Bloomberg BNA

Federal Contracts Report™

DOD

An Appraisal of Select Provisions of the FY 2013 National Defense Authorization Act

BY ROBERT S. METZGER

On December 18, 2013, the Conference Report was released on the FY 2013 National Defense Authorization Act (''NDAA'' or ''Act'') (H.R. 4310). The Conference Report on the Act was passed by both the U.S. House of Representatives and the Senate and was signed into law by President Obama on January 3, 2013. The 2013 NDAA contains a number of provisions affecting the new campaign to reduce vulnerability to counterfeit electronic parts and to improve the nation's protections, especially for critical and ''trusted'' systems and networks, against tainted parts that might harbor malicious code.

The new measures follow by about one year the enactment of Section 818 of the FY 2012 defense authorization measure. Section 818 imposed new requirements, both on DOD and industry, intended to detect, avoid and, where possible, eliminate exposure to counterfeit parts. A year before, section 806 of the FY 2011 authorization measure included new authority to exclude particular sources of supply if they presented a supply chain risk for a narrow class of ''covered systems.''

Robert S. Metzger is a partner in the Washington, D.C. office of Rogers Joseph O'Donnell, P.C., a San Francisco-based law firm with 30 years commitment to public contracting matters. He can be reached at P.C.rmetzger@rjo.com

The 2013 NDAA contains three sections that concern these problems. **Section 807** supports DOD's ''Item Unique Identification (IUID) Initiative,'' which requires special markings to facilitate authentication and tracking of parts and other assets. **Section 833** provides a very limited ''safe harbor'' to DOD contractors who receive counterfeit or suspect counterfeit parts *from the government*. **Section 1603** requires the Secretary of Defense to develop a strategy for the ''national technology and industrial base to achieve objectives'' that include reducing the presence and risk of counterfeit parts.

The three provisions are not major changes in the law. But they reflect continuing Congressional attention to the subject areas of supply chain risk management and counterfeit parts prevention. They should motivate DOD to complete the pending tasks of producing DFARS rules to implement Section 818 and OFPP to complete FAR rules for such related purposes as improving reporting of counterfeit and other nonconforming supplies. This is because all three of the sections involve functions that already are being worked by DOD or are necessarily involved in the future Section 818 rules. Those rules were expected last Fall – but have yet to emerge.

There are several propositions behind these three provisions of the 2013 NDAA. One is the attention paid to ''technical means,'' specifically item-unique marking methodologies, to give prospective buyers and users improved means to detect potential counterfeits. A second is that contractors should not be responsible for the costs of replacement of counterfeit parts if the government itself was the source of those parts. A third is a broad concern that the U.S. may not be secure if it relies upon non-U.S. sources for key systems and electronic components. As is true of many other elements of the subject of supply chain risk management, the challenge is far more complex than is easily addressed through legislation. Specific technical marking methods have drawn objection from original-source device manufacturers who believe these are unnecessary, costly, unreliable and ineffective. The ''safe harbor'' for

contractors suffers from the present absence of any means or standard to approve an ''operational system'' to detect and avoid counterfeit parts, and industry at present is unable to know how DOD will qualify trusted distributors, brokers or other sources where needed parts are not available from OEMs or authorized distributors. A preference for U.S.-made electronics, even if limited to a handful of mission-critical systems, runs counter to a trend of many decades of the globalization of the supply chain and would impose risks and costs greatly disproportionate to the security benefit, where the same objectives may be achieved by less expensive or disruptive means.

Section 807: Item-Unique Identification Requirements. Section 807 expresses the ''sense of Congress'' supporting the use of special markings to facilitate authentication and tracking of parts. DFARS 252.211-7002, when employed, requires item-unique identifiers.

One of the key strategies to deal with the threat of counterfeit parts is to improve marking techniques so that purchasers or users can verify authenticity and to use techniques for item-unique marking that will be difficult for counterfeiters to mimic. Already, there is rulemaking underway on this subject. And, the Defense Logistics Agency (DLA) has launched a controversial initiative to require a specific marking technique for some key parts.

