LIST OF ANNEXES

REPORT: May and June 2020

Annex No.	Description	Action
Annex 1	Note of Meeting with DG Customs 13th May 2020.	Update DG REFORM.
Annex 2	Note of Meeting with DG Customs 27th May 2020.	Update DG REFORM.
Annex 3	Draft KOE Working Group Plan/Road Map.	Assist IAPR & Update DG REFORM.
Annex 4	Koutas Guideline for KOE.	Update DG REFORM.
Annex 5	Analysis of Koutas KOE Paper.	Assist IAPR & Update DG REFORM.
Annex 6	Draft: Human Sources of Intelligence.	Assist IAPR & Update DG REFORM.
Annex 7	Note of Meeting with DG Customs 16th June 2020.	Update DG REFORM.
Annex 8	Draft Surveillance Code of Practice	Assist IAPR & Update DG REFORM.

Annex 1 20200513 Note of Meeting with DG Customs

Date: 13th May 2020

Location: IAPR, 5th Floor, Karagiorgi Servias 10, Athens

Present: Stephen Henderson – DG REFORM (SH)

Mr. Mourtidis – IAPR, DG Customs (KM)

Maria Pagomenou – Interpreter (MP)

The meeting started later than planned at approximately 13:20.

Customs Staffing

During the current pandemic Customs, and all IAPR staff, are working in the office one week in three, the remainder of the time they are working from home, but in reality, home working is of very limited value. Apparently, there are plans to change this to one week in two, but there's no agreed date for implementation. As a consequence, staff actually in the office feel under a great deal of pressure.

Anti-Smuggling Legislation

This is the issue that is clearly which is uppermost in KM's thoughts. It's apparent the long list of legislation requested by the Deputy Finance Minister, before the lockdown, is still a very live issue, it has not been postponed despite the current coronavirus issues.

KM advised that he has a deadline of Friday (15th May 2020) to provide a provisional response to the Deputy Minister's Office. All the relevant directors are working on the legislation specific to their commands. The provisional responses will be collated and forwarded to the Deputy Minister's Office. It seems the process lacks focus and co-ordination. At some point in the future there will be a meeting with the Deputy Minister attended by the DG, the Governor and the appropriate Directors.

It seems the Deputy Minister expects the entire list to be addressed. SH thought it would be worthwhile having an urgent meeting with the Deputy Minister to discuss how his office and Customs could work more effectively together, since they both want to challenge smuggling effectively; KM will consider the suggestion.

KM had a list of approximately ten items of legislation which his office is supervising; of these two relate to topics SH has been working on:

1. Human Sources.
2. Controlled Deliveries & Surveillance.

KM added the work on both areas has been delegated to the lawyers at D33, under the command of Mr. Lymberis. It emerged during the conversation that

KM has requested draft legislation in each instance that would result in amendments to the domestic Customs Code. SH observed, that having met with the lawyers in question, Mr. Raptis and Mrs. Apostolou, he is sceptical this is what will be produced. SH went on to say he had met with them to discuss the paper he'd prepared on possible legislation. The meeting did not go well and it became obvious that Raptis and Apostolou do not think amending the Customs Code is the best option. They would rather hand the work over to the Ministry of Justice to amend the Criminal Procedures laws. However, this would be very time consuming and would affect all law enforcement, not just Customs. KM was aware of this adding the lawyers should prepare what's been requested irrespective of whether they agree or not. SH offered to meet with Mr. Lymberis to find out if he can help in any way; KM thought this was a good idea. A meeting was subsequently arranged for Friday 15th May 2020 at 10:00.

Turning specifically to controlled deliveries SH said he had discussed these with Antonis Pyrgiotis some time ago, his understanding is the paperwork is with the Ministry of Justice. KM was not sure, SH said he would check when he meets Antonis later in the day.

The conversation then turned to CHIS. SH said if D33 were able to draft fairly simple legislation this could be supported by a code of practice. SH added that he has prepared draft CHIS Guidance which could easily be adopted as a code of practice with some adjustments. However, the work is not quite completed. It was agreed SH would complete the draft and sent it to MP for translation and onward transmission to KM. Hopefully, KM would have the translated document by the weekend. KM thanked SH for his assistance, and said he could advise the Deputy Minister that legislation would be drafted supported by guidance, procedures and processes in a Ministerial Decision.

SH said surveillance may also be capable of being dealt with in a similar fashion. SH thought he had sufficient information to prepare a draft surveillance code of practice; KM thought this was a suitable solution. SH said he would start work on the draft as soon as possible.

SH added that if he could assist in any other way, he would be happy to help.

<u>Future Technical Assistance</u>

SH said his contract would be extended until November and December; KM said he was very pleased with this development.

During the second half of 2020 SH has been tasked with concentrating on specific areas:

1. Anti-Smuggling Strategy.
2. Intelligence.
3. KOE.

KM said SH's deliverables were in keeping with the areas where he would like assistance.

The conversation then turned to KOE; SH mentioned that he has started drafting guidance for the KOE Working Group, which once agreed, would, in effect, be a

road map for the Working Group. KM said one of the KOE Officers-in-Charge is also working on a similar document. Once SH has completed his work it was agreed it would be compared with the KOE Officer's draft and a joint road map put to the Working Group.

Following some general discussion, the meeting ended at 13:30.

Stephen J. Henderson

Stephen J. Henderson

Athens

13th May 2020

Annex 2 20200527 Note of Meeting with DG Customs

Date: 27th May 2020

Location: IAPR, 5th Floor, Karagiorgi Servias 10, Athens

Present: Stephen Henderson – DG REFORM (SH)

Mr. Mourtidis – IAPR, DG Customs (KM)

Maria Pagomenou – Interpreter (MP)

The meeting started earlier than planned at approximately 10:50.

Response to Deputy Finance Minister

KM said a draft initial reply has been sent to the Deputy Finance Minister as scheduled, but to date there's been no feedback.

SH commented that he had met with Mr. Lymberis and was very impressed by his plan, to cross reference the Customs Code to the Criminal Procedures legislation. SH added he thought this was an innovative and pragmatic solution to the problem. KM added he is in full agreement with suggested the course of action. KM provided SH with a printed copy of the proposed amended legislation, and asked that he review it and pass on his thoughts. SH replied he would have the documents translated and respond as soon as possible. SH said he would treat the paperwork in confidence.

The amendments affect Articles 157 and 158 of the Customs Code and cover human sources, surveillance and controlled deliveries.

SH asked if KM had received the copy of the CHIS paper SH has drafted? KM confirmed this has been received, but he has not had an opportunity to review it. SH said the important aspect at this stage is the Deputy Minister can be reassured the new legislation is supported by a comprehensive draft code of practice.

SH added that he's working on a similar paper covering surveillance which he hopes to finalise next week. This will be sent to KM as soon as it's translated.

At some point in the future both papers will need to be discussed in detail before they are finalised and adopted.

Fuel Smuggling Public Awareness Campaign

SH said at the moment he does not have any new information for KM but would update him as soon as possible.

KOE

SH said he has also prepared a comprehensive KOE Road Map designed to assist the KOE Working Group, it covers all the aspects they may wish to consider as well as some potential solutions to problems. SH commented that he hoped the

document would focus the Working Group and assist in achieving some quick wins. SH explained the paper is largely based on his discussions with a number of KOE units.

The paper was discussed for some time and it was agreed that it would be sent to KM later in the day and discussed at a future meeting.

SH explained the paper KM had sent him following their last meeting was not a KOE plan but rather a specific piece of guidance. SH went on to say the document was nonetheless very interesting as it highlights a potential cause for concern. SH said the guidance was written in a way that is very difficult to follow and is probably much too long. Guidance should be short, to the point and written in plain language. This point was then discussed; KM said he would send SH a copy of the KOE Guidance and would welcome his thoughts on this.

Technical Assistance

SH explained that he's been contacted by Expertise France and the intention is that his new contract will not start until 1st August 2020. KM said he would much prefer for SH's work to be continuous and felt a month-long break in July would be very damaging. He pointed out this is a busy and important time and he would like SH to be available to provide assistance. SH replied he would write to Expertise France and make KM's views known to them.

The meeting ended at 11:55.

Stephen J. Henderson

Stephen J. Henderson

Athens

27th May 2020

Annex 3: 20200311 DRAFT KOE WORKING GROUP PLAN

APRIL 2020

INDEX

INTRODUCTION

The development of the KOE's is a very important task. The KOE's are a visible, public facing part of the Customs General Directorate, it therefore follows that a holistic approach should be adopted and the development exercise exploited to resolve as many of the issues affecting the Units as possible.

AIMS & OBJECTIVES

In order to accomplish the aims and objectives of the exercise the KOE Working Group (KWG) should adopt an analytical, critical, structured and phased approach, possibly utilising the protocol template below:

PROTOCOL

Phase 1

A detailed in depth, honest and critical assessment of the current state of all things relating to the KOE's. The objective of this phase is to isolate all the problem areas. Some issues are already apparent, however, in the course of this phase the KWG may uncover additional problems or dismiss some of those previously identified.

Phase 2

The conclusion of this phase should provide the following interim results:

- Proposals.
- Solutions.
- Best Practice.

All should, as far as possible, be innovative, standardised, simple and rational.

Phase 3

Validation by stakeholders; opening up the product of Phase 2 to a wider audience.

Phase 4

Implementation; testing the results of Phase 2. This might include the use of pilot projects to test their viability before full implementation across all the KOE's.

Phase 5

Dissemination; having discussed and possibly tested the product of Phase 2, which may have been changed or adapted during Phases 3 and 4, this can now be rolled out across all the KOE's.

Phase 6

Follow up and monitoring; simply checking that the product of Phase 2 actually works in practice. This should take place after a reasonable period of time, and just like Phase 1 must be in depth, honest and critical.

REPORTING

The KWG should prepare agreed minutes of their meetings and brief reports at the completion of the individual phases.

Supplementary reporting may become necessary should specific problems be encountered that require consultation or assistance out with the KWG or at a senior level.

At the conclusion of their task the KWG should prepare a Final Report for consideration by the Director General Customs, and possibly the Governor of the IAPR.

COMPOSITION OF THE KOE WORKING GROUP

Each member of the KWG should be approved by Mr. Mourtidis, the Director General of Customs. Some members should have wide ranging experience of KOE work and, if possible, experience of how other law enforcement agencies operate. Others should have relatively little experience as their input will be new, fresh and possibly innovative; this will avoid simply building on or adapting existing practices etc. Lastly, the membership should not simply be a committee of KOE Officers-in-Charge, all ranks, including support staff, should have representation and equal status. Input from the DG's Office, the Governor's Office and, if possible, Technical Assistance would add value.

POTENTIAL ISSUES TO BE CONSIDERED

There are several issues noted below and within these a number of individual aspects the KWG may wish to consider. It's obvious not all of the points raised are capable of being addressed in the short term. It may be necessary for the Group to prioritise and select only the most pressing issues for immediate attention. Some issues will be medium to long term objectives, whilst others may remain aspirational. All of the points below would relate to the idea KOE, perhaps based in Utopia, however, they are all relevant to a fully functioning, well-resourced unit and should be carefully and thoroughly considered at some point.

SIMPLIFICATION

Strictly speaking this is not a specific task, rather simplification, rationalisation and standardisation should be considered whilst the KWG is assessing and challenging all the other issues listed below.

Generally, KOE officers spend too much time on non-operational tasks, like administration, in some units such tasks can consume 60% of staff hours. All the KOE's I've spoken with agree the level of bureaucracy is far too high and most would welcome the introduction of simpler procedures, like spot fines. Therefore, the overarching principle for the KWG should be to ensure the KOE's are out of the office, visible and operational as much as possible.

ROLES & RESPONSIBILITIES

Possibly, this should be the first issue the KWG addresses. Its work would result in a clear, strict list of KOE duties and tasks the KOE officers would be responsible for carrying out; it would be applicable nationwide. Defined roles and responsibilities are essential to avoid the development of local practices and prevent officers drifting into duties unrelated to the core functions of KOE, this is common under the current system. For example, the officers based in Crete were clearly not full time KOE officers and had other unrelated duties; this should no longer be permissible.

There must be a distinct vision of the KOE's roles and responsibilities, furthermore this vision must be clearly understood not only by the KOE Officers themselves but by the entire Customs General Directorate. As a starting point and in basic terms KOE is designed to be an effective, proactive anti-fraud detection asset. As such its primary role is to carry out controls, detect fraud and transmit intelligence gathered in the course of its work to units with the capacity and capability to investigate. There must be clear differentiation between detection and investigation.

With the exception of minor infringements which the KOE's will deal with quickly, possibly by means of spot fines. Any information gathered in the course of a KOE operation will be passed on to a suitable investigation unit. This could be done by means of a concise intelligence log sent to the EYTE Regional Office with a copy sent to the Central Intelligence Service. EYTE would decide on a suitable course of action, potentially in consultation with the central service. This would release KOE Officers to carry out more checks and provide a steady stream of good quality investigations with guaranteed results, since KOE will have already established the existence of an offence.

In addition, and flowing from this work, would be a clearly defined, unambiguous KOE Job Description. This would help with recruitment.

WORKING HOURS & PAY

Possibly one of the most contentious, but important, issues affecting the KOE's which impacts on many of the other areas listed below. Working hours and pay must be dealt with diligently and in their entirety, resulting in clear, comprehensive recommendations acceptable to both the frontline officers as well as senior leaders. This will be a difficult balance to achieve, but essential to the future of KOE.

1. Working Hours: The basic principle behind the setting up of the mobile units was to give Customs a detection capacity with the ability to work 24 hours a day and seven days a week. Therefore, it's clear a fully staffed

KOE would need to implement a shift pattern, most probably a three-shift system of day shift, back shift and night shift. Whatever pattern is decided upon it has to be uniform and standard across all the KOE's nationwide.

In addition, I would suggest there should be an "on-call" system where officers could be called upon to work when there's an urgent, specific operational requirement; such as supporting a SEK operation. Officer may be on call, possibly one week in every four.

The other side of working and shift patterns is rest periods, which are just as important for officer safety, operational effectiveness and work/life balance. Currently there is no standardised system. The KWG will need to consider this and make recommendations. For example, in HMRC if an officer works for 13 hours or more, they must have a rest period of 11 hours at least. A minimum 12-hour break between standard shifts should be the norm.

Lastly, and also of great importance, is the KWG must consider the impact of the European Working Time Directive. The Directive is designed to protect the rights and wellbeing of people ordinarily working more than 48 hours a week. The KOE Officers in Piraeus and Heraklion are currently working around 60 hours per week (including weekend and unsociable hours), so are clearly in breach of the Directive. It's possible for the KOE Officers to opt out, as is the case with some HMRC staff, and this should be explored with the IAPR's Human Resources Department as soon as possible.

