November 15, 2012

Defense Logistics Agency
8725 John J Kingman Road
Fort Belvoir, VA 22060
Land and Maritime DNA Feedback
DNAfeedback@dla.mil

Public Comments - DNA Authentication Marking on Items in FSC5962

This is the second letter from the Semiconductor Industry Association (SIA) in response to the Defense Logistics Agency (DLA) proposal to mandate use of the Applied DNA Science's marker on semiconductor products covered by FSC 5962 or for future reference other semiconductor classes such as FSC 5961.

This letter responds to the Request for Information for DNA Marking Technologies posted by DLA on October 15, 2012. The SIA appreciates this additional opportunity to review the proposed mandate and suggest alternatives that help better protect military systems and personnel.

SIA recommends against mandating the DNA Marking Technologies for original component manufacturers (OCMs) and their Authorized Distributors for current and future production of FSC5962 and FSC5961 products for several practical, financial and most importantly legal reasons detailed in the SIA Conclusions in this document. Instead, DLA and the Department of Defense (DoD) should work with the entire semiconductor industry, to leverage existing technologies, individual company R&D projects underway, and a multimillion dollar research and development project to select a more effective anti-counterfeit technology.

Since our last response (Attachment 1 to this document and incorporated by reference) our industry has been able to make a more detailed review of the proposed mandate and the technology behind the Applied DNA Sciences program. In addition, we have consulted with a number of SIA members that are leading an effort in Europe to review and implement the best anti-counterfeiting technologies, and create new industry-wide standards. The attached paper (*Semiconductor Industry Anti-Counterfeiting Project* – Attachment 2) describes this effort. The SIA would be willing to provide the government a detailed confidential briefing on the status of this effort and its impact on defense procurement. This effort is the culmination of a multi-year, government funded (€36 million/$45.8 million) project, with participation by semiconductor and related industries, as well as research institutes and universities, and is close to yielding significant results.

Before proceeding any further in selecting a specific technology, the SIA respectfully recommends that DLA review the progress made to date in this extensive examination of anti-counterfeiting technologies. While we appreciate the efforts DLA has made to examine a single company's technology, we believe that proceeding as proposed will actually do more harm than good. We are more convinced than ever that the DNA marking technology has a very limited

application and could create a false sense of security. It will cost semiconductor manufacturers millions and millions of dollars, which most likely would not be recouped from sales. Moreover, it places security for an entire industry on one company and technology.

Our team of industry experts and technologists contends that to make serious progress in anti-counterfeiting technology, DLA should start their work with experts from the industry in question versus starting with a vendor selling a technology to determine the best route to integrate technology into their products. Starting with a clear problem statement, our industry can help delineate technologies that make financial sense and that can be easily and appropriately integrated into our operations. Device manufacturers are the experts on chip design. Product security is a key component of every new product. All of our customers demand these protections. Therefore, products of every type have evolved quickly to respond to this market pressure. Defense contractors and DoD deserve more than a substandard, ineffective solution. They deserve to know the origin of their critical systems and components.

After a thorough review of the proposed DLA technology, assessment with various government contractors, and discussions with other OCMs, OCM Authorized Distributors, and members of the independent reseller community, we submit to DLA the following conclusions and recommendations:

Section 1. SIA Conclusions

1) The DNA technology mandate will not aid in stopping counterfeits from entering the government supply chain.
2) The OCMs and their Authorized Distributors do not need to use this technology/process because they do not produce or ship counterfeit products to government contractors or the government through direct sales.
3) SIA believes that with proper purchasing procedures, as specified in the National Defense Authorization Act for Fiscal 2012 (NDAA), DLA would only purchase semiconductors, when available, through OCMs or their established and contracted Authorized Distributors and Resellers. NASA and DoD have discussed classifications of "trusted" versus Authorized Distributors. To meet the NDAA requirements DoD is required to purchase in-production/in-stock semiconductors from OCMs and their Authorized Distributors and not "trusted sources." The NDAA's goal is to avoid acquisition of unreliable products that could endanger missions and people. If DLA follows the NDAA purchasing requirements, counterfeits of these parts would drop to virtually zero. As part of our research, using 2012 ERAI data, SIA found that approximately 40 percent of the identified counterfeit products in the ERAI database for this year were available for sale through OCMs or OCM Authorized Distribution, but had been purchased from other sources. Thus, by simply following the NDAA mandate, DoD could readily reduce acquisition of counterfeits by some 40 percent.
4) DoD/DLA should focus their efforts on identifying critical components and ensuring they are purchased from appropriate sources to avoid acquiring non-conforming products for critical applications. As Mr. Nicholas Torelli, Jr. (Director Mission Assurance, DoD Office of the Deputy Assistant Secretary of Defense for Systems

Engineering) stated, "counterfeits are only one subset of non-conforming parts such as parts with quality issues, incorrect materials, etc."