There is an open DFARS Case, 2011-D055 that includes action to update and enhance DOD's capability to track items with item unique identifiers (IUIDs) by type designation and is to clarify the use and requirements of the contract clause, at DFARS 252.211-7003, which requires unique identification for all delivered items for which the government's unit acquisition cost is $5,000 or more, and for other items designated by the government.[1] Section 807, by putting Congressional support to item-unique identification initiative, and by linking it to efforts by DOD to ''combat the growing problem of counterfeit parts in the military supply chain,'' should give new urgency to the pending IUID rulemaking effort and may lead to a new FAR or DFARS case.[2]

At the end of October, 2012, the Defense Logistics Agency (DLA) issued a controversial ''mandate'' that would require mission-critical devices sold to DOD to be marked with botanically-derived DNA-based materials unique to each supplier.[3] This was accomplished by Defense Logistics Acquisition Directive (DLAD) 52.211-9074, which applies only to procurements made by the DLA and initially addresses items falling within Federal Supply Class (FSC) 5962 which have been determined ''high risk items.'' FSC 5962 devices are high-reliability and mission-critical. The focus of the new DLA initiative on this class of parts reflects both their importance to the successful operation of electronic systems in which they are installed as well as a determination that these microcircuits are at high risk of counterfeiting. A goal is to improve the ability of prospective customers and users to authenticate parts without potentially expensive, disruptive or even destructive test methods.[4]

DLA's ''mandate'' requires authentication marking of new purchases of FSC 5692 microcircuits using only the DNA marking technology, ''SigNature® DNA,'' provided by one company, Applied DNA Sciences, or its licensees.[5] The selection of this method was justified on the basis of a DLA R&D program, conducted between November 2010 and April 2011, in which approximately 55,000 microcircuits were marked with the SigNature® DNA and successfully distinguished in detection and comparison tests.

Industry's reaction to required item-unique identifiers, generally, and to the DLA DNA-based initiative, specifically, has been muted but mixed. As a public policy proposition, it is difficult to argue against schemes to improve authentication and frustrate counterfeits that depend on special marking rules or even advanced scientific methods. Undoubtedly, there is an evidentiary basis supporting DLA's selection of the SigNature® DNA technology; even so, DLA has taken steps to demonstrate its willingness to consider alternative technological solutions to achieve authentication marking.[6]

But there are problems in practice and application that may not be fully understood by DLA, DOD or Congress – much less resolved to the satisfaction of industrial base participants. Opposition has been registered by the Semiconductor Industry Association (SIA), for what it describes as ''several practical, financial and most importantly legal reasons.''[7]

SIA's objections to DLA assert it will ''cost semiconductor manufacturers millions and millions of dollars'' to implement the DNA-based technology. There are transaction and process costs to administration and utilization of the parts identification methods, even before one considers the potential costs of applying the DNA-based markings that DLA now would require. The semiconductor industry has expressed concern about the

[1] As of the status report for Open DFARS Cases, dated December 21, 2012, the DARC Director has tasked the Contract Placement Committee to draft a final DFARS rule. The report on this effort now is due on January 9, 2013.

[2] ''National Defense Authorization Act for Fiscal Year 2013,'' Report of the Committee on Armed Services, House of Representatives, on H.R. 4310, 112th Cong., 2d Session, Rept. 112-479 (''NDAA 2103), at 197.

[3] *See''Defense Logistics Agency requires DNA marking to combat counterfeit parts,''* October 31, 2012, available at http://www.dla.mil/DLA_Media_Center/PressRelease/Pages/pressrelease1211271406.aspx.

[4] The initial ''mandate'' applies to just mission-critical FSC 5962 devices but the DLA announcement suggests an intention to apply IUID requirements more broadly, ''for other DLA products and equipment at risk of counterfeiting.'' Potentially, the DNA method of achieving IUIDs could be applied to the larger class of general ''board level'' semiconductors as encompassed within FSC 5691.

[5] Information about this company is available at: http://www.adnas.com/anti-counterfeiting-for-electronics-microchips.