2. Pay: Potentially the most contentious and difficult issue the KWG will need to deal with. Clearly officers serving in the KOE Units are expected to work longer hours, including weekends and holidays, than most Customs Officers and carry out some very difficult tasks in the most demanding of circumstances. As such they deserve to be paid appropriately, as compensation for the disruption to their work/life balance.

   At present KOE Officers are able to claim overtime, from a budget which is decided every six months. However, what they are allowed to claim is restricted to 20 hours per month (i.e. no more than 120 hours in the six months), also they can only work 96 weekend or night hours within that six-month period. Taking into account the current low staffing levels, these restrictions are significant inhibitors to effective operational activity. There's also a persistent time lag between working overtime and receiving payment, this is simply not acceptable.

   In my opinion, though this may not necessarily be shared by the KWG, there are two options available to ensure adequate pay for KOE Officers. Firstly, they could be paid overtime for hours worked out with their scheduled working hours. If this were to be the preferred option then there would need to be some improvements to the current system.

Restrictions on the number of hours that could be worked may have to be removed as well as the definition of such hours, restricting weekend and night work. Most importantly payments must be made promptly, procedures would need to be unblocked.

The second option may be to introduce a "KOE Allowance". This could be a meaningful percentage of the basic KOE monthly salary. In return officers would ordinarily work their shift pattern, but importantly would, without question, be available to work when there's an operational necessity to do so. An allowance, which is the preferred option of HMRC, makes pay budgeting much easier and ensures funds do not run out as can sometimes happen with overtime budgets, since operational activity levels will vary. Allowances have been out of favour in Greece in recent time but I think the KOE's could be a possible exception.

In addition, I would assume the KOE Officers would be entitled to a shift allowance.

STAFFING LEVELS

Current thinking is a fully staffed KOE must consist of 15 officers, with the exceptions of Piraeus and Thessaloniki, the two largest cities/ports in Greece, where the suggested compliment would be 30 officers.

The KWG may wish to consider if this one size fits all approach is the best solution. Perhaps KOE staffing levels should be considered on a case by case basis, taking into consideration geography, local conditions and challenges.

There is evidence to support this customised approach from the KOE based in Heraklion in Crete. I visited Crete and would question the viability of a full staff complement of 15 officers. Although Crete is the largest of the Greek islands it only has a permanent population of 500,000, expanding temporarily during the holiday season. However, this is relatively small compared to the populations served by other units; 3.7 million in Athens. It's possible 15 KOE Officers on Crete could be too many. KOE Crete does not carry out its own surveillance because the officers are well known on the island; the locals recognise the officers, their vehicles (official and private) and in many instances know where they and their families live. There are obvious officer safety concerns associated with this which could affect future recruitment. Also, because the population is small the number of businesses is also small and these businesses are visited on a much more regular basis than similar enterprises elsewhere in Greece. The KOE Officers in Crete have other duties, in addition to KOE roles, reinforcing the notion that the seven officers currently in post may be sufficient for the area/population they cover.

For the islands the KWG may wish to consider alternative arrangements. For example, a small locally based KOE, that would have local knowledge and insight, supported by a partner KOE on the mainland. The partner, mainland KOE, would support the local KOE during any larger operations or project work.

Alternatively, multi-functional teams could be established on the islands combining KOE with direct tax official with similar roles.

These are just a couple of suggestion which the KWG may or may not agree with; the result of their considerations on staffing should result in adequate KOE cover for all of Greece.

As well as operational frontline officers it's essential the Units are properly reinforced with support staff. Detection is the fundamental purpose of the KOE's, its essential frontline officers are available for operational work as much as possible. Support staff would, as far as possible, deal with the majority of administrative tasks, assisting with the compilation of statistics, contributing to the preparation of prosecution reports and some routine intelligence functions. Another important function of support staff would be localised procurement. Whilst major procurement exercise may best be dealt with centrally, the Thessaloniki KOE has demonstrated the value and effectiveness of localised procurement. In short, support staff could absorb much of the bureaucracy.

Finally, consideration should be given to facilitating legal support for the KOE's. It seems at present the compilation of legal briefs takes up an inordinate amount of time. This could be alleviated if the officers had easy access to legal assistance.

RECRUITMENT

Recruitment and staff retention have been problems for the KOE's since their inception and all the Units are operating well below their optimal staffing levels. Many of the recruitment issues are closely related to the problems associated with pay and conditions, mostly dealt with above.

Put simply, the KOE vacancies are just not attractive to the majority of Customs Officers and there are a number of barriers to recruitment, all of which will need to be considered by the KWG. Some of the main problems are listed below:

- Pay: At present KOE Officers are paid the same as regular Customs staff, but expected to work irregular hours in often difficult conditions.
- Working Hours: Theses can be long and involve weekend, unsociable, night and holiday hours.
- Lack of Understanding: Because there's no KOE Job Description there's a general lack of understand of what the Units actually do.
- Customs Age Profile: The vast majority of Customs Officers are well over 40 years of age and see working in a KOE as an unattractive option. Targeting young officers is difficult since there are very few in service.
- Lack of Benefits: Currently KOE Officers purchase their own uniforms, which are expensive (work boots cost around €120).
- Public Perception: Many officers feel public respect for Customs Officers has been eroded in recent years, so a public facing, law enforcement role is not an appealing option.
- Training: Currently there is no structured, comprehensive training and mentoring programme.

The KWG may be aware of other barriers which will also need to be taken into account.

Several recruitment exercises have taken place, but results have been very disappointing. There is an ongoing exercise which will look beyond Customs and attempt to attract civil servants from other Government Departments. It's thought this may have some limited success as Customs pay is generally better than other Departments.

Other recruiting options, pending resolution of the current inhibitors, could be from the following:

- Police.
- Coast Guard.
- SDOE.

Many serving KOE Officers would like to see the Units recruit young people, directly from high school, college or university and feel a degree is not necessary for the type of work they do. Rather they think recruiting youngsters with a reasonable educational background would reinvigorate the service, on condition they would be guaranteed comprehensive training and mentoring. In addition, this course of action could be politically astute as it may help to address the very high youth unemployment in Greece.

Recruiting young people without a university degree will meet with resistance from some. However, and by way of a comparison, HMRC has a programme of recruiting straight from high schools into posts complemented by a wide-ranging training programme. During their career, with appropriate coaching, some of these recruits are expected to reach senior positions.

In order to successfully recruit, from whatever source, proper targeted marketing of the KOE posts is essential, this will require careful consideration by the KWG.

Fundamentally, KOE's must be populated by the rightminded people who are motivated and actually want to do the job. In return, they have to be guaranteed the following:

1. Training and mentoring.
2. Appropriate pay and conditions.
3. Necessary equipment.
4. Incentives – such as exemption from transfer and redeployment.

A few words of warning the KWG may also wish to take into account:

1. Compulsory transfers into KOE could be very problematic, possibly even counterproductive or corrosive.
2. When the pay and conditions issues are resolved and the KOE's become attractive, recruitment policies may need to be reviewed.

On a positive note the Finance Minister and Deputy Finance Minister are both committed to bringing the KOE up to full strength. This political will and support

will be crucial to the work of the KWG, but it also brings pressure that will need to be carefully managed.

TRAINING

Properly trained officers will be key to the future success of the KOE's and a cornerstone of an effective anti-fraud capability. When considering training the KWG will should take into account three important aspects:

- Structure.
- Content.
- Source.

Structure: What form should KOE training take? Many officers have been critical of the training they've received and consider a classroom-based approach inappropriate for teaching the skills required for an officer in a mobile unit. The majority are in favour of an apprenticeship type approach where a new officer joining a unit would be assigned a mentor for the duration of their apprenticeship.

A possible template for training could be as follows:

1. An initial induction course containing a mixture of theory and practical training. This would include learning about the extant legislation and becoming proficient in some of the basic routine tasks and tests carried out by KOE.
2. On the job practical work experience type training to put into practice what was learned during the induction course.
3. Throughout this second phase the trainee would be partnered by an experienced mentor.
4. I would suggest a probationary period for each new recruit during which regular feedback would be provided by their mentor. Those who fail the training may be offered the opportunity to repeat the course or returned to their original position.

Content: In addition to basic training dealing with the tasks and techniques, which the KWG would need to design, all KOE Officers would benefit from some supplementary training as follows:

- Safety Training: To ensure all tasks are carried out safely, lawfully and in accordance with guidelines. There should be regular safety training refresher courses.
- Arrest & Restraint: As a public facing law enforcement part of Customs it's vital KOE Officers are proficient in restraining and arresting suspects, also that they are able to use handcuffs effectively; this will ensure the safety of the officers and suspects. Again, regular refresher training is necessary.
- Intelligence: Recognising what information is important and useful is essential to the development of a good intelligence database and future operations. As frontline officers the KOE are in a unique position to gather information. They also need to know how to complete the new

intelligence forms and disseminate these to the units that can make best use of the information; as well as ensuring the centre is updated.

- Surveillance: The strategic locations of the various KOE Units mean they are ideally located to assist with SEK operations, like tracking suspect vehicle from the northern borders to Athens. As such surveillance training both mobile and foot would help the officers and improve effectiveness. Regular team exercises would help to improve and refine skills.
- Informants: KOE Officer will often come into contact with individuals involved in smuggling. Some of these individuals may be suitable to recruit as potential human sources of intelligence. With basic training and skills KOE Officers could be trained to identify these people, so called "talent spotting".
- Notebooks: If the notebook trial in Piraeus is considered by the KWG to be a success then all KOE Officers will need training in their use. I've prepared some basic guidance but this would need to be expanded.
- First Aid: Considering the environment in which the KOE's work it would be prudent for all officers to have a basic knowledge of first aid.

Source: Who would be best placed to provide the training detailed above? Ideally, the IAPR Training Academy would be the first port of call and the KWG will need to assess the capacity and ability of the Academy to meet this need. If the Academy is not able to deliver initially then alternatives may need to be considered.

- French Customs: The French Customs Liaison Officer has been a valuable source of assistance previously and as a former mobile unit commander is uniquely suited to assist. To date he's provided some basic training material which the KWG will have. I've also discussed French Officers visiting Greece provide specific training. I will update the KWG in due course.
- CELBET: CELBET is an association of the Member States on the eastern facing border of the European Union, from Finland in the north to Greece in the south. Much of the work of CELBET revolves around training. There's a CELBET Co-Ordinator in Athens and the KWG may wish to consult with them to determine what training and funding is available. The potential benefits could be reduced costs and uniformity of procedures with neighbouring Member States.
- Police: With the exception of the core training and the induction course the Police may be able to assist with arrest and restraint and surveillance training, by doing so this would provide consistency with other law enforcement agencies and strengthen the bond between the Police and KOE. I'm aware the Police have provided safety training in the past.
- HMRC: Last year two HMRC officers presented an initial seminar in Athens on human sources of intelligence. The presentation was very well received and generated a great deal of interest. It's possible HMRC could be persuaded to follow this up with a training exercise.

These are just a few examples of where training assistance might be found, the KWG will no doubt have other potential sources.

OPERATIONS

At the conclusion of their work the KWG should arrive at operational processes and procedures which are safe, effective, standardised and in accordance with the law.

I would suggest all operational activity, regardless of the task should follow the same basic, simple format:

Prior to the Operation

1. Operational Order: An operational order should be prepared and signed by the Unit's Officer-in-Charge, with a copy sent to his line manager.
2. Operational Briefing: All officers taking part in the day's activity should attend an operational briefing where roles and responsibilities will be assigned. It's also an opportunity for staff to ask questions or raise concerns.
3. Operational Risk Assessment: Every task has its own unique set of risks; these should be recorded and the actions taken to mitigate the risks noted. The risk assessment should also contain emergency information, such as the location of the nearest hospital. Each officer involved in the day's activity should read and sign the assessment.

After the Operation

1. Operational De-Brief: All officers who were on duty should attend. This is a chance to assess what happened during the operation, identify what went well and what the problems arose.
2. Intelligence: Any intelligence gathered in the course of the day should be disseminated.
3. Action: Any immediate action required as a direct result of operational activity should be completed.
4. Report: A very brief standardised narrative report should be prepared.

Standard Operating Procedures

All the KOE Officers I've spoken with have said they would welcome the introduction of standard operating procedures (SOP's); their implementation would be a sensible step for the KWG to consider. Generally, standardisation improves speed and efficiency.

There are a number of benefits to introducing SOP's:

- Every KOE Officer, no matter where they're based would do the same thing in similar circumstances.
- Ensure officers are safe.
- Procedures are lawful.
- Could assist an officer giving evidence in court; i.e. the officer complied with procedures which are accepted as lawful, in some ways similar to a Nuremburg type defence.

- Beneficial when more than one Unit is engaged in the same operation; officers from different units would do the same thing.
- Could introduce a standard set of questions when cash is discovered.

For example, when a vehicle is stopped an outline SOP could be:

1. The stop site should be pre-determined, safe and with enough space to operate comfortably.
2. The stop should be conducted by at least three officers.
3. When the vehicle comes to a halt the officers should show the driver their identification.
4. There should be a standard form of word explaining why the vehicle has been stopped, quoting appropriate legislation.
5. The ignition keys must be removed.
6. The driver (and all other occupants) must exit the vehicle and stand in a safe area, away from traffic and their vehicle.
7. One KOE officer will remain with the vehicle's occupants.
8. The driver or owner of the vehicle should then be told what is going to happen i.e. their vehicle is going to be search, again, if possible, using a standard form of words and quoting the extant legislation.

I would suggest that each KOE identifies and prepares a list of safe locations were vehicle stops can be carried out.

Generally, procedures should be as uncomplicated as safety and the legislation allows and the officers should only gather the information that's actually required. The KWG should as far as possible device simple guidelines for operational work.

They may also consider what legislative improvements could be proposed to senior leaders. It's generally accepted that the fines and penalties system would benefit from a root and branch overhaul. An obvious improvement, which most KOE Officers would support, is the introduction of spot fine for very minor infringements. These would give officers the ability to deal with these low-level type offences quickly and easily.

The KWG should also consider the drafting of a KOE Handbook where all the aspects of KOE work and what a KOE Officer is required to do, including SOP's, could be recorded and act as a point of reference and guidance for seasoned officers and new recruits alike. Its important officers have easy access to instruction and reference material. Ideal, the KOE Manual should be electronic as this is more cost effective, secure and makes editing/updating easier. I would recommend the KOE Handbook could include the Infringements Manual. As the name suggests, this contains details of the different types of infringements, the appropriate legislation and the corresponding fine and penalties; it's a fantastic aide for KOE Officers.

It might also be beneficial for officers to carry short Aide Memoires, to ensure procedures which must be dealt with strictly in accordance with a set procedure are carried out correctly; the form of words for a vehicle stop is a good example.

