

# S121 SIGINT Reporting Basics

Instructors:

SIGINT Production Training Coordinators  
DGI [REDACTED] Group)

- Introduce 'self (our credentials to teach) – Me [REDACTED]  
IRRELEVANT
- Explain how the course is structured (taught over 2 days/4 mornings)
- Explain that the students can keep the manuals and mark them up  
(except military)

## **Course Overview**

The SIGINT Reporting Basics course is part of the introductory training package offered to new analysts.

We will explore the mechanics of SIGINT reporting by taking you through the reporting process step-by-step.

We will also briefly review collection, processing, legal and CSE policies as they apply to SIGINT reporting.

[ 2 ]

**Part of the introductory training package for new analysts**

**Also part of the mandatory Report Writing package for all report producers.**

# Course Outline

## Module 1 - Requirements

- Requirements & Priorities
- Client interaction
- GCRs EXERCISE
- Legal Authorities
- Privacy information

## Module 2 - Collection

- Collection mandate
- Collection overview
- Legal concerns
- TERMINOLOGY EXERCISE

## Module 3 - Research & Analysis

- Guidelines for Analysis
- Biases & Assumptions
- Research
- RESEARCH EXERCISE

## Module 4 - SIGINT Reports

- Types of reports
- Sensitivities
- Classifications
- Serial numbers
- SERIAL NUMBERS EXERCISE
- Organizational strategies

## Module 5 - SIGINT Report Layout

- Report body
- KEY POINTS & ANALYSIS EXERCISE
- Titles
- TITLES EXERCISE

## Module 6 - SIGINT style

- Revising
- Abbreviations & acronyms
- Style guidelines
- SIGINT STYLE EXERCISE

## Module 7 - Naming Policy

- Validity wording
- Naming exemptions
- Contextual identification
- NAMING EXERCISE

## Module 8 - Write-to-release (WTR)

- [REDACTED]
- Exemptions
- WTR EXERCISES

## Module 9 - Metadata

- Report TAG lines
- TAGs EXERCISE
- Corrections and cancellations

3

- Go through the course outline – what the students can expect to cover in the 4 mornings
- Normally, Day 1 covers Modules 1-3; Day 2 covers Modules 3-6, Day 3 covers Modules 7-8, Day 4 covers Modules 8-9. Any leftover time on Day 4 can be used to complete the final (open book) quiz otherwise it will be provided as a take-home exercise.
- Takes approx. 45 mins. to complete. The quiz will review the course content.

## Icebreaker

Who are you? Where are you from originally?

What group are you in?

How long have you been at CSE/CFIOP and SIGINT?

Have you contributed to any SIGINT reports?

...(and just for fun) What was your first paid job?

[+]

- Have the students introduce themselves: name, area of work, how long they've been at CSE, where they came from geographically or study/work-wise, if they've written any SIGINT reports yet and how many
- Ice-breaker: What is your biggest fear/obstacle in writing? E.g. How to start, grammar, finding the right word, summary, how to end it?

<h2>Module 1: Requirements</h2>	
<p>Agriculture &amp; Agri-Food [REDACTED]</p> <p>Canada Border Services Agency Canada Revenue Agency [REDACTED]</p> <p>Canadian Food Inspection Agency CFIOTG [REDACTED]</p> <p>Canadian International Development Agency (CIDA) [REDACTED]</p> <p>Canadian Nuclear Safety Commission [REDACTED]</p> <p>Citizenship and Immigration Canada CSIS</p> <p>Department of Foreign Affairs and International Trade (DFAIT) DND</p>	<p>Environment Canada [REDACTED]</p> <p>Finance Fisheries and Oceans FINTRAC</p> <p>Health Canada Indian and Northern Affairs Industry Canada Justice Canada Natural Resources Canada [REDACTED]</p> <p>Privy Council Office (PCO) Public Safety and Emergency Preparedness Public Works and Government Services (PWGSC) RCMP</p> <p>Solicitor General Transport Canada Treasury Board</p>
	<p>[REDACTED]</p> <p>[REDACTED]</p>

Variety of clients from different areas of government.

Some may be as you'd expect

CSIS

CFIOTG

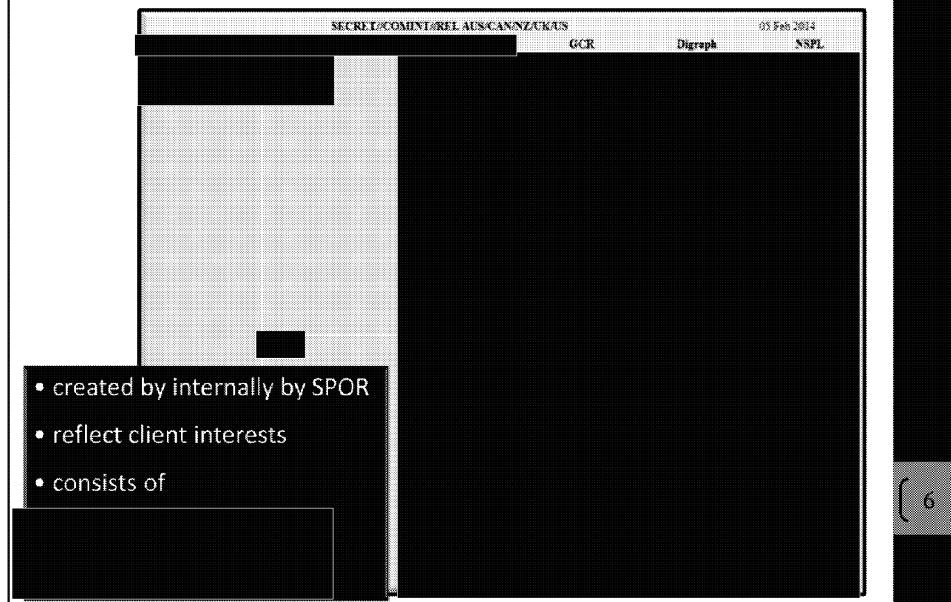
CBSA

Some may surprise you:

[REDACTED]  
[REDACTED]

Fisheries and Oceans:

## Gov. of Canada Requirements



Page 5-6

All the reports we write must meet at least one Government of Canada Requirement (GCR)

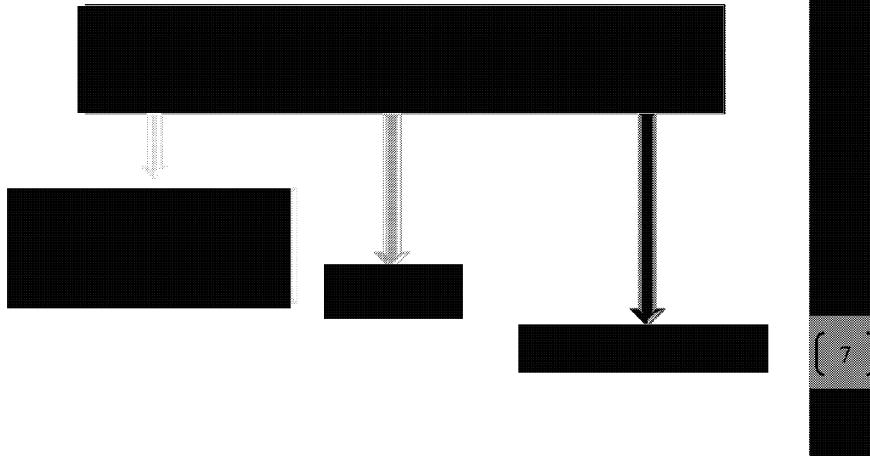
- are generated by the SIGINT Programs Operational Requirements (SPOR)
- reflect the Canadian government's ongoing intelligence requirements.
- are based on feedback from clients
- specify their needs by submitting a Client Request (CR) in [redacted]