[6] DLA issued a Request for Information on October 15, 2012, seeking ''information concerning existing techniques and technologies that provide the ability to mark items in a manner that authenticates the source of supply via an unalterable, untamperable means.'' *RFI for DNA Marking Technologies, Solicitation Number: RFI_DNA_01,* available at https://www.fbo.gov/index?s=opportunity&mode=form&id=8476fa11d4cfbf7b7019939e7a526d59&tab=core&_cview=0.

[7] *See* Letter dated November 15, 2012 from Semiconductor Industry Association to Defense Logistics Agency, available at http://www.siaonline.org/clientuploads/directory/DocumentSIA/Nov%2015%202012%20-%20Defense%20Logistics%20Agency%20Response%20from%20SIA%20FINAL.pdf (''SIA Letter'').

   ISSN 0014-9063

availability and cost of the required technologies, and has expressed doubts as to the reliability of the resulting information. Concern has been expressed about excess reliance upon a single company and its technology. Some doubts have been raised about potential, collateral but dysfunctional consequences to DNA marking, such as whether such markings could attract fungus, impact storage temperatures or produce outgassing.[8] Thus, there is less than unanimous agreement as to the scientific basis to ''mandate'' utilization of the specific DNA-based method DLA has chosen.

Some original component manufacturers (OCMs) believe the special identification measures are unnecessary, but costly, and argue that DLA needs no such requirements if it purchases all its requirements of electronic components from OCMs and their authorized distributors. They argue that DIA would avoid exposure to counterfeits if it restricts purchases to such ''trusted suppliers.''[9] Advocates of DNA marking, however, contend that the technique provides ''non-disruptive application up-stream'' and ''non-destructive authentication down-stream.''[10] DLA recognizes that implementing DNA marking will likely increase costs, and that the costs likely will be passed on to DLA during procurement, but it ''accepts that the additional costs are the result of the additional security needed to protect our warfighters from counterfeits.''[11]

A very great portion of the defense supply base, including trusted systems and sophisticated platforms, relies upon electronic component parts designed for commercial purposes and built by commercial suppliers. Commercial sources may refuse to adopt special and costly marking requirements, especially if there is no way for them to recover the additional costs that result. DOD could find that there are no affordable alternatives for some of the parts that are required. DOD may need to apply a cost-benefit analysis before broad implementation of IUID requirements, and specifically the use of DNA marking, beyond a narrow class of mission-critical microelectronics actually (rather than presumptively) at risk of counterfeiting.

Section 833: Narrow 'Safe Harbor' Provision. In Section 818, enacted a year ago, Congress required DOD to issue new DFARS regulations, by no later than September 26, 2012, to address counterfeit parts. Those regulations have not yet emerged.[12] Throughout 2012, many in industry have been very concerned that there could be serious cost impacts when companies encounter counterfeit parts (or suspect counterfeit parts) notwithstanding ''best efforts'' and counterfeit prevention plans and practices that conform to ''industry standards.'' Almost since the date of enactment of Section 818 in 2011, industry has sought a qualified ''safe harbor'' provision that would make allowable the costs of replacing some counterfeit parts and required rework or remedy.

The House version of the 2013 Defense Authorization measure contained a provision that – had it been adopted – would have made such costs *allowable* if the contractor had an operational system to detect and avoid counterfeit parts that DOD had reviewed and approved, if the parts in question had been procured ''from an approved source **or** provided as government-furnished property (GFP),'' and if the contractor had provided ''timely notice'' of the identification of a counterfeit or suspect part. (Emphasis added.)

As enacted, however, Section 833 of the Act will give only limited comfort to contractors hoping for a ''safe harbor.'' As reported by the Conference Committee, the 2013 measure omits critical language – ''from an approved source'' – that had been in the House version. Thus, the safe harbor is available **only** if the parts came from DOD as GFP – and the contractor had an operational and approved system and was timely in reporting. This sharply limits the application of the safe harbor, as higher tier contractors remain exposed to unallowable replacement and remediation expenses even when they purchase from an ''approved source.''

