

Food Crime Intelligence Bureau

Introduction to Intelligence and the

Submission of 5x5x5 Intelligence

Information Reports

1. Introduction

One of the aims of Food Standards Scotland (FSS) is to help protect the public from risks to health which may arise through the consumption of food. In that respect, FSS are defined in law as a ‘competent authority’ and an ‘enforcement authority’ to implement and monitor Scottish and EU food and feed regulations.

In support of this, the Food Crime Intelligence Bureau (FCIB), which is part of the Scottish Food Crime and Incidents Unit (SFCIU), is the gateway for intelligence which can inform on emerging trends and risks. The unit also looks to develop intelligence to support investigations relating to food crime.

In order for this to be successful, all FSS staff and partners have a role to play in providing intelligence. During the course of day to day business you may become aware of food fraud and/or regulatory issues by witnessing such activity or you may be approached by third parties who wish to ‘whistleblow’ on wrongdoings at their places of work, etc.

There is no point keeping that information to yourself – it needs to be reported and passed onwards in order for the information to be analysed and actioned appropriately.

This can simply be done by submitting information to the FCIB.

2. What is intelligence?

Intelligence can be described as information that has been subject to a defined evaluation and risk assessment process, in order to assist decision making.

3. How do I submit intelligence?

A national protocol derived from the National Intelligence Model (NIM) exists between law enforcement agencies regarding the recording and handling of intelligence:

* to ensure consistency in its assessment,
* protection of the source of the information,
* how the intelligence can be actioned; and
* confidence with intelligence sharing.

This protocol is commonly known as the ***5x5x5 Information Intelligence Report*** ). This process provides an assessment of the intelligence in 3 areas with 5 options for each, hence the term 5x5x5:

 1.       An evaluation of the Source **(S) – (A – E)**

 2.       An evaluation of the veracity of the information **(I) – (1 – 5)**; and

 3.       An evaluation of the Handling Sensitivity – Handling Code **(H) – (1 – 5)**

These three areas can be divided and explained as follows:

1. Evaluation of the Source

The evaluation of the source refers to the assessment given to the person, agency or technical equipment that provides the information. It is important this evaluation is made separately from an evaluation of the information itself, and, as with the other areas, it is also important the evaluation is not influenced by personal feelings or bias. The source characteristics which may influence the grading given can include qualities such as the source’s personal characteristics/circumstances, the quality of data recorded, or the reliability/professional capabilities of the agency providing the information.

The possible gradings for this part of the assessment are:

 A.  **Always Reliable** (100%) – This is only used when there is no doubt as to the authenticity, competence and reliability of the source. Usually, this grading will only be used where the information source is ‘technical’ rather than human (such as surveillance video, scientific data, etc.)

 B.  **Mostly Reliable (70%)** – This grading is the most commonly used and relates to a source which has, in the majority of instances, proved reliable. This may refer to FSS staff and regular informants who have proven reliable previously.

 C.  **Sometimes Reliable (30%)** – This grading is used where the source has proved to be reliable on occasion but also unreliable at times.

 D.  **Unreliable** – This refers to information from a source which has routinely proved to be unreliable in the past. There may be some doubt regarding the authenticity, trustworthiness or motive of the source.

 E.  **Untested Source** – Sometimes it will not be possible to make an informed decision as to a source’s reliability. Information from Crimestoppers, for example, is second hand and anonymous and so will be graded E. This does not mean that it cannot be used, but should be treated with caution and corroborated with more reliable information if possible.

2. Evaluation of the veracity of the information provided

The evaluation of the information provided requires an assessment of the circumstances in which the information was collected. This provenance is vital and assists greatly in assessing how genuine and reliable the information is.

 1. **Known to be true without reservation** – This information will often be collected by technical surveillance or witnessed first-hand by a FSS officer or partner.

 2.  **Known personally to the source but not to the officer** – This grade is used where the information is second hand usually comes from a non-law enforcement source, such as information from a witness. It is important to differentiate between what the source knows to be a fact and what a source heard through the ‘grapevine.’

 3. **Not known personally to the source but corroborated by information already recorded** – This is information that has been passed to a source from a third party, but is backed up by other information. It is the responsibility of the person submitting the intelligence to establish the corroboration of the information before using this grading.

 4. **Not known personally to source and cannot be corroborated** – This coding would be used if the source has received the information, but there is no way of cross referencing it to other information. The reliability of this information cannot be judged and must be treated with caution.

 5. **Suspected to be false or malicious** – This information is known or suspected to be deliberately untrue. Any information with this code should be corroborated with other information and should be handled with extreme caution.

3. Evaluation of Handling Sensitivity – Handling Code

The final assessment is designed to provide an initial risk assessment prior to disseminating the information. They allow the intelligence officer to decide whether or not to disseminate the information and, if so, to whom.

