5.3.6 Case and Custody

The details of people in police custody are an important source of information that may have an intelligence value. It is essential that the personal details of all detainees are verified to ensure the accuracy of the person record. Any details held on the custody record, for example, visitor details, contact telephone numbers or unique characteristics of the detainee should also be considered in relation to its possible intelligence value. This evaluation may occur automatically but, in other circumstances, the information may need to be recorded onto a 5x5x5 for input into the intelligence business area.

5.3.7 Incident Records

An incident report is usually the first record relating to a particular crime or incident. Once the report is recorded, it should be considered and evaluated for its intelligence value. Forces should comply with the NSIR when recording incidents.

Calls from the public for assistance or reports of incidents are initially managed through force or BCU command and control systems. Such reports are evaluated for their accuracy before being assessed for the level of policing response necessary. Incident reports are also managed through a priority assessment process, identifying the urgency of the response required. For further information on the standards which apply, see
http://www.homeoffice.gov.uk/rds/countrules.html

Many forces have adopted an immediate incident research capability or bureau (IRB). The IRB is responsible for conducting immediate research on the details of incident reports relating to high-risk issues, by examining all other business area records relevant to the report. The IRB ensures that all officers attending incidents are informed of any risks they are likely to face on attending the location or dealing with the subject of the report.

5.3.8 Firearms Licensing

Information contained in the NFLMS will be subject to the principles of evaluation in **5.2 Principles of Evaluating Police Information.** The information held within this business area may link to records held in other business areas and could provide potential intelligence, for example, the reasons for a firearms licence revocation.

For further information on the management of intelligence from CHIS and covert deployments, see ***ACPO and HMCE (2004) Manual of Standards for CHIS*** and ***ACPO and HMCE (2004) National Standards in Covert Investigations Manual of Standards for Surveillance.***

1.4.4 Source Evaluation

SOURCE EVALUATION	**A** Always Reliable	**B** Mostly Reliable	**C** Sometimes Reliable	**D** Unreliable	**E** Untested Source

Source reliability refers to the assessment given to the person, agency or technical equipment providing the information/ intelligence. The source reliability is assessed initially by the person recording the information and should be completed in all circumstances. Source evaluation is not a static process and should be subject to continual review. This will affect the whole of the information management process, particularly sharing information and the need for retaining it.

The assessment of the source should be based, as far as possible, on objective knowledge of the source as it will affect both the evaluation of the information recorded and any potential actions based on the information.

The 5x5x5 provides five gradings in respect of source evaluation.

A – ALWAYS RELIABLE

There is no doubt of the authenticity, trustworthiness and competence of the source. Information has been supplied in the past and has proved to be reliable in **all** instances. This grading should only apply to cases where reliability can be assured. This means that it will not be used frequently as a source evaluation. It is normally used only for information received from technical products, eg, DNA, interceptions, fingerprints and not usually for information gained from people, however unimpeachable, due to the possibility of human error. Even with technical products, its use should be carefully considered due to the risk of errors arising from interpretation.

Officers should remember that as this MoPI advice is a public document, then disclosure of a 5x5x5 with an A evaluation would carry a clear risk of a technical source being compromised.

1.4.5 Information/Intelligence Evaluation

INFORMATION/ INTELLIGENCE EVALUATION	**1** Known to be true without reservation	**2** Known personally to the source but not to the person reporting	**3** Not known personally to the source but corroborated	**4** Cannot be judged	**5** Suspected to be false

It is essential than any information received or recorded should be evaluated for reliability. The evaluation will involve using objective professional judgement, and the value of the information must not be exaggerated to encourage that action be taken. The assessment of the reliability of the information will be based on the person recording it and their knowledge of the circumstances at that time.

The 5x5x5 provides five information/intelligence evaluation gradings.

1 KNOWN TO BE TRUE WITHOUT RESERVATION

This could be information generated from a technical deployment or an event which was witnessed by a law enforcement officer or prosecuting agency. Information received from technical deployments should be treated with caution as although the information may have been recorded accurately the content may be misinterpreted. This grading refers to first-hand information.

Example: An officer witnessed an incident or refers to live evidence.

2 THE INFORMATION IS KNOWN PERSONALLY BY THE SOURCE BUT NOT TO THE PERSON REPORTING

Information under this grading is believed to be true by the source although is not personally known to be so by the person recording the information. The information is provided second hand.

Example: A CHIS giving information which they know of first hand, to the person recording the information.

3 THE INFORMATION IS NOT KNOWN PERSONALLY TO THE SOURCE BUT CAN BE CORROBORATED BY OTHER INFORMATION

Information given may have been received by a source from a third party and its reliability has been corroborated by other information, eg, CCTV, other force systems.

Example 3:

5x5x5 report – From a camera installed at premises looking onto 1 High Street, Anytown, John Doe called on Fred Smith at 11:00 hrs on Tuesday 12 January and Smith passed a package to Doe.

Problem – This reveals a technical source and could reveal its location.

Best practice – Intelligence indicates that John Doe collected a package from Fred Smith on Tuesday 12 January. Depending on the nature of the operation this could be further broken down into three logs:

1. John DOE and Fred SMITH are associates.
2. On Tuesday 12 January, Fred SMITH passed a package to John Doe.
3. John DOE and Fred SMITH were together at 1 High Street on 12 January.

For further guidance on sanitisation, see ***ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources.***

1.5.5 Handling Codes

HANDLING CODE To be completed by the evaluator on receipt and prior to entry onto the intelligence system. **To be reviewed on dissemination.**	**1** **Default:** Permits dissemination within the UK Police Service **and** to other law enforcement agencies as specified. [See guidance] ☐	**2** Permits dissemination to UK non-prosecuting parties. [Conditions apply, see guidance] ☐	**3** Permits dissemination to (non EU) foreign law enforcement agencies. [Conditions apply, see guidance] ☐	**4** Permits dissemination within originating force/agency only: specify reasons and internal receipient(s) Review period must be set. [See guidance] ☐	**5** Permits dissemination but receiving agency to observe conditions as specified. [See guidance on risk assessment] ☐

