How to Complete a 5x5x5 Form and Relevant Supplements

CONTENT

1. HOW TO COMPLETE A 5X5X5 FORM

1.1 Government Protective Marking Scheme (GPMS)
1.2 Reporting Member of Staff and Date Time of Report
1.3 Person Providing Information (Source)
1.4 Source Evaluation
1.5 Information/Intelligence Evaluation
1.6 Information Content
1.7 Submission of the 5x5x5
1.8 Initial Use of the Handling Codes
1.9 Responsibilities

2. EVALUATION OF A 5X5X5

2.1 Quality Assurance of the 5x5x5
2.2 Re-Evaluation of the Source and Information
2.3 GPMS
2.4 Sanitisation
2.5 Handling Codes

3. FORM ‘C’ – ADDITIONAL RISK ASSESSMENT

4. RESPONSIBILITIES

5. INTELLIGENCE ACTIONING PROCESS

5.1 Priority Assessments
5.2 Authorisations
5.3 Entry onto an Intelligence System

6. TEMPLATES

Template 1: 5x5x5 Information Intelligence Report Form A
Template 2: 5x5x5 Continuation Form B
Template 3: Risk Assessment Form C

1. HOW TO COMPLETE A 5X5X5 FORM

The 5x5x5 report contains basic details identifying the person completing and submitting the report. It will also contain the time and date of submission and the signature of the person submitting the report, if a paper copy is used. Many electronic systems for recording 5x5x5 reports include electronic identifiers and so do not require a signature.

An audit trail of the information recorded on the 5x5x5 is essential and all police staff **must** ensure that these details are completed.

The following sections outline each individual aspect of the 5x5x5 report with examples how each part of the form should be completed.

See Template 1: 5x5x5 Information/Intelligence Report Form A.

1.1 Government Protective Marking Scheme (GPMS)

Once the report contains information it needs to be allocated an appropriate protective marking. There are five levels of this marking for sensitive assets, depending on the degree of sensitivity involved: **PROTECT, RESTRICTED, CONFIDENTIAL**, **SECRET and TOP SECRET**. The majority of information/intelligence that the police service holds contains personal or sensitive data. This data, therefore, needs a level of protective marking and normally this will be **RESTRICTED**. The GPMS **TOP SECRET** marking is not included on the 5x5x5 as it is unlikely that this form would ever be used for such material. For further information on the GPMS see, 'ACPO and ACPOS Handling of Protectively Marked Material – A Guide for Police Personnel' *October 2007.*

1.2 Reporting Member of Staff and Date Time of Report

ORGANISATION AND OFFICER	Sandford Police FIB PC 123 Smith	DATE/TIME OF REPORT	25/07/05 10.08

These fields record name, rank or position, station or office of the person who completes the information/intelligence report, together with the date and time of submission.

1.3 Person Providing Information (Source)

INTELLIGENCE SOURCE REFERENCE (ISR)	ISR /FIB/1234/05 (used to protect sensitive sources*)*	REPORT URN	12345/05

The identification of the source of the information can either be the name and address of the person providing the information or an intelligence source reference (ISR) number. Details of the person providing the information should be placed in these sections and not in the body of the report. The final sanitised version of an intelligence report to be seen by operational officers and staff (i.e. those expected to act upon intelligence), should not detail the true identity of any source, either within a source field or the main body of the text. This includes police and staff as information sources. Revealing the identity of some sources on the intelligence report and not on others can result in compromising a source or a current operation. The reliability of the source and quality of the information will be reflected in the final grading of the intelligence. Individual force policy will determine who specifically will have access to un-sanitised reports. Best practice would suggest that the ISR is managed by the FIB.

A unique reference number (URN) will be added to the submitted report by the receiving intelligence unit in order to provide an audit trail of received information. Should editing or sanitisation be required, the Intelligence Unit will create a second, sanitised version of the report, ensuring the removal of the source details and will allocate a further URN to this report. The second report will then be cross referenced to the original URN to continue the audit trail of received information. The original report must be retained and stored securely to ensure that source information is not revealed. Individual force policy will determine who will have access to un-sanitised intelligence reports.

Items of information from the same source but concerning totally different matters should be recorded on separate information/intelligence reports. Where a single source of information provides several items of information relevant to the same issue, separate 5x5x5 reports should be submitted. This is to avoid a single source being identified who may be the only one to know the sum total of the information submitted. This is particularly important when intelligence reports are prepared from a sensitive source, for example, CHIS or a technical device. The purpose of this procedure is to ensure that an adverse decision on ‘disclosure’ of a 5x5x5 would only put a single sensitive source or a single record at risk of compromise.

1.4 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. Most biometric information is virtually irrefutable but the reliability of technical deployment may depend on factors such as installation, environment and previous reliability etc. This means that it will not be used frequently as a source evaluation. It is normally used only for technical sources such as recording equipment (CCTV, ANPR, Communications equipment e.g. mobile phones, MP3 players, games consoles and computers etc, digital / video recording equipment) and DNA / Fingerprint / Scientific techniques and not for people, however unimpeachable, due to the possibility of human error. Assessment of a Source of information as ‘*Always Reliable’* carries a risk. Its use should be carefully considered due to the risk of errors arising from malfunction or operator error. Vehicle tracking devices for example may vary in reliability depending upon a number of variables.