The value of Section 833 to contractors is therefore limited to the situation where the Gov't supplies the false part to the contractor. It would be manifestly unfair to assign cost responsibility to the contractor in this situation. Arguably, the same result is available under *existing* law as the usual rule is that where the government furnishes ''defective GFP'' to a contractor, the government is responsible for costs or delays caused by the defect.

Even so, Section 833 could be said to place the ''cart before the horse.'' There is neither a present system nor standard for DOD either to ''review'' or ''approve'' an ''operational system'' to detect and avoid counterfeit parts or suspect counterfeit parts. DOD has yet to issue regulations or guidance on the elements of such an ''operational system'' or to explain how a compliant system may differ depending on the placement of the particular supplier in the defense supply chain or the nature of its performance responsibilities. In addition, DOD has not yet shared guidance as to how a parts source will be ''approved'' for these purposes and it is not now known what entity will have responsibility for such approval. Nor is it known which existing or emerging industry standards will be considered, or adopted, to determine whether a source will be approved.

These are crucial uncertainties, considering the importance Congress has attached to use of secure sources to reduce the risk of counterfeits, and the financial sanction imposed by Section 818 where a covered contractor identifies a counterfeit part or suspect counterfeit part. Industry needs resolution to these questions and expects they will be addressed when DOD issues various regulations, now in later stages of development, to implement Section 818. Once the regulatory landscape is clarified, and as experience is gained, Congress should be encouraged to revisit the ''safe harbor'' con-

[8] *See* ''Semiconductor industry pushes back on unique parts requirement,'' Military & Aerospace Electronics, December 2012, available at www.militaryaerospace.com/.

[9] SIA Letter, at p.2.

[10] ''The New Federal anti-counterfeiting mandate for military electronics: what will it take to comply with Sec. 818,'' White Paper prepared by Applied DNA Sciences, available at *http://www.adnas.com/sites/default/files/downloads/applied_dna_sciences_white_paper_impact_of_ndaa_section_818_1.pdf*, at p. 11.

[11] ''DNA Marking FAQs,'' Defense Logistics Agency, Dec. 17, 2012, available at http://www.dla.mil/informationoperations/sirc/lists/news%20feed/customdispform.aspx?id=46.

[12] The pending DFARS Case No. 2012-D055 also includes an action (''Detection and Avoidance of Counterfeit Electronic Parts'') to implement portions of Section 818. The in-process rule would add definitions specific to counterfeit parts and define contractors' responsibilities and clarify the government's role. As of December 21, 2012, a draft proposed rule has been forwarded to the DAR editor for review.

cept in order to incentivize strong anti-counterfeit programs and good faith compliance. Section 818, unfortunately, is largely *prescriptive*, threatening punishment for noncompliance. Government and industry should work together to avoid and eliminate counterfeit parts – a common problem — rather than treat each other as adversaries. A harsh regulatory regime will drive up costs without proportionate benefits and risk alienation of needed elements of the industrial base.[13]

Section 1603: National Security Strategy. Section 1603 now requires the Secretary of Defense to develop a national security strategy for the national technology and industrial base that will, among other purposes, ensure that it is capable of achieving objectives that include the reduction, to the maximum extent practicable, of the presence of counterfeit parts in the supply chain and the risk associated with such parts.

Several sections of the Report of the House Armed Services Committee that accompanied the House version of the defense authorization measure, H.R. 4130, shed light on Congressional concerns that will influence future DOD actions.[14] The House Report directed DOD to assess the risks associated with obsolete or obsolescent electronic parts and to recommend measures ''incentivizing the industrial base to implement effective remedies'' and encouraged DOD ''to find ways to incentivize microelectronics manufacturers to supply components and provide system assembly within the United States.'' [15]

