatives, separate from rules affecting contracts and contractors, aimed at protecting critical functions and trusted systems and networks against cyber threat and intrusion, whether introduced by a ''malicious'' counterfeit or by other means. DoDI 5200.44 (''Protection of Mission Critical Functions to Achieve Trusted Systems and Networks''), issued on November 5, 2012, is especially informative and helps to understand more recent actions and those that can be expected henceforth.

Among the purposes of DoDI 5200.44 are to ''minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components . . . by foreign intelligence, terrorists, or other hostile elements.'' Where a potential adversary mounts an ''attack'' upon the supply chain (by insertion of a ''malicious'' part) the functionality of an infected system may be impaired or lost. DoDI 5200.44 applies to all DoD ''information systems and weapons systems'' that are or include ''National Security Systems'' or ''Mission Assurance Category (MAC) 1'' systems. The applicable definition of a ''MAC 1'' system is one that handles information ''that is determined to be vital to the operational readiness of mission effectiveness of deployed and contingency forces . . . [and] the consequences of loss or integrity or availability . . . are unacceptable.''

DoDI 5200.44 establishes that the ''criticality of the system'' determines the level of assurance that is to be sought. And, ''all-source'' intelligence analysis of ''sup-

---

[12] Joint Report, at 12.

[13] *Id.* at 17. The Joint Report, however, recognizes the tension between supply chain assurance purposes, which motivate potential restrictions on sources of supply, and other federal acquisition principles, such as ''acquisition rules, socio-economic procurement preferences, or principles of open competition.'' *Id.* A persistent challenge in protection of the supply chain against both ''ordinary'' counterfeits and tainted parts that harbor malicious code is that the protective measures come at a cost to open market access to federal procurement opportunities.

[14] *Id.* at 18. The Joint Report includes comments that the ''method'' by which the government conducts supplier evaluations ''should be based on the cyber risk of the acquisition type.'' Yet to be defined is a common process to assess ''cyber risk'' or a method to distribute information about the risk to industry. The Joint Report certainly shows that the government intends to move towards evaluation of cyber assurance in future civil and military procurements, but the implementation particulars are not evident. The Report speaks of sets of ''overlays'' for particular acquisitions. *Id.* at 16. These are described as ''fully specified sets of security requirements and supplemental guidance'' to enable tailoring of security requirements for acquisitions. *Id.* While there is merit in the idea of tailoring requirements to assessed risks, methods should be developed to better inform industry of cyber threat vectors and the government will need to work with industry to accommodate varying ''best practices'' that are suitable for the diversity of suppliers and panoply of at-risk devices.

[15] Dated January 2013, the report is available at http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf (the ''DSB Report'').

[16] *Id.* at 4.

[17] The confirmation hearings are available at http://www.armed-services.senate.gov/hearings/nominations-creedon-carson-laplante.

[18] In the same vein is Intelligence Community Directive (''ICD'') 731, published on December 7, 2013, which summarizes concisely the convergence of supply chain and cyber threats:

> Supply chain risk management is the management of risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain. It addresses the activities of foreign intelligence entities . . . and any other adversarial attempts aimed at compromising the IC [Intelligence Community] supply chain, which may include the introduction of counterfeit or malicious items into the IC supply chain.

ICD 731, Dec. 7, 2013, available at http://www.dni.gov/files/documents/ICD/ICD%20731%20-%20Supply%20Chain%20Risk%20Management.pdf.

  FCR ISSN 0014-9063

pliers of critical components'' is to be used to inform ''risk management decisions.'' The risk to the trust in applicable systems is to be managed throughout the entire system lifecycle and encompasses the ''acquisition of critical components'' whether acquired through a commodity purchase, systems acquisition, or sustainment process.

