[redacted]

Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products

Final Report

EXPERT WORKING GROUP COMMENTS BY

[redacted]

November 2017

[redacted]

I. GENERAL COMMENTS

A. Challenging Context

- The below comments take into consideration the multiple stakeholders and limitations faced by the Commission in its task to develop an EU wide solution for secure tracking and tracing of tobacco products in line with both the Tobacco Products Directive (TPD) as well as the FCTC Protocol on Illicit Trade. It must be noted that some inconsistencies between the two agreements have exacerbated this challenge. In particular, the references to the system that "obligations assigned to a Party shall not be performed by or delegated to the tobacco industry" poses a real risk that the current solution as designed may indeed comply with the language in the TPD but not of that of the Protocol. Furthermore, gaining consensus among 28 sovereign nations with varying positions related to tobacco control, customs and revenue paradigms and profiles related to the tobacco industry's activities (manufacturing/importing etc.) further exacerbate the challenges to craft regulations and corresponding system specifications that will work across the diverse member states.

B. Tobacco Industry Considerations

- Another key challenge which is often avoided is the fact that the tobacco industry itself has implemented its very own track and trace system known as Codentify to some degree1. It is unknown exactly what percentage of the tobacco industry's products are currently using Codentify and to what extent the system is active across the supply chain and includes the track and trace aspects as per the TPD (recording of supply chain events, aggregation etc.). Codentify and its main employees and directors have now been transferred to another entity known as Inexto and is branding itself as completely independent of the tobacco industry as a track and trace solution across multiple industries, although there is no publicly available evidence to support this claim. Many in the public health community have called out Inexto as an attempt to exploit a loophole in the Protocol. Although this author will not enter that debate as it is beyond the mandate of the role of external expert, I will comment on the fact that there are several elements in the current solution design that appear to be highly aligned to the tobacco industry's desired solution. A point to note is that during the original Feasibility Study there were multiple individual survey respondents that essentially submitted the same solution using the Codentify coding solution at the core. These were submitted by several manufacturers as well as system integrators (known to have been involved in the development and implementation of the system) as well as closely aligned security feature providers. It would be prudent to review these original survey results when determining whether an entity qualifies as an "independent third party" under the 3Rd party criteria to be established within the delegated acts.

- The premise of the TPD Article 15 and 16 which is based on the Article 8 of the Protocol is grounded on attempting to control an industry found time and again to be complicit in the proliferation of illicit trade. In fact, the industry as a whole can be considered serial offenders. Irrespective of the

[1] At the time of the Feasibility Study, Codentify had been implemented on <5% of total EU production lines within the EU. This was validated only after site visits to manufacturing facilities. However, in their survey response and from public sources (marketing materials, public statements and presentations at various public fora) this was dramatically exaggerated.

fact that the industry has made considerable efforts to promote itself as one of the key protagonists in the fight against illicit trade, the fact remains that incidents continue to arise (UK, South Africa, Kenya etc.). Thus, the very premise of a system for control is based on the concept of mistrust as opposed to trust. Any solution that relies on "trusting" an industry that is commercially/economically incentivized to circumvent controls is bound to fail. As articulated, during the Expert Workshop, the tobacco industry was never intended to be a "partner" with regard to implementation of Article 8 of the Protocol.

- From a governance and technical perspective, the solution should first and foremost be robust enough to prevent manipulation by the industry or other illicit traders as this is the very raison d'etre of the Protocol.

- Although the operational reality is that the solution should be minimally disruptive to industry, the current solution is in this expert's opinion far too accommodating and technically aligned to the industry's desired current operating paradigm. Further, the basis for evaluation of the various policy options (Annex I) and related methodology is in some cases unclear and in others appears to be skewed to the option that has been chosen (references) as justification for certain choices.

C. Technical Complexity of the Proposed Solution

- Considering the next step is implementation, the report unfortunately does not equip member states or the EC with the breadth and level of information required for a solution to be implemented. One of the fundamental requirements of a technical specification is that the designer, developer and builder of the intended solution should be clear about *what* needs to be delivered and *how* it should be delivered. Contrary to this end, the report presents too many questions and open-ended features that could be interpreted differently by the various competent authorities to provide a workable solution that will meet the original objectives of the EC. In some cases, the report is extremely specific (e.g., unique identifiers) and in other areas (e.g., anti-tampering, security features) much is left to question, functions and activities are vaguely defined or final specificity is left to the competent authorities. This is a recipe for a solution that will be cumbersome, difficult to manage amongst the 28 member states and has considerable potential to be compromised.