It is acknowledged that there is some concern since the downgrading of police officers as sources to a ‘B’ grade, that anything graded ‘A’ may automatically allude to technical equipment and therefore covert activity. This is not the case as can be seen above. Whilst the ‘A’ grade may be synonymous with technical equipment in a large number of cases, it does not in itself, automatically indicate a covert policing method.

Scenario: Local Authority Town Centre CCTV records a male figure spraying the closed shutters of a local butchers shop with graffiti then running east towards Brixley High Road. (Clearly seen, little possibility of misinterpretation)

Scenario: A covert video recording device, installed in an observation point and focussed on the closed shutters of a local butchers shop, captures the figure of a male, spraying graffiti then running east towards Brixley High Road. (Clearly seen, little possibility of misinterpretation)

Scenario: A member of the public records on her mobile phone, a male figure, spraying the closed shutters of a local butchers shop with graffiti then running east towards Brixley High Road. (Clearly seen, little possibility of misinterpretation)

Intelligence Report text:

A male sprayed graffiti onto the shutters of (insert name) Butchers Shop, Sandford Road at 22.35hrs on xx/xx/xx before running off towards Brixley High Road. A.1

In the examples above, assuming the reliability of the equipment warrants 'A' grades, intelligence reports can be submitted with the 'A' grade, showing the provenance of the intelligence. As the above examples demonstrate, in only one case is a covert police technique being used. If, for operational reasons and for a limited period, this intelligence should not be seen by a wider audience, then a handling code of '4' may be applied by the Intelligence Unit, specifically detailing who may have access to it.

It is of the utmost importance that care is taken when sanitising reports from technical sources. Words such as "saw", "seen" or "heard" must not be used.

'B' – MOSTLY RELIABLE

Information has been received from this source in the past and in the majority of instances has proved to be reliable. This could be the majority of law enforcement and other prosecuting agencies.

Example: Information received from police officers, some tested CHIS and agencies, e.g. UKBA, Trading Standards, Environment Agency etc. may be evaluated as this source evaluation.

'C' – SOMETIMES RELIABLE

Some of the information received from this source has proved to be both reliable and unreliable. Any information with this grading should generally not be acted upon without corroboration. Where a potential risk demands a response, the intelligence manager will need to obtain as much corroboration as possible before commissioning action.

Example: This grading may apply to some CHIS or information received from the media or product of a technical deployment where malfunction is evident.

'D' – UNRELIABLE

Information under this grading will refer to individuals who have provided information in the past which has routinely proved unreliable. There may be some doubt regarding the authenticity, trustworthiness, competency or motive of the source. Any officer applying this grade should justify the allocation of this grade within the provenance section of the report (if applicable to individual force systems) and complete a Form 'C' Risk Assessment. Any information with this grading should not be acted on without corroboration.

Example: This grading could apply to information received from anyone with a potentially malicious motive, e.g. in neighbourhood disputes, or to information received from an individual with a history of making false allegations.

'E'– UNTESTED SOURCE

This grading refers to information received from a source that has not previously provided information to the person recording it. The source may not necessarily be unreliable but the information provided should be treated with caution. Corroboration of this information should be sought.

Example: This grading will usually apply to members of the public providing information for the first time and the majority of information received from Crimestoppers.

1.5 Information/Intelligence Evaluation

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

'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 grade 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 source has first hand knowledge of the information. Care must be taken to differentiate between what a source knows to be a fact and what a source reports they have heard or been told.

Example: A source gives information that a named individual is in possession of a large quantity of Class A drugs. They know this because they were **present** when that person took possession of the drugs and personally **saw** where the individual then hid them.

Example: A source states that A.N Other is selling Crack Cocaine at the Three Tuns Public House. The source knows this because they have **witnessed** A.N.Other dealing at the public house on several occasions.

'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, e.g. CCTV, other force systems. It is the responsibility of the person recording the information to seek corroboration for this grading to be given.

Example: A source has been **told** that Michael Brown has been seen driving a car, registration ABC 123 (the source does not know this information for themselves). The PNC shows that Michael Brown is the registered keeper of car registration ABC 123.

Example: A source states that A.N.Other is dealing Crack Cocaine at the Three Tuns public house. He says he knows this because A.N. Other's girlfriend **told him**. Examples of corroboration could be: other intelligence reports already on the system alleging A.N.Other's involvement in drug supply; enquiries with the landlord of the Three Tuns confirm that A.N.Other drinks there regularly and the landlord suspects he may be dealing drugs; corroboration from a registered CHIS who attracts a Source grading of 'B'.

‘4’- THE INFORMATION CANNOT BE JUDGED

The reliability of this information cannot be judged or corroborated. Information with this grading should be treated with caution.

Example: A source provides information that a named individual may be in possession of a large quantity of Class A drugs as they have heard a number of others mention this in conversation. There is no other information on force systems to corroborate this.

