Using and Handling Intelligence Data

- A guide for Community Safety Partnerships

Content

Introduction

Information sharing is key to the delivery of better, more efficient public services that are coordinated around the needs of communities and individuals. It is essential to direct early intervention and preventative work, and to effectively tackle local community safety issues and safeguard individuals.

The sharing of data and intelligence is key to Community Safety Partnerships (CSP) work and there is evidence through the CSP self-assessment toolkit that partnerships are scoring highly in relation to having robust data sharing practices.

However it is important that the providers of data continue to have trust and confidence in the partnerships ability to use the data appropriately, and that they are compliant with government guidance and legislative requirements.

This guidance document aims to ensure that data is shared, used and stored in compliance with the HM Government Security Classifications (2014) guidance which states '*Everyone has a duty of confidentiality and a responsibility to safeguard any information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training*'.

To compliment this guidance pack and to support partnership to meet the training requirement, SCSN has also produced an eLearning course which is suitable for all partners which can be access via the SCSN website at www.safercommunitiesscotland.org

The National Intelligence Model

The roots of partnership analysis is within 'criminal intelligence analysis' which has its foundations within the National Intelligence Model (NIM). The NIM was developed in 2000 and is a well-established and recognised model used by law enforcement and community safety partnerships across the country to:

- Set strategic direction
- Make prioritised and defendable resourcing decisions
- Allocate resources intelligently
- Formulate tactical plans and manage risk.

The use of NIM is no longer the domain of the police or community safety. Guidance published in December 2012 by the Scottish Government and COSLA directed that the SOAs will "use an evidence based approach, underpinned by disaggregated data, to drive improvement in meeting the differing needs of local populations". The NIM approach is therefore now fully embedded in public sector working practices.

Through the NIM process public sector analysts regularly produce a range of products to support the development of outcome-based priorities and subsequent resolutions to tackle these issues. To create these analytical products, analysts will review data from a number of partners including police, local authority, NHS and fire service data.Table one below outlines the main products Community Safety Partnerships (CSPs) use.

Table one – NIM Products

Product	Purpose
Strategic Assessment	This is the evidence base to aid longer-term strategic planning within a CSP – it provides a broad picture of community safety within a partnership and helps to identify priorities for the coming three to five years. It also provides recommendations relating to early interventions, prevention and enforcement. It uses trend analysis but also horizon scanning informed by the national and local picture to predict future challenges and opportunities for the partnership.
Tactical Assessment	This tends to be produced on a monthly basis and is an evidence base which identifies shorter term trends in community safety. It will recommend preventative and enforcement activities and should be used by the tasking group to direct partnership resources over the short-term.

Daily and weekly briefings	This uses similar techniques as the tactical assessment and is a very short-term evidence base which identifies community safety trends. It will recommend preventative and enforcement activities and should be used by the daily/weekly tasking group or in operational briefings to direct partnership resources over the short-term.
Problem Profile	These look in much more depth at a particular community safety issue, for example underage drinking across the partnership area, a particular issue in a particular area for example ASB in a specific community or multiple community safety issues in a specific community. It identifies the 5WH of the issue and makes recommendations to resolve the issue. These are often commissioned by the Tactical T&CG or MATAC when an issue or area has been raised at the meeting on a number of occasions and requires a more focused and coordinated approach.
Target/Subject Profile	This embraces a range of analytical techniques to describe the victim(s) or criminal, their criminal activity or victimisation, lifestyle and associations. For criminals it also details the risk they pose and their strengths and weaknesses in order to give focus to the investigation targeting them. Profiles that focus on victims or groups of victims can detail the risks they face. Some examples of subject profiles are e.g. a profile on young people at risk of offending for Early and Effective Intervention (EEI) process or profiles on domestic abuse victims and offenders for monthly (Multi-Agency Risk Assessment Conference) MARAC meetings.
Outcome performance indicator monitoring	Partnership analysts can assist in recommending appropriate outcome indicators and performance measures and provide performance reports and explanation in relation to these. These can include commentary for performance in relation to the community safety strategic plan(s) and SOA.