D. Utilization of 3rd Party's to Enable Controls and Provide System Integrity

- In terms of the current proposal there is no contractual relationship between the proposed third parties and the competent authorities whatsoever: in respect of the data management contracts, the installation of anti-tampering devices, the generation of security features or audit controls related to the overall system. Although the delegated acts (Article 36) of the Commission has defined criteria for "independence" it does not eliminate the risk of compromise of these critical functions. Indeed, this expert would speculate that many of the industry's longstanding business and commercial partners would meet the criteria set out. This would likely include suppliers of packaging materials, systems integrators (who have assisted in the development of the current industry track and trace solution), audit firms and others who are large enough to generate less than 20% turnover from the tobacco sector. The current provisions around assigning the

responsibility for contracting in respect of data storage, the installation of anti-tampering devices and the generation of security features to the manufacturers is cause for concern. It creates a (direct) primary relationship between the manufacturer and the various service providers, and relegates government to an observer to contracts that are intended to serve government's purposes. Ideally, one would want to establish a fiduciary and legally binding relationship between the service provider and government directly, so that there is a duty of care on the service provider, whose client should be government – not the industry that is being regulated.

- In the absence of such contracts there are a number of critical (and unnecessary) challenges. Most critically, it means government has little or no recourse against the third party from a contractual perspective, and cannot sue the third party for breach of contract, fraud or non-compliance in a civil suit. It also makes it more difficult for government to conduct its own due diligence checks on the third-party. It also leaves undefined the process for escalation of incidents and risks back to government, and essentially relies on the integrity of the manufacturer as well as the third-party who are in a legal and fiduciary relationship. How long will a 3rd party service provider be tolerated by the company who has hired it for reporting incidents? Conversely, should the third-party fail to provide its services in an acceptable manner (most of which have not been defined in the technical specification) will they effectively report the vendor to the competent authority? This is an industry with a serial track record of non-compliance and outright fraud. What evidence exists now that would allow the competent authorities to trust them? What sanctions will be enforceable by the competent authorities where the manufacturer or third-party service provider fails to escalate issues to the competent authorities. Furthermore, without being party to these contracts it is legally ambiguous as to how the competent authorities can intervene and adjust the terms of the contract – or cancel the contract for that matter. Finally, by not being a party to these contracts, it makes it more difficult to prevent and detect indirect corruption (i.e. liability for corruption through third parties with whom an organization has a business relationship, as defined in the UN Convention against Corruption and the OECD Anti-Bribery Convention.)

- This expert sees this as the single largest flaw in the current solution design and essentially does little to change the status quo. Indeed, commencing with the solution as designed, without addressing this fundamental flaw will result in a considerable waste of time and cost for all involved. It will also result in the creation of a system that provides a false sense of security – that would be virtually undetected if collusion occurred between the parties – under the guise of control. I regret the opinion that doing nothing would be better than implementing a solution in this manner.

- This can be addressed however by further strengthening the criteria for third-parties, removing the industry from the selection process of qualifying third-parties and by making the competent authorities a party to the respective contracts. The service rendered to and fees garnered from the industry could be paid directly to the 3rd parties via this contractual mechanism. This is commonplace where government establishes a concession, or assignment of government responsibility to such third parties but fees and services are provided to others. A concession agreement is essentially a negotiated contract between a company and a government that gives the company the right to operate a specific business within the government's jurisdiction, subject to certain conditions. For example, a concession agreement exists between the governments of

France and the United Kingdom and the private companies The Channel Tunnel Group Limited and France-Manche S.A. Such concession agreements exist across many sectors and referenceable benchmarks including port services, transportation, infrastructure, food service, prison management and many others.