Example: A source states that A.N.Other is selling Crack Cocaine at the Three Tuns Public House. A.N.Other told the source that this is what he does. The source has never seen A.N.Other deal drugs at the Three Tuns Public House and there is nothing to corroborate this on force systems. The landlord states A.N.Other is an infrequent visitor to the public house and he has no suspicions.

The sanitised report should read:

“A.N.Other sells Crack Cocaine at the Three Tuns Public House”

It could be argued that the intelligence report could be written:

“A.N.Other is telling people that he sells Crack Cocaine at the Three Tuns Public House”, and graded ‘2’. This carries with it however a risk to the source should A.N.Other not have told anyone else.

‘5’- SUSPECTED TO BE FALSE

Information with this grading should be treated with extreme caution. This information should be corroborated by a reliable source before any action is taken. Any person applying this grade should justify within the provenance section of the report (if applicable to individual force systems) why it is appropriate to use this grading and must complete a Risk Assessment Form ‘C’.

Example: Malicious callers or a CHIS who is engaged in criminal activity and provides exaggerated information against others in order to deflect attention from themselves, or to prepare a defence of working for the police, should they be arrested.

Example: The source is arrested following an alleged assault at the Three Tuns public house and is barred by the landlord. During his detention the source states that the landlord sells Crack Cocaine in the Three Tuns Public House. There is nothing to corroborate this information. It is suspected by the reporting officer that the information is malicious as a result of being barred.

The importance of the provenance of the information being tested thoroughly cannot be emphasised enough.

1.6 Information Content

REPORT			
Person Record: Andrew Kent **DoB:** 21/12/79 **NIB CRO:** 15643/99V **(WHO)**			
OPERATION NAME/NUMBER (OPTIONAL)	S	I	H
Proposed robbery **(WHAT)** Andrew Kent is planning an armed robbery at a bank in Sandford town centre **(WHERE)**, exact location not known. This is to take place in 2 days time 27/07/05 when the next cash delivery is received. **(WHEN)** He will be using a red car, details unknown. **(HOW)**	**B**	**2**	

This refers to the body of the text within the report. The information provided should be clear, concise and without abbreviations. The body of the report should contain all information, whether the person submitting it believes it to be relevant or not. Where possible, the information should be corroborated and its provenance established. This could be done through interrogation of other business areas, for example, Andrew Kent is confirmed on PNC as being the registered keeper of a red Ford Escort car registration number ABC 123. This additional corroborative information should be submitted on a separate intelligence report and linked to the original intelligence report. This is because the additional information has come from another source and will have a separate 5x5x5 grading.

The information content will commence with the full name of the subject nominal, if known, together with their date of birth and/or age and, where possible, any national identification number, e.g. National Identification Bureau Criminal Records Office number.

For ongoing operations, the operational name or number may be added.

Having identified **who** the information relates to, the information should then clearly describe **what** is likely to occur, **where**, **when, why** and **how,** if known. If information is **not known,** then this should be clearly stated.

1.7 Submission of the 5X5X5

Once information has been recorded on a 5x5x5, the report should be submitted to the force/BCU intelligence unit by secure electronic or manual means. It will then be considered for its intelligence value based on research, source reliability, the content of the information and its actionable value against the force/BCU control strategy, intelligence requirement or other policing purpose.

1.8 Initial Use of the Handling Codes

Handling codes are designed to provide an initial risk assessment prior to recording material into an intelligence system. They allow recording officers and others involved in the dissemination of intelligence material to easily record their decisions on the suitability or otherwise of sharing the intelligence with other parties.

The officer completing the 5x5x5 will not usually complete the handling code unless they are officers/staff involved in the intelligence discipline, for example, trained intelligence officers and specialists. It is accepted however, that many force intelligence systems are designed so that an initial handling code must be applied by the reporting officer in order for the report to be accepted onto the system. In such cases, the default handling code should be input as Handling Code '1' upon submission until evaluated by an intelligence professional. Should the person first recording the information have concerns about disseminating the information, they should complete specific handling instructions. In cases where handling codes '4' or '5' are considered necessary, a Risk Assessment Form 'C' must be completed. The Form 'C' should be attached to the 5x5x5 when it is submitted. Unless concerns are raised, the intelligence unit will review the information/intelligence report and apply the appropriate handling code. It is, therefore, important that Form 'C' contains a comprehensive evaluation of the risk; as without this, the intelligence unit may lack the information to make an appropriate determination of the handling code.

1.9 Responsibilities

All staff should be able to identify information which may be relevant to policing purposes. They should also be able to complete an information/intelligence report and identify obvious risks about the information.

The person submitting the 5x5x5 should check the information they wish to record against other business areas before entry, to help verify the information. Anyone submitting information has a duty to ensure that it is as accurate as possible and, where it can be easily corroborated, that action is taken. The first stage of converting what may be rumour into information that can be used, is for the reporting officer to ensure that facts are accurate.