In addition to these key intelligence products, analysts also produce a wide range of other analytical products which maybe relevant to partnerships. These are listed in Appendix 4.

Information Sharing Principles

"..if information is to be shared by practitioners to prevent or detect crime or where there is a risk of significant harm or serious health risk to the service user and the information to be shared is relevant and proportionate, then the information may be shared"

Chapter 3, Getting our priorities right – Information Sharing
Scottish Government (July 2012)

Information sharing between community safety partners has been standard practise for a number of years and has taken cognisance of complementary and restrictive legislation such as:

- **Data protection act 1998** is a framework to ensure personal information about a living person is shared appropriately under the following principles:

- **Antisocial Behaviour etc. (Scotland) Act 2004** makes provisions, under section 139, to allow for information sharing without the consent of the named individuals. Where information is being shared under these provisions then consent will not be required.

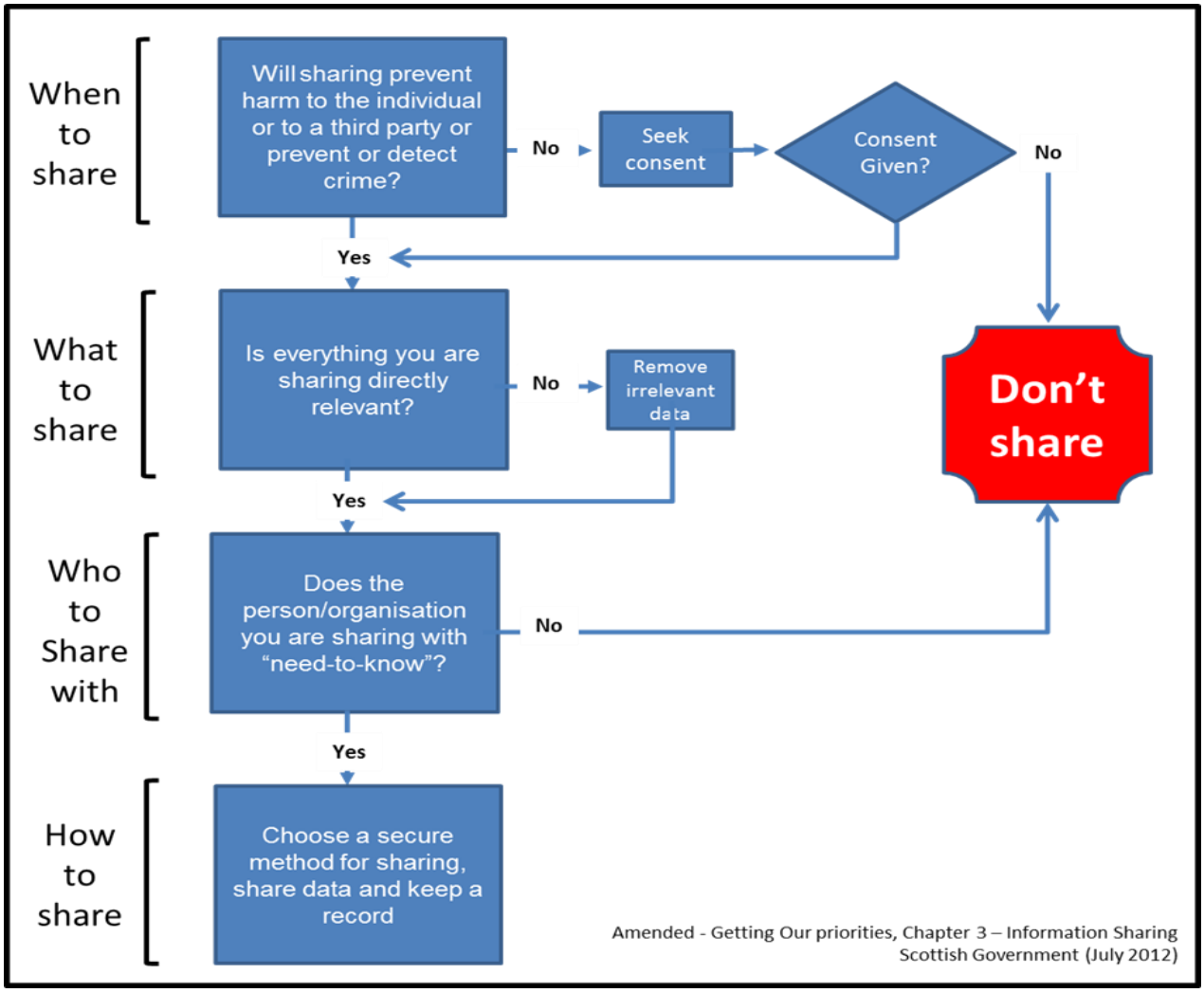
- **The Local Government in Scotland Act 2003** permits information sharing under Part 2, 'Community planning' and Part 3, 'Power to advance wellbeing'.