Also important is DoDI 4140.67 (''Counterfeit Prevention Policy''), issued on April 26, 2013, which, in contrast to Section 818, applies to all ''counterfeit materiel'' – not just electronic parts. DoDI 4140.67 also applies to ''all phases of materiel management,'' while Section 818 concentrates on acquisition and sustainment. This reflects the proposition that a comprehensive strategy to avoid counterfeits (whether ''fakes'' or ''taints'') is one that encompasses *design* (to avoid the use of obsolete or obsolescent parts, materiel of diminishing availability or at-risk manufacturing sources, and to reduce vulnerability to insertion), *acquisition* (to control sources of supply to minimize counterfeit risk and require additional testing and inspection where appropriate), *sustainment* (to anticipate future difficulties in maintenance and repair of a system that may arise if parts are not available from original or trusted sources) and *disposition* (to anticipate measures to prevent the ''recirculation'' of parts that could be repurposed for unauthorized uses). A particularly sensitive question, on which DoD has yet to give clear guidance even as to its internal practices, is how to treat the vast inventory of accumulated electronic parts and devices acquired before the contemporary emphasis on supply chain security and counterfeit parts avoidance.[19]

DoD's New Interim Rule to Protect the Supply Chain Against Malicious Parts. An important development focused on ''tainted'' parts – and protection of trusted systems and networks and critical infrastructure – occurred on November 18, 2013, when DoD issued an ''interim rule'' establishing ''Requirements Relating to Supply Chain Risk.''[20] A product of DFARS Case 2012-D050, this new interim rule implements Section 806 of the FY 2011 NDAA, Pub. L. No. 111-383, § 806, as amended by the FY 2013 NDAA.[21] The interim rule is effective immediately on a pilot basis.[22]

Industry has been critical of the interim rule. Objection has been made to the fact that it was promulgated without an opportunity for public comment and made immediately effective. Concern has been expressed at the sweeping breadth of its application and its potential reach to all sources of information technology. It has been criticized as having potentially unfair effect upon competition and competitors, and questioned for its failure to inform companies whose eligibility to supply to the federal government could be affected, even foreclosed, by the government. Carefully examined, however, the most controversial elements of the rule are dictated by the underlying statute. Some of the criticism fails to acknowledge the narrow circumstances (and few occasions) when the rule likely will apply. Fundamentally, the rule fulfills a proposition that is in the elemental if not existential self-interest of the U.S. government: it must protect its critical information and communications systems, and key national security systems, against cyber threats that can be carried out by exploiting supply chain vulnerabilities.[23] Where the

[19] Literally millions of parts, acquired over many years, remain in inventory at the Defense Logistics Agency, other DoD components and government agencies, as well as in stores at contractors at all tiers. And millions more parts are in the hands of distributors and brokers – both those authorized through sources with traceability to the original component manufacturers and those acquired in the open market with uncertain origin. Traceability of inventory may be unknown, as material has been comingled and transferred among sites and subcontractors. Few organizations have maintained paperwork for batches of parts, or paperwork may have been lost over time. When most of these parts were acquired, today's attention to the risk of counterfeiting was not present. Nor would there have been sensitivity to the risk of parts falsely represented as new or not previously used. (Such parts might pass acceptance testing but fail to function in the intended environment, or fail to operate for the planned life.) Quality management systems and conformance testing of the past may not have been adequate to detect the threat as we know it today. Counterfeit parts in inventory, acquired over time, may not harbor ''hostile'' code that could be actively manipulated by an adversary. That is a more recent threat. But such parts could introduce unintended vulnerabilities to cyber intrusion and, apart from the cyber risk, present the risk of hazardous, untimely failure that motivated the SASC's investigation and led to enactment of Section 818. While the attention of DoD and industry, understandably, has focused forward from the present, to reduce vulnerability in future purchasing, and to design away vulnerability, the fact remains that today there is indeterminate but real risk present in parts inventories. DoD will need to consider how to respond, as to DLA and its other components, and contractors will need to face this open question.

[20] 78 Fed. Reg. 69268.