- Such concessions could be based on several readily available and commonly used standards. The most obvious standard in terms of the activities of the envisaged third-party is: ISO/IEC 17021: Conformity assessment - Requirements for bodies providing audit and certification for management systems. This standard is part of a family of standards that provide clear definitions in relation to the functions and activities that would be required of a third-party that can ensure the level of system integrity that is required. ISO 17021 specifies requirements for bodies providing audit and certification of management and production systems. Observance of these requirements is intended to ensure that certification bodies providing system certification do so in a competent, consistent and impartial manner.

E. **Lack of Clear Guidelines and Specificity**

- There is a significant imbalance and potentially serious flaw in the direction that the report has taken, in that it has placed significant emphasis and provided considerable specificity in the tracking and tracing (T&T) elements of the solution but has not given equal attention to the security feature and other control aspects of the solution (e.g. audit, anti-tampering, enforcement, etc.)

- Since the former is based on the UID and the supply chain events that are associated with products which bare this mark it is indeed a critical component. However, without security the UID is worthless. UID's are not secure as they are subject to breach at multiple points in the supply chain (creation, transmission, storage, or even from being easily 'harvested' within the supply chain. Given the sheer volume (estimated 26 billion) the probability of detecting duplicate codes is statistically speaking highly improbable.

- Without the security provided by security features and the ability to authenticate the various layers of security features (overt, covert, forensic) the UID is just a number.

- There is little emphasis placed on the authentication of the codes and marks once entered into the market. No specifications are provided for authentication devices, policies or collaboration among member states.

- A review of existing tax stamps for example could provide a basis for selecting security features that meet the EC's criteria that are already common among the member states and a roadmap for further alignment could be developed. As suggested in prior comments, specificity should be provided in terms of defining a standard for security features where various internationally accepted standards exist (e.g. inter alia; ISO/IEC 12931, NASPO 2009, ISO 14298, CWA15374). The current approach of deferring the difficult decision of the types and specifications for the security feature to the competent authorities in the individual member states could result in a numerous and unmanageable array of features being deployed amongst the member states.

II. SPECIFIC COMMENTS

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
I. Governance Model	Weak	1. From a governance and technical perspective, the solution should first and foremost be robust enough to prevent manipulation by the industry or other illicit traders as this is the very raison d'etre of the Protocol. The Governance, model although characterized as "mixed" is heavily reliant on industry provided, controlled or directly subcontracted services. 2. Most of the solution components are either under the direct control of the manufacturers/importers or indirectly through contracts with "3rd parties" this model largely relies on contractual relationship (and corresponding fiduciary relationship) between the industry and these multiple "third" parties. There is a high risk of collusion. 3. Criteria or standards for approval of third-party services has not been defined. 4. Governance model is not clearly defined in several key areas e.g., generation, printing and scanning of the data	1. The Governance model is described as mixed; however, all contractual relationships lie between the industry and various service providers or third parties. This does not comport with the concept of control. 2. Third parties are responsible for generating UIDs, installing and maintaining anti-tampering devices, supplying security features, auditing, etc. These functions although can be paid for by industry should legally be bound to the competent authorities (see comments on third	Annex I the overall ranking of the A3 Mixed Model are questionable vis-à-vis the criteria stated and in some cases, are very subjective based on unknown evaluation scoring e.g., 1-1, 1-2, 2-1 to name a few. Main Report 4.2.1 "the industry may perform the scanning/verification" …. but a third party **may** be asked to install anti-tampering devices..."

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		carriers will all be provided by a sub-contractor to the industry. A model contract for data storage providers has been defined but no such similar contracts or specificity has been defined between manufacturers/importers and the various "3rd party" services provides as envisaged by the solution. 5. Several critical decisions are left to the competent authorities and this may contribute to a high degree of inconsistency of the system between and amongst member states. On the other hand, this also plays into the industry's hand as they will use their considerable lobbying resources to further shape the solution in these vague areas, focusing on the member states with manufacturing.	parties) and NOT industry. 3. The industry can and should be responsible for certain components of the system and this is a necessity: printing/affixing or other method with respect to UIDs and security features. The capturing of supply chain events and other reporting requirements.	
I. UID Generation UID Security	Strong Weak	1. The structure of the UID is sound albeit a bit long in terms of characters but the methodology around creating the progressive creation of the UID is sound. 2. No criteria for approval of entities eligible to receive UID's has been defined.	1. Generation of UIDs should be legally and contractually under the control of the competent authorities. 2. Explore links with EC systems that control excise manufacturing and movement and authorizing parties to	Annex II §1.2