- **Common Law Powers of Disclosure** focuses on disclosure where there is a public protection risk, rather than a blanket approach of passing on all information whether relevant or not. The threshold for disclosure now becomes that of "pressing social need".

- **Freedom of Information (Scotland) Act 2002** gives everyone the right to ask for any information held by a Scottish public authority (with some information being exempt from this). Freedom of information also requires Scottish public authorities to publish a lot of information under what is known as the "publication scheme" duty.

Over the years partnerships have adopted the following logic model produced by the Scottish Government in 2012 to make decisions about when to share, what to share, with whom to share and how to share information:

Table two



Information sharing protocols

Because of the nature of data being shared the majority of partnerships have established local Information Sharing Protocols which clearly defines the reasons why information sharing is required, how it supports the functions of the partnership and the principles that govern the sharing. Information Sharing Protocols aim to provide a high level multi – agency framework for the sharing of information between agencies engaged in partnership working for a defined purpose. Their function should therefore be to achieve agreement in principle, and should only include the level of information necessary for that purpose. They should not aim to detail every data sharing requirement between named agencies as the protocol is underpinned by Data Sharing Agreements which set out the specific data sharing needs between agencies.

We would encourage all members of a partnership to read and understand the local Information Sharing Protocol.

Some partnerships also have confidentiality agreements at daily, weekly and monthly tasking meetings and restrictions will apply to information shared verbally at these meetings too.

Confidentiality Statement

Information discussed by the agency representatives within this meeting is strictly confidential and classified as **OFFICIAL** and must not be disclosed to third parties who have not signed up to the_____ Information Sharing Protocol. By signing this document you accept total liability for any breach of information made by you should legal proceedings be initiated in relation to that breach.

All agencies will ensure that the analytical documents and task sheets supporting this meeting are retained in a confidential and appropriately restricted manner. These documents will aim to reflect that all individuals who are discussed at these meetings should be treated fairly, with respect and without discrimination. All work undertaken at the meetings will be based on a commitment to equal opportunities and effective practice in relation to race, gender, sexuality and disability.

Please provide your name and organisation and sign this sheet to indicate your compliance with this data protection statement.

Name: Organisation:

Siganture:

Handling Protectively Marked Information

The sharing and storage of data is regulated through and must comply with HM Government guidance (2014); and as such the following points should always be considered when sharing analytical products, irrespective of the information source.

- All information that needs to be collected, stored, processed, generated or shared to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection.

- Everyone has a duty of confidentiality and a responsibility to safeguard any information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.

- Access to sensitive information must ONLY be granted on the basis of a genuine "need to know" and an appropriate personnel security control. But remember that over or under marking of material can overly restrict or risk the accidental or deliberate leaking of information.

- Assets received from or exchanged with external partners MUST be protected in accordance with any relevant legislative or regulatory requirements, including any agreements and obligations. When receiving material, it becomes the recipient's responsibility and ownership falls to them.