A list of GCRs can be found on [redacted]

[redacted]

## Gov. of Canada Requirements

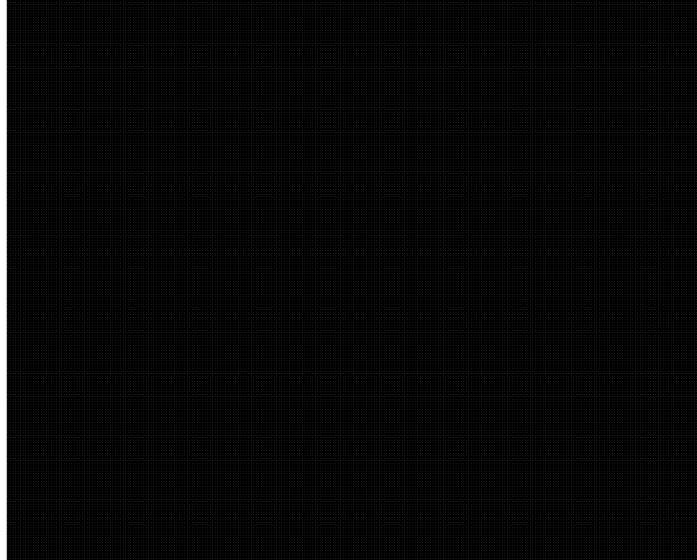
**Example –** The GCR [REDACTED] can be broken up in the following way:



- It is a **three-level indexing system**
- GCRs can be broken down into [REDACTED] (**general**), [REDACTED] (**more specific**) and [REDACTED] (**very specific**)
- They are then **grouped in Tiers** to reflect their respective importance.
- Analysts technically **assign GCRs** to the product they write by selecting specific **TAGS** or **using specific keywords** in the text of the product which are scanned by [REDACTED] for dissemination.
- These GCRs are **mapped to all product** whether authored by CSE, CFIOG, or by the allies and are used to deliver the right product to the right client's channel(s).
- The requirements for information represented by a GCR will direct our tasking of selectors
- Reports are then written based on the information collected from these selectors and linked back to the initial requirement so the report can be delivered to the original client.

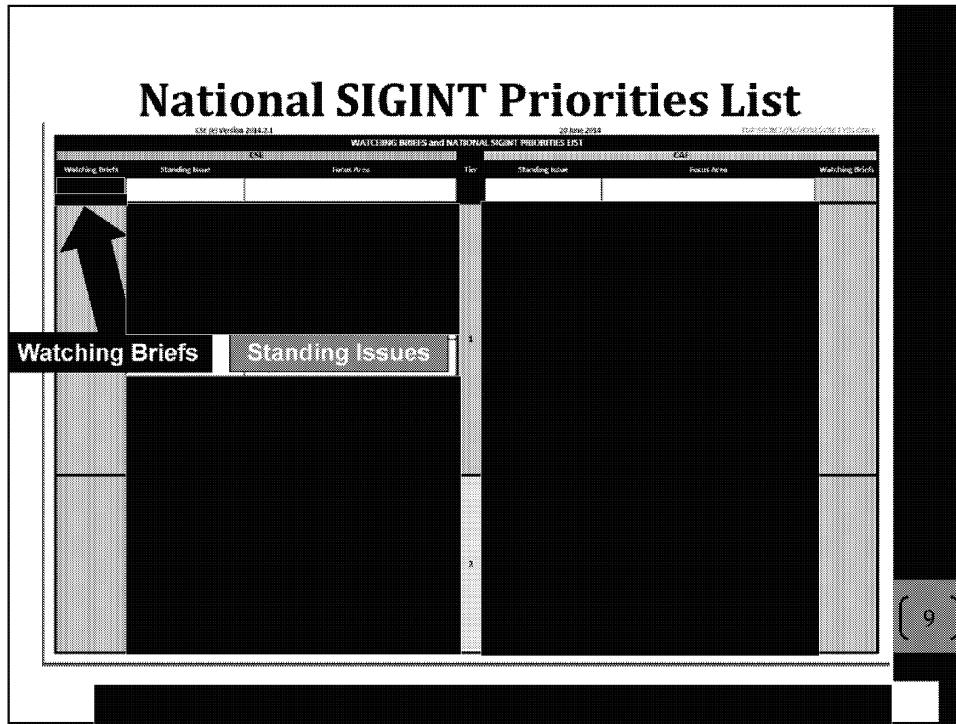
## Gov. of Canada Requirements

TAGs



[redacted]  
8

This report meets five requirements, as listed under "GCRs".



Page 7-9

The NSPL is a document which consists of **two tiered lists**: Standing Issues and Watching Briefs.

These define the priorities for the National SIGINT System, which comprises **CSE and CFIOG**.

The NSPL **provides strategic direction** to focus resources on areas of highest priority. As circumstances change, target sets may be **added** to the list or **elevated** in priority, as required. Target sets no longer of critical importance may also be **removed** or **downgraded** in priority

#### **Standing Issues:**

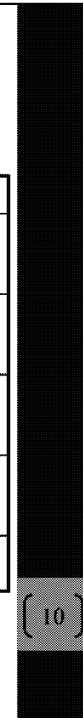
- Items of **long-term** interest;
- updated **3-4 times/year** based on information gathered from the annual CSE Government of Canada Intelligence Priorities Ministerial Directive (**MD**) among other sources

#### **Watching briefs:**

- Can be items of short- (3 months) or medium-term (6 months) interest
- Issues can rise and fall in priority

## National SIGINT Priorities List

Tier	Description
1	[REDACTED]
2	[REDACTED]
3	[REDACTED]
4	[REDACTED]



■% of CSE reporting comes from Tier ■ Currently there are no Tier ■ operations although should any imminent threats arise [REDACTED] we may see that moving from Tier ■ to Tier ■.

## GCRs, Client Requests and RFIs

- GCR: a group of client's general information requirements.
- Client Request (CR): single client's specific information needs. Client Requests can be seen through [REDACTED]
- Request for Information (RFI): details of a client request further refined. The client may set an expiry date for the request (default expiry is 6 months).

**GCR** is the general information requirement **agreed upon by numerous clients that share similar needs**.

A Client Request (**CR**) is an individual client's information need that **falls under the more general GCR**.

You can search for **Client Requests** in [REDACTED], or set up a channel to have them sent to you.

A Client Request can be further refined through a narrative **RFI**. It's an opportunity for the client to **expand on their information need**.

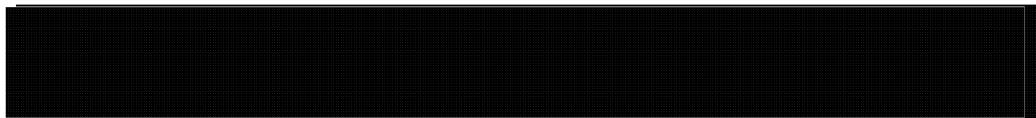
An RFI typically has a **short shelf life** and the client can choose the lifespan by setting an **expiry date**.