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		3. No vetting criteria has been defined for would be registrants e.g., company registration, names of directors, importer I.D., physical premises inspection, criminal record etc. 4. It is not clear if information or a master register of registrants will be shared and vetted among the Member States. This could prevent potential abuse or fraud in the registration of those entities eligible to receive UID's and the fact that there the potential for 28 such issuers, this risk is compounded thus increasing the importance of communication amongst the UID generators. 5. The cost of UID generation Euro 11.154 million seems excessive considering the function that is being performed is a technologically rudimentary algorithm. 6. Allowing for the potential of 28 different entities to generate UID's is also potentially a wasteful and duplicative effort but also increases risk as up to 28 entities will need to be monitored for potential data breaches or even internal conspiracies where codes can be compromised (see	engage in complimentary activities. For example, if excise producers or importers are required to register with Customs or the EMTC system, that information could be used as a vetting element.	

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		comments related to anti-tampering devices). 7. As discussed in the prior expert meeting "clones" of legitimate product could be introduced into the market simply by having access to the production or distribution environments and harvesting codes and somehow acquiring the yet to be determined security features. Commercially available security features currently in use by the tobacco industry as well as those that are difficult or even impossible to account for (e.g., digital fingerprinting, tagants in packaging) significantly amplify this risk. 8. The inclusion of the UID generator as a 'role' or 'entity' has been created around what is essentially a technological component (computer, algorithm, storage and communications). This role is even intended to be revenue generating when in fact it does not have to be. This is exacerbated by the fact that each member state could appoint independent UID generators with no categorical specifications governing how they should operate. This will		

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		create an EU wide integration and enforcement complexity that is unnecessary. If this course of action is pursued, then at the very least the UID generator should be appointed as well as contracted by the competent authorities. 9. The communications channel within which UID's communicate to manufacturers and supply chain actors will need to be done via secure encrypted channels. 10. Since primary information is required at the time of a code request, this place a significant "real time" dependence on the generation of UID's. It is unclear if this approach has been tested and it what is the fallback should this function go offline. This could result in production down time for manufacturers/importers. 11. The increased emphasis and prominence of the UID generator is premised on the fact that the UID forms part of the security of the track and trace solution when in fact it does not have to. The UID's primary function is as a track and trace enabler. The security features that accompany (some of		

[redacted]

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		which can be integrated into the UID) is what should ensure reliability and integrity of the solution.		
Printing/Affixing		1. This function resides solely in the hands of the industry with no intended monitoring or control other than the anti-tampering step, which itself is under the contractual control of industry and not clearly defined in terms of functionality or definition of controls. In-keeping with the spirit of the report, (and approach in general) there seems to be very little –if any- intended control of the production environment. Once again, under the guise of 'limited intervention' this appears to be highly consistent with the existing industry developed systems. 2. The report has chosen to adopt the loosely interpreted and less secure meaning of the word 'affixed'. This is has created an ambiguity with respect to the security features as no guiding specifications have been defined. As mentioned in prior comments it is rated and weighted in the Analysis of Policy Options Annex I but without a clear definition of what "mixed" means it is arbitrary.	1. The current trust based approach of the solution needs to be revisited. Many of the controls are based on the assumption that the industry are partners and not potentially complicit in the fraudulent activities. 2. Clarify the TPD position of affixed which has been liberally interpreted. This would not only provide clear direction for the solution and report but will also avoid ambiguity at the implementation level. 3. Specify strict technical and procedural controls of transmission between	

[redacted]

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		3. The link between the UID and printing/affixing function has not been clearly defined. This poses a risk as it is an opportunity for compromising the UID's that have been provided unless there is a closely coupled 'monitored' link between the UID and the printing solution.	the UID generator and the printing solution of the manufacturer to avoid potential interception or appropriation of the transmission and legitimate UID's. 4. it is suggested that encryption is used between UID generator that can only be decrypted by the printer software with no outside intervention ensuring a closed-loop secure transmission.	
Scanning/Verification				
Anti-Tampering	Weak	1. The definition of the "anti-tampering" devices is vague and in some cases inconsistent within and is not a technical specification. It is unclear as to what specifically is meant by this critical function. Is it CCTV, image production control, production counters, intrusion detection? Some, or all of the above?[2] Without further	1. Providers of anti-tampering devices and related services should be the responsible party (and not simply the informed party) for the scanning and verification of the	Final Report §5.1.5 Annex II §1.4.2 RACI Matrix