Checklist: Recording Information on a 5x5x5

The person completing a 5x5x5 must:

- Complete all submission fields.
- Assess the source reporting the information and apply the correct grading.
- Evaluate and grade the information given.
- Complete text of report.
- Use the correct GPMS marker.
- If necessary, give specific handling instructions and apply a risk assessment
- to the information. Where that is done, the Risk Assessment Form C should
- be attached and sent to the intelligence unit.
- Send report to appropriate intelligence unit in line with force security policy.

2 Evaluation of the 5x5x5

Once a 5x5x5 has been received by the intelligence unit, it will be further assessed for:

- Compliance with this guidance for the completion of 5x5x5 reports;
- Risks and duty of care issues, including CHIS safety;
- Its intelligence value;
- Accurate and full provenance of the information completed by the person submitting;
- Consideration for further research and development;
- Consideration for dissemination and requirements for sanitisation;
- Entry onto the intelligence system.

2.1 Quality Assurance of the 5X5X5

When the 5x5x5 has been received, the initial report should be quality assured. The information contained within the 5x5x5 should be checked for completeness and accuracy.

Competent use of information is a key requirement for all staff and is integral to the management of performance at personal and team levels.

Any amendment to the 5x5x5 should have an audit trail. This may include the resubmission of a sanitised 5x5x5 linked directly to the original report.

2.2 Re-Evaluation of the Source and Information

The content of the 5x5x5 should be read and reviewed by the nominated intelligence officer with responsibility for quality assurance within the intelligence unit. The 5x5x5 will be examined in line with the initial gradings given. Reliance should be placed on the person submitting the report with regards to the source reliability and information evaluation unless there is an obvious discrepancy or incompatibility. If further clarity or corroboration is required on any issue, contact should be made with the person who submitted the report.

2.3 GPMS

The intelligence unit should note the GPMS (Government Protective Marking Scheme) marking contained on the 5x5x5. When quality assuring the 5x5x5 the document's protective marking should be checked to make sure it has the correct one attached to it.

2.4 Sanitisation

Reports should be sanitised for onward transmissions by removing material which explicitly or implicitly identifies a source or police methodology. The text (as opposed to the source reference) should give no indication of the nature of the source, whether human or technical or the proximity of the source to the information. Words such as "seen" "saw" or "heard" should not be used. The proximity of the source may be compromised by using words such as "come" "turn up" or "appear" or "arrive at". Alternatives may be "attend" or "go to".

Compare:

- Two men come to A.N.Other's address every evening in a black BMW convertible.
- Two men attend A.N.Other's address every evening in a black BMW convertible

Persons should not put material into a 5x5x5 that adds no value or leads to the identification of the source or any sensitive operational details. For example, care should be taken not to reveal sensitive police tactics such as observation points, surveillance, covert human intelligence sources or other confidential information. The term "intelligence suggests" at the beginning of a report is no longer encouraged. This phrase detracts from the grading and calls its accuracy into question. In addition, this phrase may allude to the fact that the source is human and most likely not to have come from a police officer. Where this phrase is used in some reports and not in others, a distinction is able to be drawn. Persons should report only the facts of what was told to them and not place any additional interpretation within the report, changing the meaning of what was told to them. This is essential to maintain the integrity of the information.

Example: An officer is told by a source that John Smith is storing stolen car parts in his garage for A.N.Other. The source knows this as he was shown the parts in the garage by John Smith and was told by him that they came from cars stolen from a hospital car park. The report should read: "John Smith is storing stolen car parts in his garage for A.N.Other" as opposed to, "Intelligence suggests that John Smith may be storing stolen car parts in his garage for A.N.Other" or, "John Smith is believed to be storing car parts which may be stolen, in his garage for A.N.Other"

If the intelligence unit needs to sanitise the 5x5x5 before dissemination or inputting into an intelligence system, a new 5x5x5 should be submitted. The new report should not only be given a new unique reference number (URN) but also be cross-referenced to the original report to identify provenance and provide an audit trail. The original report should be retained but stored securely to ensure that the source is not revealed.

The following examples highlight specific issues, and then illustrate good practice for recording :

Example 1:

5x5x5 report – Yesterday I met John Clarke at 12.00hrs at the dog track. He said the day before he was round at Tommy Smith's place and he overheard him on the phone. Tommy said there wouldn't be a problem. He'd got enough cash and he would take as much speed (amphetamine) and coke (cocaine) as the man could provide him with, but that he didn't want any smack (heroin) this time. Clarke said the number Smith called was 01234 56789, dialled from a piece of scrap paper on the living room table.

Problem – The report identifies the source at the subject's address at a specific time. The informant provides two pieces of information which, taken together may only be known by this one person. This may identify the source even without the source being named.

Best Practice: Two separate intelligence reports;

1. Tommy Smith is arranging to buy large quantities of amphetamine and cocaine.

2. Tommy Smith has an associate concerned in the supply of amphetamine, cocaine and heroin who uses the telephone number 01234 56789

Example 2:

5x5x5 report – At approximately 10.00hrs on Saturday 27th February 2011, the subject, Richard Smith was seen from an observation post at number 2, High Street Anytown, to return home driving a red Saab A123 ABC.
Problem – The report identifies that a covert operation is in place against Richard Smith and identifies the location of the OP.