## Client Request (CR)



Page 10

Here's an example of a Client Request with an RFI.



## Feedback

The feedback component contains 3 rating categories:

1. **Satisfied Need** (default rating)
2. **Exceptional**
3. **Improvements Needed**

Exceptional feedback may also indicate **Actionable Intelligence**.

A **comments field** may be completed for feedback indicating the reasoning for the rating selected.

Page 11-12

### Actionable Intelligence

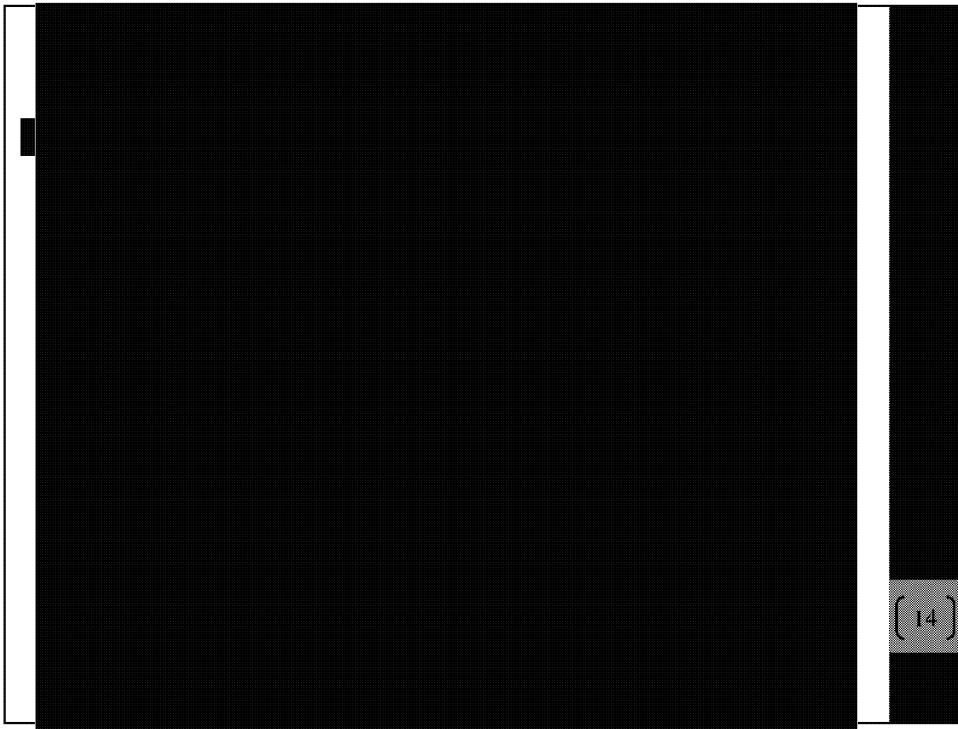
Further broken down into the following categories:

**Identified a Threat**

**Influenced a decision**

**Significant action taken**

There are examples of feedback on page 12 of your manual.

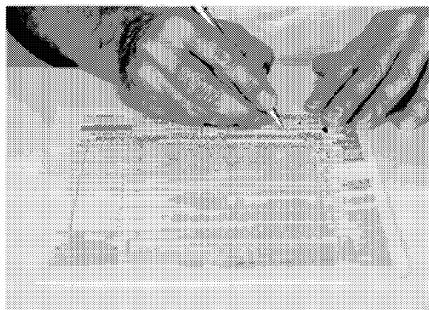


Notice under Exceptional and Improvements needed there is a drop down indicating possible explanations.

For the default response “Satisfied Need” there is no comment required but there is a place lower on the form for free flow comments.

Show examples of Feedback?

## GCRs EXERCISE



Resources: [REDACTED]

[REDACTED]



Have the students refer to the list of GCRs online [REDACTED] and find the [REDACTED] for the three GCRs on page provided.

## National Defence Act

According to the *National Defence Act* (NDA), the mandate of CSE has three parts:

**Part A**

- To acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence in accordance with Government of Canada intelligence priorities

**Part B:**

- To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada

**Part C:**

- To provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties

Explain the 3 mandates of CSE:

- Part A is the Foreign Intelligence (FI) mandate
- Part B is the Information Technology Security (ITS) mandate
- Part C consists of technical and operational assistance to federal law enforcement (RCMP) and security agencies (CSIS)

Analysts in DGI operate mostly under Mandate A [REDACTED]  
[REDACTED] very rarely under Mandate B [REDACTED]

Analysts should understand and be able to explain under which Mandate they're operating.

## National Defence Act (273.61)

### Foreign Intelligence (FI) (*Defn.*):

Information or intelligence about the  
capabilities, intentions or activities  
of a  
foreign individual, state, organization or terrorist group  
as they relate to  
international affairs, defence or security.

CSE is a foreign intelligence agency. This is the definition of foreign intelligence as per the National Defence Act.

IRRELEVANT

[REDACTED]

Page 13

We have a Memorandum of Understanding (**MOU**) with CSIS which establishes an arrangement under which the two organizations will **cooperate** for the purpose of **information and intelligence collection, information sharing and operational support** in accordance with their **respective mandates**.

IRRELEVANT

## CSIS Act

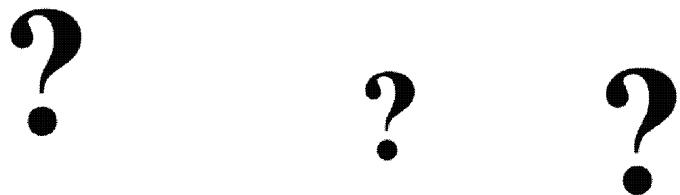
IRRELEVANT



IRRELEVANT

# Question

Which CSE Operational Policy governs the **protection of privacy of Canadians?**



[redacted]

Answer on next slide: OPS-1

## OPS-1

### *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*

Analysts must apply **SIGINT privacy annotations** to traffic containing recognized:

- Private communications
- Communications of a Canadian located outside Canada
- Information about Canadians (and no FI value)
- Solicitor-client communications

Privacy Information must be:

- stored in Mandate AIRRE folders
- shredded when no longer needed, not put in burn bags

The events of September 11, 2001, led to an increase in authorities being granted to CSE

With these additional authorities there is a **greater potential for collecting communications with privacy information (PRIVATE COMMUNICATIONS)**.

As a result, procedures such as applying privacy annotations to traffic have been put in place to **protect** this type of information.