[2] Final report p72-76

[redacted]

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		definition this provides nothing more than an implied sense of security. 2. The anti-tampering devices to be supplied and installed by third parties implies that the device will be operated by manufacturers and importers. The exact role and functionalities of these "devices" is also vague and in some cases contradictory – from "identifying all potential methods of unauthorized access into a product, package or system to limiting access to products or systems of interest, making tampering more time consuming, and features to indicate the existence of tampering". Some of these appear to be real time whilst others appear to be after the fact. 3. Furthermore, the RACI Matrix in Annex II clearly defines the role of the "third party" anti-tampering devices as "informed" and not responsible. Since the anti-tampering function forms the very basis for trusting the prior steps performed by industry this cannot in any way be characterized as a 3rd party control. 4. The current technical specification uses terminology such as "necessary checks"	codes. Indeed, the concept of "code activation" may also be added as an additional integrity measure and could dramatically simplify the entire UID process (see above). 2. For this critical function, clear business requirements with respect to the functioning of the devices, *inter alia* technical specifications, software requirements, performance criteria (e.g., line speeds) should be clearly defined. 3. For this to be a true third party control the anti-tampering devices and related service providers	

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		otherwise this is not a technical specification. 5. Detect disconnection from power or connectivity to the network and should have battery backup if they are disconnected from power.	MUST be the responsible party. Standard Operating Procedures (SOPs), Service Level Agreements (SLA's) and tolerances can be put in place to ensure there any disruptions to production can be dealt with. *4.* Since the anti-tampering device/mechanism is touted as the means upon which the preceding steps – all of which are informed by the industry –e.g., printing, scanning, verification clear guidelines should be put in place to govern the selection of the anti-tampering device and its operators.. 5. Anti-tampering devices shall report to the repository, in near real time, the	

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
			following information for each tobacco pack: • The UID • Date and time of scanning • The manufacturing facility, machine where they are located 6. Anti-tampering devices should be able to identify non-compliant cigarette packs, e.g. which do not carry the required markings, or carry invalid markings. 7. The anti-tampering device should be equipped with sensors capable to detect activity on the production line. This can be achieved with sensors placed on the machine producing tobacco products to determine whether	

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
			products are being manufactured. 8. The anti-tampering device should be capable to send an alert message to the repository in case of anomaly situations. 9. Anti-tampering devices should themselves should be protected from tampering (disconnected from power, the network etc.). 10. These devices should be equipped with battery backups in the case of disconnection from power	
Security feature	Weak	1. No clear definition or standard of what would qualify as security feature(s) has been identified leaving it up to the individual Member States.	1. A potential choice to achieve the overall objectives is to leverage the fact that 24 member states currently use tax	

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		2. The current draft and delegated acts requires a minimum of 5 security features, of which at least one should be chosen by the competent authorities. However, allowing the industry to select the security features of their choice introduces technical complexity amongst and between member states, unnecessary risks and does not meet the standard of "independent from industry" as proscribed by the FCTC. Tobacco manufacturers are not in the business of manufacturing security features so by definition any feature procured by them could be considered from a 3rd party. The prior referenced standards should rather be used as a determinant of 3rd party. 3. The current proposal does not ensure that security features are actually secure by design as not all security features carry the same level of strength). 4. The current design does not ensure that security features are procured from independent and trustworthy suppliers (certified and governed by	stamps. Although the specification does mention this as an option it leaves it wide open and does nothing to attempt to establish a common basis for enforcement by the member states. Ideally serialized tax stamps carrying security features that are selected / designed by government authorities and supplied by trustworthy independent providers should be the preferred choice. All tax stamps currently in operation in 24 Member States meet these objectives. In addition, many of the tax stamps currently in use by Member States also carry a serialized code, which is used to account the number of packs manufactured	