5) As noted in point 2 above, the OCMs and their Authorized Distributors do not need to use this technology/process because they sell genuine products directly to government contractors or the government. However, it cannot be emphasized enough that the DNA taggant, or any simple taggant technology, cannot guarantee the most important factor related to the purchase and use of semiconductors beyond authenticity – the parts must meet the performance and reliability required for the specified product. Many people do not recognize that an authentic part that has not been handled properly, subjected to electrostatic discharge, or that has been stored in the wrong conditions will most likely not perform properly or may fail under operational stress. After expensive and time-consuming testing, the DNA taggant will only identify the company[s] that applied the taggant (or that the taggant was faked to pass the field test). Accordingly, such a simple technology would only allow DoD/DLA to more easily identify the seller in some instances when parts are found to be counterfeit or non-conforming or have failed in the field causing injury, death or loss of expensive hardware and systems. Another critical failure is that the DNA markers will only have been applied by the last one or two companies that would have bought and sold the units to the government or a contractor. If the part had been in the market for many years, and handled by various companies, DLA would not be able to trace and identify the entire supply chain that handled the suspect part. Moreover, as set forth in Attachment 2, it is clear that there are better, more efficient, and less expensive technologies that accomplish more than simply identifying what entity might have applied the DNA.

6) If a technology that only identifies what entity marked the part were to be applied, it might be best utilized by requiring unauthorized distributors/resellers to use the selected markers on specific classes of products, such as FSC5962. DLA could therefore provide a new traceability for open market products; and, if contractors and the DoD segregate their inventory by seller and not by product category, it could make it easier to identify the source of questionable products. Despite this potential benefit of using such a marker for products from unauthorized sources, our experts believe there are far better methods than the proposed DNA plan to aid in identifying source and authenticity. The government should recognize that if the part is acquired from an unauthorized source, no marking technology devised will guarantee that the product had been properly handled, stored, and transported to avoid damage that could affect functionality and reliability.

7) SIA has serious concerns about relying on a sole source for the current program without competitive bidding for the product/service. We identified several of these problems in our attached letter. Two additional concerns are the lack of cost controls and the lack of industry-wide participation in establishing contractor/supplier requirements (i.e., delivery, quality, process/tool assurance, supplier business continuity plans, warranty, etc.). Initial reports are that just procuring the DNA material will be far more expensive than DLA anticipates. Moreover, the DNA plan would put our members in a position they would never accept in any vendor-manufacturer relationship. Semiconductor manufacturing is a complex and delicate

operation producing highly complex products which are sensitive to many environmental factors. (See the extensive testing summarized in the attached paper.) The semiconductor industry would never blindly accept changes in its production – which the DNA plan requires – without thorough testing, strict delivery requirements, quality controls, assurance that the product would perform as specified, alternative sources of supply, etc. Even though semiconductors sold to the DoD and its contractors represent a tiny fraction of overall sales, SIA members regard this as an important business segment. Therefore, to continue supplying this important market segment, DLA would put our members in a position of losing control over part of their own production.

8) From the information supplied by DNA to date, it is clear that compared to the effort summarized in Attachment 2, testing has been inadequate; for example, DLA documents state that the DNA will be infused into ink but do not mention how it will be applied where parts are only marked with laser etchers.

Section 2. SIA Inputs and Recommendations

1) We strongly recommend against adopting the purposed DNA plan and urge the government to consult with the semiconductor industry and its partners to develop a more comprehensive and effective anti-counterfeiting technology and to take advantage of the tens of millions of dollars already invested in the anti-counterfeiting R&D project in Europe.

2) Neither the OCMs, nor their Authorized Distributors, make or sell counterfeit products. Products purchased from those two sources, and segregated in secure DoD inventory, would eliminate the need for them to mark products. *Quixotically*, the increased cost for manufacturers of marking legitimate products and adding the licensed marker (which will be substantial) could drive more procurement to unauthorized sources. This does not even include the added cost of significant changes in production and/or handling (with attendant quality issues). This unnecessary step will add significant cost to the government and to the manufacturer, because all of the cost won't be covered by the government. If most of the cost cannot be passed on to the government it may result in a loss of suppliers available to the government and its contractors. In short, this move will further exacerbate DoD's counterfeit acquisition problem by further increasing the price advantage counterfeiters enjoy when targeting the DoD market and potentially reducing the number of legitimate suppliers.

3) Products purchased on the open market are at a much higher risk of being non-conforming or counterfeit/remarked parts. If the DLA intends to press ahead with a marking scheme, vendors of such parts could be required to use the DNA marking system or other marking system if applicable. This might enable DLA to determine what vendor sold the part, even if it did not provide information on reliability or product handling as noted in point 6 above. However, we recommend against selecting the DNA scheme; it would be far more cost, time, and security effective to leverage the five years of work already invested in finding the best solution.

4) As set forth in Attachment 2, for the last five years SIA International Associate Member Companies have been developing and testing technologies for our industry. SIA member companies would like to work cooperatively with DLA/DoD to review technologies in development and review solutions that satisfy the goal of identifying authentic products and using processes and tools that have been in testing for more than two years. As Mr Torelli stated recently (November 2nd, in Phoenix, AZ, at the SAE G19 Anti-Counterfeit Conference): "… solutions for DoD should be ***driven by industry*** and not mandated by government." (Emphasis supplied.) We heartily agree and look forward to discussing potential solutions further. Accordingly, we strongly recommend DoD postpone adopting any technology until it has received the confidential briefing and confidential materials offered in Attachment 2.