[21] As originally enacted, Section 806 was subject to a ''sunset'' provision that would have caused its authority to expire three years after the date of enactment. The FY 2013 amendment extended the date for the authority through September 30, 2018. The Intelligence Authorization Act for Fiscal Year 2012 contained a provision extending similar authority to intelligence agencies. Pub. L. No. 112-87, § 309, 125 Stat. 1876, 1884-85 (2012). The new FY 2014 NDAA makes the same ''enhanced procurement authority to manage supply chain risk'' available to the Department of Energy. *See* Pub. L. No. 113-66, § 3113, H.R. 3304-382 (2013).

[22] The interim rule is described as a ''pilot program'' to ''mitigate supply chain risk'' which is to expire on September 30, 2018. 78 Fed. Reg. 69268. The action to promulgate the interim rule without prior opportunity for public comment was justified, according to the narrative accompanying the promulgation, as ''necessary because of the urgent need to protect National Security Systems (NSS) and the integrity of the supply chain to NSS.'' 78 Fed. Reg. 69270.

[23] The DSB Report, referenced previously, allocates cyber threats into a hierarchy of six ''tiers.'' Recognizing that U.S. military forces are ''critically dependent on networks and information systems to execute missions,'' the Report distinguishes among the levels of sophistication of threat actors and mechanisms. DSB Report, at 21. The most serious threats, at Tiers V and VI, encompass actors who can ''insert malicious software or modified hardware into computer and network systems at various points during their lifecycle for later exploit (e.g., a 'cyber time bomb').'' *Id*. At Tier V, the threat includes the ability of state actors to ''impact products while in the supply chain to enable exploitation of networks and systems of interest.'' *Id*. The Report postulates that a threat could be executed by removal of an integrated circuit from its packaging and replacement with a ''subversive die'' in the same package that would modify processor behavior. *Id*. at 25. In this extreme example, the Report postulates that the subversive die would not affect system performance through testing qualification or operation until a triggering operation was activated. That such a tainted part can operate as expected, except when commanded otherwise, distinguishes it from most counterfeits that will not pass ordinary device or system level tests. Should

government has intelligence information that gives it cause to believe that the source of a device may present such a national security risk, it cannot be objectionable that Congress has authorized the government to exclude such a source or that the DoD has implemented rules to use this authority. There will be room – and time – to improve the implementation to reflect experience and to minimize unfairness and improve transparency.

Statutory Authority for the Interim Rule. Section 806, which became law, Pub. L. 111-383, on January 7, 2011 gave DoD the authority to control sources of supply that present supply chain risk on certain procurements. The definition of ''supply chain risk'' clearly focuses on the risk of malicious hardware, firmware or software:

The term ''supply chain risk'' means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.[24]

The authority is to be used on a narrow class of ''covered procurement'' actions which involve a source selection (or task or delivery order) for a ''covered system'' or ''covered item of supply.''[25] In turn, these are defined, respectively, as a ''national security system,'' as defined by 44 U.S.C. § 3542(b), or the procurement of items that are ''information technology,'' as defined in 44 U.S.C. § 1101(6), that are purchased for inclusion in a national security system.[26] For this limited class of systems and items, the statute authorizes the Secretary of Defense, and each of the Service Secretaries, to exclude a source that fails to meet ''qualification standards'' or fails to achieve ''an acceptable rating'' with regard to an evaluation factor that considers supply chain risk. These officials also are authorized to withhold consent to a subcontract with a particular source or to direct a higher tier contractor to exclude a particular source from consideration for a subcontract.[27] These actions may be taken only after several demanding predicate actions. A joint recommendation must be obtained on the basis of a ''risk assessment'' that there is a ''significant supply chain risk.'' A written determination must be made that use of the authority is ''necessary to protect national security'' and that ''less intrusive means'' are not reasonably available.[28] Notice must be provided to appropriate Congressional committees, i.e., the Congressional defense and intelligence committees.[29]