The principle governing the use of protective marking is that **dissemination of sensitive information should be no wider than is required for the efficient conduct of an individual's job function**. Such dissemination must be restricted to those who are authorised to have access on a 'need to know' basis.

Until April 2014 the Government Protective Marking Scheme (GMPS) employed by public bodies provided four levels for protectively marking materials:

RESTRICTED CONFIDENTIAL SECRET TOP SECRET

This has now changed and there are three levels for protectively marking material:

There is no tier below OFFICIAL – this is different to GPMS where there was a 'NOT PROTECTIVELY MARKED' option. All information that is created, collected, processed, stored or shared within the public sector has value, belongs to the organisation and must be handled with due care. This includes published data where integrity and availability considerations (and often Crown Copyright) may continue to apply.

In addition to the protective marking, organisations may apply a DESCRIPTOR to identify certain categories of sensitive information and indicate the need for common sense precautions to limit access. Where descriptors are permitted they must be supported by local policies and business processes, including information sharing protocols. Descriptors should be used in conjunction with a security classification and applied in the format:

"OFFICIAL - SENSITIVE [DESCRIPTOR]"

We suggest that a partnership creates and maintains the following list of core descriptors to ensure a consistent approach is adopted across all departments. For example:

- 'PERSONAL': Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to investigations or vulnerable individuals.

- 'ORGANISATIONAL': Sensitive information which could damage the organisation/partnership if improperly accessed.

Regarding handling and storage:

To defend against these typical threat profiles, protective security controls should achieve the following outcomes at each classification level:

	OFFICIAL	SECRET	TOP SECRET
Outcome	• Meet legal and regulatory requirements • Promote responsible sharing and discretion • Proportionate controls appropriate to an asset's sensitivity • Make accidental compromise or damage unlikely	• Make accidental compromise or damage highly unlikely • Detect and resist deliberate attempts at compromise • Make it highly likely those responsible will be identified	• Prevent unauthorised access • Detect actual or attempted compromise • Identify those responsible and respond appropriately
Personnel Security	• Access by authorised individuals for legitimate business reasons	• Assurance that access is only by known and trusted individuals	• High assurance that access is strictly limited to known and trusted individuals
Physical Security (handling, use, storage, transport and disposal)	• Proportionate good practice precautions against accidental or opportunistic compromise • Control access to sensitive assets through local business processes and dispose of with care to make reconstitution unlikely	• Detect and resist deliberate compromise by forced and surreptitious attack • Destroy / sanitise to make reconstitution and / or identification of constituent parts highly unlikely	• Robust measures to prevent compromise by a sustained and sophisticated or violent attack • Destroy / sanitise to prevent retrieval and reconstitution
Information Security (storage, use, processing or transmission)	• Protect against deliberate compromise by automated or opportunist attack • Aim to detect actual or attempted compromise and respond.	• Detect and resist deliberate compromise by a sophisticated, determined and well resourced threat actors	• Robust measures to prevent compromise from sustained attack by sophisticated, determined and well resourced threat actors

Where the previous GPMS set out very specific guidance on how to store, transport and handle protectively marked documents, the ethos of the new system is to move away from process driven approaches that seek to do all the thinking for people. Individuals are expected to think about the nature and context of the information they work with and to exercise good judgement to ensure that information (and other assets) is handled and safeguarded appropriately.

Within Community Safety Partnerships you are most likely to be handling information that is OFFICIAL rather than SECRET/TOP SECRET and we would encourage you to consider the following in relation to physical and information security. Always record your decision to share the information and reasons behind this.

