The new Federal anti-counterfeiting mandate for military electronics: what will it take to comply with Sec. 818?

The costs of counterfeiting vs. the costs of compliance

By Dr. James A. Hayward, Janice Meraglia, Mitchell Miller
Applied DNA Sciences, Inc.

Introduction

On December 31, 2011 the President signed into law a mandate for the electronics industry which will affect the business and personal lives of all of us. That mandate is embodied in Section 818 of the National Defense Authorization Act for Fiscal 2012, which aims to eliminate counterfeit electronics from the military supply chain. Some of the features of that law will come into effect very quickly - only months from now. And, although focused on the Department of Defense (DOD), in fact commercial product will be impacted since the commercial manufacturers also supply the military. What's more, according to a study by the research firm IHS iSupply, the law will also have direct impact on companies abroad, especially in Europe.

Section 818 will impact everything from the safety of medical devices to the quality and cost of chips in consumer electronics. Nothing short of the nature of the entire defense supply system and the contours of a leading U.S. industry are at stake.

At the moment you would not know this from reading the news and financial press, who were busy with other controversies in the law when it was passed. But in the EEE industries (Electrical, Electronic, and Electro-Mechanical), the din is deafening. Following a series of recent high-profile convictions of suppliers of counterfeit electronics to the military, and a dramatic hearing in November of 2011 before the Senate Armed Services Committee (SASC),[1] Section 818 has tossed the sector into intense activity and caused a great deal of concern.

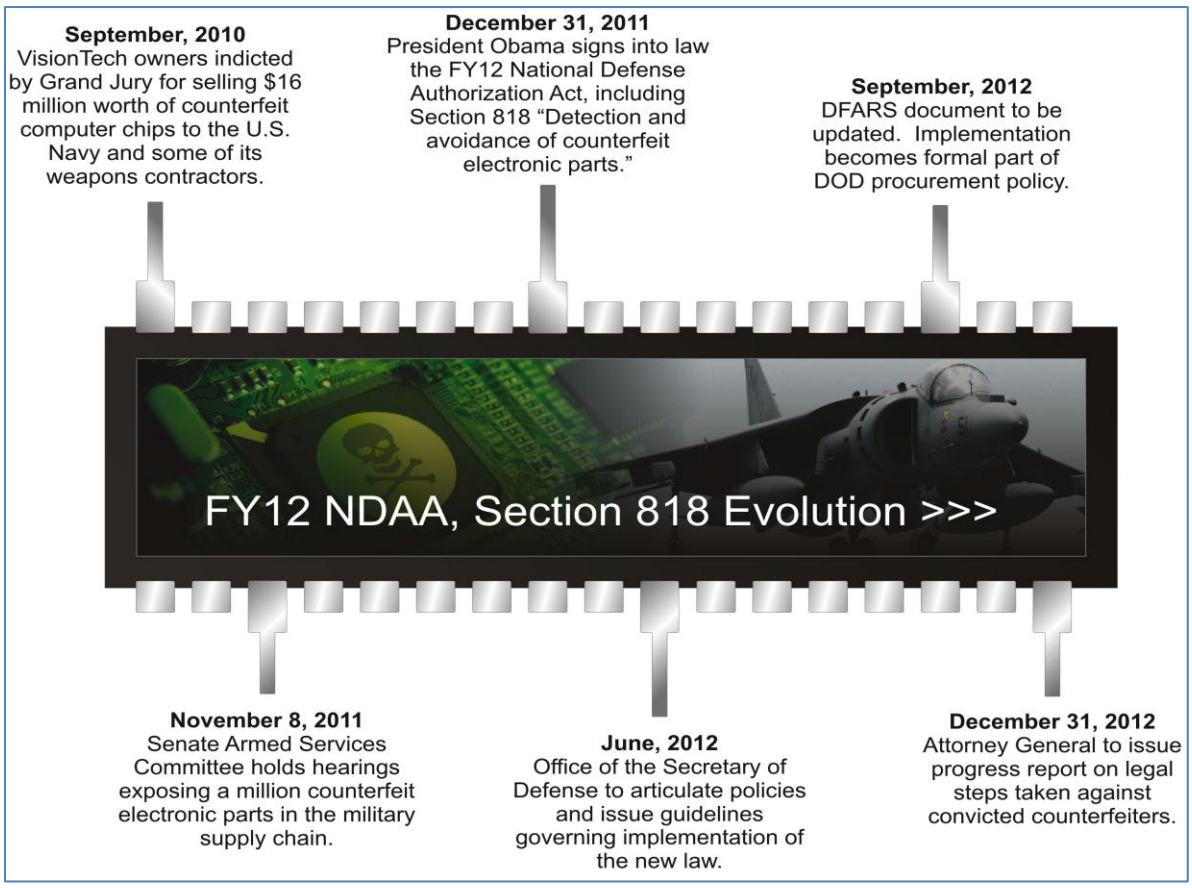
A February 21, 2012 public letter from the Council of Defense and Space Industry Association (CODSIA), while expressing support for "many positive steps" in Section 818, also underlines industry concern about the quickly approaching deadlines imposed by the law: "3 months is simply not enough time to fundamentally change the nature of the existing global supply chain for the defense industrial base."[2]