Next: Legal definition of a Private Communication

## Private communications

### - Legal Definition

**Any oral communication, or any telecommunication, that is made by an originator who is in Canada or intended by an originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it. (*Criminal Code*, section 183)**

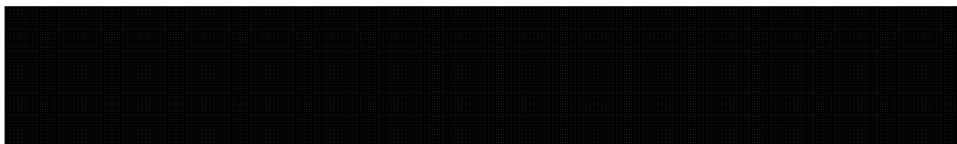
Next: Practical definition of a Private Communication

## Private communications

### - Practical Definition

**Any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by an originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any telephone communication that is treated electronically, otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it. (Criminal Code, section 183)**

Example:



## Privacy Annotations

### For non-solicitor-client communications

Location	If one communication is physically located in Canada	If one communication is a Canadian physically located outside Canada	Both communications are foreigners located outside Canada, but the communication contains information about a Canadian	Recommended one end Canadian emails			
Source	[Redacted]						
Essentiality	Contains FI essential to international affairs, defence or security of Canada	Not essential/ annotate for deletion	Contains FI essential to international affairs, defence or security of Canada	Not essential/ annotate for deletion	Contains FI essential to international affairs, defence or security of Canada	Not essential/ annotate for deletion	Contains FI essential to international affairs, defence or security of Canada
Annotation	INCA	INCAN	OUCA	OUCAN	(None required)	IACN	AM

### For solicitor-client communications

Location	If one communication is physically located in Canada	If one communication is a Canadian physically located outside Canada		
Source	[Redacted]			
Essentiality	Contains FI essential to international affairs, defence or security of Canada			
Annotation	INCAS	INCASN	OUCAS	OUCASN

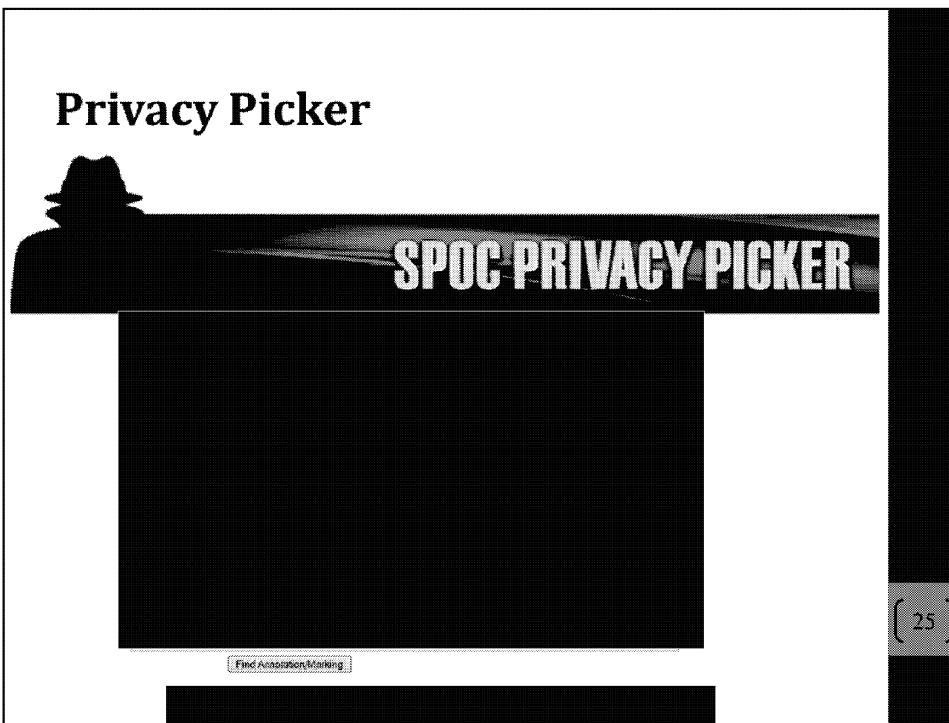
Also found on page 19

#### Privacy annotations based on:

Location of communicants

Source of information

How essential the information is to our reporting (ie: does it contain FI)



New tool designed by SPOC to assist analysts in deciding what privacy annotation their traffic requires based on:  
Location of communicant,  
FI, and  
traffic source.

## Module 2: Collection

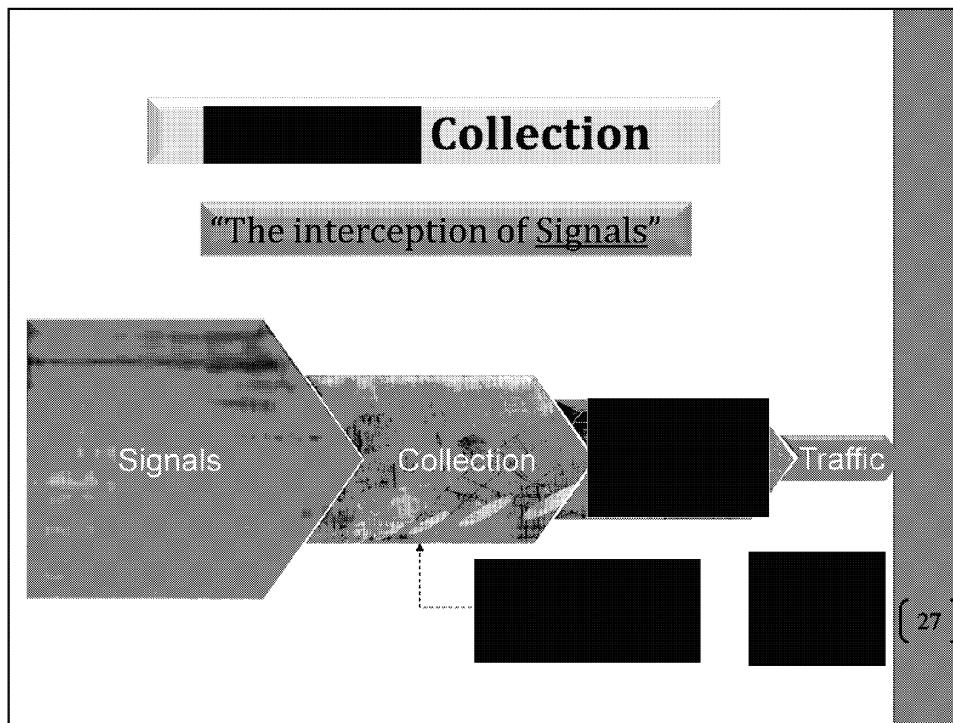
(26)

Page 19

Before 9-11, we could do [REDACTED] but limited collection. No collection was possible if there was a risk of intercepting Canadian communications.

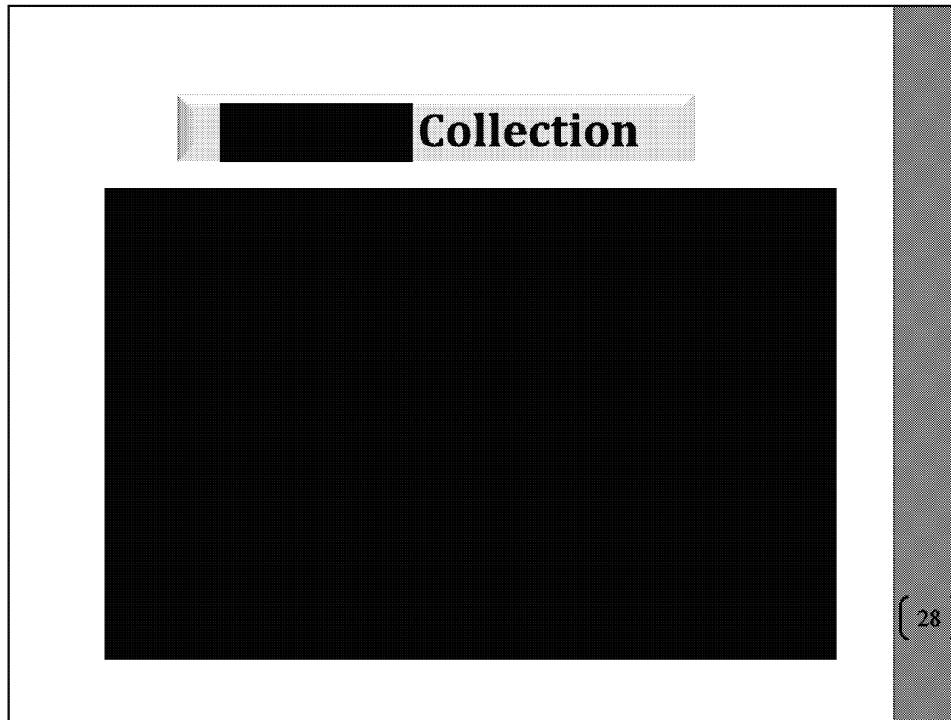
It's extremely important to understand where your collection is coming from on any given target so that if it should disappear you will be better positioned to assist [REDACTED] in retrieving it. To help diagnose the problem [REDACTED] will likely need to know:

[REDACTED] your traffic; [REDACTED] (this can all be done by knowing your [REDACTED])



We look at [REDACTED] the available **signals**. **Collection** is [REDACTED] before it even enters the building (eg: [REDACTED] etc.)