The law also authorizes DoD to decide to limit the disclosure of information relating to the basis for exclusion of a source. No action taken under the authority of Section 806 shall be subject to review in a bid protest by the GAO or in any federal court.[30]

The Interim Rule. The interim rule implements Section 806 through three measures that address supply chain risk. First, a source may be excluded if it fails to meet ''qualification standards.'' Second, exclusion is permitted where a source fails to achieve an acceptable rating with regard to an ''evaluation factor providing for the consideration of supply chain risk.'' Third, the government may decide to withhold consent for a contractor to subcontract with a particular source, or may direct a contractor to exclude a particular source for consideration for a subcontract. DFARS 239.7305. These provisions track the statute, at Section 806(e)(2).

Similarly, the interim rule also tracks the statute in that it applies only to a source selection for a ''covered item'' or a ''covered system,'' and a ''covered item'' is defined as an ''item of information technology'' purchased for inclusion in a covered system.[31] Persons authorized to take actions under the interim rule are the same as in the statute.[32] Also in accord with the statute is the ''determination and notification'' process.[33] Restrictions on disclosure of these decisions are identical.[34]

Several features of the interim rule, allowing that they implement the predicate statute, are very troubling to industry:

■ *Breadth of Applicability*. The interim rule establishes a new provision (DFARS 239.239-7017) and clause (DFARS 239.239-7018) for inclusion in *all* solicitations and contracts, including contracts for *commercial items* or *commercial off-the-shelf* items, involving the *development* or *delivery* of *any information technology*, whether acquired as a *service* or as a *supply*.

This is an extraordinarily broad application of a law that, by its express terms, was to be applied only to ''significant supply chain risk'' within a narrow class of national security systems. The breadth of application, predictably, has prompted various trade and professional associations to express concern that this interim rule will impose costs and burdens across a whole range of suppliers, large and small, whose products may never be included in the critical systems that were the object of Section 806. DoD explains this extraordinary breadth as necessary because ''portions of these contracts may be used to support or link with one or more NSS.''[35] Further, DoD advises that there are ''operational security'' risks present if it were to include the supply chain risk clause only in ''very sensitive DoD procurements,'' thereby ''identifying those very procurements as a target for the risk section 806 aims to

unintended functionality be inserted into tainted devices that are installed in critical systems and networks, the results could be catastrophic; as described by the DSB, they include degradation of critical communications links, failure of weapon systems or operation of weapons in ways harmful to U.S. forces, and potential destruction of U.S. systems. *Id*. at 28.

[24] Section 806(e)(4).

[25] Section 806(e)(3).

[26] Section 806(e)(5), (6). A ''national security system'' according to 44 U.S.C. § 3542(b)(2)(A) , is ''any information system (including any telecommunications system)'' used by a contractor or agency for such functions as intelligence, cryptologic activities, command and control, equipment that is an integral part of a weapon or weapons systems, or is critical to the fulfillment of military or military intelligence missions.

[27] Section 806(e)(2).

[28] Section 806(b).

[29] Section 806(e)(7).

[30] Section 806(d)(1).

[31] *Compare* DFARS 239.7302 (definitions of ''covered item'' and ''covered system'' *with* Section 806(e)(5), (6).

[32] *Compare* DFARS 239.7303 *with* Section 806(e)(1) and 806(c).

[33] *Compare* DFARS 239.7304 *with* Section 806(b).

[34] *Compare* DFARS 239.7305 *with* Section 806(d).

[35] 78 Fed. Reg. 69268.

  FCR ISSN 0014-9063

defer.''[36] DoD should reconsider whether it truly is necessary or effective to include the supply chain risk clause in so many contracts when very few procurements actually will be subject to supply chain risk analysis and exclusion. In the comments that accompany the interim rule, DoD claims that ''no viable alternatives'' exist to the broad rule. But this seems more rationalization for the result than a convincing justification. DoD has limited security resources; it could have decided to selectively apply special supply chain security rules to potentially vulnerable procurements by disclosing evaluation standards and other notification and consent clauses. There is no known evidence that this approach was attempted or would not have worked.