5) Finally, SIA would also recommend that DoD and the OCMs develop a multi-layered security acquisition system that takes into account some of the examples illustrated in Table 1 and the associated notes below.

SIA appreciates the opportunity to respond to the Defense Logistics Agency and is ready to discuss any of the key points in our conclusions or recommendations.

Respectfully submitted,

Andrew Olney
Chairman
Semiconductor Industry Association
Anti-Counterfeiting Task Force

Brian Toohey
President
Semiconductor Industry Association

Table 1. Planning for Appropriate Purchasing, Traceability and Inventory Control

	Mission or Life/Safety[1]	Critical Components[2]	Non-Critical Components[3]
Products No Longer Available In OCM Authorized Distribution			
Products Still In Production or OCM Authorized Distribution			
Future Products			

Critical for appropriate planning, design, purchasing, traceability and inventory control

More leeway in planning, proper categorization, and purchasing will alleviate issues

Less critical and there is time to properly plan the acquisitions

Note:

1. Mission critical or life/health/safety installations where the failure or partial/erratic failure could or would cause a catastrophic failure or incident.
2. Critical parts for which failure would cause a system, process, equipment to either fail or act inappropriately, but would also be part of a backup system or have a duplicate in the system for redundancy.
3. Non-critical parts that are not the cause of major system failures, but are part of the identified counterfeits in the DoD supply chain.

ATTACHMENT 1

VIA E-MAIL

Defense Logistics Agency
8725 John J Kingman Road
Fort Belvoir, VA 22060

Land and Maritime DNA Feedback
DNAfeedback@dla.mil

Re: Special Notice - DNA Authentication Marking on Items in FSC5962, August 3, 2012

Semiconductors are one of America's top export industries and a bellwether of the United States' economy. Semiconductor innovations form a foundation for America's 1.1 trillion dollar technology industry, affecting a U.S. workforce of nearly 6 million. The Semiconductor Industry Association (SIA) was founded in 1977 by five microelectronics pioneers and now unites over 60 companies that account for 80 percent of domestic semiconductor production. The SIA seeks to strengthen U.S. leadership of semiconductor design and manufacturing by working with Congress, the Administration, and other industry groups related to our sector. The SIA champions policies and regulations that fuel innovation, propel business, and stimulate competition, to better maintain a thriving domestic semiconductor industry. For more information on SIA, see http://www.sia-online.org.

The SIA Anti-Counterfeiting Task Force (ACTF) was formed in 2006 to support the SIA's efforts to eliminate the flow of counterfeit semiconductors into civilian and government supply chains. Since its inception, the ACTF has worked with many enforcement agencies, including prosecutors from the Department of Justice, military law enforcement (e.g., Naval Criminal Investigative Service), the Federal Bureau of Investigation, Customs and Border Protection, and Immigration and Customs Enforcement. The ACTF's participants have a wide range of experience in supporting anti-counterfeiting operations and have been a valuable part of nearly every successful government effort to interdict counterfeits and to prosecute those responsible.

SIA appreciates the opportunity to comment on the Special Notice issued by the Defense Logistics Agency (DLA) related to the mandatory use of Applied DNA Science's marker on semiconductor products covered by FSC 5962.[1] Thank you for considering our comments.

[1] The SIA is concerned with the issuance of this change to a Federal Supply Class as opposed to a proposed rule under the OFPP Act. The Office of Federal Procurement Policy (OFPP) Act, 41 U.S.C. § 1707(a)(1) provides, in pertinent part, that "a procurement policy, regulation, procedure, or form…may not take effect until 60 days after it is published for comment in the Federal Register….." Section (a)(2) states that such agency issuance "may take effect earlier than 60 days after the publication date when there are compelling circumstances for the earlier effective date, but the effective date may not be less than 30 days after the publication date." Subsection (d) authorizes agencies to waive this advance-notice requirement "if urgent and compelling circumstances make compliance with the requirements impracticable." Id. at § 1707(d). The current Special Notice does not indicate that it was ever published in the Federal Register or that any comment period was sought before the Interim change went into effect. While, as we note here, the SIA believes that counterfeit part risks are significant and of grave

I. Comments

1. Counterfeit semiconductors in supply chains threaten both national security and SIA member companies.

The ACTF's existence is evidence of the importance SIA's member companies place on addressing and stemming the problem of counterfeit semiconductors. We recognize that the existence of counterfeit components in military supply chains threatens the safety of the United States' soldiers, sailors, airmen, and marines and that counterfeit components in civilian supply chains threaten the operation of crucial equipment that protects our nation's first responders, manages life-saving and sustaining medical care and enables virtually all distance communications. We also face significant reputational and financial risk created by counterfeit semiconductors—a risk that increases costs and threatens our ability to support customers. The SIA actively works to eliminate these threats to our nation and our industry, and we support the DLA and the U.S. Government's efforts to address this problem. In this regard, the interests of the SIA and the U.S. Government are aligned.