[REDACTED]  
[REDACTED] SIGINT collection is the process of **intercepting foreign communications** as they [REDACTED] the Global Information Infrastructure (GII).

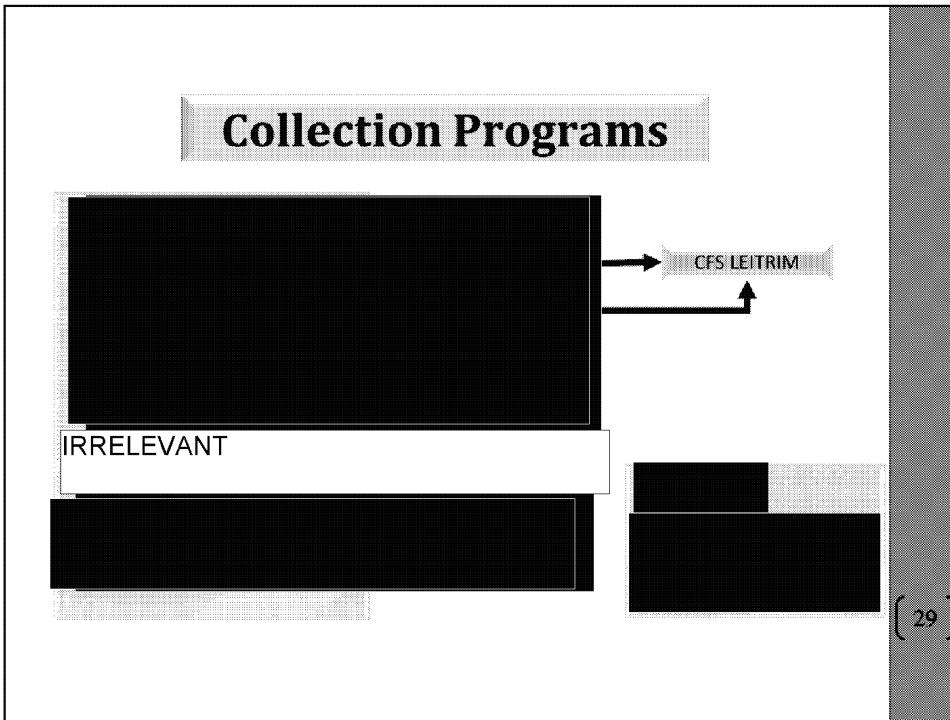


[REDACTED] is mainly responsible for [REDACTED]  
[REDACTED]

[REDACTED] collection could involve:

Very sensitive information/procedures  
risk of embarrassment to GoC





CFS Leitrim is the site that [REDACTED]

[REDACTED]

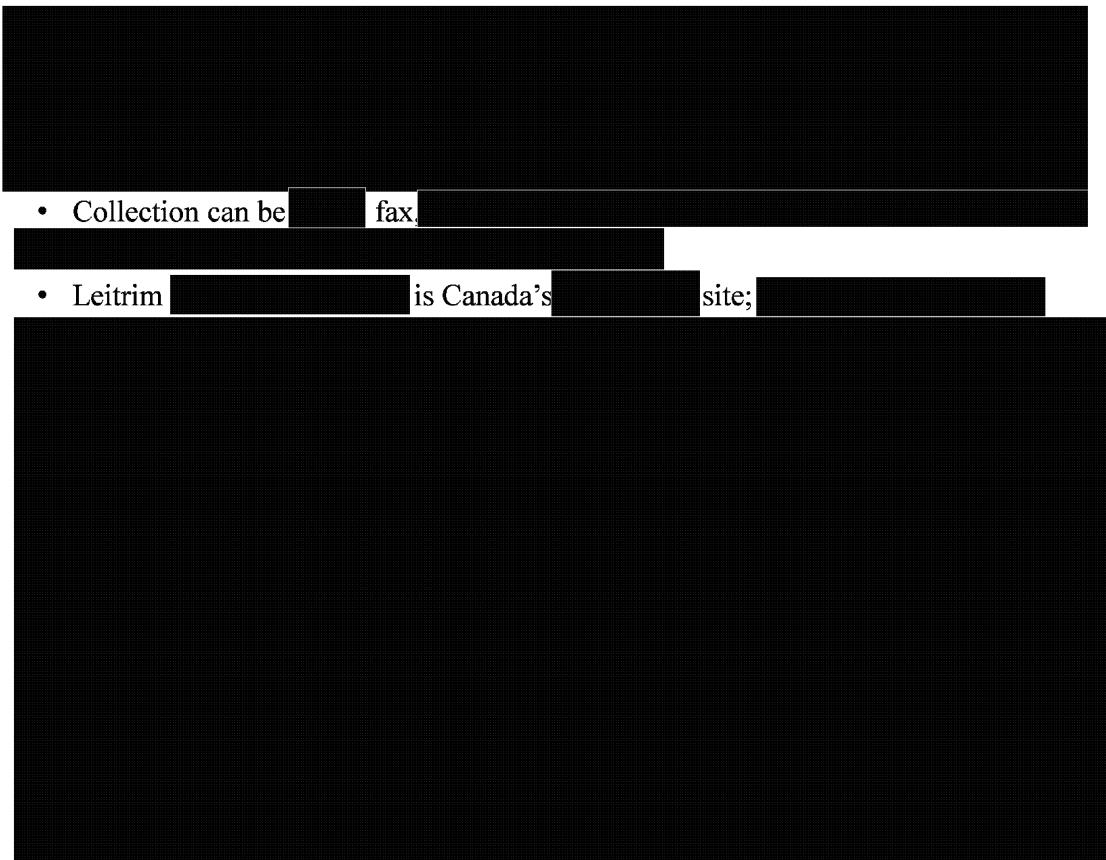
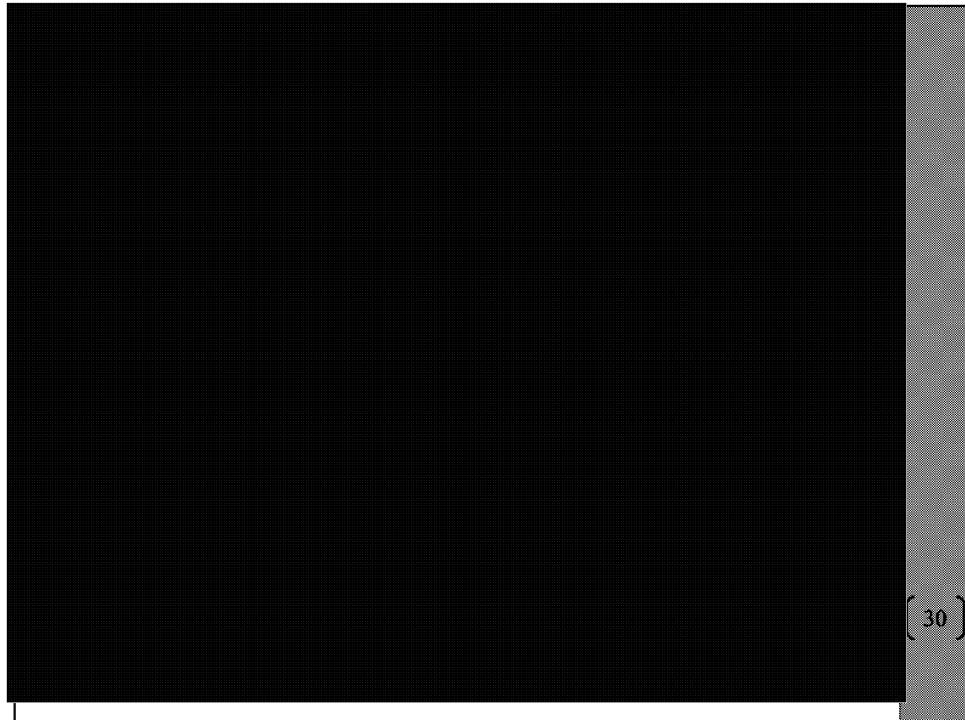
[REDACTED]