■ *Absence of Standards*. The new ''Supply Chain Risk'' clause, at DFARS 252.239-7018(b), requires contractors subject to the clause to ''maintain controls in the provision of supplies and services to the government to minimize supply chain risk.'' At DFARS 252.239-7018(e), the clause requires contractors to include the substance of the clause in all subcontracts for the development or delivery of any IT. The consent provision, at DFARS 252.239-7017, essentially requires that contractors agree that the government may exercise the authorities provided by Section 806. These include the authority, explained at DFARS 239.7305(a), to exclude a source that ''fails to meet qualification standards'' for the purpose of reducing supply chain risk.

The interim rule does not address how or by whom the ''qualification standards'' are established or whether and by what means, if any, they are to be communicated to prospective contractors.[37] Second, the proposition that a rating may be ''acceptable'' (or not) implies that there will be a stated evaluation factor in an RFP and that such factor(s) will reasonably communicate what is to be assessed as sufficiency for ''supply chain risk'' management. There is no present standard that sets metrics, vis-à-vis cyber threats, for supply chain risk assessment or management, though there are analytic methods available to consider supply chain threat, vulnerability, consequence and countermeasures. Further, there are many potential practical problems in controlling the selection of prospective sources or in their prophylactic exclusion. The government advises its suppliers, by the consent provision at DFARS 252.239-7017(b), that it may consider ''information, public and non-public, including all-source intelligence, relating to an offeror and its supply chain.'' Unless DoD officials exercise their authority to release information that explains a decision, the higher tier supplier, whose inclusion of a suspect source may put its proposal or contract at risk, will have neither knowledge of nor access to these sources of information that cause the government to downgrade a proposal or reject a source.[38] In other cases, the contractor may not have the ability to timely identify or employ an alternative source, and the government may find that its own interests are prejudiced if it applies these sanctions against higher tier suppliers for sensitive equipment in situations where only one capable source is immediately available and where additional protective measures might suffice to achieve required confidence in device authenticity.

■ *Potentially Unfair Effects*. The interim rule implements Section 806 by enabling DoD to exclude a source for reasons of supply chain risk. And it has exceptional breadth, reaching companies who may have no idea that their products might find their way into the National Security Systems that are the focus of the rule. The promulgation comments cite six ''limiting provisions'' that exist before the government can exercise these authorities: (1) the authority is limited to NSS; (2) decisions can be made only by the head of a covered agency; (3) a joint recommendation must be received from senior DoD officials based on an intelligence risk assessment; (4) a written determination must be made that justifies the use of the authority as necessary and that there are no less intrusive measures available; (5) notice must be given to appropriate Congressional committees; and (6) the authority of Section 806 expires on September 30, 2018.[39]

All of these ''limiting provisions'' involve actions internal to the government and none call for disclosure to contractors or sources affected by use of the Section 806 authority. Essentially, these are ''surrogates'' for the processes that ordinarily involve suppliers in decisions that affect their eligibility for award or their choice of lower tier sources. Especially because standards are absent (see above), and because the contractor community is generally excluded from the intelligence-driven information that produces decisions about supply chain risk, the government will make decisions prejudicial to its contractors (and their sources) without giving them notice, opportunity to challenge, or other redress. And, inevitably, there is risk that these decisions will be wrong, however well intended. Contractors can suffer competitive and business injury by reason of decisions authorized by Section 806 and implemented by the interim rule. To those so affected, it is no consolation that the ''limiting provisions'' will reduce the incidence of use of these exclusionary authorities. Nor is it any relief that a few members of Congress will be informed of what happened, or why.