Best Practice:
Richard Smith was driving a red Saab A123ABC in the High Street, Anytown, at 10.00am on 27th February

Note: The decision to include the time within the report must be made on a case by case basis dependant upon the circumstances. In this training scenario it can be argued that the inclusion of the time does not automatically reveal covert activity on the subject's address. This is because the "return home" aspect has been omitted. If this were a real High Street it may be that any number of people could have seen Smith driving including passing patrolling officers. The decision to leave out the "return home" aspect deliberately distances the source from the subject. Evidentially however, nothing has been lost as the original report is still recorded on the system.

.

2.5 Handling Codes

HANDLING CODE	**1**	**2**	**3**	**4**	**5**
To be completed by the evaluator on receipt and prior to entry onto the intelligence system **To be reviewed on dissemination**	**Default:** Permits dissemination within the UK Police Service AND to other law enforcement agencies as specified [see 5x5x5 guidance]	Permits dissemination to UK non-prosecuting parties [conditions apply see 5x5x5 guidance]	Permits dissemination to (non-EU) foreign law enforcement agencies [conditions apply see 5x5x5 guidance]	Permits dissemination within originating service/ agency only Specify reasons for this and Identify internal recipient(s) A review period should be set [see 5x5x5 guidance]	Permits dissemination but receiving agency to observe conditions as specified [see 5x5x5 guidance on risk assessment]

Handling codes are designed to assist the intelligence unit in the risk assessment decision of whether to disseminate intelligence or not and, if so, to whom. The codes provide clarity over the purpose for communicating the piece of intelligence to others. By recording this on the 5x5x5, it clearly outlines the conditions which should be met when disseminating that specific piece of intelligence to other parties. It is accepted that whilst persons trained in applying handling codes, for example, those in the intelligence unit, should be the only ones applying them, force intelligence systems often insist on a handling code being selected to accept the submission. In these cases the submitting officer should select Handling Code '1' as a default code. The intelligence unit professional will then review the code and change it where necessary. The intelligence professional should have an overview of other information which is relevant in the dissemination of the intelligence.

Individual officers and designated employees of the police are authorising officers for the purpose of disseminating intelligence material to other law enforcement and prosecuting agencies.

Before a decision to disseminate is made, the intelligence unit should apply one of the five handling codes. All the handling codes allow dissemination of the information where appropriate.

CODE '1' – DEFAULT: PERMITS DISSEMINATION WITHIN THE UK POLICE SERVICE AND TO OTHER LAW ENFORCEMENT AGENCIES AS SPECIFIED

This handling code permits intelligence to be disseminated within the UK Police Service and other law enforcement agencies, which must be specified. Under this code the police service is defined in its entirety and not just a local force area.

This is the **default** code for general dissemination within the police service and will directly link to the development of common person records across the organisation.

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. Specific questions to be asked when considering dissemination of Code '1' intelligence are: Who is asking for it? Why do they want it? What are they going to do with it? If a reporting officer has any concerns around how widely the intelligence being submitted may be disseminated within other law enforcement and other prosecuting agencies, they should complete a risk assessment Form 'C', justifying any reasons for suggested restrictions.

For the purpose of this handling code, other law enforcement agencies include SOCA, the United Kingdom Border Agency, and Europol. Prosecuting agencies are regarded as law enforcement agencies for the purpose of this handling code, including the Crown Prosecution Service, the Department of Work and Pensions and Local Authority departments, for example, Trading Standards.

Example: Information that Andrew Brown a convicted drug dealer, is currently using a red Ford Escort ABC 123 to transport Class A drugs between London and Birmingham. No current ongoing operation in relation to Brown in the reporting force, Handling Code '1' applies to disseminate across the police service.

Example: Information that Bob Clark, who has a fleet of lorries travelling throughout Europe and the UK, is believed to be involved in people smuggling, dropping off illegal immigrants at motorway service areas. Handling Code '1' applies as the information would need to be disseminated to the whole police service and United Kingdom Border Agency.

CODE '2' – PERMITS DISSEMINATION TO UK NON-PROSECUTING PARTIES

This handling code permits intelligence to be disseminated to non-prosecuting parties in the UK. For the purpose of this handling code, non-prosecuting parties include commercial organisations such as credit card companies.

This code can permit the dissemination of certain relevant information but will not necessarily require the full record to be disclosed. The intelligence unit must ensure that non-relevant information contained within a report is removed by sufficient editing.

When intelligence is disseminated to non-prosecuting parties, a record should be kept of the recipient, the material disseminated, the purpose of dissemination, the authorisation and any restrictions on the use or further dissemination of the information. In some cases Form ‘C’ may be appropriate. Any intelligence which is disseminated to non-prosecuting parties should be authorised by an officer of at least inspector or equivalent.