Apart from written guidance it's important the KOE Teams learn from each other. Shared experience, used to formulate best practice, is a great way to advance and improve working procedures and build a team spirit; camaraderie. With this in mind the KWG should give serious consideration to an annual KOE Conference. A conference would allow representatives from each unit to come together and discuss what they do and how they do it. It could also be used as an opportunity for upskilling through presentations on KOE-related subjects. Delegates would then disseminate what they've learned to their colleagues at their home station.

EQUIPMENT & ACCOMMODATION

I don't feel qualified to detailed exactly what technical equipment the Units may require. This is best determined by those who actually do the work and have the appropriate experience; members of the KWG will know best.

However, I would recommend that before any potential procurement exercise is launched the KWG undertake a detailed needs analysis to clearly establish what equipment is actually required and useful to officers on the frontline.

A number of officers have highlighted the testing equipment in the vans used by KOE's is of very little practical value. Test results are only valid in law if the test is carried out by a certified chemist, i.e. by the State Laboratory. However, some indicative test equipment would be essential. Most officers would much prefer the vans to contain a desk and laptops. These laptops should have the ability to access central databases whilst out of the office.

Remaining with computers, these are the most pressing problem. Currently, many use Windows Vista operating system which is no longer supported by Microsoft. Because of this it's often impossible to open documents received; there's also an increased risk of viruses and malware. A procurement exercise for 1000 laptops and 500 tablets is apparently underway, this should be completed as soon as possible.

Each KOE should have a van for use during roadside checks etc. and these vehicles should have clear Customs/IAPR signage for public recognition purposes.

Conversely, any cars used by the Units should have either no outward indication they are Customs vehicles or have removable, magnetic signage this would allow these vehicles to be used in surveillance. Rotating cars between the Units would prevent criminal gangs being able to identify KOE cars easily.

Turning to the personal equipment required by individual KOE Officers. In my opinion, the most important piece of equipment every KOE Officer must have, and should have at the earliest possible opportunity, is a photo identification card, to include the Customs/IAPR logo. These are essential for working with the public and should be clearly displayed when officers are on duty.

Similarly, uniforms; at present officers are responsible for purchasing their own uniforms and much of their personal equipment; personally, I think this is completely unacceptable. Uniforms and boots must be supplied, free of charge,

to all officers serving in KOE and should be standardised, good quality, practical and distinctive. Central procurement of uniforms, and other items of personal equipment would be more cost effective. It's important for KOE Officers to wear a uniform whilst operational, with the exception of surveillance work, and that the uniform is recognisable to the general public, this has some deterrent effect in itself. The components of the uniform package should contain clothing suitable for working in both summer and winter conditions for year-round visibility and recognition.

As well as the basics the KWG may wish to consider having officers' issues with at least some of the following items of personal equipment:

- Mobile 'Phone: Each officer should be issued with an official mobile 'phone, basically for work use only. This would assist if an on-call system is adopted.
- Radios: Personal issue and in-car for secure communications during operational activity.
- High Visibility Jackets: Officers should be easy to see, especially when working at the road side. Ideally the jackets should have Customs written on them as well as a Customs/IAPR logo.
- Body Armour: Essential for officer safety.
- Handcuffs: Only after appropriate arrest and restraint training has been successfully completed.
- Business Cards: Very useful when dealing with members of the public and can be good for generating intelligence by providing a point of contact.

Finally, many of the items mentioned will require regular maintenance, particularly vehicles, this is essential for both safety and efficiency. Regular maintenance schedules should be prepared and adhered to.

Touching only briefly on accommodation; I would suggest all KOE Units should have access to two facilities associated with accommodation. Firstly, secure parking for both official and private vehicles, ideally this should be enclosed. Secondly, a secure storage facility where seized items can be kept safely prior to release or destruction.

RESTRICTIONS

There are a number of administrative restrictions on the activities of the KOE which I would suggest the KWG should examine critically to determine if they are conducive to efficient operational activity.

Restrictions on overtime were dealt with earlier, but there are others:

1. Restricted Distance: The number of kilometres a KOE vehicle is permitted to travel in a given period is restricted. Whilst this is an issue for all KOE's, it's a particular problem for those with large geographical areas or long stretch of border to patrol. For the KOE's to function correctly and be able react to operational developments, I would suggest this restriction needs to be re-visited urgently.
2. Restricted Detached Duty: KOE Officers are only allowed to work outside their home area for 60 days each year. This clearly impedes their

operational scope and ability and could seriously impact on both joint working and SEK co-ordinated operations. It would be more reasonable for KOE's to have the ability to work where ever they're needed, when ever they're needed and for as long as they're needed. Unless there's a really good reason for this restriction the KWG may wish to try and have it revoked.

3. Travel & Subsistence: It seems the current travel and subsistence rates have lost touch with reality and possibly not been updated for a considerable number of years. The KWG may wish to instigate a review of these with the aim that officers should not be out of pocket when working away from home.
4. Road Tolls: At the moment KOE staff are paying road tolls from their own pockets when on duty. If at all possible, the KWG should investigate if it's possible for theses to be waived by the private companies involved. As far as I'm aware the Police do not pay tolls, so it's possible for arrangements and agreements to be made. The KWG could possibly liaise with the Police on this.

REPORTING

The consensus of opinion indicates the system of reporting in place at present is simply a vehicle for statistical reporting of progress, by the individual KOE's, against their targets. As such these reports are of only limited value to both the KOE's and the senior leadership team.

KOE Officers-in-Charge prepare purely statistical reports monthly, quarterly and half yearly which are submitted to D33. Most Officers-in-Charge I've spoken with are of the opinion that D33, through ICISNet, has the ability to compile these statistics independently. If this is case, the KWG might consider a complete overhaul of the reporting regime with a view to crafting it into a more informative, useful system that's standardised, simplified and minimised so as not to impinge on operational work.

One option would be to introduce a short monthly narrative report using a standard computerised template. The report would focus on operational activity emphasising what went well, what didn't go well and where possible why. It could be a tool for isolating problems at an early stage and identifying best practices. Also, this type of reporting would assist with tasking and co-ordination and could help to pinpoint project or targeted work. Serious issues highlighted in the reports could be taken forward for discussion at the next KOE Conference.

As well as a monthly report a year-end report could also be useful, again, it need not be a long document.

LEGACY SDOE CASES

Exactly what these cases constitute has never been made clear. It seems all the KOE's are or have been in possession of a large amounts of intelligence or cases previously held by SDOE. Furthermore, it appears there is a legal obligation to deal with this work. The consensus, from speaking to a number of KOE's, is that

the SDOE information is old and of little or no operational value, any useable material has long since been extracted.

How the material has been dealt with varies from KOE to KOE. It's a significant problem in Piraeus, but less of a problem in Crete and Thessaloniki. Clearly, a consistent approach is needed and to this end a committee has been set up to examine the problem. The KWG, in its initial period of working, should establish what progress has been made and ensure the KOE's are not obliged to do any work on the SDOE Cases until there's a definitive decision on a unified approach.

Ultimately, the committee should endeavour to find a solution which involves as little time and effort as possible, but is sufficient to satisfy and discharge any legal obligation.

As a footnote, when Mr. Mourtidis was a Director in Piraeus he was able to write-off some of this work. It would be good starting point for the committee to establish what he did and, if it's possible, to replicate this on a nationwide basis. Perhaps the new Director of EYTE could simply instruct that the cases be archived.

CUSTOM FUND?

This is something else that I don't have a clear image of, however, it's an interesting potential factor.

During an informal discussion with some KOE Officers I was told about something call the Customs Fund, containing money derived from the fuel companies. Before the financial crisis this was distributed amongst Customs Officers, it's not clear if all Customs Officers got a share or only some. In any event, it seems the fund contains in the region of €120million. The trades unions have taken the government to the European Court in an effort to have funds released, but although they won their case, the funds have not been disbursed.

If there are funds that could be used for the benefit of Customs then every effort should be made to have this money made available and to ascertain precisely what conditions are placed on its use.

OTHER MEASURES

There are a couple of structures that could be beneficial to KOE as well as the wider EYTE Directorate.

1. Tasking & Co-Ordination: It's essential for EYTE and KOE to have a good awareness of exactly what's happening in the wider Customs community. The Tasking & Co-Ordination Unit would ensure there's no overlap or duplication of efforts. As such it would be responsible for monitoring the activities of the individual units, perhaps receiving copies of the monthly narrative reports. With an awareness of what the Units are concentrating on, as well as a good grasp of current trends and threats, the Tasking and Co-Ordination Unit would be ideally placed to instigate targeted or project work where KOE's would be tasked and focus on one particular issue, possibly foreign registered cars or cigarette smuggling.

2. Intelligence Unit: This would be a small unit responsible for dissemination of intelligence received from the central intelligence service to the operational unit, or units best placed to utilise the intelligence. In addition, the unit would receive intelligence from the KOE's and pass this on either to the centre for further development/analysis or a suitable unit with the larger Customs community. By liaising with Tasking & Co-Ordination intelligence could help determine targeted and project work.

I've tried to prepare a comprehensive template of issues the KOE Working Group may wish to consider in the course of their work. As mentioned earlier I'm fully aware that all these issues are not capable of being addressed immediately but I would suggest they will all need to be taken into account at some juncture in the future.

Also, this is not a definitive template, the Working Group, drawing on their experience of practical, operational work, may know of other problems which need to be resolved.

Lastly, I would be happy to assist with this work in any way possible.

Stephen J. Henderson

Stephen J. Henderson

DG REFORM

Athens

Annex 4 20200518 Koutas Guidelines KOE

HELLENIC REPUBLIC
IAPR
DG CUSTOMS & EXCISE
ELYT ATTICA
ADDRESS: Akti Kondyli 32
POST CODE: 18545 Piraeus
Director's Office
TEL: 2132112617 & 657

Piraeus, 24 April 2020
Ref.No. 3380
TO: **Heads of KOE Departments, Piraeus, Igoumenitsa, Patras & Irakleion and Marine KOE**
CC:
- Director's Office
- Sub-Director's Office
- Dpt B' Intelligence & Risk Analysis
- Legal Support Office

SUBJECT: "Provision of supplementary guidelines"

Following the "Operating Manual for the Mobile Units (KOE)" we had sent you, we are bringing the following to your attention:

A. Book of Control Cases – YSDE :

- Concerning the update of the "BOOK OF CONTROL CASES – YSDE" and issuance of the numbered form "Official Note of Control Findings-YSDE", instructions have been given on how this is issued, for the pending cases of the KOE departments transferred when those came under our Unit on 01/01/2020 and for the cases created after 01/01/2020 , as well as for the use & mandatory numbering of the forms:
  - Provisional Confiscation Report
  - Seizure Report, as well as the relevant Seizure & Arrest Report
  - Infringement Notice under art.4 of L.3446/2006
  - Infringement Notice under art.20 of L.2873/2000
- Moreover, we are pointing out, on the procedure, that the use of the aforementioned numbered forms and delivery thereof to the staff of the departments, initially and until newer orders, **will take place** under **the oversight** of their head-officer, **day by day** and according to the number of control orders and teams, to be issued, who must **be contacted** by the control officers, prior to the issuance of the relevant forms, to confirm the relevant serial number (e.g. if on 13/04 the control of the 1st team has used the YSDE No 01-02, then the 2nd team, should it need to issue an YSDE, shall liaise to find out and use the next number No 03).

Also note that:

a) The monthly **Electronic Registry** of the maintained Book of Cases-YSDE and

b) The monthly maintained Detailed Statement of conducted controls in excel file, **must** be sent promptly to our Unit, **within the first three days of the following month** to the email:
- riskanalysis@1986.syzefxis.gov.gr
- elytattikis@1986.syzefxis.gov.gr

B. Handling the relevant forms (summons to a Hearing or Defense):

i) Summons to a Hearing – article 6 of L.2690/99

1st Case – simple customs infringements:

It follows from interpretation of the relevant provisions on summons to a hearing under article 6 of L.2690/99, as described below, that the administrative authorities are required to invite the person under control to express his views on the control findings, **which only lead to administrative sanctions** (e.g. non-submission of Vehicle Arrival Declaration, expire of the ADR etc), thus excluding the smuggling cases.

Thereafter, the legal department of the Customs Office the relevant findings report will be sent to, shall ensure the imposition of administrative sanctions, followed by administrative interrogation, including also the answers of the offenders, inviting the person under control to an **administrative plea**, in view of assessing the infringement once the customs infringement protocol is issued.

2nd Case – infringements of other agencies:

In the case of infringements of other agencies (e.g. the Chemical Laboratory, i.e. samples with irregular indications), **it is exceptionally possible**, pursuant to item c of art. 6 of L.2690/99, in order to prevent risks or because of imperative public interest, **without prior summoning** of the interested person, **therefore** in this case he shall be **summoned** by the competent service the case is forwarded to.

ii) **Calling the defendant to account, Code of Criminal Proceedings**

It follows from interpretation of the relevant provisions of art. 270, 271, 273 of L.4620/19 of the Code of Criminal Proceedings, also described below, that in any smuggling case under L.2960/01 (alcohol, fuel, cigarettes etc), we proceed to calling the defendant to account, after determining their identity and explaining their rights.

In this case, **given** that before drafting the report a **Subpoena** under the criminal law is **delivered**, **there is no need** for **summons to a hearing** under art.6 of L.2690/09, **because** the person under control has **become aware** of the offenses he committed, as well as the administrative and criminal sanctions involved and **furthermore** he will be called to account by the competent Customs Office during the administrative interrogation, in view of proceeding to the assessment, issuing the relevant customs infringement protocol.

Relevant provisions of article 6 – L.2690/99 – Summons to a hearing:

a) The administrative authorities, before any action or measure against the rights or interests of a specific person, are required to invite the interested person to express his views, in writing or orally, on the relevant issues.

b) Summons to a hearing shall be in writing, indicating the place, date and time of the hearing, specifying the scope of the measure or action.

The above summons shall be notified to the concerned person at least five (5) full days before the hearing date. The person concerned shall have the right to become aware of the relevant evidence and proceed to counterevidence.

c) If it is necessary to take adverse measures immediately to prevent risk or because of imperative public interest, it is exceptionally possible without prior summoning of the concerned person.