As a provider of protectively marked information …	***Things to consider and steps to take…***	**As a receiver or requester of protectively marked information…**	***Steps to consider…***
Is everything you're sharing directly relevant? i.e. Does the person/organisation you're sharing with 'need to know?	• *Refer to ISP if unsure* • *Remove irrelevant data*	Is everything you're asking for directly relevant?	• *Amend information or tasking request.* • *Refer to ISP if unsure.* • *Some information may be redacted.*
If this information was compromised would it… Cause substantial distress to an individual, prejudice individual security or liberty? Prejudice the investigation of/or facilitate the commission of serious crime or impede its investigation Disadvantage government or the police service in commercial or police negotiations with others Undermine the proper management of the public sector and its operations	*Recommend to receivers:* • *Storage with protection by one barrier (for example a locked container such as a drawer) or by two barriers (for example a locked container in a locked room).* • *Dispose/destroy in a manner to make reconstruction unlikely for example disposal in a shredder or a cross-shredder.* • *Dispose/destroy in a manner to make reconstruction and retrieval unlikely, for example disposal using a confidential waste bag and service.*	If this information was compromised would it… Cause substantial distress to an individual, prejudice individual security or liberty? Prejudice the investigation of/or facilitate the commission of serious crime or impede its investigation Disadvantage government or the police service in commercial or police negotiations with others Undermine the proper management of the public sector and its operations	• *Storage with protection by one barrier (for example a locked container such as a drawer) or by two barriers (for example a locked container in a locked room).* • *Dispose/destroy in a manner to make reconstruction unlikely for example disposal in a shredder or a cross-shredder.* • *Dispose/destroy in a manner to make reconstruction and retrieval unlikely, for example disposal using a confidential waste bag and service.*

Is this information only relevant for a certain time period or meeting?	• *Add a timescale for use and destruction* • *Content of the document can be shared at a named meeting but copies may not be distributed.* • *No electronic transmission and may only be circulated at a meeting, used for the meeting and copies retrieved from attendees when the meeting concludes.* • *The document may only be used for the purpose they were requested for – for example "This is a tactical assessment and may only be used at Areas March 2016 partnership tasking meeting".*	Is this information only relevant for a certain time period or meeting?	*Follow the guidance given on the document e.g. destroy within the given timescale, hand your copy in at the end of the meeting, do not forward to any other parties or share information from one meeting to another.*
General protection	• *Password protect electronic copies of the document. Make electronic copies of the document un-editable.* • *Transmission maybe limited to using GSX/GCSX secure email only.* • *Transmission in an opaque envelope through internal mail systems, delivered by hand in an opaque envelope and signed for.*	General protection	• *You may only receive certain types/levels of information if you have a secure GSX/GCSX email.* • *Some documents may be password protected and/or electronically uneditable.* • *Some documents may only be transmitted by hand and you will have to sign for them.*

Requesting Data

It is important that appropriate processes are put in place for requesting data to ensure timely and appropriate reports are produced, and to ensure data handling and marking are compliant.

Recommended practice is that all requests should be in writing clearly stating what information is required, for what purpose and all relevant timescales. This provides a paper audit of data shared and evidence to support compliance with data handling guidelines. Appendix 2 contains a tasking request template which can be amended for local use.

Having received the written request the analyst will normally contact you or the nominated officer to discuss the request in more detail to ensure that the end product is fit and appropriate for the purpose stated. The analyst may recommend other products or approaches proportionate to the task.

It is also recommended that all tasking requests are processed through a nominated officer who is familiar with the range of analytical products (Appendix 4) and techniques available (Appendix 1). This ensures a level of governance and control over data releases and allows competing requests to be priorities and managed.

In addition to ad hoc tasking, to support partnership priorities, partnerships should be clear in relation to their ongoing Intelligence Requirements. Specifically, what information and intelligence should be collected in relation to the priorities, but also crimes/incidents which show a trend that is of concern and/or constitute a high risk.

Not all partnerships have dedicated analysts, and even those that do also require in-kind support from partners to produce analytical products. It is therefore important that we are able to evidence the value and impact these products have in effectively tackling crime and safety issues. Recommended good practice suggests that following the production of any analytical product the recipient should complete a feedback form. The forms will enable partnerships to evaluate the quality, content levels, outcomes and actions generated through using analytical evidence. A sample is attached in Appendix 3.