The letter's characterization is accurate: the fundamentals of the existing global supply chain for the defense industrial base are indeed in play. The new legislation is a watershed, especially for the U.S. industry—semiconductors-- which leads all others in exports (or all other industries but one, according to some sources).[3] How the industry responds to this challenge in the early stage, what actions it begins to plan and take now, will powerfully shape the practical effect of the new law.

Timeline

The law may be new, but the scope of the counterfeit problem has been evident since at least the middle of the last decade. Especially in the last two years, both government and industry have been actively tracking the crisis and developing options for response. Our own company is already in the midst of a eighteen-month project funded by the Defense Logistics Agency using our technology to authenticate microchips. As a result of all this, we believe that technology is poised for a quick ramp-up, plans for which can be in place before the three and sixth month milestones set out by the bill (Figure 1).

Figure 1 Timeline of the anti-counterfeiting mandate



In this paper, we highlight the main points of Section 818, and illustrate how we have reached this historic point where drastic changes have become necessary in a foundational industry. We will attempt to set out some parameters for understanding how the Section might impact the various players, and we will describe how our company's technology, DNA-based authentication, resolves key problems in response to the crisis.

Section 818: The Details

At its heart, NDAA Section 818 demands for the first time that defense contractors must establish policies and procedures to eliminate counterfeit electronics from their parts lists destined for the military. Contractors must "monitor and detect" counterfeits, or face rework and replacement charges, or legal remedies including suspension and debarment. And, we believe, the proven counterfeit supplier, accidental or not, will surely face the expectation of a better and proven form of parts authentication.

The legal language in Section 818 would change things drastically both for military suppliers and for the entire industry, globally, since the same fabs, clean rooms, assembly lines, and distribution centers are turning out both commercial and military-grade products. How exactly things will change is not yet determined. The law sets up milestones (to which the CODSIA letter alludes) in both June and September. By June, the OSD and Office of Homeland Security will "articulate policies," and issue guidance for remedial action. By roughly end of September, the government will revise the Federal Acquisition document known as DFARS (Defense Federal Acquisition Regulation Supplement) and the new age of industry compliance will officially begin.

Until Section 818 there has been no formal and comprehensive system of financial or legal accountability for monitoring, detecting, and eliminating counterfeit parts in the military supply chain. While important DOD programs have attempted to get at the roots of the crisis, such as the Trusted Foundries Program, and the GEM (Generalized Emulation of Semiconductors) program for the manufacture of post-production chips, there have been few financial or legal consequences for failure to eliminate inauthentic or "non-conforming" microchips and other electronic parts-- "escapes" in the trade. We do not mean to imply that there has been a failure to respond from industry or from the military. To the contrary, the flood of counterfeits has elicited a very significant response from the Defense Logistics Agency (DLA), from industry associations, and standards groups. But the law recognizes that the counterfeit crisis is systemic and ultimately cannot be addressed one piece at a time.

Section 818 is qualitatively new because it does in fact mandate a systematic response. It would:

1. Prohibit defense suppliers and their contractors and subcontractors from charging the DOD or Department of Homeland Security (DHS) for the cost of counterfeit parts included in their products, or for the cost of rework or corrective action required to remove and replace those counterfeit parts.

2. Require DOD and DOD suppliers to purchase electronic parts from original equipment manufacturers and their authorized distributors, or from trusted suppliers. Trusted suppliers must prove and document their compliance with established standards for detecting and avoiding counterfeit parts.

3. Establish requirements for notification, inspection, testing, and authentication of any electronic parts that are not available from such suppliers.

4. Require DOD officials and DOD contractors who become aware of counterfeit parts in the supply chain to provide written notification to the DOD Inspector General, the contracting officer, and the Government-Industry Data Exchange Program (GIDEP) or similar program designated by the Secretary of Defense.

5. Require the Secretary of Homeland Security to establish a program of enhanced inspection of electronic parts imported from any country that is determined by the Secretary of Defense to be a significant source of counterfeit parts in the DOD supply chain.