**1.** The first handling code permits dissemination to UK Police Services and other law enforcement agencies as specified. The use of this code permits dissemination to a wide range of police and law enforcement agencies, but only those agencies with a specific need to know the information will receive it.

**2.** The second handling code permits dissemination to UK-non prosecuting parties. This code allows for the dissemination of information to partner agencies. The information can be disclosed in full or just certain selections from it.

**3.** The third code permits dissemination to non EU foreign law enforcement agencies.

**4.** The fourth code restricts the dissemination of the intelligence to within the originating agency. Information with this code must be reviewed to ensure that dissemination can take place at the earliest possible point. This code should never be used as the default handling code.

**5.** The final handling code permits dissemination, but requires the receiving agency to observe specified conditions of handling and dissemination. This code should not be overused, and should only really be considered if there is a clear risk of harm to the source, operation or technique.

4. Using the 5x5x5 Gradings

The correct grading of the intelligence submission is extremely important in order to allow a proper assessment of the information, to inform how the information can be used and whether it is permitted to share the information with partners. Therefore a submitted 5x5x5 must contain one grading from all the 3 evaluations described earlier, e.g.

* **Evaluation of Source** - If a trusted individual (source) from within industry who has previously provided information which has proved to be reliable

– the first grading would be **B**

* **Evaluation of the Information** - If the information was known to the source (they were present and saw the actions they are reporting on) but not known to the FSS officer receiving the information

- the second grading would be **2**

* **Handling Sensitivity and Handling Code** – This determines who, if anyone, can receive the information. If the information received can be shared with all partners without concern of compromising the source or investigation

- the third grading would be **1**

Therefore the completed log would be graded **B21.**

5. How do I complete the 5x5x5 Intelligence Report Form

The form is a series of boxes which should be completed by the person who received the information. For quickness, it can be found in the FSS website by inputting **Intelligence Form** in the search field.

The body of the text must NOT identify the source of the information.

A separate Intelligence Provenance Form should be completed, whereby the personal details of the source is recorded and comprehensive detail surrounding how the source knows the information and the Officer’s opinion of the credibility and reliability of the source and information received. Again, this form can be found in the FSS website by inputting **Provenance Form** in the search field.

The intelligence must be succinct and accurate, to include the date the information was received, where applicable full names, dates of birth (if known), full postal addresses, vehicle makes and registration numbers. If only scant detail is known efforts must be made to clarify the intelligence, e.g. if a nickname is used by the source establish their proper name.

This type of information will allow for a proper assessment of the intelligence and its subsequent development and action.

If in receipt of information relating to unconnected events or persons, it MUST be recorded on separate intelligence forms. It is important the completed report is not a running log of various events and is put together in a logical and easy to understand manner.

If using technical terms, make sure the recipient of the information will understand the terminology used. It is also important that abbreviations are not used to avoid any misinterpretation.

Detailed below is some suggested text to provide an example of how intelligence could be recorded on a 5x5x5 Information Intelligence Form:

‘*Intelligence received on 22/02/2016 provides that*

 *Joe BLOGGS*

*Born 01/02/1970*

*Farmer*

*Pilgrim Farm*

*Union Street*

*Aberdeen*

*AB10 1BT*

*is believed to be involved in the faciliting of the illegal slaughtering of cattle.*

*He is understood to be using his green Ford Transit van VRM ABC123 to transport injured cattle from numerous meantime unidentified farms in the Aberdeenshire area to*

*North East Abattoir Ltd*

*North Street*

*Dundee*

*DD12FT*

*where the cattle are being slaughtered out with the normal operating hours of the business so the Vets and Inspectors are unaware.’*

This log has been graded **E41** as:

**E** – the information was received from untested source

**4** – the information cannot be judged as it came from an anonymous source

**1** – the information was not sensitive in nature and was suitable for sharing with partners.

The detail provided in the 5x5x5 was sufficient to inform who is doing what, where, how and when without compromising the source of that information.

The completed 5x5x5 Information Intelligence Report and the Provenance Report should be forwarded by email to:

FoodCrimeIntelligenceBureau@scotland.gsi.gov.uk

6. Conclusion

The flow of intelligence is critical for FSS to function effectively in identifying emerging risks and identifying potential criminal activity which may adversely affect consumers.

This is an area where you can make a positive contribution by submitting intelligence whenever information becomes known to you. Do not feel embarrassed to submit information you may deem is not important enough - let the FCIB be the judge of that. You never know what is already known and that small piece of information which you provided could be the key.

At any time, telephone the unit (01224 288364) for advice or guidance.

Food Crime Intelligence Bureau

March 2016