- **Relevant provisions of L.4620/19 of the Code of Criminal Proceedings, i.e.:**

a) **Article 270 – Defendant's plea;** the main interrogation cannot be considered completed if the defendant has not pleaded.

b) **Article 271 – Summoning of defendant;** the summons shall be in writing and must indicate the offense the interrogation is about.

c) **Article 273 – Examination of defendant;** when the defendant appears before the interrogating judge or the prosecutor, the misdemeanor court or district court judge carrying out the preliminary questioning or the investigation officers specified in articles 33 and 34, they shall be required to verify his identity details from his ID card or passport, inviting him to state his current home or residence address (city, town, village, neighborhood, street, number).

d) Once the identity of the defendant has been verified and all his/her rights are clearly explained to them, pursuant to art. 103 of the CCP, as laid down in art. 99A, 100, 101, 102, 103, 104, 105 & 273 of the Code of Criminal Proceedings, the examiner shall present clearly and comprehensively the act for which he/she is accused and invite him/her to plead and indicate his defense instruments. The defendant shall have the right to refuse to answer. He/she shall also have the right to deliver the defense in writing. In this case, the interrogator shall raise to the defendant the necessary questions to clarify the content of the written defense.

C. <u>Management of Cases under Criminal Proceedings – preparation of reports</u>

i) In the document of our unit No. 2390/03/04/2020, we referred to the management of cases under criminal proceedings: upon completion of the control actions, **we shall proceed**: **a)** to lawfully summoning the person under control and receiving his speech in defense (**relevant template 1-2**), **b)** to **preparation of the Reports – Findings** reports, <u>the last section of which must in any case</u> start with the heading **"CONTROL FINDINGS"** and **NOT** the term "**CONCLUSIONS**", and then the next line must be **"(A1) SATISFACTORY" OR "(B1) NON- SATISFACTORY with the relevant infringement code**" and **c**) to **submission of the case file** to the competent Public Prosecutor Office (**relevant template 3).**

ii) <u>In addition to the above and depending on the amount of tax and duties, the following are also required</u>:

a) **Submission of a REPORT** under **article 25 – L. 4557/2018**, where the amount of charges is **above 50,000 euro (rel. template 4**), which shall also be submitted together with the main case file to the competent Public Prosecutor.

b) **Submission of a SPECIAL CONTROL REPORT** under **article 153 OF L.2960/01,** where the amount of charges is **above** 1**50,000 euro (rel. template 5).**

D. <u>Procedure of forwarding the Cases of KOE controls</u>

i) a) In the document of our unit No. 2390/03/04/2020, we referred to the process of forwarding the cases of KOEs to the competent authorities (Customs, Tax Offices, Chemical Lab, Ministry of Development, Ministry of Commerce), <u>distinguishing two (2) cases of transmission (a) & (b)</u>, **however**, **<u>because of the structure</u>** both of the KOE Departments in Attica and the competent Stand-Alone Department A' – Administrative & Legal Support of ELYT Attica, which **we have requested** to be separated and establish a new Legal Department in ELYTs Attica and Thessaloniki, prompt receipt and forwarding of the cases to the competent authorities **is not ensured**.

b) It was also deemed necessary to **<u>keep</u>** the set of the **original** attached **evidence** of the KOE cases **<u>in the archive of KOE departments</u>**, and forward photocopies to the competent unit that will proceed to the administrative proceedings.

ii) <u>For this reason, we define below the process to forward Cases of KOE DEPARTMENTS</u>:

a) The Control Reports – Finding Reports / Lawsuits / Special Control Reports under art. 153 of L.2960/01 **&** the Reports of art. 25 – L.4557/2018 of the **KOE** Departments of **Igoumenitsa, Patras & Irakleion**, shall be sent initially **by e-mail** to ELYT Attica **for the preliminary audit** and shall then be sent by **COURIER,** undersigned by the Heads of Departments, **to be authenticated and signed** by the competent Directors/Subdirectors, along **with a set** of attached copies.
b) Thereafter, the said reports of the above KOE Departments, having been signed, shall be **returned** electronically **by e-mail to the departments;** the heads thereof shall **print out** and **stamp** them with the round seal of their department, **make** as many true copies as required to be forwarded to the competent authorities (Customs, Public Prosecutor Office, Tax Office, Chemical Lab, Ministry of Development, Infrastructure & Transport), with a set of attached copies (where necessary), **keeping for their records** copies of the relevant control-findings reports, with **the** corresponding **set of original evidence.**
c) The above case-forwarding process also **applies** to the **1st Department of KOE Piraeus, i.e.**: the aforementioned Control-Findings Reports etc. shall be sent initially **by e-mail** to ELYT Attica **for the preliminary audit** and then the relevant Reports shall be **furnished**, signed by the Head of the Department, **to be authenticated and signed,** with a set of attached copies.
d) The above Control Reports – Finding Reports, Lawsuits, Reports of art. 25 – L.4557/2018, Special Control Reports under art. 153 of L.2960/01, along with the set of attached copies for the records of the unit, may be sent on a weekly basis to ELYT ATTICA, **so that** the Stand-Alone Department A' – Administrative & Legal Support of ELYT ATTICA can **perform** the **notifications specified in the law**, to the IAPR services (D33, Directorate for Excise & VAT etc).

E. Instructions on the stocktaking on the targets for 2020

According to **a)** D33 document …. and **b)** the e-mail of EYTE on 16/04/2020 (**att. 6 & 7**), instructions are given on taking stock of the targets of GD Customs & Excise for the A' Class Customs Offices and ELYTs, and the relevant targets are defined accordingly, which are allocated by the Head of each Directorate to the heads of the relevant Departments, as those are laid down in the IAPR Governor's decision, and the heads of Departments of the said Customs Authorities, as well as of the B' Class Customs Offices, proceed to the allocation of the targets to the competent staff (art. 23, item 2, L.4389/16).

According to the above, regarding the targets of B' Sub-Directorate of ELYT Attica, the following is pointed out:

i) Result of Control

- Upon completion of the control, the responsible controller, as also stated in the relevant "Operating Manual for the Mobile Unit Departments (KOE)", shall enter into the IT system ELENXIS the result of the control, which is counted in the statistics, based on the end date entered by the controller in the respective field of the control result in ELENXIS.
- **When the result is recorded, in cases where the order used concerns several categories and types of control, to ensure the correct presentation of the data:**
  - → The categories and types of control for which no control was conducted are deleted
  - → Where an infringement is found, the exact categories and types of control for which an infringement was found are selected (in the control verifications of the category where the infringement was found, select "INFRINGEMENT" YES in the type of control where it was found).

→ For each category of control (e.g. lawful ownership and circulation of passenger vehicles etc), the control result is entered into ELENXIS per controlled person. For the same controlled person, a result is recorded in a specific category and type of control.

→ For each category of control, one type of control is recorded for the same controlled person. For example, where a person is subject to physical control and accounting audit, one type of control shall be recorded, e.g. the one that triggered the control, because the detailed control verifications are described in the control report.

→ **The category and type of control are selected taking the following into account**:

- The **Accounting Audit-5200,** when conducted in the seat of the auditee's business, on the accounting entries and tax records, trade correspondence etc.
- The **Physical Control-5000**, where the goods are physically examined.
- The **Inspection of Facilities-5300**, where the premises of the auditee's enterprise are inspected (e.g. site inspection of the facilities)
- The **Control of Persons-5400**, where an individual is checked (e.g. a passenger)
- The **Inspection of means of transport-5500**, where a transport medium is inspected.

ii) Entry of results into Table I

The competent KOE departments and the Marine Unit of ELYT Attica **shall enter into table I only the completed control carried out upon issuance of a control order** by the competent departments of ELYT Attica, as those are indicated in the IAPR Organisation, **as well as any infringement** that was **found** and **entered** into **ELENXIS**.

Given that the aforementioned departments of ELYT Attica **conduct controls that** may **be in progress**, in each monthly submission of data **those shall be recorded** in the outturn data of the month they are **completed** in (the control is completed when the control results have been submitted and entered into ELENXIS and the relevant Control Report-Findings Report has been drafted).

- ELYTs shall submit the model table IV, KOE, Marine KOE, by email, with the detailed results of the previous month, on a monthly basis, the first week of each month, to the electronic address d33info@2002.syzefxisgov.gr of D33/Department A' according to the relevant order of D33.

The Head of B' Sub-Directorate
Paris Stanis

The Head of ELYT Attica
Andreas Koutas

Annex 5 20200519 Analysis of Koutas KOE Paper

NOTES ON KOUTAS KOE PAPER

PROVISION OF SUPPLEMENTARY GUIDELINES

The Koutas paper was given to me by Mr. Mourtidis following a discussion about the guidance I've written designed to assist the KOE Working Group (KWG). However, the two documents are not at all comparable. Mr. Koutas' paper is not intended to assist the KWG, rather it's a specific piece of guidance for KOE Officers. Despite this it's a very interesting piece of work, possibly giving an insight into how instructions and guidance are written and presented. There's a reference at the beginning to an "Operating Manual for the Mobile Units (KOE)" and it would be interesting to see the rest of the manual.

The question is whether this supplementary guidance is indicative of what all guidance looks like, if it is, then there are a number of problems which need to be addressed.

By way of a preface to my comments, I'm not familiar with may of the roles structures and procedures associated with Customs compliance work, and from this guidance these are no clearer.

The guidance is complex, difficult to follow and probably too long; it does not encourage the reader to understand the processes it describes. It was difficult for me to understand who is responsible for the various steps described, KOE, ELYT, the Prosecutor or the Judge. This is not a criticism of Mr. Koutas, writing instructions is very difficult and takes practice. Clearly, Mr. Koutas understands what he's trying to convey.

There are a few general principles associated with writing guidance, it should:

1. use plain and simple language;
2. avoid jargon;
3. be short and to the point;
4. be logically structured;
5. be easy and quick to read;
6. be easy to assimilate the information;
7. be prefaced by a short summary of the subject matter;
8. be sent to everyone it affects (this instruction is not addressed to all KOE's, instructions must be universal and consistent which prevents local practices developing).

Supplementary guidance should be capable of being integrated into the main Manual, otherwise it will become detached and forgotten about, which defeats the purpose. This is unlikely to be the case with this supplemental guidance; it covers a couple of different topics. If the KOE Manual is electronic then adding new parts is relatively easy; much more troublesome if a paper copy is to be maintained.

It's possible producing aide memoire cards for some routine tasks could be beneficial; preparation of legal brief could be an example.

Turning to the actual contents of the guidance, it's clear, even with my limited knowledge, that preparing a legal case is very difficult. This point was raised by the KOE in Thessaloniki. They suggested each KOE should have on site legal support for the preparation of legal briefs. This would reduce the time the officers spend on paperwork and increase operational activity.

There are a number of training and development opportunities arising from Mr. Koutas' paper:

- a Customs/KOE Officer should be trained to write and maintain the KOE Manual, in simple plain language;
- if there's no localised legal support KOE Officers must be trained in preparing legal briefs;
- use of ELENXIS should be a part of the KOE basic training package; this should include support officers.

Guidance which is easy to use and kept up to date is essential to effective, safe and lawful operational work.

Stephen J. Henderson

Stephen J. Henderson

Athens

19th May 2020

Annex 6 20200427 DRAFT HUMAN SOURCES OF INTELLIGENCE

INDEX

INTRODUCTION

To effectively target organised criminality law enforcement agencies must have the ability to deploy a variety of techniques and assets. The deployment of properly managed human sources offers unique and unparalleled access to information and intelligence on criminals and their activities.

The ability to gather intelligence on organised crime groups allows law enforcement to better understand how they operate, thus providing high quality intervention opportunities. It's thought the deployment of human sources may be up to seven times cheaper than technical alternatives.

However, the use of human sources is very risky and demands the highest standards of organisation and integrity to ensure the safety of the source and the officers who manage them.

TYPES OF HUMAN SOURCES OF INTELLIGENCE

There are two distinct categories of human sources of intelligence and it's essential to be able to differentiate between the two in order to prevent unmanaged status drift.

HumInt: A Human Intelligence Source, HumInt, is any person who willingly provides information to any law enforcement agency relating to a possible criminal offence, including any offence that may ultimately be dealt with under civil provisions, or as a regulatory breach.

The term HumInt covers any individual, either named or anonymous, who provides information whether received in the course of their trade, profession, business, employment or personal life, either by 'phone, face to face, via written correspondence, fax, text voicemail or email.

CHIS: A Covert Human Intelligence Source, CHIS, is defined in the UK legislation, the Regulation of Investigatory Powers Act 2000 (RIPA), Part 2, as a person who establishes or maintains a personal relationship for the covert purposes of facilitating the doing of anything falling within the following paragraphs:

- he covertly uses such a relationship to obtain information or to provide access to any information to another person.

OR

- he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

In addition, there are other fundamental differences between a HumInt and a CHIS; it's important these are well understood to prevent status drift.

1. A CHIS may have a long-lasting relationship with an agency which is developed and manged over a period of time.
2. A CHIS is likely to receive some form of reward in return for the information they provide.
3. Most importantly, a CHIS can be tasked.

FIRST CONTACT

It's absolutely essential the first contact with any potential source, whether they develop into a CHIS or remain as a HumInt, is handled correctly and competently. As it's impossible to predict who will receive the initial contact it's prudent for all officers within the IAPR to have a basic understanding of what to do.

All HMRC staff complete a basic, annual online course and each has a copy of an Aide Memoire designed to assist them and highlight some vital do's and don'ts when dealing with an individual who wants to give information.

Below is what an IAPR Aide Memoire might look like:

IAPR HumInt Aide Memoire

IAPR staff members must report any information received which relates to the smuggling of excisable goods such as tobacco products (cigarettes and hand rolling tobacco), fuel/oils and alcohol.

A person giving this information is known as a Human Intelligence source (HumInt).

When you receive information, you must prepare a HumInt Contact Report and send it to ……...

Written information on the smuggling of excisable goods such as tobacco products (cigarettes and hand rolling tobacco), fuel/oils and alcohol must be sent to ……

You must also report any information that you personally become aware of even if it occurs outside work.

When you are given information, you must record:

All the details about the allegation:

- ***Who** is the allegation against?*
- ***What** is being alleged/what is happening?*
- ***Where** is it taking place?*
- ***When** did it happen and how long did it last?*
- ***How** is the alleged offence committed?*

All the details about the person providing the information:

- *What is their name, date of birth, address, telephone number and when it would be safe to call if we need to contact them again?*
- *Why are they giving us the information?*
- *How do they know this?*
- *Who else knows?*
- *Is there a connection between the person giving the information and the subject of the allegation?*

When you are given information – <u>some DO's and DON'Ts</u>

<u>DO</u>:

- *TRY to get their personal details if they are willing to let you have them.*
- *TAKE their information even if they don't want to let you have their personal details.*
- *ADVISE them NOT to tell others they have reported the allegation to IAPR.*
- *ASK if IAPR can act on the information without putting them or others at risk (e.g. are they the only people who could know this information?).*
- *ASK if they would be willing to be a witness, if a case went to court.*
- *KEEP any notes of your conversation securely under lock and key.*

<u>DON'T</u>:

- *ASK them to find out further information.*
- *GUARANTEE confidentiality but do assure them that IAPR will keep the information safe.*
- *PROMISE feedback on how we use the information.*
- *PROMISE a reward.*

For further information and instructions on contacts relating to the smuggling of excisable goods such as tobacco products (cigarettes & hand rolling tobacco), fuel/oils and alcohol refer to ……

<u>NOTE</u>: The remainder of this document refers <u>only</u> to CHIS.