---

[36] *Id.* There is some illogic present in DoD's stated justification. As noted, the interim rule posits that a source may be excluded should it fail to meet ''qualification standards'' and if it fails to receive a suitable evaluation with regard to an ''evaluation factor providing for the consideration of supply chain risk.'' Unless DoD intends to make qualification and selection decisions on the basis of undisclosed standards and evaluation factors – a *very* dubious proposition, practically and legally – future RFPs will reveal the standards and evaluation factors, thus creating some exposure of special requirements for the subject solicitations.

[37] The comments accompanying the interim rule indicate that the rule ''does not require any specific reporting, recordkeeping or compliance requirements'' and that ''[t]his rule, by itself, does not require contractors to deploy additional supply chain risk protections.'' 48 Fed. Reg. 69269. These comments are somewhat disingenuous and they certainly ''beg the question'' of what DoD *does* expect of its vendors to avoid the sanctions that are authorized by the interim rule. This contradiction is elsewhere evident in the comments, which acknowledge at once that the rule does ''recognize the need for information technology contractors to implement appropriate safeguards and countermeasures to minimize supply chain risk'' while stating that it is ''up to the individual contractors to take the steps they think are necessary to maintain existing or otherwise required safeguards.'' *Id*.

[38] Both the statute and the regulation allow senior DoD officials to limit the disclosure of information, relating to the basis for carrying out of any of the supplier exclusion actions, ''in whole *or in part*.'' *Compare* Section 806(a)(2) *with* DFARS 239.7305(d) (emphasis added).

[39] 78 Fed. Reg. 69268-69.

The government can reduce the risk of unfairness by giving better information to its contractor community so that they can implement supply chain protection measures and improve assurance of item authenticity for procurements the government deems to be sensitive to supply chain risk. But more is needed. Initially, DoD should establish a mechanism for evaluating the sources of information and national security implications of each exclusion decision, and, where possible without compromise to intelligence methods, sources or results, share information. Second, DoD should work to develop a means to anticipate risky sources on procurements for systems ''covered'' by Section 806 and the interim rule so that, in many cases, DoD can give early advice to prospective contractors of lower tier sources perceived to have supply chain risk. Similarly, and especially where there is ambiguous or conflicting information as to the existence of supply chain risk, DoD should establish a way to involve the affected supplier and provide an opportunity to correct or rebut adverse information. DoD should also afford higher tier suppliers with as much advance notice, as is possible, of intended action under the Section 806 authority. It is in DoD's interest, in many cases, to extend to its suppliers an opportunity to respond to intended action – whether by providing assurance about the identified supply chain risk or identifying an alternative source. It has the authority to take these actions. Neither the statute nor the regulation *require* DoD to withhold from affected suppliers the information that explains actions taken to reduce supply chain risk; the decision to limit disclosure is clearly discretionary. The statute provides that the head of an agency that makes an exclusion decision ''may'' limit the disclosure of information related to carrying out the action.[40] Only if the head of a covered agency exercises this authority, to limit disclosure, do the prohibitions on protest remedy apply.[41] This implies that if an agency head elects not to exercise this authority, then information may be shared with affected contractors and a protest remedy would be available. Similar language is contained in the interim rule at DFARS 239.7305.

■ *Insufficient Transparency; Absence of Remedy*. When DoD decides to act under the authorities of Section 806, it is required (among other actions) to give notice to the congressional intelligence and defense committees. DFARS 239.7304(c)(1). The details of the notice are more extensive in the interim rule than are required by Section 806. The notice is to include six categories of information, including a determination that the anticipated cost will be fair and reasonable and a statement of actions that the agency will take to remove any barrier to future competition. DFARS 239.7304(c)(2)(i). Where an authorized official decides to limit the disclosure of information related to a supply chain exclusion action, no such action shall be subject to review in a bid protest before the GAO or a federal court. DFARS 239.7305(d).