2. Applied DNA's technology is not the appropriate cure for the counterfeit problem.

A. We believe Applied DNA's technology will not provide the security the DLA seeks.

Applied DNA markets its products as providing two types of authentication. A cursory authentication is performed by determining whether a DNA or other authentication marker is present on a suspected counterfeit article. We believe this type of authentication is easily circumvented because a counterfeiter need only mimic the material of the marker when counterfeiting a product. A more rigorous authentication is performed by confirming a sample of the DNA-doped material matches the correct DNA signature stored in the Applied DNA database. This rigorous authentication requires both a well-staffed laboratory to perform the confirmation and a secure database of the DNA signatures. We believe that rigorously authenticating marked devices will be very time consuming, particularly as the volume of semiconductors to be authenticated increases.[2] As of August 14, Applied DNA reported that 17

---

concern, SIA questions whether urgent and compelling circumstances exist for issuance of what in this situation amounts to an interim rule relating to the procurement of semiconductors. Our understanding is that there is no statutory deadline for implementation of this rule and there has been no opportunity for any affected or potentially affected parties, or the public, to review and comment on it. Further, as detailed below, we are under the impression that the proposed marking method has not yet completed testing and is not a generally accepted industry practice. Regardless how DLA classifies this Special Notice, SIA believes that, with rare exception, the better practice for making changes with such broad reaching implications is for agencies to provide the public with an opportunity to assess and comment on the proposed action before implementation.

[2] For example, each next-generation Joint Strike Fighter contains more than 3,500 integrated circuits. Senate Armed Services Committee, *Inquiry Into Counterfeit Electronic Parts In The Department of Defense Supply Chain* at 1 (May 21, 2012) (SASC Report).

of its 27 employees are engaged in "operations." Even assuming that all 17 operations employees are engaged in performing authentication services, it is highly unlikely that Applied DNA has the capacity to support the many, many requests for authentication that ought to result from implementation of this mandatory marking technology.[3] Therefore, rigorous authentication will be unavailable or not pursued by the DLA (eliminating any benefit to the DLA requirement in either case), or else Applied DNA will need to utilize third parties to perform the authentication (introducing significant risk to database security). In either event, the DLA goal of having a robust authentication tool is not met.

Additionally, we believe it is possible for a counterfeiter to transfer a marker that has been applied to an authentic device to a counterfeit one either physically or by cloning the marker. A sophisticated counterfeiter could sample a marker from an authentic device, clone the DNA from the marker and affix the cloned DNA to a counterfeit device. Mitigating these risks requires frequently changing the marker used by each manufacturer, quickly complicating the DNA database, increasing the cost of implementing the technology, and creating logistical issues, such as how to securely dispose of surplus marker material. Although changing the marker mitigates these risks, it does not eliminate them, limiting the usefulness of the technology.

The DLA's rule mandating use of only this Applied DNA technology would also leave control of authentication for a multi-billion dollar industry in the hands of only one source rather than multiple sources, violating a basic tenet of quality systems. (In addition, as stated above, it appears that this one source may lack the financial resources and operational capabilities to execute the requirements of this program. This concern raises additional vulnerability risks.) Doing so increases risk to quality, delivery performance, and potential for non-competitive pricing and unsatisfactory customer support. Sole-sourcing authentication technology also creates a single point of vulnerability, violating a basic tenet of security. Because the proposed DNA marker system will be the sole system used, once defeated or circumvented, the investment made by all participants in implementing the DNA marking scheme would then be wasted.

[3] We note that in its Quarterly Report on Form 10-Q filed in mid-August, Applied DNA's balance sheet showed assets of less than $2,000,000 and liabilities of over $650,000. We are concerned about Applied DNA's financial condition being able to support the authentication burden that could result from implementation of the DLA directive. Applied DNA states in the report's Liquidity and Capital Resources discussion in Management Discussion and Analysis that, "We have sufficient funds to conduct our operations until approximately November 2012. There can be no assurance that financing will be available in amounts or on terms acceptable to us, if at all. … [I]f … we are not successful in generating sufficient liquidity from operations or in raising sufficient capital resources on terms acceptable to us, this could have a material adverse effect on our business, results of operations liquidity and financial condition." Moreover, in addition to being concerned about Applied DNA having adequate financial capacity to support the increased authentication burden, we are also concerned about Applied DNA's capacity to purchase the equipment necessary to create the material needed to mark the billions of semiconductors manufactured each year.

B. Applied DNA's technology does not adequately authenticate counterfeit legacy semiconductor products.

Products no longer being produced (so-called "legacy" products) are a frequent target of counterfeiters. Indeed, a recent Congressional hearing and a Senate investigative report demonstrated that government procurement is particularly concerned with authenticating these types of products.[4] Use of Applied DNA's technology will not provide any near-term benefit for legacy product authentication. Problematically, DLA's own materials expect that distributors and brokers would be using Applied DNA's technology to mark existing inventory.[5] However, for the marking to provide the sought-after security, unauthorized dealers (independent distributors and brokers) must first ensure their inventory contains no counterfeit semiconductors. Current counterfeit identification methods employed by such unauthorized dealers (such as the Independent Distributors of Electronics Association (IDEA) standards) are only partially effective at identifying counterfeits. Some independent brokers, distributors, and third-party labs acknowledge that their success rate at identifying a counterfeit semiconductor is dependent on how poor the counterfeit is, how discernible any remarking may be, how much testing they perform, and is limited by those entities' lack of access to the original manufacturer's trade secret product identification information. Marking potentially counterfeit devices creates the dangerous illusion of security, defeating the DLA's desire to eliminate counterfeits from their supply chain.