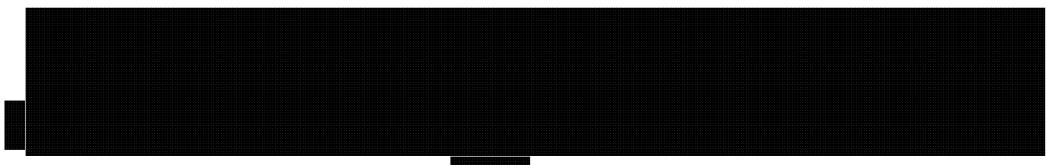
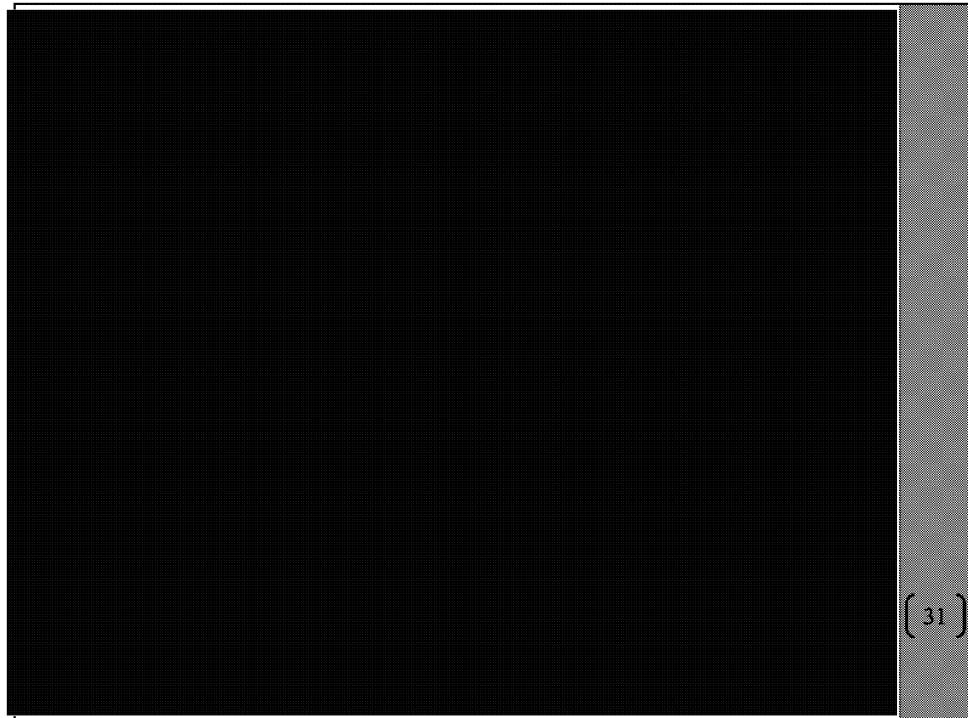
[REDACTED]

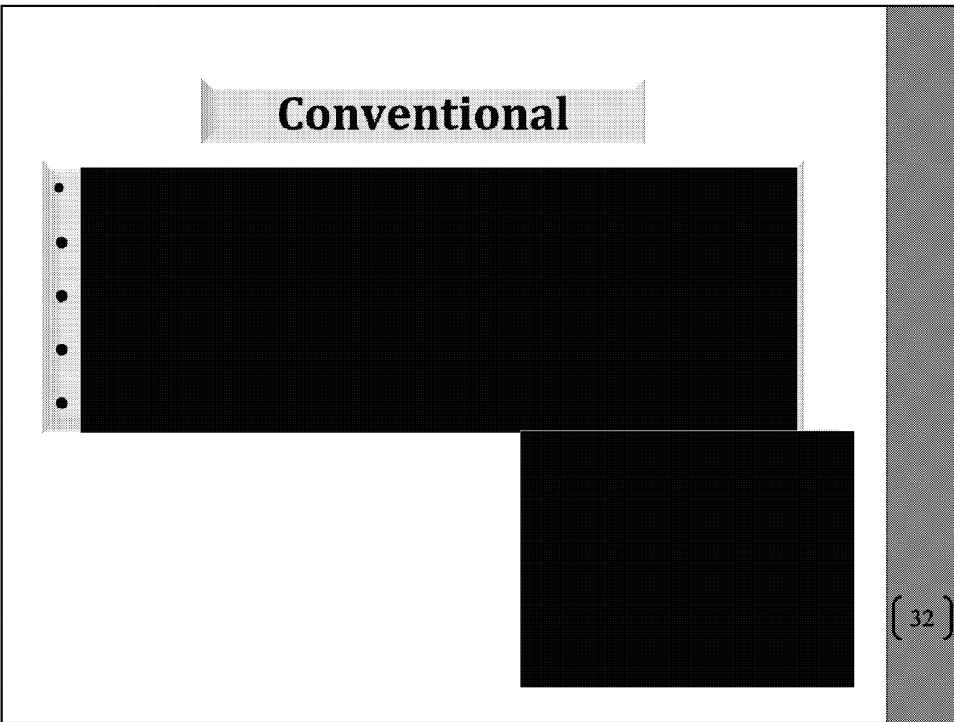
[REDACTED]

IRRELEVANT

can be either [REDACTED]

