

Evaluation Checklists for Intelligence Units

A. Possible Questions to be Included in Compliance Audits/Surveys for Intelligence Units – Paul R. Roger

Personnel Security

- What personnel security vetting procedures exist in respect of personnel working within the intelligence area?
- Are periodic security updates conducted for intelligence personnel on a regularly basis?
- Are guidelines in place for disclosure by members should their personal circumstances change?
- What measures are taken by the intelligence unit and its personnel to guard against subversion or other risks to the intelligence unit?
(In the context of personnel security, subversion is the altering of a person's loyalties, or changing a person's moral standards, by the application of some form of coercion. This coercion normally takes the form of bribery, blackmail, psychological pressure or physical threats. Subversion, as a general threat, is best countered by education of staff as to methods, thus allowing individuals to recognize and counter it.)

Physical Security

- Is the intelligence unit physically secure? (If yes, how?)
- Does the security prevent access by unauthorised persons?
- Is access and egress of authorized personnel monitored and recorded?
- Is access ability terminated when personnel are on leave or cease to work in the intelligence unit?
- Are there guidelines on staff taking intelligence material home or out of the building?
- Are there guidelines for transferring material to or from floppy disks?

Capture of Intelligence Material

- Do you have a data capture plan? (Attach copy of relevant documents)
- Does this plan detail procedures/guidelines that govern what intelligence is to be collected and the methods for collection? (Attach copy of relevant documents)
- What procedures are practiced to ensure that only designated data is captured and entered onto

the intelligence database?

- Who is responsible for collecting data?
- Who is responsible for ensuring correct procedures are followed in respect of collection?

Storage of Intelligence Material

Hard Copy Storage

- What procedures are in place to govern the storage, handling and security of hard copy source material? (Give details or attach copies of relevant documents.)
- Do you retain hard copy source documents regarding intelligence information?
- Where are they stored?
- Who has access to these documents?
- How is access controlled?

Electronic Storage

- Are there guidelines for recording intelligence material on electronic (IT) systems? (Give details or attach copies of documents.)
- Are there adequate access checks and scrutiny, e.g. Passwords, etc
- How often are passwords changed?
- Is facility access deleted when personnel are on leave or cease to work in the intelligence unit?
- Is the IT system capable of producing an audit trail for any system interrogation?
- Is access graded on a 'need to access' basis?
- Are files adequately safeguarded through back-up and recovery routines, and off-site storage of critical files, programs and systems?
- Is the IT system isolated from other networks and, if not, are appropriate “firewalls” in place?

Integrity of Intelligence Material

Quality Control

- What quality control procedures are in place to ensure quality of data is maintained?

- In respect of electronic databases, what procedures are in place to ensure quality of data?
- Is there a clear responsibility in a particular position for the continued development, maintenance and implementation of quality control systems.

Culling and Destruction

- Do you have procedures for the culling and destruction of intelligence material?
- What criteria is used during the culling process?
- Who is responsible for culling and the subsequent destruction?
- Are staff aware of any relevant Archive or related legislation?
- When hard copy material is culled, is corresponding electronic data also culled? (If yes, who is responsible for culling electronic data?)
- Are records maintained of culling and destruction exercises? (If yes, are they available for inspection?)

Availability of Intelligence Material

Access

- What electronic databases are maintained that contain intelligence material?
- Who has access to these databases?
- What level of access do officers possess (e.g. read/write etc.)?
- Who is responsible for controlling access?
- Who audits access?
- How often are audits conducted?
- How are audits performed (e.g. reactively, proactively, regularly, randomly etc.)?
- What records are maintained in respect of audits of access?
- Is access immediately deleted when personnel leave or transfer?
- Are regular reviews undertaken to determine the continued necessity for current personnel to have intelligence system access?