C. We believe Applied DNA's technology has not been adequately tested.

Applied DNA's technology, despite marketing and other public statements, has not been independently reviewed and tested to adequately determine whether it can be applied and used to meet the needs of the Department of Defense (DoD). We are aware that Applied DNA has tested their technology in semiconductor manufacturing on a limited basis, but we are not aware of any testing at a broad-line semiconductor company that utilizes multiple, geographically distributed manufacturing facilities, creating thousands of different semiconductor products. Many of these products are manufactured in a multi-flow manner, requiring a product to move from site-to-site across the globe to complete numerous manufacturing and testing steps. Testing Applied DNA's technology at a company that manufactures a relatively small number of semiconductor products is wholly different than implementing the technology at a broad-line manufacturer because of the multitude of different manufacturing techniques and processes used in creating semiconductors of differing shapes, sizes, and complexities, packaged in various materials. Furthermore, semiconductor manufacturers employ different manufacturing processes to produce billions of semiconductors each year. There is no assurance that Applied DNA's technology will work in

[4] See Testimony of Lieutenant General Patrick J. O'Reilly, Director, Missile Defense Agency, before the Senate Armed Services Committee, Investigating Counterfeit Electronic Parts in the Department of Defense Supply Chain, November 8, 2011 at 7, available at http://armed-services.senate.gov/statemnt/2011/11%20November/OReilly%2011-08-11.pdf and SASC Report at 27-29.
[5] See Defense Logistics Agency, DNA Marking Feasibility Demonstration Phase 2 at slide 10 (June 2011).

each of these different processes. Moreover, overall semiconductor design may be impacted because of the uncertainty of the effect Applied DNA's chemicals will have on semiconductor functionality and reliability. Semiconductor manufacturing involves chemically intensive processes and highly advanced manufacturing techniques and controls. Semiconductors are produced in ultra-clean facilities and under strict controls, and introduction of the tiniest errant particle of dust or chemical could corrupt an entire batch of semiconductors. This is inconsistent with our industry's handling standards and ultimately endangers both functionality and the reputation of the original manufacturers.

Additionally, before being released to market, semiconductors undergo rigorous qualification testing to ensure they function properly. However, Applied DNA's technology has not been subjected to the broader semiconductor industry's standard reliability qualification and failure prevention tests. Because of the highly technical nature of semiconductor manufacturing, introducing a DNA marker could require requalification of products or increase failure rates. Given these uncertainties, manufacturers may also not be able to warranty or guarantee products that have been altered by their distributors with DNA markings. Until adequate testing has been completed to evaluate these concerns, introduction of Applied DNA's technology is inappropriate and potentially dangerous. Furthermore, the time required to adequately test and implement the marking technology will greatly exceed the modest 90-day allowance envisioned by the DLA's notification email.[6]

D. Implementing Applied DNA's markers will greatly increase semiconductor manufacturing costs.

If Applied DNA's process was to be implemented by semiconductor manufacturers for all of their products, they would be required to modify long-standing qualified manufacturing flows installed in existing billion-dollar facilities, at a cost of millions of dollars. So too, these modifications could trigger requalification requirements both of these manufacturing flows and the devices they produce. These modifications would significantly interrupt manufacturing and provide very limited or no benefit to manufacturers or their customers.

While it is difficult to accurately quantify the cost increase semiconductor manufacturers would have to bear, that increase is prohibitive for some products. The increase is difficult to quantify because, among other reasons, the SIA is not aware of a price list or any cost information for purchasing Applied DNA's marker or the equipment necessary to apply it. Regardless, because the price of some semiconductors can be as low as a fraction of a cent, imposing even a modest one-cent per-chip price increase is insupportable.

It is important to note that only a small portion of semiconductor manufacturers' commercial off-the-shelf production is purchased by government contractors. Less than 1% of the

[6] "However, within the next 90 days, we anticipate the [DNA marking] requirement spreading to all items within FSC 5962." email from Renee Frederick (DLA CIV Land and Maritime) (August 9, 2012).

semiconductor market is sold to the military, and only approximately one percent of that is sold directly by the manufacturer to the government.[7] Therefore, due to the costs involved, a manufacturer may choose not to implement the authentication process, denying government contractors access to that manufacturer's critical parts.

Any increase in semiconductor manufacturing costs should be justified by the benefit that results. In light of the security concerns raised, Applied DNA's technology does not provide this justifiable benefit.

E. Implementing Applied DNA's markers will create significant logistical issues for semiconductor manufacturers.

Most major semiconductor manufacturers laser etch part numbers and proprietary (and secret) production codes onto the surface of their products. The SIA is not aware that the DNA marker process has been successfully used in conjunction with laser etching. Published articles indicate the DNA marker has only been used in conjunction with ink marking,[8] which the industry no longer uses as extensively as it once did. Applied DNA has also confirmed to at least one SIA member company that its technology has not been tested with all semiconductor packaging materials. Therefore, there is no assurance the marking would work with all semiconductors.