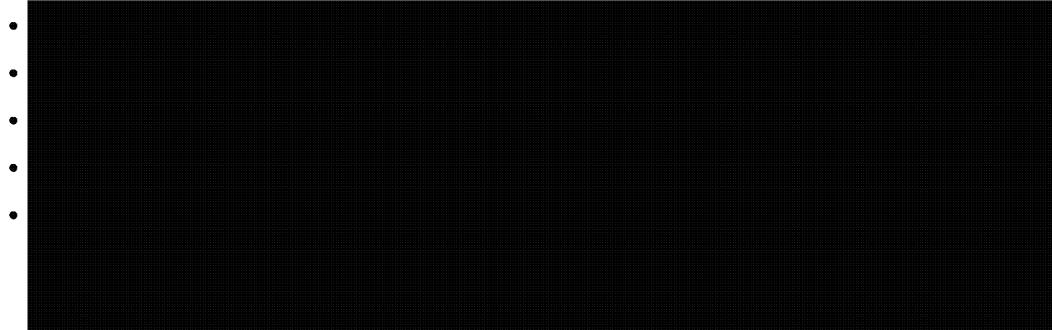


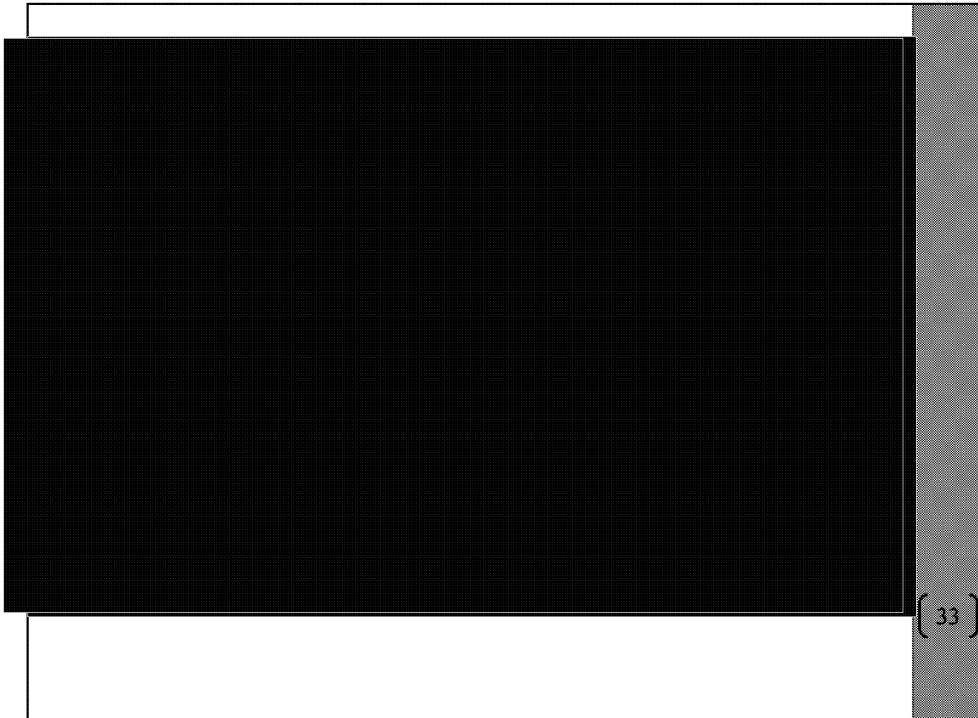




Conventional

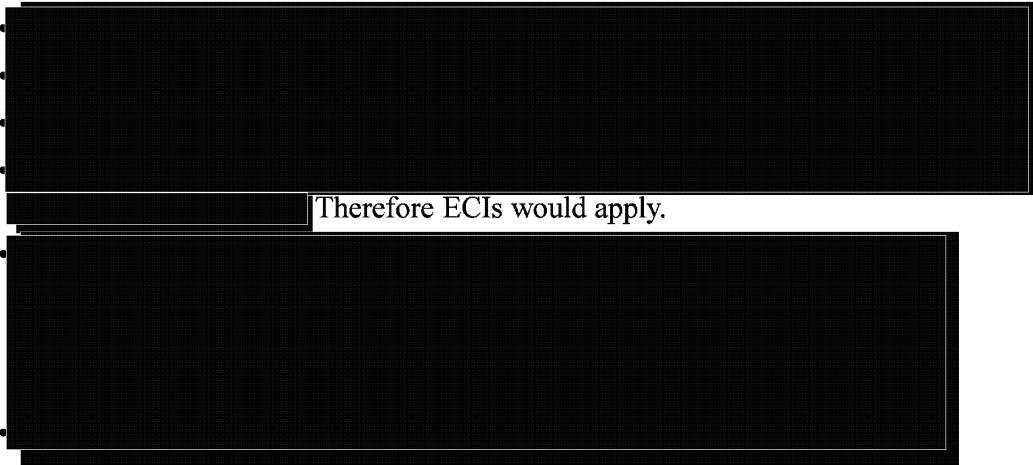
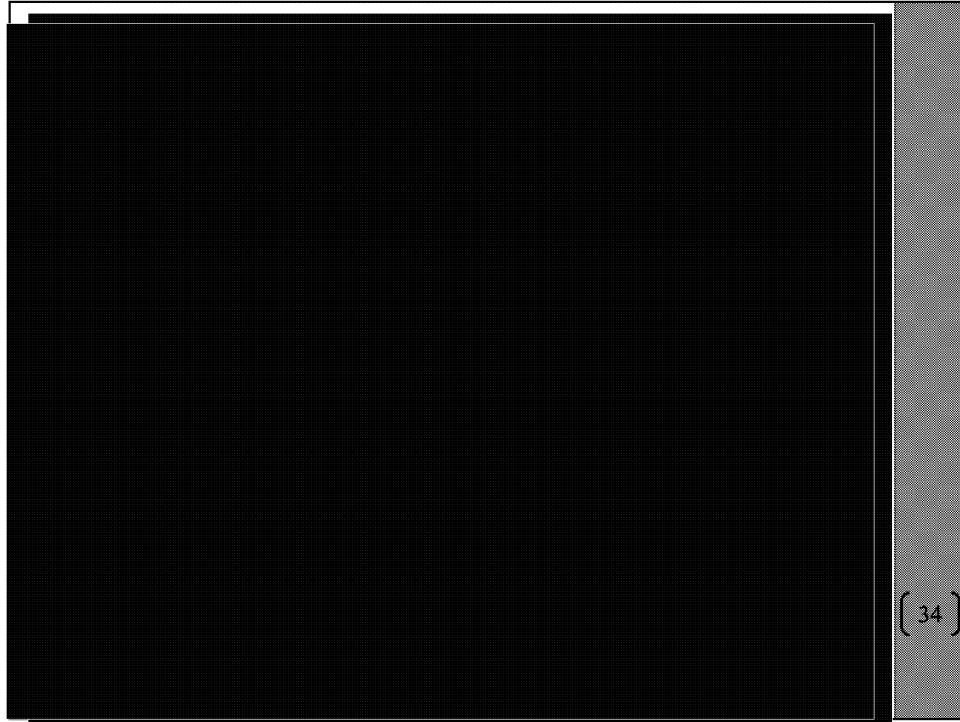
- mainly intercept of [REDACTED]