Dissemination of Intelligence Material

At Own Initiative

- Are there procedures covering the dissemination of intelligence material? (If yes, attach procedures.)
- Who may authorize dissemination of intelligence material?
- What records are kept of dissemination of intelligence material?
- Are these records audited?
- If audits are conducted, who by?
- Are records kept of such audits for inspection purposes?

Responses to Requests

- Do you have procedures that govern the way intelligence personnel will respond to a request for information? (If yes, attach procedures.)
- What criteria is used in reaching a decision regarding the need and right of the requesting person to receive information?
- What records are kept of requests and responses?
- Are these records audited?
- If yes, by whom and how frequently?
- Are records kept of such audits?

Transmission of Material

- Do you have procedures which govern the methods of enveloping, dispatching and recording of such dispatch of classified material from the intelligence unit? (If yes, attach procedures.)
- What methods of dispatch are used for intelligence documents dispatched from your unit (e.g. courier, safe hand, internal dispatches, postal services etc.)?
- What criteria is used in reaching a decision as to which method of dispatch to use?
- Are there appropriate mechanisms in place to identify the non-receipt of classified material? (If yes, attach procedures.)

Accountability and Management of System

Responsibilities

- Is there are regular assessment of the purposes and goals of the intelligence system and an evaluation of the extent and effectiveness of the achievement of these goals?
- Are there clear lines of responsibility and accountability for the functions of the intelligence unit?
- Are individual responsibility statements regularly reviewed and updated?
- Are there adequate resources to meet the responsibilities in a practical way?
- Is a regular Security Risk Review of the intelligence unit and its systems carried out?
- Are managers and those responsible for the effective operation of the intelligence system adequately trained and kept up to date in the required operation of the system?
- Are delegations and authority limits regularly reviewed?

Awareness

- Are staff generally aware of the security and privacy implications of the intelligence function and the collection and storage of intelligence material?
- Is there an adequate system to ensure any amendments or updates to procedures are read and understood?
- Are staff aware of actions they should take and procedures to follow should they encounter any departures from approved policy and procedures in the operation of the intelligence system?
- Does unit management clearly demonstrate that it insists on the highest standards of ethical and professional behaviour?

B. Numeric Intelligence Evaluation System from Harris (1976:134-138)

This approach is based on an evaluation in terms of questions relating to the major elements of the functions within the intelligence process. On the basis that each function is essential to the process, each is assigned a value of 100 as follows:

| | |
|---|-----|
| Collection/flow of information | 100 |
| Processing/collation of information | 100 |
| Analysis | 100 |
| Production/dissemination of information | 100 |
| Management procedures | 100 |

Points are then assigned based on the following breakdown of each function.

a. Collection

| | |
|--|-----------|
| (1) Intelligence unit receives as part of normal flow of information, copies of all (the bulk of) investigator reports (except in large units where reports relating to known or suspected persons associated with organized crime and major criminal activity would be sufficient). | 30 |
| (2) Intelligence unit has its own investigators or can task the department's investigative unit to probe areas determined to be important as a result of the intelligence unit's assessment. A procedure exists for the tasking of non-intelligence unit personnel on the basis of agreement between the intelligence and operational unit commanders or orders of the department chief. | 25 |
| (3) Department has an effective procedure operating whereby the officer on patrol can report on specified subjects directly to the intelligence unit. | 20 |
| (4) Intelligence unit receives (or at least records information contained in) sensitive reports from undercover units, informants, or other specialized sources. | 15 |
| (5) Intelligence unit has a plan of action to gain information from other law enforcement agencies—local in area, state, and federal. | <u>10</u> |
| Total | 100 |

b. Processing/Collation

| | |
|--|----|
| (1) Information, once filed, can be quickly and correctly retrieved | 30 |
| (2) The information filing system has a capability to focus data received by major crime figures, area/location, type of crime, and other subjects the analysts find useful. | 30 |
| (3) Unit has an information flow system that causes reports to be reviewed distributed, and earmarked for filing in a manner that ensures the analysts (or other persons responsible for performing analyst functions) reads important reports relating to his/her area of responsibility. | 25 |