6. Require covered contractors that supply electronic parts or systems that contain electronic parts to establish policies and procedures to eliminate counterfeit electronic parts from the defense supply chain.

7. Require DOD to adopt policies and procedures for detecting and avoiding counterfeit parts in its own direct purchases, and for assessing and acting upon reports of counterfeit parts from DOD officials and DOD contractors.

8. Authorize the suspension and debarment of contractors who repeatedly fail to detect and avoid counterfeit parts or otherwise fail to exercise due diligence in the detection and avoidance of counterfeit parts.

9. Require DOD to establish Department-wide definitions of the terms "counterfeit electronic part" and "suspect counterfeit electronic part", which definitions shall include previously used parts represented as new.

10. Establishes new criminal actions against and penalties for those convicted of purveying counterfeit electronics to the military. Penalties would be as much as $2M for individuals, and $5M for companies.

These provisions will be fleshed out in synchrony with the two deadlines in June and September. By December 31, 2012, the one-year anniversary of the law, the Attorney General must make a full report on progress using the anti-counterfeiting legal weapons against counterfeit electronics and those unfortunate enough to have been their ultimate source of supply to our government.

Why Now?

The global tsunami of counterfeits in recent years, including in the vital EEE space, has been called a "perfect storm." The U.S. military has taken a direct hit. All of the conditions, which have conspired to create a new, efficient and global black market of counterfeit goods, contrive to amplify the damage. For the following assessment we owe much to the groundbreaking 2010 paper by Gary Shade and Bhanu Sood,[4] and to remarks by Dr. James A. Hayward, CEO and President of Applied DNA Sciences.[5]

First and foremost, the risk impact for products going to the military could scarcely be higher. Life and death are in the balance; granted the military shares this vulnerability with certain other industries also

afflicted with electronics counterfeiting. Today's armed services are vitally dependent on electronics for their normal, reliable functioning.

In what must appear to some as counter-intuitive, the military's vulnerability to counterfeits is exacerbated by the very robustness and high quality that typifies a mil-grade part. That is because for counterfeiters it is all too tempting to disguise a conventional part as mil-grade, grabbing the higher profit brought by the military part. The dangerously deceptive result is that such counterfeit parts can be functional and even pass some basic inspection hurdles, but are ready to fail in operational conditions.

Paradoxically, even as the U.S. military has come to depend on advanced electronics, it is today a minor buyer of electronic parts compared to commercial manufacturers. Only about 2% of the global production of microchips is procured by the Department of Defense.[6] So the power of the DOD to dictate to the electronics private sector through buying power has largely evaporated, despite the seminal influence once exerted by military expenditures in electronics and aerospace.[7]

A further issue is the product life for military parts, which can be far longer than is typical in commercial production. The B-52 bomber, first designed in the 1950s and used in Vietnam, is still in active service, for example. The need for spare parts is therefore also active even though those parts are often no longer manufactured in volume or at all. Contractors can be sometimes forced to reach out to distributors who have or claim to have stock in post-production parts, thus striking out into troubled waters where counterfeiters thrive.

The result is illustrated by a startling experiment in 2011, in which the General Accounting Office (GAO) issued, under the name of an imaginary OEM, open RFPs on the internet for electronic parts. All of the part numbers requested were either post-production or entirely fictional. At the time of publication of this memo, the GAO had received seven prototype parts in response to its RFP: *every single one was counterfeit.* (Needless to say, the rogue suppliers are no longer working with the DOD.)

Although not as pronounced as in the military supply chain, electronics product life is lengthening in the commercial sector also as the industry matures, as pointed out by Shade and Sood.[8] Production cycles wind down or conclude, but products live on and shortages result. Shade also observes that the severe economic crisis, which began in 2007-2008, resulted in reduced production volumes, further contributing to shortages.

Underlying all these trends has been the steady globalization of the economy. The electronics supply chain, globalized, has been engulfed by a multiplicity of legal and accounting systems, differing cultures and national interests, and a very high degree of complexity. It has become difficult to accurately monitor parts through such a complicated supply system, especially when not all participants are incented to exert controls.

One by-product of globalization has, by itself, created an opening for counterfeiters: the regular dumping of electronic refuse in third-world countries, especially after the European Union passed the globally influential Restriction of Hazardous Substances Directive (RoHS), and especially the related

Waste Electrical and Electronic Equipment Directive (WEEE Directive). [9] As has often been noted, the overseas dumping has ended in the deposit of millions of tons of discarded electronic components, raw materials gifted to the electronics counterfeiters right in their backyard, and they have taken advantage.[10]

We have today, in sum, a global supply system with far fewer checks and balances than existed in the more compartmentalized national economies of the past, an environment buffeted by recession and parts shortages, and preyed upon by an array of bad actors. Counterfeiting has grown from an opportunistic criminal activity, to an organized and global black market. In the EEE space, the military incurs all this risk, magnified several times, and pays, literally, a high price for it, or rather taxpayers pay the price. Section 818 is meant to drive some of this risk and cost back upstream to military suppliers, in the form of costs for increased controls and financial and legal penalties should those controls not be followed.