<u>BASIC PRINCIPLES OF CHIS MANAGEMENT</u>

CHIS management must be underpinned by, at least, basic legislation. Operational activity should adhere to structures, rules and procedures to ensure the safety and integrity of the system and those who operate within it.

<u>Four Level Structure</u>

Europol suggests a four-level structure for the operational management of CHIS as follows:

<u>Level 1</u>:

Either a high-ranking Customs officer or prosecutor should be appointed to oversee the efficiency and integrity of the entire CHIS management system. They would be responsible for regular checks and audits to include all the other levels.

Level 2:

Customs should appoint an officer, of suitable rank, to maintain a register of all CHIS and take responsibility for their authorisation. This officer would be responsible for the development and maintenance of suitable internal governance policies relating to the use and security of CHIS, their handlers and controllers.

Level 3:

Customs would appoint trained controllers with responsibility for the day to day implementation of policy and the governance of recruitment, tasking and general administration of the systems. One of their primary roles would be the monitoring of the CHIS handlers as well as their relationship with their sources. The wellbeing of the handlers is of prime importance.

Level 4:

Customs would also have to appoint trained CHIS handlers responsible for the routine management of sources, in particular briefing, de-briefing and associated contact. Each source requires two handlers, its therefore essential sufficient handlers are trained to meet the perceived need.

General Principles

- A CHIS does not belong to an individual officer.
- They are a resource to be deployed for the benefit of Customs.
- No officer should encourage a CHIS to commit an offence.
- A CHIS must always be under control, properly briefed with a clear understanding of legal boundaries.
- A CHIS should not be recruited if there are insufficient handlers.
- All staff populating the structure must be properly trained.
- Only experienced officer should have responsibility for the more difficult sources.
- CHIS are entitled to protection and should be able to contact their handler at all times (duty of care).
- Senior Manager are responsible for overseeing the legality, integrity, security and safety of operations.

RULES FOR CHIS

In the vast majority of cases a CHIS is likely to either be a criminal, or be closely associated with a criminal activity or entity, if this were not the case, they would not have access to the information sought by Customs and other law enforcement agencies. Because of this they can be untrustworthy and need firm control and clear instructions on what they can and cannot do.

The relationship between the source and the handler is similar to a partnership which must be kept on a strictly professional basis. The CHIS must be in no doubt that they have responsibilities and are obliged to respect the following:

- They must be responsible for their own safety and not take any risks without consulting their handler.
- If they commit a crime whilst a CHIS, they are liable to be arrested, unless they have participating informant* status and remain within pre-defined limits.
- Appointments must be kept.
- Agreed communications methods must be complied with.
- If instructions are not clear they must seek clarification.
- They must not introduce anyone into meetings without the prior consent of the handler.
- They must let the handler know immediately if they are exposed.
- It's not the job of the CHIS to decide what information is needed; all information gathered must be forwarded.
- They should never act as an "agent provocateur", entice or entrap others.

(*: A participating informant has approval and is permitted to participate in a crime which others already intend to perpetrate. This requires not only a specific authorisation but also legislation.)

REGISTRATION

National Register

To maximise the benefits from a CHIS it would be prudent for Customs to maintain a basic national register. This should contain sufficient information for a competent audit to be done, but must not include the true identity of the source. In addition, the register would facilitate tasking, help protect against multiple registrations, identify the sources local area and included dates of registration, re-registration and de-registration.

Local Register

The local register would contain more detail than its national counterpart and ideally should be computerised for greater security.

The local register would contain the following data:

- Dates of required reviews.
- Dates when authorisations expire.
- Details of the controller and handlers as well as the dates they assumed responsibility.
- Main risks associated with the CHIS.
- Reward record.
- Central tasking requests received.
- Arrest record.
- Date authorisation withdrawn.

Registration Process

Registration is an absolute requirement. Failure to register a CHIS, and operate outside accepted practices, exposes Customs, the source and their handlers to serious and unacceptable risks.

A registered CHIS file may contain the information listed below:

- Local Customs registration.
- Notification to the National Register.
- Separate sub-files should also be maintained-
    1. True identity file: store securely away from the other information.
    2. Policy records concerning the CHIS.
    3. Records of activities.
    4. Rewards.
    5. Operational matters.
    6. Reports of all contact between the CHIS, their handlers and controller.
- All information received should be recorded evaluated and disseminated as appropriate.

RISK ASSESSMENTS

A detailed, unique risk assessment is essential at all the key stages of working with a CHIS. Each CHIS will have individual characteristics that need to be assessed and suitable control measures implemented to manage the associated risks. The risk assessment and the risk management plan flowing from the assessment are integral components of the process.

The risks associated with the deployment, management and protection of a source as well as their handlers is of paramount importance. Considerable thought must be given to the likelihood of failure and the exposure of the sources, which could have serious consequences. Since Customs has assumed responsibility for deploying the CHIS it's likely a duty of care exists; a moral duty is undoubtably created.

The type and seriousness of risks will vary on a case by case and operational basis and may be influenced by a large number of factors. The purpose of the risk assessment is for the controller to demonstrate to the authorising officer that a plan exists to manage or mitigate the risk factors. The authorising officer must not authorise a registration unless they are assured all risks have been considered and planned for.

When is a Risk Assessment Required?

- At registration/authorisation.
- On at least an annual basis.
- When applying for participating informant status.
- When requested by the controller, authorising officer or registrar, perhaps due to a change in circumstances.

Handlers and controllers have a constant, ongoing obligation to monitor risk and must complete a new risk assessment where, in their opinion circumstance have changed. Any revised assessment will be notified to the authorising officer.

Risk Assessment Considerations

When preparing a risk assessment, it may be of assistance to consider the risks by type, under a number of headings, which might include the following:

Political

- Would exposure of the source cause political embarrassment?

Community

- Would the use of the source receive public support if it became known?
- What are the motivations of the source?
- What's the impact on other law enforcement activity, other than Customs?

Psychological

- Is the source mentally fit enough for the tasking?

Physical

- What is the threat from the subject against which the source is being deployed?
- What are the risks to the source and the handlers?
- Will the source encounter dangerous, confrontational situations?
- Are there environmental threats?

Legal

- What is the legal opinion on the deployment?
- Would the judiciary protect the sources identity?
- How would the sources involvement in criminality be viewed?

Moral & Ethical

- Is there a moral and/or ethical barrier to the use of a CHIS?
- Would there be a detrimental effect on the source?
- Would less intrusive techniques yield the same results?
- Is the criminality of the source more serious than the crime being investigated (necessity and proportionality)?

The list is not exhaustive and will vary from source to source and by deployment, but it may help to isolate threats and risk that need to be managed or mitigated. It's possible, the assessment may lead to the conclusion that the risks cannot be managed and are therefore unacceptable i.e. the risks outweigh the benefits.

Psychological Support

The relationship between the handlers and the source can be both stressful and intense. It's an environment when boundaries and red lines can easily become

blurred. For these reasons its essential handlers have ready access to professional psychological support.

It may be sensible for handlers to be accompanied by the controller on some occasions when they meet with the CHIS. This will enable monitoring by the controller and help prevent manipulation by the source.

THE HANDLER

Definition

The handler is a well-trained experienced officer who will have day-to-day responsibility for contact and management of a CHIS. In addition, the handler will be responsible for the initial evaluation of material delivered by the source. Generally, the handler will work in close co-operation with the controller.

The handler must:

- ensure they are properly trained and equipped for the role.
- have an in-depth, up to date knowledge of the law, policy and procedures.
- have a good knowledge of operational security.

The handler must not be involved in the investigation of any case the source is supplying information about. It's best practice to completely separate any CHIS related function from investigations.

Responsibilities

In broad terms the handler should be aware of and manage the following:

- Maintain a professional relationship with the CHIS.
- Ensure the CHIS's welfare is always considered.
- Prepare accurate reports to make sure the source is suitably rewarded.
- Ensure a contact report is prepared following any/all interaction with the source.
- When the source is tasked the handler must ensure the source fully understands their role and the boundaries, they are to work within
- Make sure the source is compliant with the tasking authorisation.
- Prepare accurate and timely reports on the information supplied allowing the controller to evaluate and disseminate any actionable intelligence, using a standard intelligence reporting form.
- Identify opportunities to recruit new sources (talent spotting).
- Ensure the source is able to make contact whenever necessary.

Guidelines for Handler/CHIS Contact

All contact with a CHIS should comply with the following best practice guidelines to ensure the integrity and safety of the system.

- The controller must approve, in advance, all meeting with the CHIS.
- The controller must all approve all other planned contact with the CHIS.

- If advance approval is given for a sequence of contacts this decision must be recorded.
- The controller has to be satisfied all planned meetings can be conducted safely and define any appropriate conditions.
- The handler must advise the controller of any concerns they have about the ability to conduct a meeting safely.
- A log of authorised contact with the CHIS is to be maintained.
- Any ad hoc or unanticipated meetings must be notified to the controller as soon as possible.
- Two handlers must be allocated to each source.
- The source must be able to contact their handlers at all times.
- The handlers must also be able to contact the controller at all times.
- Handlers should complete signed, timed and dated contact reports as soon as possible after every contact.
- The CHIS should always be met by two handlers.

Safe Handling

The most important considerations are the safety, wellbeing and security of the source and the handlers. Any compromise will cause danger, embarrassment and make the recruitment of additional CHIS all but impossible.

Sources will come from all different levels of society, as such they have to be dealt with on an individual basis with handling carefully tailored to their social background; one size does not fit all. This bespoke approach will give the source confidence and help build trust in their handlers.

The source must never be allowed to dictate when or where a meeting is to take place. This adds a layer of protection for the handlers in the event that the motivation of the CHIS is exposing the identity of the handlers.

The location of any meeting must be thoroughly reconnoitred in advance, with the source instructed to follow a pre-determined route. A surveillance team deployed along the route will be able to ensure the source is not being followed and it's safe for the meeting to proceed. A safe method of communication with the CHIS is essential.

Cover Stories

A cover story is simply an explanation for an activity designed to mask its true purpose; it need not be complicated, but it must be plausible.

A cover story should be:

- A robust cover story should be considered by the handlers at the earliest possible opportunity.
- It should reflect the sources lifestyle.
- The location must be in keeping with the sources background; it should look and feel natural.
- The cover story has to be agreed with the source.
- It must explain why the CHIS is in a particular place, what they are doing and why they are meeting the handlers.

- The story must be rehearsed with the source, to ensure it will stand up to scrutiny.
- It must be robust and credible; ideally unremarkable and uncheckable.
- The source will need to explain why they are not at work or home and not following their usual routine.
- Explanations must be believable.

Exit Strategy

An exit strategy is a detailed plan which will allow the CHIS to safely disengage from the criminals they have been informing on, without arousing suspicion. The strategy would be implemented upon completion of an investigation or if the level of risk becomes unmanageable and the safety of the source is under threat.

The exit strategy should be planned by the handlers and source at and early stage since a situation may arise where it has to be implemented at short notice. A successful strategy will be based on the profile of the CHIS, their background and lifestyle.

THE CONTROLLER

Definition

The controller is a thoroughly trained experienced officer with responsibility for the supervision of handlers and the sources they manage. Controller should have the ability to meet sources, as required and discuss with the handlers their source management strategy. Controllers should be mindful of the needs of both sources and handlers, they are obliged to check the accuracy of all records and risk assessments.

Responsibilities

In broad terms the controller should be aware of and manage the following:

- Control, supervise and manage the source handlers.
- Maintain operational legal and ethical standards.
- Assess the suitability of rewards.
- Evaluate and disseminate information gathered. (*It's vital that when intelligence is disseminated there is nothing to indicate the presence of the source. Ideally, the intelligence should be firewalled through another intelligence unit.*)
- Conduct risk assessments.
- Closely monitor the well-being of:
    1. the source,
    2. the handler,
    3. the relationship between the two.
- Supervise the use of the CHIS.
- Match suitable handlers and sources.
- Meet sources when required.
- With the assistance of the handlers, identify and manage risk.

- Supervise the application and payment of rewards and operating expenses in accordance with legislation.
- Maintain CHIS files.
- Ensure actionable intelligence is disseminated properly.
- Ensure the security of informant information.
- Manage the secure access and retention of source files.
- Advise the authorising officer of any issues.
- Maintain and overview of local source coverage; identify knowledge gaps and recruitment opportunities.
- Review completed deployments to identify good and poor practices; learning points.
- Meet with sources on at least an annual basis.

THE AUTHORISING OFFICER

Definition

The authorising officer will be of a senior rank with responsibility for the registration and authorisation of all sources. They will ensure policies and procedures are strictly adhered to and will also fulfil governance and audit functions.

Responsibilities

In broad terms the controller should be aware of and manage the following:

- Maintain the register of sources in accordance with established principles and legislation.
- Ensure procedures are in place to record the cultivation of sources.
- Set any profile requirements.
- Manage the tasking capacity of the register.
- Liaise with other authorising officers.
- Allocate controllers to new CHIS.
- Oversee risk assessment and management.
- Responsibility for forward planning.
- Grant rewards.

INFORMANT REWARDS

Definition

A reward is a consideration in cash, goods or other benefits, from official or other sources, given to a source, or another on behalf of a source, in return for or connected with the supply of information by a source.

A benefit could include providing information to a court designed to assist in the potential mitigation of a sentence for a source who has been convicted of an offence.

Any reward to a CHIS is always discretionary, there is no automatic entitlement.

Eligibility

No reward application can be considered unless the source is registered at both the local and national levels.

Priority is given to cases where:

1. Substantial assets have been identified or are likely to be identified.
2. The most serious of cases.

Reward Considerations

In addition to the value of the intelligence provided the following factors may also be taken into consideration:

- Impact on the organised crime group.
- Volume and type of commodity seized or likely to be seized.
- Volume and value of assets identified or likely to be confiscated.
- Nature and value of the intelligence provided.
- The role played by the source, including risk.
- Future potential of the CHIS.
- Incentivisation of the source.

Timing of Reward Payments

The timing of the payment of the reward has to be given careful consideration and may be influenced by operational factors. However, the overall working of the system and the relationship between the source and the handlers will be enhanced by paying as promptly as possible. This is because:

- It demonstrates good faith on the part of the handler/controller.
- Enhance the self-esteem of the CHIS – the feel-good factor.
- Strengthens the bond between handler and source.
- Encourages the source to continue.