Further Reading and Training

Legislation guidance

- HM Government's Security Classifications (2014) bit.ly/1oNpoI9
- Data Protection Act 1998 bit.ly/1RgNYjj
- Freedom of Information Act 2000 bit.ly/1SMrkOO

SCSN Training

- History and context of Community Safety eLearning
- Using and Handling Intelligence Data eLearning
- Evidence Based Strategic Planning eLearning (Module 1 – introduction)
- Evidence based Strategic Planning training (Modules 2-4 basic course)
- Evidence based Strategic Planning training (Modules 5- 6 advanced)

SCSN Toolkits

- National Data Guidance
- Partnership self-assessment toolkit

Scottish Government Guidance Documents

- A Partnership Strategic Assessment (2011)
- Strategic Assessment: Partnership prioritisation (2010)
- A Strategic Assessment Guide for Senior Managers (2010)

Appendix 1 – Analytical Techniques

Technique	*Description*
Criminal business profile	Contain detailed analysis of how criminal operations or techniques work, in the same way that a legitimate business might be explained.
Crime pattern analysis	Generic term for a number of related disciplines such as crime or incident series identification, crime trend analysis, hot spot analysis and general profile analysis. The aim of crime pattern analysis is to identify the nature and scale of emerging and current crime trends, patterns, linked crimes or incidents, and hot spots of activity.
Demographic / social trends analysis	Centred on demographic changes and their impact, analyses social factors such as unemployment and homelessness, and considers the significance of population shifts, attitudes and activities.
Horizon Scanning	A systematic examination of information to identify potential threats, risks, emerging issues and opportunities, long-term, allowing for better preparedness and the incorporation of mitigation and exploitation into the policy making process. This is a particularly valuable part of the strategic assessment process.
Market profiles	Continually reviewed and updated assessments that survey the criminal market around a particular commodity, such as drugs or stolen vehicles, or of a service, such as prostitution, in an area.
Mapping	Using a GIS (Geographic Information System) allows analysts to manage and visualise data from a geographic perspective. It can identify hotspots, geographical trends over time (for example displacement of ASB following a partnership operation) and community safety (trends) in relation to physical characteristics and landmarks for example offending patterns in relation to sites of interest for an offender (e.g. their home, school, shops, community centres etc.) GIS also allows partnership analysts to layer multiple datasets from various partners and see how they interrelate.

Network analysis	Describes the links between people who form criminal networks, but also the significance of these links, the roles played by individuals and the strengths and weaknesses of a criminal organisation.
Risk analysis	Assesses the scale of risks posed by individual offenders or organisations to individual potential victims, the general public, and also to law enforcement agencies.
Operational Intelligence Assessment	An operational intelligence assessment (OIA) involves evaluating incoming intelligence to maintain the focus of an operation on previously agreed objectives, particularly in the case of a sizeable intelligence collection plan or other large-scale operation.
Results analysis	Evaluates the effectiveness of law enforcement activities in order to inform future decision-making.
SWOT analysis	A SWOT analysis/matrix is a structured planning method used to evaluate the strengths, weaknesses, opportunities and threats involved and is particularly valuable when used as part of the strategic assessment process.

APPENDIX 2 – Tasking Form Template

<Insert CSP name and logo>

ANALYTICAL TASKING REQUEST FORM

NAME:	POSITION:
SERVICE/ DEPARTMENT:	CONTACT NO:
DATE REQUESTED:	DATE REQUIRED BY:

The tasking sheet must be as specific as possible in defining what exactly is required. It must be submitted to _____ for approval.

Once authorised the analyst will contact you to discuss it in more depth.

1. NATURE OF ENQUIRY

Give a brief outline of the subject matter, what you are hoping to achieve by asking for analysis, and how the information will be used:

What are you trying to achieve by asking for analysis e.g. to support a funding bid, assist in developing a strategy, provide evidence for introduction of road safety measures etc.

What is the problem e.g. an increasing issue with antisocial behaviour?

2. DISSEMINATION

Specify who this analysis will be shared with

Include names and organisations of all recipients.