Impact: OEMs

Original Equipment Manufacturers (OEMs) and Prime Contractors will be directly affected by the new law. The penultimate node in the supply chain, the primes and their contractors and subs, are responsible for any counterfeits that they allow into their production environment. During the Senate Armed Service Committee (SASC) hearings last November, an aerospace manufacturer was placed under intense scrutiny for their failure to detect the presence of counterfeit electronic parts in the aircraft that was sold to the Defense Department.

The problem for OEMs is sharply drawn. On the one hand, there are already, without 818, spiking costs related to counterfeits, both explicit and hidden. On the other hand, the new legislation aggressively pushes the problem at the OEMs for quick resolution, since it mandates a strict time frame for response and sets the primes at the center of the action and accountability scenarios. There are immediate steps that might put them on the road to compliance, one of which, we believe, is DNA marking, which provides a form of traceability and strong authentication. But the primes need time to digest the new situation.

The explicit costs of counterfeits to the primes start, but only start, with loss of revenue, licensing fees, and royalties. There is in effect a nameless competitor, siphoning revenue and market share, all of which in semiconductors may come in at about 2% of TAM (Total Addressable Market) according to data assembled by Stradley[11]. In the over $300B semiconductor global market for 2011 this would amount to over $6B. [12] (see also Figure 2).

But for equipment manufacturers that is hardly the end of the story. As in all QC, the cost of fixing defects spikes sharply as a product moves toward and then into service. Stradley also casts light on this aspect of counterfeiting's financial damage, estimating the cost of remediation at ten times the product cost if found at board check, one hundred times cost if found at equipment final test, and a thousand times cost if found in service.[13] This is how a $20 part becomes a $20,000 problem.

Let us take this a step further. The analytics research firm IHS estimates that for any military parts list, a percentage of line items ranging from .5% to 5% can match suspicious entries in one of the industry's most widely used incident-tracking databases, the ERAI High-Risk Parts Database [14]. Since a parts list for a major program can extend to tens of thousands of line items, there is clearly potential for a great deal of $2000 problems.

In the SASC hearings last November, General Patrick O'Reilly testified that the Missile Defense Agency (MDA) incurred $2.74 M in costs for a single counterfeit incident in the mission computer of the THAAD interceptor missile. Eight hundred counterfeit parts were identified in this incident during which one of the mission computers was used in a flight test. [15]

One can see how remediation can generate skyrocketing costs for the manufacturer—both in remediation directly or in strengthening its detection and failure-analysis efforts.

Impact: OCMs

The Original Chip Manufacturers (OCMs) realize tangible and intangible, losses from counterfeiting, but they are clearly positioned differently from their customers, the primes, in relation to the new legislation.