Example: Information received that Jane Smith is planning to open a number of mail order catalogue accounts in a false name as she is registered bankrupt. Handling Code ‘2’ applies, the information is appropriate for dissemination to the applicable commercial organisation as this likely offence can best be tackled by passing the information on to the partner who is able to intervene immediately and prevent it.

CODE ‘3’ – PERMITS DISSEMINATION TO (NON-EU) FOREIGN LAW ENFORCEMENT AGENCIES

This handling code permits intelligence to be disseminated to non-EU foreign law enforcement agencies. In the case of non-EU law enforcement agencies, forces should risk assess each on an individual basis.

This code arises directly from the requirement of the Data Protection Act 1998 for personal information to be disseminated outside the EU only after the risks have been assessed and on the grounds of substantial public interest. Public interest in this context will include tackling serious crime and the maintenance of the security and integrity of law enforcement agencies.

All forces should ensure that a local policy is in place which specifies the procedure and authority level for Code ‘3’ dissemination requests.

Example: Information is received that a dangerous paedophile currently living in the UK is moving abroad to Thailand. Handling Code ‘3’ applies as the intelligence could be sent to the authorities in Thailand.

CODE '4' – PERMITS DISSEMINATION WITHIN ORIGNATING SERVICE/AGENCY ONLY. SPECIFY REASONS AND INTERNAL RECIPIENT(S).

This handling code restricts the dissemination of the intelligence to the originating service/agency. It provides for the need to retain particularly sensitive information within a tight community with a specific need to know. It is likely to be of use in restricting access to material that is relevant to current sensitive operations. This may include restricting dissemination to a particular operational team within that service or agency.

Prior to applying this handling code, a rigorous evaluation should take place to justify why further dissemination is not appropriate. A Risk Assessment Form 'C' must be completed to justify the restrictions imposed. Any internal recipients identified may be recorded on the Form 'C'. Any intelligence report given a Code '4' **should** remain under constant review to ensure that wider dissemination can occur as soon as is feasible, such as when an operation has been concluded or is no longer being pursued.

There will be an assumption that any information/intelligence marked with this grading will not be further disseminated without contacting the originator of the report. The application of this handling code does not mean that the information/intelligence to which it relates can NEVER be disseminated outside of the originating service/agency whilst it remains at Code 4, but provides an additional safeguard to protect particularly sensitive information for the relevant time period. Certain circumstances may arise which may make it necessary for such information to be disseminated outside of the originating service/agency. The decision to release such information should be made after a thorough re-evaluation and further Risk Assessment, detailing the justification for the release of the information/intelligence, to whom the information will be made known and any other restrictions on the use of the information/intelligence.

This is **not** the default handling code.

Example: Information received from an undercover officer currently deployed in a long-term class A drugs infiltration operation states that one of the operational subjects has had meetings in another force area. This reveals the identity and current activity of suppliers in that force area. The undercover officer is currently the only other person who can possibly know of those contacts. Handling Code '4' applies as dissemination outside of the undercover operational team is likely to seriously compromise the officer and operation. In this situation a risk assessment Form 'C' must be used. An authorising officer should stipulate regular review. Handling Code '4' does not prevent the release of some of the relevant material where sanitisation is possible although the whole report cannot be disseminated at this point.

CODE ‘5’ – PERMITS DISSEMINATION BUT RECEIVING AGENCY TO OBSERVE CONDITIONS AS SPECIFIED.

Any information marked with this handling code requires special attention. Application of this code means the originator has applied specific handling instructions in respect of this information. A Risk Assessment Form ‘C’ will be required in respect of the information concerned and that if it is subsequently used in court, an application for Public Interest Immunity will be sought. Where handling code options are insufficient against the perceived risk of the information to a source, a Form ‘C’ must be completed.

Example: Information from a CHIS relating to potential serious harm to a child is deemed suitable for dissemination to social services. Due to the sensitive nature of the information, the social services department receiving it may only use this information in a confidential case conference rather than at an open forum. Handling Code ‘5’ applies, subject to the completion of a risk assessment Form ‘C’.

3 Form 'C' – Additional Risk Assessment

Form 'C' is a method by which information/intelligence received through the 5x5x5 process can be risk assessed, see Template 3.

If there are concerns regarding the source of the information or there being a risk to others is identified, a Form 'C' must be completed by the reporting officer and included with the report.

A further risk assessment will take place when the report is evaluated for dissemination and the handling codes are applied by the intelligence unit.

The risk assessment process also includes consideration of ethical, personal and operational risks in respect of the source, the information content, its use, dissemination and compliance with a legislative requirement or policing purpose.

This process will also include a justification for the decisions made and the appropriate authority of the person making them. It will consider the proportionality, accountability and necessity for recording, disseminating and retaining the information.

Ethical risks

Assessments of ethical risks concern the issues of proportionality and necessity (justification), including addressing the following questions:

- Is the recording or dissemination of the intelligence proportionate to the problem it is intended to solve?
- Does the recording or dissemination of the intelligence comply with the policing purposes?
- Does the intelligence contain material relating to persons other than the target? Are the risks of such collateral intrusion being passed on acceptable? Can the risk be sifted out?
- Does the character of any individual concerned have any impact on proportionality? An individual's character needs to be taken into account when considering the issue of proportionality. If someone has a string of convictions for similar offences, proportionality of any proposed action may become less of an issue than if the person was of previous good character.