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		the aforementioned standards), who could ostensibly provide such features to counterfeiters and non-compliant producers. Minimum professional standards should therefore be defined and based on the vast array of accepted international standards. 5. By not providing any – even high level – specificity with regard to the security features, ensuring that authentication of the security features can be done easily and securely by all stakeholders, including law enforcement and consumers is impossible. If the tobacco manufacturers are allowed to choose the security features, there may be up to hundreds of possible configurations, by producer, brand, and country, making it extremely confusing and complex for stakeholders to authenticate them. Consider the following scenario: 28 member states x 100 tobacco brands x 5 security features = 14,000 possible configurations. This presents a near authentication impossibility as how can competent authorities have any	or imported in the country. This is an effective check and balance to the potential misuse (e.g. disconnection) of anti-tampering devices that scan UIDs on production lines.	

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		chance of using standard devices for authentication. 6. §1.6 of Annex II states the following: *"It is important to highlight that the responsibility of implementing these controls must not belong to the competent authorities alone. On the contrary, this responsibility must be shared between all the stakeholders involved in the operation of the solution, as a coordinated effort of the entities participating in the regulated supply chain to fight against illicit trade".* This is later in the table named as a control mechanism – but there is no specification for it. 7. Furthermore, the concept of authentication is only generally described and not specified in the technical specifications – that is **the very point of a security feature** in the first place. In the current solution specification, the ONLY party that would be in a position to authenticate the security features is the industry itself.		

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		8. Ensuring that the security features prevent a possible fraud consisting of applying the same (valid) UID multiple times (duplicated) on undeclared cigarette packs is completely lost in the current solution design.		
Data Repository		1. The report states in section 4.1.2.1: *"Manufacturers and importers **shall propose** the providers of the Primary Data Storage"* and *"As required by art. 15.8 of the TPD, the European Commission must approve the suitability, independence and technical capabilities, as well as the contract, of the third party providing the Primary Data Storage"* However, TPD Article 15.8: actually states "Member States shall ensure that manufacturers and importers of tobacco products conclude data storage contracts with an independent third party, for the purpose of hosting the data storage facility for all relevant data. The data storage facility shall be physically located on the territory of the Union. The suitability of the third party, in particular its independence and technical capacities, as well as the data storage contract, shall be approved by the Commission."	1. Manufacturers and importers should not be party or involved in the decision of appointing the data storage providers. This should be done independently by the EC, member state or the competent authorities. 2. Furthermore, the contracts for such data storage providers should be between the service provider and the relevant authority and not directly with the industry or importer.	

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		The report has made the assertion that the industry should propose auditors, to be approved by the EC, with no mention of the member state role as defined in Art.15.8. Considering the significant control and accountability being given to the industry in the proposed solution design, an opportunity has been missed to wrest some of the oversight control completely away from the industry by not having them play any role in the suggestion, appointment or engagement of the auditor. This is not an isolated example, see comments on the interpretation of 'affixed' regarding security features where the report chooses an interpretation of the word 'affixed' against the interpretation which would ensure better control as envisioned in the spirit of the TPD.	3. In order to avoid conflicts of interest, partiality, favoritism, the provider of the Secondary repository should not be a provider of any primary repository, which are contracted and paid by the tobacco industry. Instead, it should be procured by a public authority. The cost for the procurement and operation of the secondary repository could be charged back to the producers and importers, with a cost allocation model based on volume.	
Field Enforcement		1. This is, and has been a significant gap in the approach as the report makes the assumption that a lot of the controls or oversight and monitoring will be achieved through the surveillance activities of the competent authorities, and yet no attempt has been made to define the standards, procedures or even minimum requirements for such	1. The report should include a section on surveillance requirements at all levels from EC tight down to competent authority level, taking into account the various risks that	

Component	Control Measure(s)	Issues & Risks	Recommendation(s)	Citation(s)
		activities. In the position of a Member state control body or one of the competent authorities intended to implement and control such a solution. No attempt has been made at defining the oversight or surveillance role of the EC or similar oversight body that would have a union view of the solution to ensure it is operating as intended. This does not come as a surprise considering the other compromises that have been made in favor of an 'industry centric' solution which imposes minimal monitoring, control and oversight.	would need to be mitigated at all levels. 2. A thorough review of the surveillance and reporting requirements for the solution should be considered, defining the roles, responsibilities and specifications for such surveillance and reporting requirement	