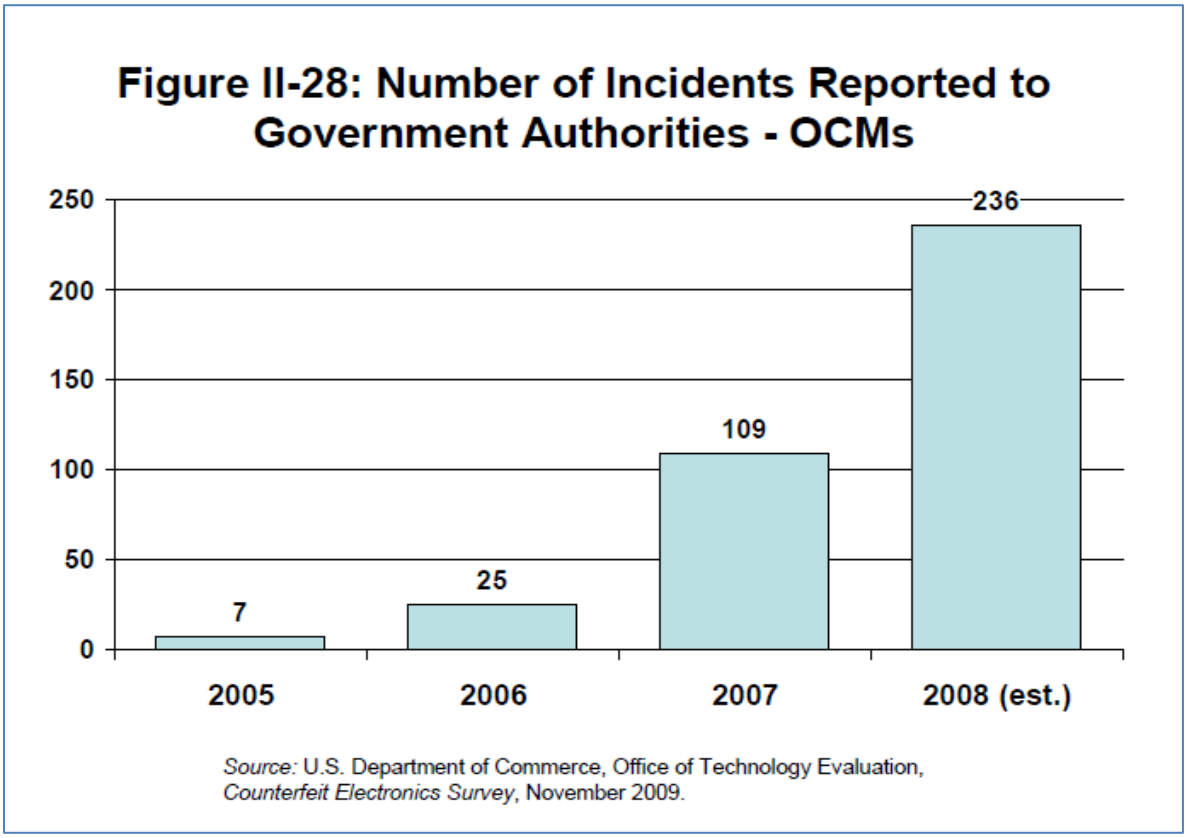
The OCMs confront the phantom competition of the counterfeiting black market, as do the primes. They, too, in effect, lose market share to this "competitor." In a business which counted annual sales at greater than $300 billion in 2011, this may not be so immediately evident. But its pernicious effect still plays out in a loss of revenue, jobs, brand reputation, and increased long-term volatility in margins.

OCMs also suffer the costs of control of shipments threatened by diversion, costs of other vendor controls and of returns.

But the chip manufacturers, being somewhat upstream, offer a reasonable solution: they urge their customers to buy only from trusted sources. And in a perfect world, there is sense to this. But we have seen how parts-shortages and long lead times, business cycles, and military supply particularities do nonetheless force buyers to go to independents, including to distributors whose reputation is unknown. Section 818 does directly address this as we have seen, but in order to work, any solution must be industry-wide and this only intensifies the pressure on the OCMs to be participants.

All this is to say that the OCMs are also in a bind, even if one that can seem to be masked by their own current

Figure 2 Number of Incidents Reported to Government Authorities



prosperity. True, with some exceptions, counterfeit semiconductors do not come through them. They certainly do not produce them. But the OCMs are nonetheless part of a larger manufacturing and supply system into which electronics counterfeits are infiltrating in very significant numbers. They are in fact suffering short-term losses and long-term risks. For any authentication program to work, such as those that will comply with Section 818, they must participate and be compensated accordingly, in flow from their customers.

Figure 2 Steady increase in Counterfeit Incidents reported to federal agencies between 2005 and 2008.

Impact: Distributors

Distributors are often divided into authorized distributors, who have a contractual relationship with an OCM or OEM, independent distributors who do not, and brokers, smaller companies often without on-hand inventory. (Figure 3). Because they serve so many needs for the other players-- sales, storage, marketing to name a few- and because they are very diverse, the channel is a natural target for

counterfeits entering the supply chain. As well, many distributors act at the behest of their customers to track down out-of-production parts.

The problem for the distributors overall is that their channel is perceived as being marred by the counterfeit problem, especially when independents are the focus. In the independent channel, a consistently high percentage of counterfeit incidents are reported: about 72-75% of total for each year during 2005-2009, according to a U.S. Department of Commerce study.[16]

This has unfairly tarnished the reputation of the vast majority of legitimate independents, and many have responded by implementing very rigorous testing and overall controls on their process.

Figure 3 Distribution Companies Encountering Counterfeit Electronics

Type of Company	Encountered Counterfeits	Did Not Encounter Counterfeits	Total
Authorized Distributor	10	35	**45**
Unauthorized Distributor	44	9	**53**
Total	**54**	**44**	**98**

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

But the matter doesn't end there. In the same study by the U.S. Department of Commerce, in a test group of 98 distributors, more than half reported they had encountered counterfeits in their channel (54). Strikingly, 10 of 45 or 22% of *authorized* distributors reported counterfeit incidents.[17]

While the total figures, outside of this study, for counterfeit incidents among authorized distributors is much lower, still the incident rate for the authorized sector doubled between 2005 and 2007, just before the economic crisis, and may still be growing at a comparable rate.