Also, commercial products (by their very nature) are sold worldwide. Once one government requires an authentication system, such as the DNA marker, other countries might require use of either the same or a different authentication system. Use of a different system would duplicate all of the expenses manufacturers would be forced to bear in implementing the U.S. system, while if a foreign government was to require the DNA system, it may insist upon access to the DNA database, further eroding the system's security.

3. The SIA is committed to working with government to find an appropriate cure to the counterfeit problem.

A. Government should work with the semiconductor industry to find technical solutions

Semiconductor companies have tested the implementation of several different anti-counterfeiting technologies (e.g., ink, engraving/embossing, other DNA, powder, etc.). Each has different detection characteristics (e.g., optical, electrical, bio-chemical). We are pursuing other similar or more efficient technologies than that mandated by the Special Notice. For example, one method under development is more sophisticated and foolproof than the DNA marker because each chip generates its own unique, self-generated identifier. This identifier is not painted on like the DNA

[7] Electronics Industry Study Report: Semiconductors and Defense Electronics page 3, available at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA524792

[8] See, IEEE Spectrum, *Plant DNA vs. Counterfeit Chips*, available at http://spectrum.ieee.org/semiconductors/devices/plant-dna-vs-counterfeit-chips

marker but is intrinsic to the part and unalterable. More importantly the chip can self-authenticate—something a DNA marker cannot achieve.

While we do not object to DLA and DARPA *testing* the DNA marker, instead of establishing a new requirement through the Special Notice, we urge the DLA to issue a Request for Information seeking comments about *all* potential anti-counterfeiting solutions. DLA should then work with the industry and its technology experts to determine what solution adequately balances efficacy and expense. SIA stands ready to work with DLA in evaluating the various anti-counterfeiting solutions, but the goal should be to find solutions that work for both government and industry. Most especially, we should both help ensure that whatever technology is adopted, it does not inadvertently place DoD customers at risk. We believe that this effort can be completed expeditiously, and SIA is committed to doing its part to identify and implement a solution that can meet the needs of the industry and DoD customers.

B. The government should enact or revise purchasing and Customs regulations to help combat counterfeiters—this will help protect against counterfeit legacy semiconductor products entering DoD's supply chain.

As DoD and industry work cooperatively to identify and implement suitable solutions to address the problem of counterfeit semiconductor products, there are actions the Government can and should take now to help address this important issue.

Purchasing regulations

Because of government procurement practices, a significant percentage of semiconductors purchased through the government procurement channel are not purchased from manufacturers or their authorized distributors. Implementation of any authentication technology will have less effect than the government changing its purchasing and supply requirements, as required by Section 818(c)(3) of the National Defense Authorization Act for Fiscal 2012 ("NDAA"). If a product is critical to safety, health, life, infrastructure and or mission-critical applications, the product should be identified/classified properly and purchased appropriately from trusted sources, including manufacturers and their authorized distributors ("authorized sources"), trusted product flow from suppliers accredited through the Defense Microelectronics Activities' "Trusted IC Supplier Program," and, for out-of-production or "legacy" products, trusted suppliers as envisioned by the NDAA. Correctly purchased products should then be tracked in government inventory to ensure a chain of custody from the manufacturer to the government end user.

Implementing such a rule helps address another characteristic of counterfeit semiconductors—they are frequently damaged by tampering, refurbishing, remarking or improper storage. Non-authorized semiconductor distributors frequently store semiconductors improperly, without appropriate static protection and environmental controls. Therefore, while technological authentication might detect some counterfeits, it does not guarantee a semiconductor has been

handled in such a way that its quality is maintained. Semiconductor manufacturers contractually impose proper handling requirements on their authorized distributors, greatly reducing the risk to quality issues. If the purchase of semiconductors from manufacturers or authorized distributors is mandated, a government purchaser reaps this additional benefit.

Authenticating legacy products presents another set of challenges. Defining "trusted sources" for legacy products will require great effort to ensure that each trusted source can reliably find products that haven't been tampered with, remarked or otherwise damaged. A program that only procures legacy parts either from trusted suppliers that have demonstrated control over their purchasing supply chain, both as to genuine parts and as to handling of such parts (a program like the trusted supplier program in the NDAA) or from companies that are authorized by semiconductor manufacturers to sell the manufacturer's legacy products or to continue manufacturing legacy products will accomplish more than a DNA marker program to assure semiconductors in the military supply chain are genuine and function reliably. Purchasing from these sources is the single most effective method to prevent counterfeits from entering the supply chain.

Customs Regulation

Law enforcement limits the introduction of counterfeit legacy devices into supply chains, first at the border and then by prosecuting those that would sell counterfeit semiconductors into the military supply chain. Our industry is grateful that Congress recently increased the criminal penalties for trafficking counterfeits to the U.S. Armed Forces (Section 818(h) of the NDAA). Because the vast majority of counterfeit semiconductors enter the US from abroad,[9] the first line of defense is at the U.S. border. Moreover, border enforcement has a secondary salutary effect: identifying and prosecuting criminals in this country who sell counterfeits into the military supply chain.