That the interim rule requires disclosures to Congressional committees may serve to respect the public's interest in assuring that the powerful authority of Section 806 is not used to exclude sources erroneously and to give Congress confidence in the relationship between the cost and benefit of such decisions. However, again this approach suffers from insularity. DoD's contractors and their suppliers surely are stakeholders with an interest in knowing when they are at risk of exclusion or negative evaluation or loss of award due to supply chain risk. As noted above, both the statute and the interim rule confer to DoD the discretion to decide how much or how little (if any) to limit disclosure. When DoD fails to share what information it might have with the affected suppliers, it prevents its supply base from learning from that information. DoD also has reason to give its suppliers confidence that the authority of Section 806 will not be used unreasonably or arbitrarily. Should DoD suppliers find themselves at the receiving end of supply chain risk exclusions, some desirable members of the diverse and deep supply chain will elect not to participate in defense procurements. Not only will DoD suffer adverse cost consequences, it also could find itself unable to access the innovations in electronics and information technology that have proven vital to many government functions.

Conclusion. The federal government has good reason to protect critical systems against cyber threats that exploit supply chain vulnerabilities. Cyber attacks can be mounted through tainted, counterfeit electronic parts. Where such parts are used in NSS and other critical systems, the government has an interest and a duty to protect against supply chain risk that could compromise or disable such systems. Section 806 and related statutes give DoD and other federal agencies powerful authority to protect the supply chain against sources that present a supply chain risk. Hence, in the new interim rules that implement Section 806, DoD fulfills the requirements of Congress and gives itself the means to act where it is informed of and can avert such harm.

At the same time, the interim rule that implements Section 806 suffers from important limitations, ambiguities and contradictions. There is a fundamental absence of transparency and accountability that operate against the bona fide interests of contractors as stakeholders in the defense acquisition system. There is a risk of error and unfairness that presently are not bounded or checked by oversight or available remedies. To minimize or avert such harms, DoD should exercise the discretion it has, by statute and rule, to use selectively and prudently the powers it has to exclude sources that present supply chain risk. DoD should actively seek industry input, even though it has already issued the interim rule on an effective basis, and should be prepared to change the rule and adjust its implementation with the benefit of experience and industry views.

The threat that the interim rule seeks to address is one informed by national intelligence functions. Necessarily, these functions must remain private and this means that affected vendors will not be informed of intelligence sources and methods where they are impacted by the results. Every DoD contractor has some ability to assess its existing supply chain for source risk and to manage selection of sources to reduce future risk. What suppliers do not now have is access to information that already is available to the government, from open as well as classified sources. Nor do suppliers have the same knowledge as does the government to assess vulnerability to cyber and supply chain attack or the same understanding as to the consequences of

[40] Section 806(a)(2).
[41] *Id.* at § 806(d).

   ISSN 0014-9063

such an attack. The government should make it a high priority to coordinate its intelligence information and to create a mechanism to provide consultation and, where appropriate, give advance warning to suppliers of identified source risk and supply chain vulnerability.

The interim rule serves to protect the public from genuine threats, but the rule in operation also could prove disruptive and unfair to suppliers who may have no way to know of the threat that causes the government to act to their detriment or and no way to anticipate that their product will be incorporated into a NSS. In this sense, the new rules operate *ex post*, in that the government applies the various sanctions authorized by the interim rule upon its suppliers *after* the government identifies a risky source in a proposal received from the supplier. With good cause, suppliers are concerned about the costs and consequences of such action in connection with their eligibility for contracts, evaluation in a competitive setting, or ability to perform without unplanned and directed changes in their sources for critical components. An *ex ante* approach to the same threat seems plausible and preferred. If the government organizes and mobilizes its data resources, classified and open source, and uses data analytic techniques well known to be within its competence, it can provide a means to inform its suppliers of risk vectors and suspect sources earlier in the acquisition cycle, so that the stringent sanctions of the Section 806 rules will be exercised only rarely.