DOD already has taken a number of forward-looking actions to design and engineer new systems to avoid vulnerability to parts obsolescence. The ''Program Protection Plan'' (PPP) guidance has the purpose ''to help programs ensure that they adequately protect their technology, components, and information.''[16] The ''Diminishing Manufacturing Sources and Material Shortages (DMSMS)'' program is intended to deal with the loss or impending loss of the last known (or original) manufacturer or supplier of raw material, production parts or repair parts''.[17] The Defense Microelectronics Activity (DMEA) has several important responsibilities in supporting effective microelectronics technologies.[18] DMEA asserts it has special capabilities in dealing with the ongoing problem of parts obsolescence. In the new efforts to improve security of national security systems that rely on mission-critical electronic parts, DMEA's role is expanding both in function and importance. DMEA is responsible for the ''Trusted Foundry Program,'' by which it oversees secure design, fabrication and test services for a small but important category of mission-critical parts used for key ''Mission Assurance Category I'' systems where only trusted foundries are used for custom-designed ICs. [19] DMEA also has implemented a ''Trusted Supplier Accreditation Program'' (TSAP) and, in furtherance of Section 818, DMEA is working with other DOD elements to develop a ''Trusted Supplier List of Distributors.''[20]

On November 5, 2012, a new DOD Instruction, DODI No. 5200.44, was issued on the subject of ''Protection of Mission Critical Functions to achieve Trusted Systems and Networks.''[21] Its purpose is to minimize risk to mission capability due to vulnerabilities in system design or sabotage or subversion of mission-critical functions. It also serves to implement DOD's ''Trusted Systems & Networks'' (TSN) strategy, and it applies to all DOD information systems and weapons systems that are or include ''National Security Systems'' or ''Mission Assurance Category 1'' systems. It includes IUID requirements ''for national level traceability of critical components'' and, in applicable systems, directs the use of ''trusted suppliers'' accredited by DMEA, for custom products for a specific DOD military end use.

Conclusion. These various initiatives show that DOD already is well aware of the challenge posed to maintain and support old and obsolescent systems, and has methods in place to look to domestic, high security sources for critical parts for key systems. However,

[13] As noted in the text, the Senate version of the 2013 Defense Authorization contained no ''safe harbor'' language. However, the Senate Armed Services Committee was aware of the challenges and complexities of implementation of Section 8181. The Committee raised a number of questions for DOD to consider, and encouraged the Department to ''solicit the views of both independent experts and interested parties – including representatives of original equipment manufacturers, DOD prime contractors, and lower tier contractors in affected industries,'' as it works to address implementation issues. ''National Defense Authorization Act for Fiscal Year 2013,'' Report of the Committee on Armed Services, United States Senate, on S.3254, 112th Cong., 2d Session, Report. 112-73 (''Senate NDAA Report''), at 102. The rulemaking process affords DOD an opportunity to put proposed 818 implementation rules out for comment before putting them into effect, on an ''interim'' basis or otherwise.

[14] NDAA 2013, at 186-87.

[15] Concerns about U.S. dependence on foreign-sources for electronic systems were highlighted in October 2012, when the House Permanent Select Committee on Intelligence published a report suggesting the U.S. was at risk in using telecommunications equipment from certain large Chinese companies. *See* ''Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,'' October 8, 2012.

[16] The Memorandum of July 18, 2011, describing the PPP Outline & Guidance, is available at http://www.doncio.navy.mil/uploads/0113CCP28319.pdf.

[17] The DMSMS program is managed by the Defense Standardization Program Office. *See* http://www.dsp.dla.mil/app_uil/displayPage.aspx?action=content&accounttype=displayHTML&contentid=56. The DMSMS ''knowledge sharing portal'' is at https://acc.dau.mil/dmsms.

[18] DMEA's website is at http://www.dmea.osd.mil/home.html.

[19] *See* DoDI 8500.2. The Trusted Foundry Program was initiated in 2004 to ensure that mission-critical national defense systems have access to leading-edge microelectronic parts from secure, domestic sources. It is a joint DOD/NSA program, administered by NSA's Trusted Access Program Office. The Trusted Foundry Program website is at http://www.trustedfoundryprogram.org/. DMEA is responsible for the accreditation of suppliers in the Trusted Foundry Program. Its ''Trusted IC Supplier Accreditation Program'' is described at http://www.dmea.osd.mil/trustedic.html.