We are hopeful that all government agencies will work together to protect life, health and safety, particularly that of our military personnel. Recently, the SIA requested an exception to a recent Customs rule to permit immediate disclosure to semiconductor manufacturers of information related to detained imports of semiconductors Customs Officers suspect may be counterfeit.

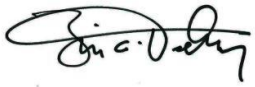
We believe strongly that granting this exception will accomplish more than any marking system to staunch the flow of counterfeit semiconductors into the military supply chain.

[9] See e.g., *United States of America v. Stephanie A. McCloskey*, Government's Consolidated Memorandum in Aid Of Sentencing and Motion for Downward Departure Pursuant to U.S.S.G. § 5K1.1. ("McCloskey") (Available at http://media.cmgdigital.com/shared/news/documents/2011/11/01/mccloskey_sentencing_memo.pdf.)

II. Conclusion

The SIA is dedicated to working diligently to fight the efforts of counterfeiters, the influx of their wares into supply chains, and the introduction of illicit goods into the American marketplace. Nevertheless, the Defense Logistics Agency proposed DNA marker solution will not solve current counterfeit, reliability, or performance problems faced in procurement. It significantly burdens manufacturers and does not reduce risks to people, systems and missions. The SIA ACTF recommends DLA withdraw the Special Notice and issue a Request for Information seeking industry assistance to review all options before establishing a firm requirement and to determine whether there is an anti-counterfeiting solution that is performance-proven and cost effective. We have proposed alternative solutions and look forward to a productive collaboration with government to determine which solution is best.

Respectfully submitted,



Andrew Olney
Chairman
Semiconductor Industry Association
Anti-Counterfeiting Task Force

Brian Toohey
President
Semiconductor Industry Association

ATTACHMENT 2

Semiconductor Industry Anti-Counterfeiting Project

As noted in the attached SIA comments, if the government is to select an ***effective*** anti-counterfeiting technology for semiconductors, it should work with the industry experts and the companies that fabricate semiconductors, as well as other key stakeholders in the manufacturing, distribution and sale of these products. Implementation of any new technology requires testing across many different manufacturing facilities and thousands of different semiconductor products. Indeed, over the past five years – one of SIA's International Associate Members– ST Microelectronics ("ST"), along with some 50 other organizations and companies, has been leading just such an effort. This includes many SIA and European Semiconductor Industry Association ("ESIA") members. This effort has been identifying and testing appropriate technological innovations with the goal of selecting the best technology to protect semiconductor products against counterfeiting. SIA is prepared to provide a detailed confidential briefing to the Department of Defense including the Defense Logistics Agency ("DoD") on the effort outlined below and work together to help provide information to define an effective anti-counterfeiting technology.

In addition to this European joint effort, other individual SIA member companies have established research efforts in secure computing, authentication and anti-counterfeiting which we believe merit further investigation. We believe incorporating the US semiconductor industry in this effort, along with the Department of Defense, will result in the adoption of far more effective guidelines and standards. It is our strongly held view that this will certainly be more effective than DLA simply adopting a solution that industry technologists believe to be weak; such as the DNA type taggant tracing technology.

Introduction to the EU Project

Five years ago, ST and 20 other potential providers of anti-counterfeiting technology began an evaluation of different product authentication concepts and initiated benchmarking of existing state-of-the-art counterfeit-proof technologies. The objective was to implement the most adaptable and appropriate ones into integrated circuit (IC) packages for additional extensive testing.
For the last two and a half years, ST has been leading the development and testing of those anti-counterfeiting technologies. The objective is to apply the best technology to IC packages. The effort is under the auspices of a European-funded research and development project with a budget of 36 million Euros ($45.8 million) and a consortium of 41 partners from nine European countries.

The consortium includes the largest European semiconductor companies (ST, Infineon Technologies, NXP Semiconductors, AMS (Austria Mikro Systeme), etc.), test equipment and process tool suppliers, end users (Siemens, Philips, EADS (European Aeronautic Defence and Space Company), etc.), and Europe's world leading research institutes (Interuniversity Microelectronics Centre, Fraunhofer-Gesellschaft, CEA-LETI/LITEN (Laboratory for Electronics & Information Technology and NanoChemistry and NanoSafety Laboratory, both at the French Atomic Energy Commission), TNO (Netherlands Organization for Applied Scientific Research), Austrian Institute of Technology, VTT (Technical Research Centre of Finland)), etc., and academic universities (Technology University of Delft, University College London, and University of Bologna). For obvious reasons, this effort has not been publicized. SIA is willing to provide the following information to DoD in this non-confidential proceeding.

The funded program tasked the consortium to:

- Define a comprehensive requirements specification to enable rapid and reliable semiconductor authentication and to assure compatibility with existing industrial fabrication and product specifications;
- Develop and adapt the counterfeit-proof technologies and tools for IC packages;
- Demonstrate the feasibility, test the reliability and failure modes on high volume IC production;
- Test the technologies in the application board environment;
- Test the technologies' resistance to copy, imitation and forgery as well as product authentication efficiency; and
- Provide guidelines and standards for the semiconductor industry to incorporate the technology into its mass production environment.