Personal risks

Assessment of the personal risks includes addressing the following questions:

- Is there a risk of personal injury to the subject, the public or a member of the law enforcement agencies?
- Are there any obvious physical risks faced by operatives involved in any operation reliant on the use of the material? (Where the intelligence leads to an operational response, for example, a covert operation, the techniques employed will also be risk assessed.)
- Are there risks to the safety of the subject, individuals who may assist the law enforcement agencies or be subject to collateral intrusion, for example, the source?
- Are the risks to the data subject, arising from the dissemination of the intelligence material, acceptable?

Operational risks

Assessment of operational risks includes addressing the following questions:

- Is there a risk of disproportionate damage to the professional reputation of the force should the intelligence be exposed or a prosecution collapse?
- Is there a risk of damage to community relations in the event of a compromise?
- Would exposure by disclosure or any other event compromise a sensitive technique, a current operation or a source?
- Does the intelligence contain 'confidential material'? If so, before the material can be recorded onto an intelligence system or disseminated, due account should be taken of any restrictions on its use or requirement for special handling imposed by the officer who authorised its collection. An assessment should be made of the risks arising from the use of the material, or from its potential disclosure in court proceedings. The Risk Assessment process must be carried out on Form 'C', see Template 3.

4 RESPONSIBILITIES

The Intelligence Unit should ensure that all intelligence is managed in line with this guidance. Once a person has submitted a 5x5x5 for the Intelligence Unit's attention, there is an expectation that the intelligence will be properly evaluated and considered for appropriate dissemination.

Checklist : Evaluation of the 5x5x5

On receipt of a 5x5x5, the following actions should be taken:

- Quality assure the original 5x5x5 for its completeness, accuracy and provenance;
- Re-evaluate the reliability of the source and information;
- Apply the GPMS marking;
- Sanitise the content if appropriate;
- Apply the appropriate handling code;
- Is a Form C needed? If so has it been completed?

5 INTELLIGENCE ACTIONING PROCESS

Once information within the 5x5x5 has been reviewed, the appropriate handling codes applied and the required level of authorisation obtained, it may be actioned and entered into the intelligence system. A priority assessment process for the information may be adopted at this stage to manage workload and resources, while ensuring that the highest priority intelligence is actioned at the earliest opportunity.

5.1 Priority Assessments

A priority assessment can determine the appropriate action for a specific piece of information.

The priority assessment may change over time depending on research and development. The application of this process will usually take place in the intelligence unit because of the nature of the information recorded, evaluated and held in the intelligence business area.

Priority assessments are dynamic and affected by a number of factors. The protection of particular members of society such as children and vulnerable adults will always have a bearing on priority assessments, see 2.3 Critical Information Areas. Other priority assessments will be agreed locally at force or BCU level and will depend on the control strategy and the policing priorities for the area in question.

The following priority assessment criteria are intended as a guide, but will be set at a local force level.

Priority Assessment HIGH (H): Risk of Serious Harm

- This refers to information which indicates a risk of death and/or serious harm.
- The information could relate to the imminent commission of other serious crime.
- When a piece of information is assessed as high priority, it should be marked as such and immediately brought to the attention of the appropriate supervisor and actioned. This action should include further evaluation and risk assessment against known or believed facts and its immediate entry into the intelligence system should be considered.

Example: A reliable source states Michael Brown, a known offender, has a shotgun (confirmed on firearms licensing register) and intends to shoot Simon Smith. The name of the victim is known, the name of the offender is known and there is, potentially, a public and officer safety issue here.

Priority Assessment MEDIUM (M): NIM Control Strategy/Intelligence Requirements/Current Operation/Tactical Menu

- This refers to information focused on NIM Control Strategy Areas, intelligence requirements, any current operations or information relating to a high-risk offender or an offence *that may not be committed imminently,* such as a sex/dangerous/violent offender who has been released on licence.
- There is an expectation that information assessed as a medium priority will remain subject to further evaluation, risk assessment and development, and consideration for early entry onto the intelligence system.

Example: A reliable source states Simon Smith and Michael Brown intend to commit a dwelling house burglary on the High Street some time this week. Burglary is part of the BCU control strategy and intelligence requirement. The High Street is subject to a current problem profile in respect of dwelling house burglaries.

Priority Assessment LOW (L): Other Information

- This is information which falls outside the parameters of high and medium priorities. The information has been recorded as it meets the policing purpose criteria, and could also relate to matters that would benefit from further research and development. Such information may identify emerging trends and issues or problem localities which will inform the NIM process.
- This information requires evaluation and risk assessment and needs to be recorded appropriately.

Example: A reliable source states that Michael Brown and Simon Smith intend to go shoplifting in the town centre. They do this on a regular basis. Shoplifting is not part of the BCU control strategy or intelligence requirement. The information is relevant for the purposes of the prevention and detection of crime, and is recorded accordingly. Further research and development may assist in developing subject profiles and intervention strategies against Brown and Smith who, as well as shoplifting, are known to be active in a number of other types of crimes.