[20] The ''Trusted Supplier List of Distributors'' initiative is part of DOD's efforts to comply with Section 818(c)(3)(a) of the FY 2012 NDAA. This key feature of the law directs DOD suppliers, whenever possible, to acquire electronic parts from OEMs or authorized dealers. It authorizes, however, purchase of parts not in production or currently available from ''trusted suppliers.'' These may be independent distributors, brokers or companies that engage in contract manufacture or remanufacture. Industry is especially eager to see how DOD will determine ''trusted suppliers'' in these categories.

[21] DoDI 5200.44 is available at http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf.

   ISSN 0014-9063

many DOD systems have been in service for decades and their sustainment requires electronic parts long out of production and no longer available from any OEM, OCM or authorized distributor. There is no practical or affordable method to satisfy, from exclusively domestic sources, the entire demand for parts that are required to sustain fielded systems.[22]

For the ''industrial base'' to deal with the absence of necessary parts, contractors will have to use parts fabricated by non-U.S. sources or made originally by U.S. sources but now available only from foreign brokers or distributors. The answer will not be to erect barriers to foreign sources, or to require exclusively domestic sources (excepting certain situations for mission-critical, ''trusted systems and networks'' as dealt with by DoDI 5200.44). DOD suppliers now, and for several decades, have relied upon a *global*, *commercial* electronics industry for microelectronic parts. There are solutions to the risk of counterfeit parts that do not purport to ''turn back'' the clock to promote or rely upon an exclusively domestic industrial base for electronic devices. (Indeed, many prominent U.S.-based electronics companies are multinational and rely upon their own foreign affiliates or trusted foreign companies in their supply chain.) Even for critical infrastructure and national systems, there are responsible methods to verify the authenticity and integrity of systems and parts from foreign sources. Should U.S. policy tilt to buy electronics just from American sources, the necessary corollary of exclusion of foreign suppliers would be highly disruptive to international commerce generally and would be very difficult to reconcile with U.S. security initiatives that promote international industrial collaboration, such as is accomplished through multinational programs such as the F-35 Joint Strike Fighter.

Counterfeit parts are a serious problem, but the causes and solutions are complex. DOD is working on the new regulatory regime to enforce Section 818. Measures will include improved use of item-unique identification, as promoted by Section 807 of the FY 2103 NDAA. The combination of sanctions and standards, and improved contractor systems, as will follow from implementation of Section 818, will reduce the threat. Improved reporting and strengthened enforcement also will help. While Congress has decreed that the U.S. national security strategy should include measures to reduce, ''to the maximum extent practicable,'' the presence and risk of counterfeit parts, this can be accomplished without the costs and industrial base impact that would flow from an attempted resurrection of an exclusive U.S. supply base. The Senate Armed Services Committee, in its 2013 NDAA Report, recognized and emphasized the ''linkages'' between the ''Trusted Systems and Networks'' program, where DOD procures DOD-unique items for critical systems from specially certified suppliers, and the broader effort to combat counterfeit parts through increased reliance on ''trustworthy suppliers'' of microelectronic parts.[23] As DOD and the OFPP complete their drafting of rules on these complex, interrelated subjects, they should enable all stakeholders to comment on proposed regulations before they take effect.

[22] In theory, rather than purchase from foreign sources, fielded systems can be supported through re-manufacture of date-expired or used devices, contract manufacturing to original designs or legal surrogates, and/or design and development, and limited volume manufacture, of new replacement circuit cards, assemblies or whole systems. These alternatives are very expensive and take more time, for approval and execution, than may be available. Interestingly, the Senate Report on the 2013 NDAA expressed concern about both the cost and the time to develop DOD-specific fabrication capabilities for microelectronics that are obsolete and no longer produced by the commercial sector, but still needed to support weapon systems. Senate NDAA Report, at 102.

[23] Senate NDAA 2013 Report, at 102.