I. Semiconductor Industry Anti-Counterfeiting Criteria

A key analysis element was to establish criteria against which to measure potential solutions. Criteria were necessary to address existing counterfeiting scenarios, i.e., remarking and copying. At the same time the criteria needed to take into account maintaining high-quality volume production, safety, cost and semiconductor environmental constraints. Therefore, prior to deployment, any anti-counterfeiting technology ***must*** be tested and qualified to semiconductor industry-identified criteria for both effectiveness and efficiency.
The consortium broke down the criteria into six areas:

1. Principles of Authentication

These requirements specified the conditions of counterfeit identification as well as time to authenticate. This included measuring the detection time, false positives or negatives, and operating lifetime including maintaining functionality under a wide range of product operating conditions.

2. Resistance to Piracy

These requirements specified the technology's resistance to tampering, forgery, copying or imitation. This includes the technology itself, the process to apply it to the semiconductor, as well as the tools and procedures to read the technology.

3. Reading of the Authentication Target

These requirements specified the pass/fail information output. This applies to the required properties of the reader, including the need for automated reading, for example, in the production line, as well as manual reading, for example, in government supply depots.

4. Application to the Semiconductor Environment

These requirements specified conditions dictated by the many varieties among semiconductor products and the semiconductor production environments. It covers:

- Appearance of the tag;
- Area/volume available for tagging;
- Types of semiconductor packages included; and,
- Requirements with respect to safety and the production environment.

5. Impact on Component Specifications

These requirements related to device specifications and its intended application. The technology must:

- Not alter device performance;
- Work according to specifications under all device operating conditions;
- Pass all existing device reliability tests; and,
- Resist environmental/physical/chemical treatments common in electronics manufacturing and in the application of electronic equipment in its intended operational environment (automotive, industrial, medical, security, military, etc.).

6. Impact on Production

These requirements related to integration of the technology into the production line, including rapid automatic reading.

II. Types of Anti-Counterfeiting Technologies

After thorough investigation of available anti-counterfeiting methodologies, the consortium narrowed the field to 20 potential technologies usable in semiconductor production and worthy of further examination and testing.

The consortium's approach was to categorize potential anti-counterfeiting technologies according to the taggant's nature (e.g., ink, engraving/embossing, DNA, powder) and the characteristics of the read-out (e.g., optical, electrical, bio-chemical). Six logical categories emerged:

1. Encrypted Overt Tags;
2. Tags using Image Analysis;
3. Optical Tags;
4. DNA-like Tags;
5. Tags using Non-optical Material Properties; and,
6. Tagless Authentication.

The three-year European consortium project thoroughly tested the following types of anti-counterfeiting technologies in volume, which have shown very good results when measured against the above semiconductor industry-defined criteria:

1. Optical Tag – Nanotags

This tested technology consists of an invisible code created by the optical properties of engineered Nano-particles. The code can be read out as a complex fluorescence pattern and is decoded with a proprietary reader tool within seconds.

2. Optical Tag – IR Pigment

This tested technology consists of using a proprietary pigment that generates a special emission in the infrared (one or more wavelengths) under special excitation conditions. The IR signal fingerprint can be verified with a proprietary reader tool within seconds.

3. Tags using Non-optical Material Properties – Sub-molecular tag

This tested technology is based on a proprietary marking substance, in the form of micron-sized mineral powder. The taggant is manufactured in a proprietary process, to provide unique materials ("Fingerprint") families. Each unique Fingerprint taggant is assigned to a different manufacturer (possibly per product family). Authentication is based on sub-molecular magnetic resonance effects. The identification signal is emitted by the taggant in response to a specific excitation radio frequency signal transmitted by the specific detector (reader).

III. Next Steps

ST and its European partners are in the final stages of examining the best of available anti-counterfeiting technologies. As detailed in the main body of the response, SIA believes the DNA taggant to be an ineffective choice which will not aid anti-counterfeiting efforts; after careful examination the European consortium came to the same conclusion. DNA cannot indicate either authenticity or functionality; at best it can be used to trace legacy ICs back to the unauthorized source that supplied them.

SIA, including ST and its European SIA and ESIA partners, would be pleased to work closely with the DoD to review the results of the extensive European effort. The information should not, however, be made public, but would be provided on a confidential basis. It would not be prudent to share this detailed information with those that are counterfeiting our products. We believe that after such a detailed briefing, DoD and the semiconductor industry could establish a viable plan to select an ***effective*** anti-counterfeiting technology in the nea**r** term.

We understand the urgency of deploying an anti-counterfeiting technology in the semiconductor industry. Indeed, as you know, SIA and its members have been waging a constant battle against the proliferation of counterfeit chips. Accordingly, we feel the same urgency. However, urgency must be tempered by the fact that selecting the wrong technology could delay deployment of an effective anti-counterfeiting technology by years. Such a mistake would not serve the civilians and military personnel who depend upon incorporation of authentic ICs into devices they use in critical applications, nor would it serve DoD generally or the semiconductor industry.

We look forward to working with the DoD to protect our civilians and warfighters against counterfeit semiconductors.