It's not essential, and may be undesirable, to delay payment until the conclusion of the investigation. Should this be a necessity then arrangements should be made for interim payments.

Level of Reward

The amount of effort, risk and the time taken by the CHIS to achieve the results required by the handler will vary from deployment to deployment. Similarly, the value of the intelligence to Customs is also a variable. Because of this it's not possible to formulate a standardised tariff for intelligence supplied by a CHIS, therefore it's essential to manage the expectations of the source.

Any system adopted has to be objective to:

- Reduce the opportunity for personal bias.
- Introduce consistency in the basic considerations.
- Formalise the application of management discretion.
- Supports value for money considerations.

Risk Associated with Reward

The sudden acquisition of a large sum of money requires a plausible explanation and this is a serious consideration for the handler, the controller as well as the CHIS, if the risk of exposure is to be avoided. How a payment or payments are made, and the sources explanation, must be planned for and rehearsed. If necessary, an instalment arrangement could be put in place. Alternatively, thought could be given to other non-cash rewards, for example if the CHIS is a known drug user any cash reward may be used to feed their habit.

Any reward authorisation procedure should assess suitability and appropriateness of the proposed amount and method of payment.

Reward Authorisation & Documentation

Any system must attempt, as far as possible, to balance the need for high levels of supervision, because large amounts of cash may be involved, and the risks involved.

Payments and payment authorisation should be delegated to a suitable level whilst retaining confidence in the overall governance of the system.

- The Authorising Officer/Registrar has primary responsibility.
- They should prepare clear guidance on who can pay rewards and in what circumstances.
- Controllers should have the authority to pay rewards.
- All payments must be witnessed, ideally by the controller.
- The level of the supervising officer is a reflection of the risk involved and not the amount of the reward being paid.
- The supervising officer is responsible for having a receipt signed by the source using the pseudonym allocated to the source.
- If the source refuses to sign, a report should be prepared, signed and witnessed.
- Secure, robust internal procedures for financial controls and the accounting for of monetary rewards paid to sources must be in place.

Stephen J. Henderson

Stephen J. Henderson

DG REFORM

Athens

APPENDIX 1

Access

A source is a person first and foremost and a CHIS second, as such they must be treated and handled with respect.

Initially it's important to establish, as far as possible, details of what information, especially documents and technical data, the source can access in order to evaluate their potential and understand the risks involved.

Degree of Access

- Direct Access: Consider the circle of knowledge.
- Peripheral/Fringe: May be limited.
- "Eyes and Ears": May be very limited.

Type of Access

- Current or Potential: Very important.
- Previous or Historical: May be of limited value unless it's ongoing.

Capability of the Source

- Reliability: Can be tested by corroboration or a simple tasking.
- Determination: Can require careful management.
- "Streetwise": Are they actually capable, secure and safe.

APPENDIX 2

Initial Follow Up Telephone Contact

Planning & Preparation

- Why are we contacting the HumInt?
- What are the objectives?
- Assess the HumInt and the information.
- Status of the HumInt – how do they know and who else knows?
- Prepare a list of questions.
- Personal Details of HumInt:
    1. Profile.
    2. Background checks.
    3. Separate file for true identity, will be secret when completed.
- Knowledge of Subject:
    1. Do I know enough about what the HumInt wants to talk about?
    2. Alternative strategy – find an expert.
    3. Research.
    4. Ensure value of information can be appreciated.
- HumInt Personal Details:
    1. Consider how these can be obtained.
    2. Name.
    3. Address.
    4. Date of Birth.
    5. Telephone Number – who else might answer?
- My Details:
    1. Real first name only.
    2. Work for HMRC.
    3. No family details.

- What is the HumInt likely to ask?

NOTE: An accurate and comprehensive record of ALL meetings and conversations with a source MUST be maintained. Ideally a contact report form should be completed.

APPENDIX 3

Briefing a HumInt

This would apply to an initial meeting perhaps following a telephone conversation. At this stage the source remains a HumInt, their potential is under review, they have not been tasked, therefore they are not a CHIS.

The following should be considered when briefing the HumInt prior to the initial meeting:

- The HumInt must be thoroughly briefed prior to the meeting; this will ensure they do exactly what's required.
- Explain exactly what you want them to do – be specific.
- Tell the HumInt that you will approach them – have a detailed description.
- The HumInt does not need to know what you look like.
- Arrange a warning signal.
- HumInt must bring photo identification to the first meeting.
- The HumInt must attend alone.
- Always attend with another handler – tell the HumInt there will be two officers.
- Tell the source they should not discuss this with anyone.
- Consider:
    1. How will the HumInt get to the meeting?
    2. Is there enough time?
    3. Is an interpreter required?
- Agree a cut off time with the controller.
- Advise controller immediately the meeting finishes.
- Do not carry identification.
- Prepare a contact report as soon as possible.

APPENDIX 4

Planning a Meeting with a CHIS

The following basics should always be considered:

- Always use an official vehicle and 'phone.
- The "pick-up point"/meeting place is your choice and should be a neutral location.
- The CHIS does not need to know the location of the de-brief point.
- Consider the "pick-up" and de-brief locations carefully.
- Carry out a thorough reconnaissance in real time.
- Have a Plan B.

- Consider the motivation of the CHIS – public places are safer.
- Consider tasking – based on what the CHIS says and in consultation with the controller.
- Expenses – if discussed and agreed.
- Other resources – Cover/surveillance team and additional support.
- Anti and counter surveillance.
- All arrangements must be authorised by the controller.
- Advise the controller of:
    1. The "pick-up" point.
    2. De-brief point.
    3. Timings.
    4. When the meeting will finish.
    5. What action may be required if you are late.

APPENDIX 5

Conducting a Meeting with a CHIS

The following should all be taken into account, particularly at a first meeting with a CHIS:

- Arrive at the "pick-up" point early, watch the CHIS arrive.
- Look for the safety signal.
- Introduce yourself.
- Mobile on silent.
- Check CHIS identification.
- Confirm the amount of time the CHIS has available.
- Show interest.
- Control the meeting.
- Why did the CHIS come forward?
- Do not get too close – empathise, don't sympathise.
- Maintain honesty and integrity.
- Make notes if possible.
- Establish a rapport.
- Give warnings (see Hints & Tips).
- CHIS should sign terms and conditions document.
- Don't make promises that can't be kept.
- Don't promise rewards.
- Find out about the personal circumstances of the CHIS, background and lifestyle – this will help with planning and security.
- If authorised by the controller, give tasking. Make sure the CHIS understands and won't go too far.
- Cover confidentiality – record what's said and get the CHIS to sign.
- Anything said when the co-handler is not present must be repeated.
- Confirm date and time of next contact.
- Do not leave with the CHIS.
- Use anti and counter surveillance.
- Split from the co-handler.

Subsequent Meetings:

- Source should not change routine – this could attract suspicion.
- Do not meet at the same place twice in succession.
- Always give warnings:
    1. Participation in crime.
    2. Participation in the offence.
    3. Security issues.
- Always consider the motivation of the CHIS – why have they come forward?

After the Meeting:

- Contact the controller before the cut off time.
- De-brief the controller.
- Complete all documentation – with 72 hours.
- Sanitise information in preparation for dissemination.
- Always report unplanned contact to the controller.
- Never take paperwork home.
- Remember: There is a duty of care and responsibility for the safety and wellbeing of the CHIS throughout the working relationship and beyond.

APPENDIX 6

Hints & Tips

1. Be aware of any notes/recordings made by the CHIS.
2. Ensure they are able to withstand the pressure of being a CHIS.
3. Always use anti and counter surveillance.
4. Be wary of taking documents to a meeting – no ID.
5. Avoid jargon.
6. Use open questions.
7. Get as much information as possible – probe and question.
8. Summarise.
9. Don't talk too much.
10. Don't give any personal information.
11. Take appropriate steps if CHIS has sample or evidence.

Warnings:

- MUST be given at every meeting.
- The CHIS MUST NOT:
    1. Commit or incite others to commit a criminal offence.
    2. Providing information to Customs does not give immunity from prosecution.
    3. Participation is an offence.
    4. Tell anyone about their role.

The handler must record that the warnings were given and understood, with the entry signed, timed and dated.

If the CHIS provides information about an offence they have committed:

- Do not deliver a caution.
- Stop them.
- Remind them you are an officer of law.
- Consider options?

APPENDIX 7

HMRC Structures

Source Management Units

In 1998 following corruption issues and a number of failed prosecutions HMRC adopted dedicated Source Management Units (SMU's); some of the benefits are listed below:

1. Handlers are not involved in investigations or the evidential chain.
2. Reduces the handler's exposure to the court system.
3. Reduces potential corruption.
4. Handers only manage a source for two years.
5. Better protection for the source.
6. More effective management of the source and the handlers.

National Source Unit

Above the regional SMU's is the National Source Unit with responsibility for:

1. Source policy and procedures.
2. Central co-ordination of CHIS authorisations and activities.
3. Co-ordination of disclosure and tasking.
4. Relations with external partners.
5. Represents HMRC on national and international source working groups.

Annex 7 20200616 Note of Meeting with DG Customs

NOTE OF MEETING

Date: 16th June 2020

Location: IAPR, 5th Floor, Karagiorgi Servias 10, Athens

Present: Stephen Henderson – DG REFORM (SH)

Mr. Mourtidis – IAPR, DG Customs (KM)

Maria Pagomenou – Interpreter (MP)

The meeting started as planned at 13:00.

Customs Staffing

KM advised that all Customs staff have now returned to work and are no longer working restricted hours in response to covid-19.

Reply from the Deputy Finance Minister

SH said he had met with Antonis Pyrgiotis earlier who seemed quietly optimistic that the work with the Deputy Finance Minister's Office was progressing well, and there may be some initial anti-smuggling legislation in the near future. KM replied that he's neither optimistic nor pessimistic, but he does have some concerns. However, he went on to say there are a number of more pressing issues that may delay the anti-smuggling laws.

Customs are working to some very strict deadlines, mainly associated with procurements exercises for:

- X-ray scanners,
- Laptops and tablets,
- Endoscopes,
- Weigh bridges, and
- New Software.

Some of these projects have very challenging time limits that must be adhered to or their funding will be lost. KM felt some of the delays so far were the responsibility of the Management Board, whilst others were caused by an inability to change the original funding request. Other serious issues in this regard are the IAPR's lack of a Technical Unit and only limited experience of project management. These factors have made the process very complex and slow.

Moving on, SH said the draft Surveillance Code of Practice has been completed and is being translated. This and the Human Sources Code of Practice will need to be discussed in the near future.

SH confirmed the that he will review the proposed amendments to Articles 157 and 158 of the Customs Code in due course and report to KM.

Fuel Smuggling Public Awareness Campaign

SH will enquire about this at a video conference with DG REFORM on Thursday (18/6) and update KM at their next meeting.

KOE

SH suggested that a meeting should be organised to discuss the draft KOE Road Map which he had prepared recently. KM agreed adding he would like to discuss this at a teleconference with the two EYTE Commanders. However, there may be changes in Thessaloniki and KM would like to wait until the situation is clearer, probably in July. In the meantime, SH will give some thought to a draft agenda.

SH now has a translation of the KOE Manual and will review this as soon as time allows. KM said the Manual was prepared by the Officer-in-Charge of EYTE for southern Greece, based in Piraeus. SH noted that guidance must be universal. KM agreed, adding there's some friction between commander in the south and his counterpart for northern Greece; one is very experience whilst the other is new, but has a lot of fresh ideas. KM hoped the Manual might be a way of encouraging them to work together. SH suggested this could be the subject of a separate video conference with the two officers.

It seems recruitment is still a serious issue for the KOE's especially as five new units (three on islands and two on the mainland) are planned. Only two of the existing units, Patras and Crete, are close to full compliment. The situation is especially difficult in the north.

The recruitment, transfer and re-location processes are very slow, complex and difficult, although the Governor is supportive there have been issues with the Service Board who must approve all staff movements. Both agreed this is very disappointing and frustrating.

In addition to the Codes mentioned earlier, SH will also prepare a number of shorter papers that will assist both the KOE's and officers deployed on any operational activity, especially surveillance. They will also help provide consistency which is important to KOE joint working. KM said these would be of great assistance.

Intelligence Working Group

SH said he has discussed this with Mr. Lymberis and reminded KM that the adoption of the recommendations in Working Groups Final Report were instrumental to the use of the proposed new legislation on covert techniques. These all rely on the ability to disseminate intelligence quickly, securely and to carefully, targeted recipients.

Technical Assistance

SH advised that his new contract will start on 1st July 2020, KM said he was very pleased with this outcome.

Following some general discussion, the meeting ended at 14:10.

Stephen J. Henderson

Stephen J. Henderson

Athens

16th June 2020

Annex 8 20200520 Draft Initial Surveillance CoP

SURVEILLANCE DRAFT INITIAL CODE OF PRACTICE

INDEX

INTRODUCTION

Surveillance is a unique means of gathering vital real-time intelligence capable of identifying and assisting in high impact targeted operational interventions. As such it's an important tool in combating many different kinds of criminality. However, any type of surveillance is a difficult balancing act between the needs of law enforcement and the impact it's use can have on the human rights of those targeted as well as their associates and public at large. Because of this the use of these techniques must be carefully considered, based on sound practices and field craft as well as strictly regulated and monitored.

This paper is a summary based on the Code of Practice designed to be used in parallel with the UK legislation, the Regulation of Investigatory Powers Act. It seeks to set out clearly the general principles associated with surveillance. However, before a Code of Practice for Greece can be prepared there are a number of aspects which will require to be re-visited to determine the precise interaction between the techniques employed and specific parts of the existing Greek legislation. Therefore, this paper should be considered as a starting point or framework, it is not the finished article.

GENERAL DEFINITIONS

In general terms surveillance is the monitoring and observing of a person's movements, conversations and communications. It can be done with or without the assistance or use of a surveillance device.

Surveillance becomes covert when it's carried out in a way specifically designed to ensure the subject or target is unaware of the activity.

Surveillance can be sub-divided into two distinct types:

1. Directed Surveillance: This is covert surveillance which is not intrusive and carried out as part of a specific operation or investigation. It's likely the activity will result in the gathering of some private information about any person, not necessarily the specific target of the activity.

2. Intrusive Surveillance: This is covert surveillance carried out in relation to something that may take place in a private residence or a private vehicle. It may include the use of a surveillance device. Again, in relation to a specific operation or investigation.

NOTE: Property Interference - An additional factor that must always be taken into account is the possibility of interference with private property in the course, preparation or aftermath of a surveillance operation. This is of particular importance when intrusive surveillance is being considered. It's likely this would require a separate body of law.

HUMAN RIGHTS

It's essential any surveillance activity and the legislation which underpins it is compatible and in accordance with the European Convention on Human Rights (ECHR).