We can see then that authorized distributors are also the victim of counterfeit electronics and an unknowing participant in the proliferation of the problem. Despite their contractual and often exclusive rights with an OCM or OEM, there is opportunity for bad parts to enter this good supply chain via returns. If the distributor sells parts, it will typically accept returns, accompanied by supporting documentation. However, the paperwork does not typically account for co-mingling of product. This allows counterfeit product to be returned instead of, or along with, legitimate product and so enter the authorized channel. Since aggregate risk is a product of each sub-supplier's risk, the cumulative impact quickly snowballs out of control.

Another reason the authorized channel becomes polluted is the pull on an authorized distributor to act, paradoxically, as an unauthorized distributor to some degree, buying and selling parts outside of their authorized channel in order to meet customer needs.

In both of these scenarios, the lack of an industry-wide mechanism for authentication is sorely felt. A universal (and standardized) authentication system would allow the distribution channel to accept only legitimate product into inventory and thereby sell only authentic product to their customer base.

Impact: Failure Analysts

The Failure Analysis (FA) community confronts counterfeits in a way which is closely linked to the issues faced by the manufacturers, be they primes, OCMS, or distributors. Obviously, defect tracking and analysis has a central role to play even if we had a more perfect counterfeit-free world. However, FA specialists tell us that the wave of counterfeits has caused such a barrage of noise in recent years that distinguishing legitimate defects from the vagaries caused by dodgy counterfeits has become an enormous and expensive headache. The FA community desperately needs to be freed to do its real work, while instead it is tied up and inundated by counterfeits.

The situation is compounded by methodologies which often do not, or have not the tools, to authenticate a part at the front end of their process. If FA testing is destructive, it is then impossible to identify a counterfeit at the back end. Rich data is in this way lost, the FA process is slowed, costs escalate, and there is risk of loss in QC efficiency.

DNA Authentication marking

One of the solutions now being explored in an eighteen-month pilot by the Defense Logistics Agency (DLA), the supply arm of the DOD, is the application of DNA marking using technology from Applied DNA Sciences. The not-for-profit consultancy LMI is managing the project.

Applied DNA Sciences believes that DNA marking will confer compliance with Section 818 on all the major impacted players. Below, we aim to show how, in our view, the pilot has provided significant experience in identifying goals which a compliant company must reach in order to achieve compliance.

Figure 4 DNA Marking - Seamless in the Supply Chain

DNA marking represents both a traceability solution and a form of absolute authentication. SigNature DNA is a molecular mark, derived from botanical DNA, that embodies identifying data that may be scanned in real time or, sampled for a full forensic analysis. This mark has proven impossible to copy thanks to a combination of the sheer density of the content which nature provides and to processes developed by our company[18].

The utility of the DNA mark in the electronics supply chain is dependent on the point at which it is applied (Figure 5):

- During production, a chip manufacturer can apply its unique DNA to prove forensic authenticity further down stream in the supply chain. (Authenticity Mark)
- A mark might be applied by a test facility after a successful inspection process (Testing-Release Mark)
- The franchise distributor could place its mark on chips directly received from original manufacturers which would document the authorized channel (Source Verification Mark)
- An assembler or prime mark would represent their participation in the supply chain (Provenance Mark)

The following are goals that we believe any 818-compliant organization must meet:

Accountability

Section 818 flatly prohibits contractors from charging DOD for the cost of counterfeit parts included in their products, or for the cost of rework or corrective action required to remove and replace those counterfeit parts. If there is one critical operational requirement in the document this is it. *The primes and their designated trusted contractors and subcontractors are financially liable for remedial costs.*

To avoid this liability the primes must be able to prove authenticity of their deliverables, and must be able to document that proof. Since a DNA mark is portable it is in effect a traveling assurance of authenticity which proves and documents originality (or verifies test results) for the military as well as for the contractor. Thus, the system provides both traceability and forensic-level (uncopyable) authentication. We believe any solution needs to combine these two properties in order to confer compliance with the new law.