5.2 Authorisations

5x5x5 REVIEWED BY: RE-EVALUATED: Yes/No	CROSS-REF URN:	TIME/DATE OF REVIEW:
DISSEMINATED TO:	PERSON DISSEMINATING TIME/DATE:	
DETAILED HANDLING INSTRUCTIONS:	PUBLIC INTEREST IMMUNITY:	
INPUT ONTO AN INTELLIGENCE SYSTEM Yes □ No □		
SIGNATURE (PAPER COPY):		

Individual officers and designated employees of the police, are self-authorising officers for the purpose of their duty to record intelligence material.

Individual officers are responsible for making the decision to record information on a 5x5x5. Before recording intelligence material, the officer should be satisfied that:

- The activity conforms to a policing purpose;
- The intelligence to be recorded onto intelligence systems has been properly evaluated and its provenance established;
- Where the intelligence is to be recorded onto intelligence systems for later action, it has been assessed for risks arising from its use or from its potential disclosure in court proceedings;
- Any linked 5x5x5 reports are cross-referred by a URN;
- Any changes to the original 5x5x5 should have been audited by the intelligence unit;
- Any paper copy 5x5x5 has been signed by the authorising officer.

5.3 Entry onto an Intelligence System

NIM identifies a number of key roles and functions responsible for information IT management and data entry. NIM also provides details of minimum standards which specify that there should be sufficient resources available to carry out data entry and to ensure that its quality is maintained.

Once authority has been given for data to be entered onto the intelligence system, persons responsible for its input should have regard to the appropriate handling code, specific handling and dissemination instructions, and any risk assessments. This will ensure that all data entry is compliant with the instructions of the authorising officer.

TEMPLATES

TEMPLATE 1

NOT PROTECTIVELY MARKED UNTIL COMPLETED

GPMS	PROTECT □	RESTRICTED □	CONFIDENTIAL □	SECRET □

5x5x5 Information Intelligence Report Form A

ORGANISATION AND OFFICER		DATE/TIME OF REPORT	
INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE SOURCE REF NO. (ISR)		REPORT URN	

SOURCE AND INFORMATION/INTELLIGENCE EVALUATION TO BE COMPLETED BY SUBMITTING OFFICER					
SOURCE EVALUATION	A Always Reliable	B Mostly Reliable	C Sometimes Reliable	D Unreliable	E Untested Source
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
REPORT					

PERSON RECORD:	DoB:	NIB CRO:

OPERATION NAME/NUMBER:	S	I	H

INTELLIGENCE UNIT ONLY					
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 □	2 Permits dissemination to UK non-prosecuting parties □	3 Permits dissemination to (non-EU) foreign law enforcement agencies □	4 Permits dissemination within originating service/agency only: specify reasons and internal recipient(s) Review period must be set □	5 Permits dissemination but receiving agency to observe conditions as specified □

5x5x5 REVIEWED BY: RE-EVALUATED: Yes □ No □	CROSS-REF URN:	TIME/DATE OF REVIEW:

DISSEMINATED TO:	PERSON DISSEMINATING TIME/DATE:
DETAILED HANDLING INSTRUCTIONS:	PUBLIC INTEREST IMMUNITY:

INPUT ON TO AN INTELLIGENCE SYSTEM Yes □ No □
SIGNATURE (PAPER COPY):

GPMS	PROTECT □	RESTRICTED □	CONFIDENTIAL □	SECRET □

TEMPLATE 2

5x5x5 Continuation Form B

INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE SOURCE REF NO. (ISR)			REPORT URN				
REPORT							
NOMINAL:		DoB		NIB CRO			
OPERATION NAME/NUMBER:					**S**	**I**	**H**
GPMS	**PROTECT** ☐	**RESTRICTED** ☐	**CONFIDENTIAL** ☐	**SECRET** ☐			

TEMPLATE 3

Risk Assessment Form C

FOR THE USE IN DISSEMINATION OF INFORMATION/INTELLIGENCE

1	Does the information contain confidential material or sensitive material as identified in law?	**YES/NO**
2	If yes, are there any restrictions on use, or requirements for special handling, imposed by the person submitting the report?	**YES/NO**
3	What are the ethical, personal or operational risks which are likely to result as a consequence of any dissemination or disclosure? Consideration must be given to the risk to the source and the content of information within the report.	**DETAIL THE RISKS**
4	What is the purpose of dissemination or disclosure? Is it for a policing purpose or a legislative requirement?	
5	Having identified the risks, justify the decision-making process. This must include the justification, authority, proportionality, accountability and necessity of a dissemination or disclosure.	
FOR INTELLIGENCE UNIT ONLY		
6	In light of the risk assessment is the Handling Code correct?	**YES/NO**
Risk Assessment and Management Plan authorised by…… (Intelligence Manager)		**Person Completing Risk Assessment:**
Cross-ref URN:		**Time/Date:**