Whilst some of the rights detailed in the Convention are absolute others are qualified. Broadly speaking this means it's permissible, in certain circumstances where strict conditions are satisfied, for the state to set aside these qualified rights.

The rights flowing from ECHR which are most likely to be engaged during surveillance are:

- Article 8: the right to a private life.
- Article 6: the right to a fair trial.

NOTE: As for property interference, it's possible this could impact on Article 1; the right to peaceful enjoyment of possessions.

DIRECTED & INTRUSIVE SURVEILLANCE OVERVIEW

In order for any surveillance operation to be lawful and compatible with ECHR it's important to clearly differentiate between what constitutes directed and intrusive surveillance. This may affect the level of authorisation required and whether that authorisation is the responsibility of the law enforcement agency itself or an outside independent authority.

Directed Surveillance

A surveillance operation is directed surveillance if **all** of the following are true:

- it's covert, but not intrusive;
- it's part of a specific operation or investigation;
- it's likely to result in the collection of private information about a person, but not necessarily the target of the operation.

Private Information

Private information includes any information concerning a person's private, family or business life and relationships. Conversely, non-private information may be publicly available from newspapers, websites, books etc. This would include information which is commercially available upon payment of a fee.

Although the expectation of privacy is reduced when entering a public space, it's still possible some private information may be gathered and the person may retain a reasonable expectation of privacy. This premise can be carried forward when considering information gathered from the internet where there would be some expectation of privacy associated with, for example, social media websites (see Online Covert Activity, below).

Private information will include personal information like names, addresses and telephone numbers, where the data has been gathered by means of covert surveillance of an individual when they would have a reasonable expectation of privacy. If these circumstances are likely to arise a directed surveillance authorisation is appropriate.

Vehicle Tracking Devices

The use of a devise whether designed or adapted to provide information on the position of a vehicle is not intrusive surveillance. In fact, the use of such a device on its own does not necessarily amount to directed surveillance as it only provides information about its position at a given point in time. However, this changes when use is made of this basic information which could amount to monitoring the occupants of the vehicle, or when another surveillance activity is added and its likely private information relating to the occupants will be gathered. At this point Article 8 of ECHR is engaged and a directed surveillance authorisation is required.

NOTE: Property interference authorisation may be required for the installation and retrieval of the device.

Online Covert Activity

The growth of the internet and the amount of information that's available online presents several opportunities for law enforcement agencies to gather information which can assist with investigations and operational work; it's important such information is accessed lawfully. Much of this can be accessed without any kind of authorisation, use of the internet in the preliminary stages of an enquiry are unlikely to engage with any privacy considerations. This will change if the research carried out is persistent, or where material is extracted and recorded. Some form of surveillance authorisation should be carefully considered.

The internet is a valuable tool for gathering information. Where any online monitoring is conducted covertly, and in connection with a specific investigation or operation, and private information is likely to be gathered, then a directed surveillance authorisation must be considered.

Initially, it's necessary to determine if the online activity is covert. Is there a realistic prospect of the subject knowing the surveillance is taking place? Use of

the internet, in preference to other surveillance techniques, may be seen as engaging in surveillance designed to ensure the subject is unaware.

The expectation of privacy will vary depending on the platform, so in certain instances privacy implications will be a live issue. Where an individual puts information on a publicly accessible database, like a telephone directory, they are unlikely to have any significant expectation of privacy. To a lesser extent, information posted on social media websites, specifically for the purpose of messaging or communicating with a wider audience, also carries a reduced expectation of privacy. A preliminary check of a site to see if it contains anything of interest is unlikely to interfere with a person's expectation of privacy, a surveillance authorisation is probably unnecessary. However, if data is systematically collected from a site and recorded in another place then a directed surveillance authorisation should be considered.

To determine if a directed surveillance authorisation should be sought in connection with accessing a website as part of a covert operation the primary consideration is the purpose of the online activity. The following should be considered:

- is the research, investigation or operation targeting a specific individual or organisation;
- is it likely to result in obtaining private information;
- will visiting internet sites result in the building of an intelligence profile;
- could it indicate a pattern of lifestyle;
- is the information being combined with other information relating to a person's private life;
- is it part of ongoing work involving repeated viewing;
- is it likely to result in the identification and recording of information in relation to family and friends of the subject as this would constitute collateral intrusion into the privacy of the third parties?

Aerial Covert Surveillance

When aerial surveillance is planned using an airborne device such as a helicopter or drone all the factors detailed previously must be considered in order to determine if a surveillance authorisation is appropriate.

Intrusive Surveillance

Intrusive surveillance is covert surveillance which is:

- carried out in relation to anything taking place on residential premises, or
- in any private vehicle, and
- involves the presence of an individual on the premises or in the vehicle, or
- is carried out by means of a surveillance device.

The very nature of intrusive surveillance should have the effect of restricting its availability to law enforcement agencies. In addition, its use should be approved by an authority independent of the requesting agency, with that approval subject to close scrutiny.

The definition of intrusive surveillance relates to the location of the surveillance and not the nature of the information likely to be obtained. It's assumed intrusive surveillance will result in the gathering of private information.

Residential Premises

For the purposes of surveillance legislation residential premises may be considered as any premises for the time being occupied or used by any person, including temporarily, for residential purposes or living accommodation. Specifically, this would include hotel or prison accommodation that is occupied or used. Common areas, such as hotel dining rooms, to which a person has access, are excluded.

Examples of residential premises would include:

- a rented apartment or house occupied for residential purposes;
- a prison cell;
- a hotel bedroom or suite.

Examples of premises that would not be regarded as residential include:

- a communal stairway in an apartment block;
- a police cell;
- a prison canteen;
- a police interview room;
- a hotel reception or dining area;
- the garden or driveway of premises that are visible to the public.

Private Vehicles

A private vehicle may be defined as any vehicle, including vessels and aircraft, that's primarily used for the private purposes of the person who owns it or a person having the right to use it. For example, this would include a company car owned by a leasing company but used for business and pleasure by an employee of a company.

Places Used for Legal Consultation

Surveillance carried out premises used for legal consultation, at a time when those premises are being used for legal consultation is treated as intrusive surveillance. Examples of such premises are:

- the place of business of any professional legal adviser;
- a place used for the business of a court, tribunal or enquiry.

An Additional Consideration

As discussed, intrusive surveillance is surveillance by means of a person or device located inside residential premises or a private vehicle. However, a device placed outside the residence or vehicle, and capable of delivering the same quality of detail as a device inside, also constitutes intrusive surveillance.

Activity Not Falling Within the Definition of Covert Surveillance

Some surveillance activities do not fall within the scope of either directed or intrusive surveillance and no authorisation should be sought for such activities, for example:

- covert surveillance as an immediate response to events;
- the overt use of CCTV systems.

There will be many other instances some of which will be dependent on the interaction between surveillance legislation and other bodies of existing Greek law.

GENERAL RULES ON AUTHORISATIONS

Overview

An authorisation, on condition that specific tests are met, provides a lawful basis to carry out covert surveillance which is likely to result in the gathering of private information. Also, the officer capable of granting authorisations may vary depending on the level of intrusion envisaged by the planned operation. For example, whilst it may be considered appropriate for directed surveillance to be authorised in house, by a suitably senior law enforcement officer, it might also be deemed appropriate for intrusive surveillance to be authorised by an independent member of the judiciary. This higher, independent authorisation level could be seen as providing more objective, impartial decision making.

Necessity & Proportionality

Any officer granting an authorisation for either directed or intrusive surveillance must be convinced the activity to be authorised is both necessary and proportionate to what it seeks achieve. They must be able to balance the seriousness of the planned intrusion against the need for the activity in terms of the investigation and operation. Each and every action authorised must bring a benefit to the investigation or operation and must not be arbitrary or disproportionate. No activity may be considered proportionate if the information sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should be considered:

- balancing the size and scope of the planned activity against the gravity, seriousness and extent of the perceived crime;
- will the methods to be employed cause the least possible intrusion on the subject and others;
- whether the planned activity is an appropriate use of the legislation and a reasonable course of action, having considered alternatives, for obtaining the information sought;
- evidencing what other methods had been considered and why these were not implemented, or were implemented unsuccessfully.

All officers involved in the activity must have a clear understanding of the limitations of the authorised activity.

An authorisation application must be balanced; it should present the facts in a fair way taking into account information which may weaken the application.

Collateral Intrusion

As well as taking into account proportionality and necessity the authorising officer must also consider the risk of obtaining private information about persons who are not the intended subject of the surveillance operation – collateral intrusion. This is especially important when the perceived risk concerns religious, medical, journalistic or legally privileged material, or where communication between a Member of Parliament and another person is involved.

All practicable steps should be taken to minimise the intrusion into the privacy of those who are not the intended subject of the surveillance. Where the collateral intrusion is unavoidable, the activity may still be authorised, on condition the collateral intrusion is thought to be proportionate to what the operation is seeking to achieve. This same proportionality test applies to the anticipated collateral intrusion into the privacy of the intended target of the surveillance.

All applications must include an assessment of the risk of collateral intrusion and details of the measures to be taken intended to mitigate that risk. This will allow the authorising officer to fully consider the proportionality of the planned operation.

In order to properly and fully consider collateral intrusion, the authorising officer should be given detailed information regarding the potential scope of the surveillance. This should include the likelihood that any equipment or software to be deployed may cause intrusion on persons or property other than the intended subject of the application. If an automated system, like an online search engine, is to be used to obtain information, the authorising officer must be aware of its possible limitations. Any material not necessary or proportionate to the objectives of the operation or investigation should be discarded, or securely retained. The authorising officer should also consider safeguards for the handling, retention or destruction of such material in accordance with data protection obligations.

In cases where the intention is to access social media and other online accounts, and where permission to access the account has been given by the owner, consideration will have to be given to whether the account contains information about others who have not consented. If it's likely private information will be gathered a directed surveillance authorisation should be considered. This is of particular importance if the intension is to monitor the account going forward.

Collaborative Working

The authorising officer should also be aware of any specific sensitivities in the local community which could affect the planned operation, or if another law enforcement agency is undertaking a similar activity. It's good practice for the authorising officer to consult with a senior police officer within the local force area.

Where one law enforcement agency is acting on behalf of another the tasking agency will ordinarily be responsible for arranging the necessary authorisation.

Where ever possible law enforcement agencies should avoid duplication of authorisations forming part of a single investigation or operation. Whilst duplication is unlikely to affect the lawfulness of the activity it may create an unnecessary and unwelcome administrative burden.

Reviewing Authorisations & Warrants

Regular reviews of authorisations are required to assess the need for the surveillance activity to continue. The results of these reviews must be retained for a suitable, statutory period of time. In particular, frequent reviews are important in instances where the surveillance involves a high degree of intrusion into private life, or significant collateral intrusion, or confidential material is likely to be gathered. The frequency of reviews should be taken into account by the authorising officer at the outset.

Any changes, whether planned or unforeseen, to the nature or extent of the activity and that might result in further intrusion into private life should be notified to the authorising officer by means of a review. The authorising officer can then assess the changes before approving or rejecting them.

Where the directed or intrusive surveillance authorisation is in respect of individuals whose identity is not known at the time of the application, and where they are subsequently positively identified, the authorisation should be amended, at a review, to include the identities. It would be appropriate to convene a review specifically for this purpose.

During a review the authorising officer may cancel specific aspects of the authorisation. For example, terminate surveillance targeting a specifically named individual or discontinuing the use of a particular tactic.

General Best Practice

The following guideline may be considered as best practice:

- applications should avoid repetition of information;
- the information contained in an application should be limited to what the legislation and any associated code of practice requires;
- the application must be fair and balanced, taking account of information that either supports or weakens the application;
- where authorisation is granted orally, under urgent provisions, the applicant and the authorising officer must record the activity authorised and the reason the use of urgent procedures was necessary;
- if other law enforcement agencies are to be involved in the activity they must be detailed in the application.

In addition, it's considered good practice that within each law enforcement agency a senior officer should be responsible for:

- the integrity of the processes in place;
- compliance with all the relevant legislation;

- oversight of the reporting of errors to the appropriate statutory body, as well as identification of the cause of the error and remedial measures taken to avoid repetition
- engagement with the appropriate regulatory body and implementation of any recommendations;
- ensuring all authorising officers are of an appropriate standard.

Covert surveillance of a CHIS

It may be deemed necessary to deploy covert surveillance against a potential or authorised CHIS. For example, as part of the process of assessing their suitability for recruitment or deployment. In these circumstances a directed surveillance authorisation may be justified under Article 8 of ECHR.

AUTHORISATION PROCEDURES FOR DIRECTED SURVEILLANCE

Authorisation Criteria

An authorisation for directed surveillance may be granted when the authorising officer believes the planned surveillance activity is necessary when considered in the circumstances of the particular case or investigation. In addition, the activity must be in accordance with statutory criteria, which in turn should recognise ECHR.

For example, the criteria in UK legislation are as follows:

1. in the interests of national security;
2. for the purpose of preventing or detecting crime, or for preventing disorder;
3. in the interests of the economic well-being of the UK;
4. in the interests of public safety;
5. for the purpose of protecting public health;
6. for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
7. for any other purpose prescribed by an order made by the Secretary of State.

From the UK criteria it's clear reasons 2 and 6 are most appropriate to Customs work. Although the criteria in Greece would probably be different depending on the extant legislation, something along these lines of these criteria may be considered. However, any criteria are adopted would still have to be compliant with ECHR.

The authorising officer must also believe the surveillance is proportionate to what the operation seeks to achieve.

Information to be Provided in Applications

An application for directed surveillance will ordinarily be in writing and should describe the activity to be authorised as well as the purpose of the investigation or operation. The application should include:

- the reason why the authorisation is necessary in relation to the particular investigation or operation;
- the statutory grounds;
- the nature of the surveillance;
- the identities, where know, of the intended subject of the surveillance;
- a summary of the intelligence case;
- an explanation of the information sought as a result of the surveillance;
- details of any collateral intrusion and why that intrusion is justified;
- details of any confidential or privileged information that's likely to be obtained as a consequence of the surveillance;
- where the purpose, or one of the purposes, of the authorisation is to obtain information which is subject to legal privilege, a detailed assessment of why there are exceptional and compelling circumstances which make this necessary;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve; and
- the level of authorisation required for the surveillance.

Authorisation Procedures

The responsibility for authorising directed surveillance rests with the authorising officer and requires the personal authorisation of that officer. Authorisations must be in writing, with the exception of urgent cases, where authorisation may be given orally, or in writing by an officer entitled to act only in urgent cases.

Where an authorisation for directed surveillance is combined with an authorisation for intrusive surveillance, that requires a higher authorisation level, perhaps from a member of the judiciary or an independent external body, the authorisation must be issued by the higher authorising officer.