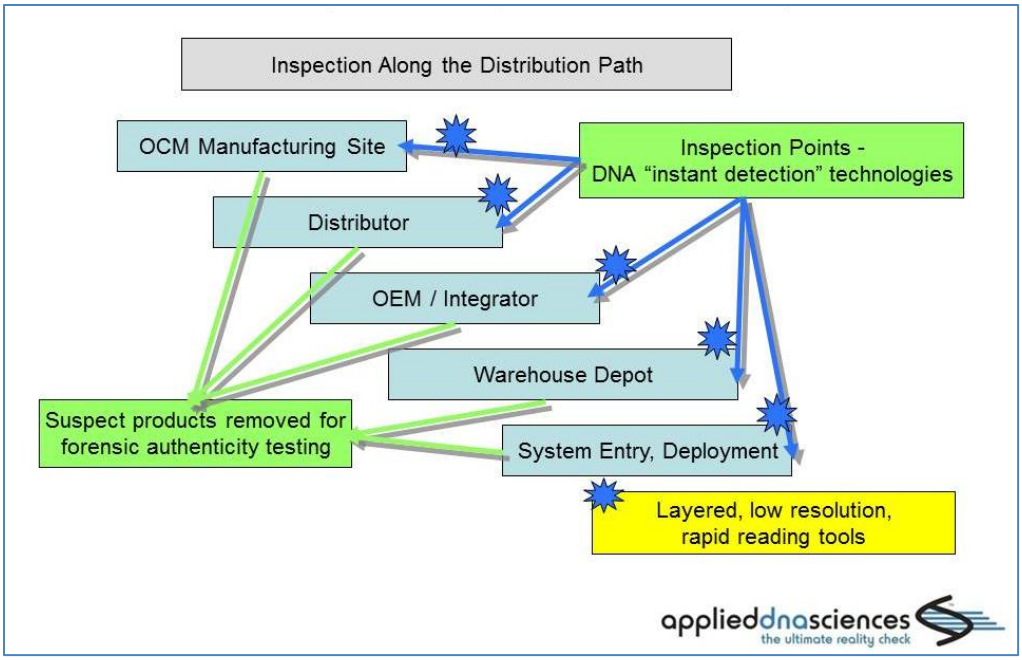
Seamless integration

Section 818 requires covered contractors that supply electronic parts or systems that contain electronic parts to establish policies and procedures to eliminate counterfeit electronic parts from the defense supply chain.

Given the tight time frame and the need to control costs, such systems must ramp up with little friction, with a minimum of change in the existing process map for contractors. DNA marking achieves this by supplying authentication options embedded within the existing manufacturing processes; it is not destructive, and it does not necessitate investment in sophisticated inspection systems. (Figure 4)

Any candidate, which aims to render compliance with 818, must similarly ramp quickly and remain cost effective. Our experience in full-scale chip manufacturing operations completed offshore, indicates that the time required to implement DNA-marking from start to full-scale, can be surprisingly compressed. Thus, it is fully possible to initiate a commercial-scale program even before the first Section 818 regulatory deadline in June.

Figure 5 DNA Marking - Site-Specific Functionality



Ease of adoption by federal agencies

Sec. 818 also requires action by the DOD and Department of Homeland Security (DHS). Specifically, it mandates that those agencies implement detection, assessment and action policies and procedures aimed at eliminating counterfeit escapes.

The SigNature DNA mark offers the agencies not only forensic authentication, but, in a best-practice implementation, easy access to a history of test results The history relies on systematic database entry of first level scanning data, while the system programmatically records a history of any forensic (second-level) testing.

SigNature DNA marking, with its simplicity and portability, offers Federal oversight agencies something any candidate technology must strive to deliver: a standard. From the DOD and DHS point of view, a patchwork of differing technologies, procedures, and data formats would blunt the intended effect. Only a set of standards offered by a universal system will support efficient and timely oversight.

Legal Protection

NDAA Section 818 is the law of the land. It authorizes suspension and debarment for contractors who repeatedly fail to detect and avoid counterfeit parts or otherwise fail to exercise due diligence.

DNA marking provides robust support in any audit, since it provides for scientific proof of authenticity with full reporting as part of a licensing agreement. This reporting can be the basis for quantitative analysis in the event a company is reviewed for compliance with legislation. At the forensic level, DNA identification is legally tested as a court-approved method of proving identity. In the same way that human DNA is used in court to verify identity of witnesses or suspects, the reporting data generated by botanical DNA authentication systems can legally document a pattern of compliance for auditors.

With draconian legal consequences, a contractor must adopt some system that easily delivers proven, systematic and incontrovertible authenticity data.

Conclusion

It is widely understood that the electronics industry, a foundation of U.S. economic growth, innovation, and national security, is facing a turning point. The immediate trigger in this historic moment is the language in National Defense Authorization Act for Fiscal Year 2012, Section 818. But the fundamentals of the crisis have been years in the making, and represent the intersection of economic and cultural forces which, in their combined effect, are only just now becoming clear. Even if the law fails to have its intended effect, the crisis itself will not go away. If ignored, the nation and the world will suffer the consequences.