3. FREQUENCY OF REQUEST

Please provide details of how often you would like this request produced.

Is it a one off to provide evidence for tasking or performance measuring, or part of an ongoing project/initiative which will require monthly/quarterly updates?

4. ANY OTHER RELEVANT INFORMATION

Please provide any details of the time period, geographical area and specific nature of the problem that requires analysis. If known, you may specify which analytical processes, products or charts you would like.

You can also include any background information here, for example which strategic priorities this request links to and who approved the tasking request (if applicable).

FEEDBACK

5. AGREED WORK

To be completed by the analyst

Please note the work agreed including analytical product(s), detail and scope, completion date and any other relevant information.

Include protective marking, storage and use.

Following the completion and submission of each analytical product, feedback must be provided within 10 working days using the analytical product feedback form.

Signed: Name (Print):

Date:

Please email your completed form to <insert name>

APPROVED/Not Approved by Nominated Officer

Signed: Name: Date:

APPENDIX 3 – Analytical Product - Feedback Form

<Insert CSP name and logo>

ANALYTICAL PRODUCT

FEEDBACK FORM

NAME:	POSITION:
SERVICE/ DEPARTMENT:	CONTACT NO:
DATE PRODUCT RECEIVED:	EMAIL:

ANALYTICAL PRODUCT CONTENT AND DEVELOPMENT	
Did the information meet your expectations?	Yes / No / In part
Was the information in too little or too much detail?	Yes / No / In part
Could the information be provided in a more useful way?	Yes / No / In part
Was the product produced with in the agreed timescales?	Yes / No / In part
Please rate how helpful you found the analyst(s)? 1 (not helpful) to 5 (very helpful)	☐
Any additional comments on the product content and development?	

PRODUCT USE
How did you use the analytical product?
What outcomes and actions did the analytical data support?

Appendix 4 – Analytical Products and their Purpose

Product	Purpose
Cost-benefit analysis	Cost-benefit analysis enables partnerships to evidence not only the cost benefits of initiatives but also how they have contributed financially to preventing public sector spending. SCSN has created a toolkit and training to assist with this available on the Safer Communities Scotland Website[1]:
Alcohol overprovision report	Overprovision reports use data on the level of alcohol availability and alcohol-related harm, both in relation to health and community life, and identifies areas which are over-provided for in respect of both off-sales and on-sales licensed premises.
Special event profile	This covers a range of events including bonfire night, gala days and parades or partnership operations focusing on antisocial behaviour. It allows the partnership to draw together a proactive plan and direct resources for events where there is likely to be unusually high demand. It uses a range of analytical techniques to identify: where issues are likely to occur, who could be involved, what the issues could be, when they are likely to occur.
Vulnerable Localities Index (VLI)	The Vulnerable Localities Index is a method which can identify communities that require prioritised attention. It integrates neighbourhood level data to form an overall composite index value of vulnerability for a locality. The Index value is calculated using six variables -housebreaking, vandalism to a dwelling, income deprivation, employment deprivation, educational attainment, and can be applied anywhere where access to reliable data on these variables exists.

[1] http://www.safercommunitiesscotland.org/training/toolkits-and-resources

Demand analysis	Incident and/or crime and offence data can be analysed to identify demand for resources. This could be used for developing a seasonal community safety program of preventative 'operations' and/or for understanding operational staffing requirements.
Results analysis	Combined with feedback on the analytical product, results analysis is used to find out what worked / what didn't work and any unintended outcomes; and informs future products and recommendations.
Comparative Case Analysis	Comparing the information on a criminal incident(s) with a view to identifying/eliminating the characteristics of a known offender(s) potentially linked to the type of incident.
Market Profiles	A market profile is an assessment that surveys the criminal market around a particular commodity, such as drugs or stolen vehicles; or of a service, such as prostitution. It will detail how active the market is, the trends in availability and price, the key individuals, networks and criminal assets. It will highlight associated trends in related criminality which are driven by or connected to the criminal market