Ordinarily an authorising officer would not normally have responsibility for authorising operations which they are directly involved with. However, this may be unavoidable in cases of urgency or for security reasons. In these circumstances the records of the authorisations should be made available to any inspecting body at their next inspection.

Urgent Cases

Authorisations will normally be given in writing. However, in urgent cases oral authorisation may be provided by the authorising officer. In these circumstances the applicant must make a written record of the authorisation as soon as is practicable, and this must include information on the activity authorised.

Alternatively, in an urgent case, when it not possible for the authorising officer to consider the application, authorisation may be given by a person entitled to act as an authorising officer only in urgent cases.

An authorisation is not regarded as being urgent unless the time that would elapse before the authorising officer is available to consider the application would, in the judgement of the person applying for the authorisation, be likely to endanger life or jeopardise the investigation for which the authorisation is sought. An authorisation is also not regarded as urgent if there has been delay caused by either the authorising officer or the applicant.

In urgent cases the information mentioned above may be supplied orally. The authorising officer and the applicant should record the following information, in writing, as soon as is practicable:

- the identities of the subjects of the surveillance;
- the nature of the surveillance;
- the reason the authorising officer considered the case to be so urgent that oral rather than written authorisation was given; and
- were written authorisation has been given by an officer entitled only to act in urgent cases the reason why the application could not be submitted to the usual authorising officer.

Duration of Authorisation

An authorisation in writing granted by the authorising officer will automatically cease to have effect, unless renewed or cancelled after a specific period laid down in statute. In UK legislation this period is generally three months, beginning on the day the authorisation took effect. Even if it's anticipated the authorised activity will require less time than allowed by law the statutory time this period should still be applied; there should be a review at an interval in keeping with the expected duration, and the authorisation cancelled when it's no longer required.

In UK legislation, urgent authorisations, unless they are renewed, will cease to have effect after 72 hours, beginning from the time the authorisation was granted.

Renewals

When deciding whether to renew an authorisation for directed surveillance the authorising officer must take into account the same criteria they would consider if it were a new application.

At any point in time before an authorisation for directed surveillance would cease to have effect and the authorising officer considers it necessary for the authorisation to continue, for the purpose for which it was originally granted, they may renew it in writing for a further statutory period. In urgent cases renewals may be granted orally and would last for 72 hours, in the UK. The renewal comes into effect at the point when the previous authorisation would have expired. A renewal application should not be made until a short time before the original authorisation is due to end.

All applications to renew a directed surveillance application should record at the time, or in urgent cases as soon as practicable:

- is it a first renewal, if not the date of every other renewals;
- any significant changes from the information in the original application;
- the reasons why the authorisation for directed surveillance should continue;
- the content and value to the investigation or operation of the information gathered to date from the surveillance;
- whether any privileged or confidential material/information has been obtained;
- the results of the regular reviews of the investigation or operation.

Authorisations can be renewed more than once provided they remain necessary and proportionate and meet the criteria for authorisation. Details of all renewals should be held centrally.

Cancellations

The authorising officer must cancel the directed surveillance authorisation if they consider it no longer meets the criteria upon which it was originally authorised. If the original authorising officer is not available this can be done by the officer who has taken over or a person acting as authorising officer.

Officers actioning an authorisation must ensure these are reviewed and let the authorising officer know as soon as they consider the authorisation is no longer necessary or proportionate and so should be cancelled. As soon as the cancellation decision is made all those involved must be instructed to cease the directed surveillance of the subject as soon as reasonably practicable. The date the authorisation was cancelled should be centrally recorded as well as the instruction to terminate surveillance. It's good practice to retain details of the product of the surveillance and whether or not the objectives were achieved.

AUTHORISATION PROCEDURES FOR INTRUSIVE SURVEILLANCE

Because of the elevated intrusion associated with this type of covert surveillance its authorisation, in UK legislation, is different from the authorisation of directed surveillance. The rank of the authorising officer is more senior and the criteria for its use much narrower; its use is reserved for the investigation of the most serious crimes.

Authorisation Criteria

Using the UK as an example, intrusive surveillance is only available to a small number of agencies and can only be authorised by a senior authorising officer within that agency or in specific instances a government minister. Some believe intrusive surveillance should always be authorised independently of the agency seeking to carry out the surveillance and this could be something Greece may wish to consider.

A senior authorising officer may only authorise intrusive surveillance if they believe the application meets the limited statutory criteria. For example, the statutory criteria used in the UK legislation are as follows:

1. the authorisation is necessary in the circumstances of the particular case on the grounds that it is:
    - in the interests of national security;
    - for the purpose of preventing or detecting serious crime;
    - in the interests of the economic well-being of the UK, and
2. the surveillance is proportionate to what is sought to be achieved by carrying it out.

Like directed surveillance, the criteria in Greece would be different depending on pre-existing laws, but the overarching principle is they must be compliant with ECHR.

In addition, the authorising officer when deciding if the authorisation is necessary and proportionate must also consider if the information sought could reasonably be obtained using other less intrusive means.

Information to be Provided in All Applications

Applications will be in writing, unless urgent, should describe the intrusive surveillance to be authorised as well as the purpose of the investigation or operation. The application should specify:

- the reason the authorisation is necessary in the particular case and the statutory grounds;
- the nature of the surveillance;
- where known, the residential premises or private vehicle that the surveillance will target;
- the identities, where known, of the subject of the surveillance;
- an explanation of the information it's hoped will result from the surveillance;
- details of the potential collateral intrusion and why the intrusion is justified;
- details of any confidential or privileged information likely to be obtained as a consequence of the surveillance;
- where the purpose, or a purpose, of the authorisation is to obtain information subject to legal privilege, a detailed assessment of why there are exceptional and compelling circumstances that make this necessary, and
- the reason the surveillance is thought to be proportionate to what it seeks to achieve.

Urgent Cases

Whenever possible the senior authorising officer should give their authorisation in writing. However, in urgent cases, oral authorisation may be given by the senior authorising officer or their deputy. A statement that the activity has been authorised should be recorded in writing at the earliest opportunity by the applicant, together with the required information.

Where neither the senior authorising officer or their deputy is available then the urgent application may be granted in writing by an officer entitled to act only in urgent cases.

A case will not normally be regarded as urgent unless the time that would elapse before the senior authorising officer would become available to grant the authorisation would, in the judgement of the applicant, be likely to endanger life or jeopardise the operation for which the authorisation is sought. An authorisation is not urgent where there's been neglect or the urgency is of the authorising officer or applicant's own making.

In urgent cases the information noted above can be supplied orally. In addition, the applicant should also record the following in writing as soon as possible:

- the identities, where known, of the subjects of the surveillance;
- the nature and location of the surveillance;
- the reason the case is considered as urgent and that oral rather than written authorisation was given; and/or
- the reason it wasn't considered practicable for the application to be considered by the authorising officer.

Notification to a Judicial Commissioner

Under the UK legislation, where a person grants, renews or cancels an authorisation for intrusive surveillance, they must, as soon as is practicable give notice in writing to the Judicial Commissioner.

In urgent cases, the notification must also specify the grounds for believing the application is urgent. Urgent provisions must not be used as a matter of routine. If the Judicial Commissioner is not satisfied the urgent provisions are met, they have the power to quash the authorisation.

Judicial Commissioner Approval

In UK law, with the exception of urgent cases, an authorisation for intrusive surveillance, granted by a senior authorising officer, will not come into effect until it's been approved by a Judicial Commissioner and written notice has been given to the authorising officer.

When an authorisation is urgent it will take effect when notice is given to the Judicial Commissioner.

On occasion a case may become urgent after approval by the senior authorising officer but before a response is received form the Judicial Commissioner. The authorising officer must notify the Judicial Commissioner that the case is now urgent; in these cases, the authorisation will take effect immediately.

Duration of Intrusive Surveillance Authorisations

Under UK legislation a written authorisation granted by a senior authorising officer will cease to have effect, unless renewed, at the end of a period of three months from the day the authorisation took effect. For example, an authorisation granted on 12th February will expire at 23:59 on 11th May.

In urgent cases oral authorisations, unless renewed, will cease to be effective after a period of 72 hours beginning at the time, they took effect.

Renewal of Authorisations

If, at any point prior to the expiration of an authorisation the authorising officer considers the authorisation should continue to have effect, for the purpose for which it was originally granted, they may renew it in writing for the additional three-month period allowed under UK law.

Just like the initial authorisation approval must be sought from the Judicial Commissioner; the renewal will only be effective once this approval is received.

Information to be Provided for all Renewals of Authorisations

All renewal of an intrusive surveillance application should contain the following:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information provided previously;
- the reasons why it's necessary to continue the intrusive surveillance;
- details of any confidential or privileged information likely to be gathered as a consequence of the surveillance;
- where the purpose, or one of the purposes, of the authorisation is to obtain legally privileged information, an assessment of why there continues to be exceptional or compelling circumstances;
- the content and value to the operation of the product obtained by the surveillance to date;
- the results of any reviews.

Authorisations may be renewed more than once, if required. Details of all renewals should be held in a central record.

Cancellations

The senior authorising officer who granted or last renewed an authorisation must cancel it if they consider the surveillance no longer meets the criteria upon which it was authorised.

As soon as the decision is made that the intrusive surveillance is to cease an instruction must be given to those involved to terminate surveillance as soon as practicable. The cancellation date should be recorded centrally along with the instruction to cease. Good practice indicates that a record of the product obtained from the surveillance should be retained whether or not the objectives were achieved.

The Judicial Commissioner must be notified of the cancellation.

Authorisations Quashed by the Judicial Commissioner

When an authorisation is quashed or cancelled by a Judicial Commissioner the senior authorising officer must instruct all those involved in the intrusive surveillance to cease. Details of the date and time of the instruction should be retained.

RECORD KEEPING

Directed & Intrusive Records of Authorisation

As a matter of best practice, it's prudent to maintain a central, retrievable record of all authorisation for a statutory period; this is three years in the UK. The record should be updated when an authorisation is granted, renewed or cancelled and should be made available to any regulatory body responsible for monitoring surveillance activities.

The record should contain the following information:

- the type of authorisation;
- the date the authorisation was granted;
- the unique reference number (URN) assigned to the investigation or operation;
- the investigation/operation name, including a brief description and the names of the subjects, where known;
- if the urgency provision where used and why;
- the dates of any reviews;
- the dates of any renewals, including the name and rank of the authorising officer;
- whether the activity is likely to result in obtaining confidential or privileged information;
- was the authorisation granted by an officer directly involved in the investigation;
- the date the authorisation was cancelled;
- whether any application has been refused, including the grounds for refusal.

The following documentation should also be stored centrally during the statutory retention period:

- a copy of the application and authorisation as well as any supplementary documentation and the approval granted by the authorising officer;
- a record of the period the surveillance took place;
- the frequency of reviews;
- copy renewals along with any supporting documentation;
- the date and time when instructions were issued to cease surveillance;
- the date and time of any other instructions issued by the authorising office.

Retention of Records

Where there's a statutory independent organisation tasked with monitoring the conduct of surveillance all records of operations must be retained for a suitable period of time. These should be made available to the monitoring authority on demand in order for them to carry out their statutory obligations. This is particularly relevant in instance where there's been a complaint or an error.

Errors

The scope and frequency of errors can be reduced through adherence to robust processes and procedures. Any errors discovered may be reviewed by a senior officer with a full written record retained.

An error becomes a relevant error when it's a failure to comply with the legislation to the extent that the error must be made known to the independent monitoring authority. Examples of relevant errors would include circumstances where:

- surveillance has taken place without lawful authorisation;
- there's been a failure to adhere to safeguards.

Errors can have very serious consequences for affected individuals and must be reported to the relevant authority within a pre-determined timescale. Where it's not possible to provide full details of the error in the initial report these must follow within a reasonable period of time. The preliminary report should include details of the measures being taken to establish the full facts surrounding the error and when it was uncovered.

The report should clearly set out the facts and include:

- information on the cause of the error;
- the amount of surveillance conducted;
- material obtained;
- any unintended collateral intrusion;
- any analysis or action taken;
- whether material has been retained or destroyed, and;
- a summary of steps taken to prevent any recurrence.

This will enable the monitoring authority to issue guidance.

Errors can also arise in relation to information obtained that subsequently proves to be incorrect, but has been acted on in good faith. Although this may not constitute a relevant error it should still be brought to the attention of the monitoring body.

SAFEGUARDS

Safeguards refers to the procedures that need to be put in place to protect material gathered in the process of directed or intrusive surveillance. This material may include private and confidential material or material subject to legal privilege or journalistic material. Much of the treatment of these types of material will be dependent on existing legal definitions which may already exist in Greek law and how these may interact with surveillance legislation; this may require some form of legal review.

It's important the handling of information obtained by means of covert surveillance is compliant with the relevant legal frameworks. Any interference with privacy has to be justifiable and in accordance with Article 8(2) of ECHR and Data Protection legislation. Doing so will ensure the handling of this type of private information will remain lawful, justified and strictly controlled; as well as

subject to robust, effective safeguards. The safeguarding measures put in place must be notified, in detail, to the independent monitoring body.

Any breaches of these safeguards should be reported immediately. Similarly, beaches of a data protection nature should be reported to the relevant, responsible authority.

Safeguarding measures should be subjected to regular review and scrutiny to ensure they are up to date, relevant and fit for purpose.

Dissemination, copying and retention of material should be kept to the minimum required for authorisation purposes. For example, material that:

- is or likely to become necessary for a statutory purpose relating to covert surveillance;
- is necessary to the function of the monitoring authority;
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of a function in accordance with the legislation.

Whether information resulting from covert surveillance activity can be used in an investigation other than the investigation for which it was intended would, possibly, be reliant on any existing legislation governing the use, retention and dissemination of such material, as well as rules relating to the evidential chain.

OVERSIGHT

To effectively regulate and monitor the legitimate use of the processes and procedures detailed in this paper it's essential there is a statutory requirement for an entirely independent, impartial body tasked with ensuring compliance. In addition, the independent body must be properly staffed and resourced with the ability to carry out both scheduled and random inspections as well as having the legal authority to review records and intervene when this is deemed necessary.

In the interests of transparency, it may be considered in the public interest for the independent monitoring body to prepare an annual report, initially for the Government, but also made available to the public having been suitably redacted.

COMPLAINTS

Finally, there should be a mechanism where people who have been the subject of covert surveillance and have concerns are given the ability to voice those concerns and feel confident their complaint will be dealt with fairly.

This could be achieved by setting up a tribunal which is independent of the Government, possible comprising retired members of the judiciary. In summary, such a tribunal should have the ability investigate, hear evidence and deliver legally binding rulings.

Stephen J. Henderson

Stephen J. Henderson

DG REFORM

Athens