The defense industry prime contractors, the entire semiconductor industry, and even the Department of Defense are, even as we write this, being forced to make sharply defined choices. Yes, there are costs to compliance with Section 818. In our view, they are far outweighed by the present and future costs of counterfeits in every part of the industry. It is not hyperbole to say that all parties will need to step up, to rise to the challenge for the greater economic and national good. The actions taken by all players now will determine much for many years ahead.

References

[1] The purpose of the Senate hearings were vividly described in the opening remarks by co-chair **Senator Carl Levin (D-Mich)**. Among his comments: "The failure of a single electronic part can leave a soldier, sailor, airman, or Marine vulnerable at the worst possible time. A flood of counterfeit electronic parts has made it a lot harder to have confidence that won't happen. Link

2 **Council of Defense and Space Industry Association (CODSIA),** Open Letter, "Subject: Implementation of Section 818, Detection and Avoidance of Counterfeit Electronic Parts, National Defense Authorization Act (NDAA) for Fiscal Year 2012, To: Mr. Richard T. Ginman, Director, Defense Procurement and Acquisition Policy, and Mr. Alan F. Estevez, Assistant Secretary for Logistics and Materiel Readiness (OUSD (AT&L))" February 21, 2012. Link

[3] **Brian Toohey, president, Semiconductor Industry Association**, "Semiconductor Industry Association, in "America's #1 export Industry Applauds Passage of Free Trade Agreements", October 13, 2011. Toohey states: "Semiconductors are America's top exporting industry …with three quarters of semiconductors being designed and manufactured here and 82 percent of our sales outside the U.S…" Link.

[4] **Gary F. Shade, Bhanu Sood**, "'The Perfect Storm.' Now appearing in FA Labs Everywhere." Monograph delivered to the International Symposium for Testing and Failure Analysis, (ISTFA) 2010. Link

[5] **Dr. James A Hayward,** President and CEO, Applied DNA Sciences, **"**DNA Marking and Authentication of Microchips" October 11, 2011, Link

[6] **Rochester Electronics White Paper**, "The Cost of Counterfeit Semiconductors to the Electronics Industry" Link

[7] Examples are the military and academic Advanced Research Projects Agency Network (ARPANET), the core network of a set that came to compose the global internet, and the rise of Silicon Valley as the semiconductor and then digital enterprise capital of the world, which owed its first great successes in large part to military and government contractual work.

[8] **Shade, Sood,** op. cit.

[9] So-called 'RoHS' laws have been passed world-wide, on the model of the EU legislation, including in the U.S.

[10] **Grow, Brian, Chi-Chu Tschang, Cliff Edwards, and D. Burnsed.** "Dangerous Fakes." Business Week 2 Oct. 2008: 1-8. Link

[11] **Jack Stradley**, Jack Stradley Consulting, "The Cost of Counterfeiting," p. 6., presentation delivered at Center for Advanced Life Cycle Engineering, Winter, 2012. See other data in this presentation useful for calculating costs of electronics counterfeiting to the industry, and implicitly the net financial and process gains which may be projected with implementation of industry-wide anti-counterfeiting measures. Unpublished.

[12] **IHS iSupply,** "Preliminary Worldwide Ranking of Top Twenty Suppliers of Semiconductors in 2011," Published Images, where the market total is given as $312.8B.

[13] **Stradley**, op. sit, p. 12

[14] **IHS iSupply Market Research Report,** "Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defense Industry and National Security," February 14, 2012. "A typical bill of materials (BOM) or parts list for a

military/defense program can have anywhere from a few hundred to over tens of thousands of purchased parts, of which between 0.5 to 5 percent typically match incidents of counterfeit parts reported to ERAI." Link.

[15] **U.S. Senate Committee on Armed Services,** "HEARING TO RECEIVE TESTIMONY ON THE COMMITTEE'S INVESTIGATION INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN, Testimony of General Patrick O'Reilly, Missile Defense Agency, November 8, 2011. The Terminal High Altitude Area Defense (THAAD) missile system was formerly the Theater High Altitude Area Defense, a United States Army system to intercept and destroy short, medium, and intermediate ballistic missiles.

[16] **U.S. Department of Commerce**, Office of Technology Evaluation, "Defense Industrial Base Assessment: Counterfeit Electronics," January, 2010, p.43 Link

[17] **U.S. Department of Commerce, Office of Technology Evaluation,** op.cit., p. 40

[18] As an indication of the incomparable storage density of DNA consider the complex architecture of humans contained within a single cell.