| | |
|---|-----------|
| (4) There is an efficient and effective operating system for updating biographies (abstracts or biographic forms) of known or suspected major criminals in the area (not necessarily restricted to persons residing within the boundaries of the jurisdiction). | 25 |
| (5) There is an operational plan for purging the files of outdated and non-pertinent material. | <u>10</u> |
| Total | 100 |

c. Analysis

| | |
|--|-----------|
| (1) The intelligence unit has one or more persons tasked to analyze information received to develop/project/estimate: | 50 |
| - patterns of organized crime by type of crime | |
| - patterns of association among persons believed to be part of organized crime | |
| - interrelationships among criminals and types of organized crimes in which they are suspected of being involved. | |
| (2) The intelligence unit has a procedure whereby the person or persons responsible for analysis are available to assist departmental investigators, in person or by phone, by applying information in the intelligence file and his/her own expertise to a current investigation. | <u>50</u> |
| Total | 100 |

d. Production/Dissemination

| | |
|--|-----------|
| (1) The intelligence unit is responsive to requirements of on-going investigations, including having a procedure to keep its members aware of major cases. | 40 |
| (2) The intelligence unit produces periodically and/or on order reports on major trends in criminal activity in its jurisdiction, emphasizing new or developing types of organized crime activities. | 30 |
| (3) Intelligence reports are disseminated as widely as possible within limits set by need-to-know and sensitivity of information (the rule should be positive, giving the benefit of dissemination to those who need and can use the information). | <u>30</u> |
| Total | 100 |

e. Management Procedures

| | |
|---|----|
| (1) The intelligence unit has a procedure for obtaining the reactions of consumers to its products. | 25 |
|---|----|

| | |
|---|-----------|
| (2) The intelligence unit has a collection plan to assist it in focusing its efforts on the most important of the crime problems. The plan is periodically updated (monthly) and is coordinated with the chief of investigations and approved by the department head. | 20 |
| (3) There is an element in the department's training program to prepare personnel for the specialized activities of the intelligence unit, especially analysis and intelligence investigation. | 20 |
| (4) Security guidelines are in existence and observed, especially in limiting access to the files to analysts and file clerks, distributing intelligence reports only to those with a need-to-know within the organization and only to other law enforcement agencies on the outside with whom there is an agreement for the protection of the intelligence material. | 20 |
| (5) There is a procedure for evaluation of the effectiveness of the intelligence unit's operation. | <u>15</u> |
| Total | 100 |

In evaluating performance, each element will be graded in terms of the following scale:

1. The element is being implemented effectively 1.0
2. The unit is organized to accomplish the element but the operation is only partially effective .80/.70/.60
3. The unit is in the process of organizing to accomplish the element but is not yet operational .50
4. The unit has been organized to accomplish the element but the operation is ineffective .30
5. The unit has not/does not recognize the requirement to accomplish the element 0

An example of how this system would apply follows.

- A. *The intelligence unit is responsive to investigations including having a procedure to keep its members aware of major cases.* The evaluator found there was no procedure to keep its members aware of major cases; thus he gave the unit .60 of the total value of the item or .60 times 40 which equals 24 points.
- B. *The intelligence unit produces periodically and/or on order reports on major trends in criminal activity in its jurisdiction, emphasizing new or developing types of organized crime activities.* The evaluator, after reviewing reports, found that they were being produced, but only infrequently highlighted new and developing organized crime activity. Thus, he gave the unit only .70 of this value, or .70 times 30 which equals 21 points.
- C. *Intelligence reports are disseminated as widely as possible within limits set by need-to-know and sensitivity of dissemination.* The evaluator finds that the unit stresses dissemination and gives the unit full value, or 1.00 times 30 which equals 30 points.

Total for this portion of evaluation: 75 points