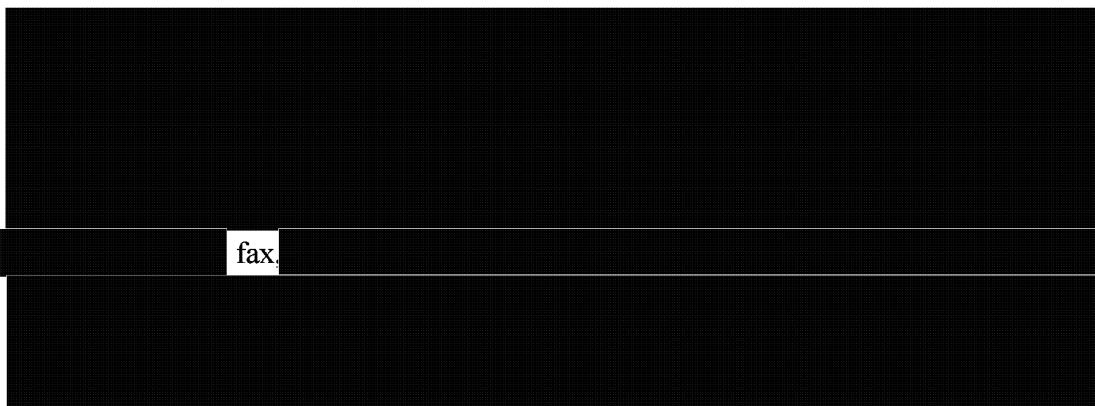
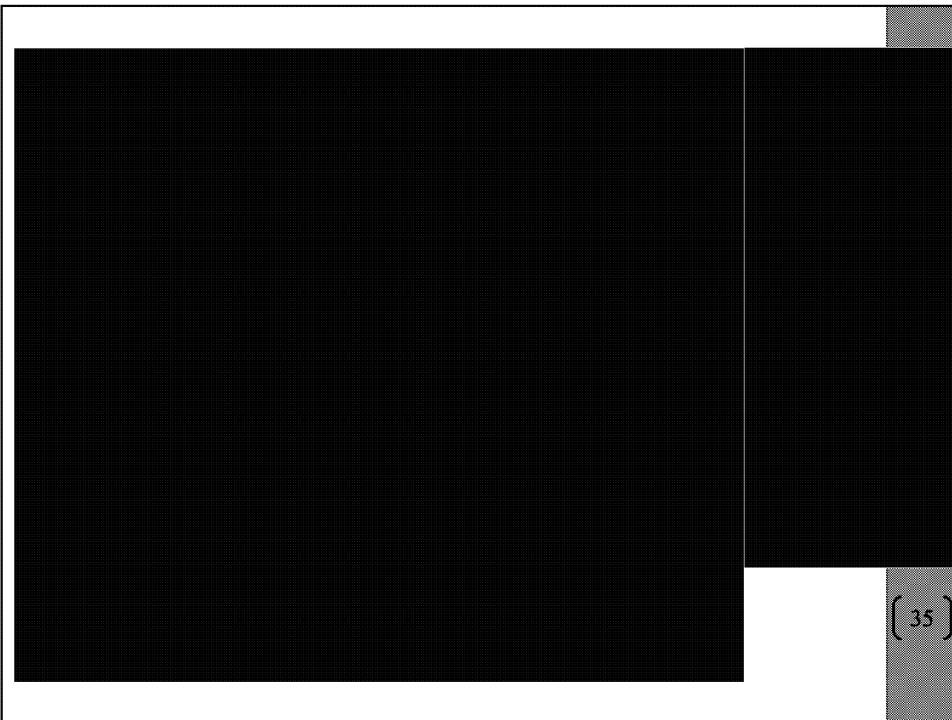




- [REDACTED]
- [REDACTED]
- Collection of [REDACTED] fax, [REDACTED] DNI [REDACTED]
- [REDACTED]

IRRELEVANT

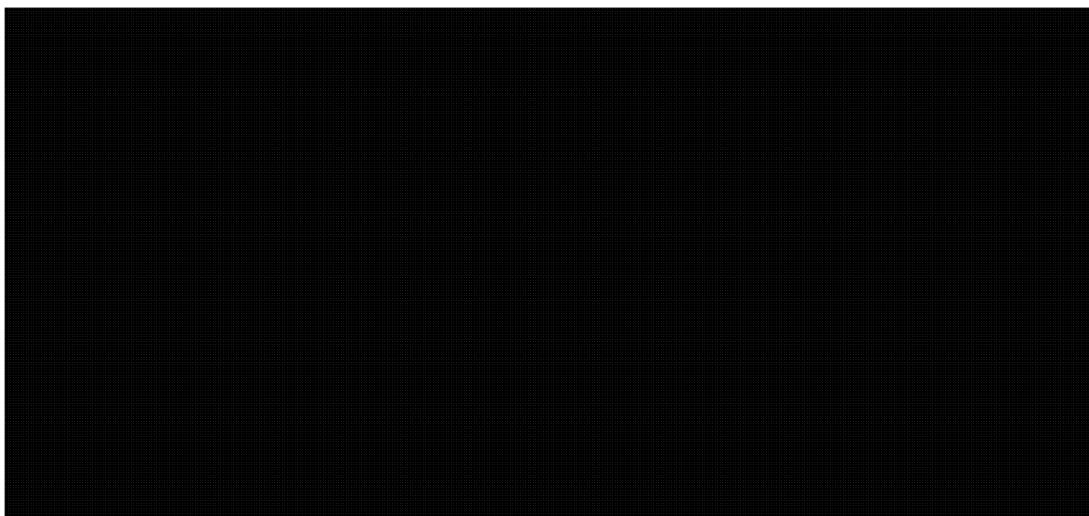
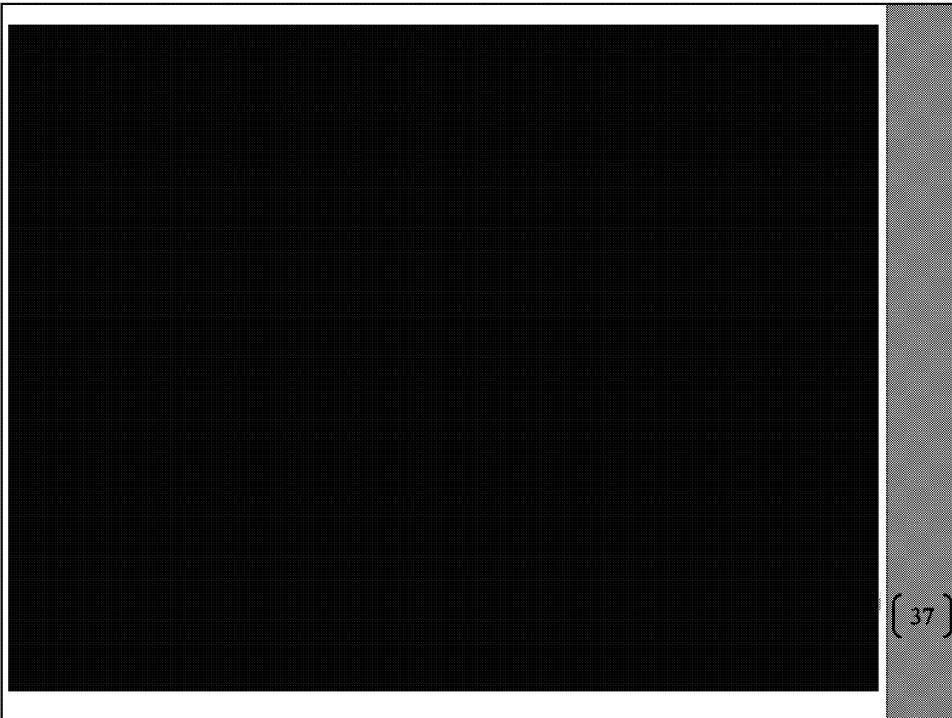




IRRELEVANT

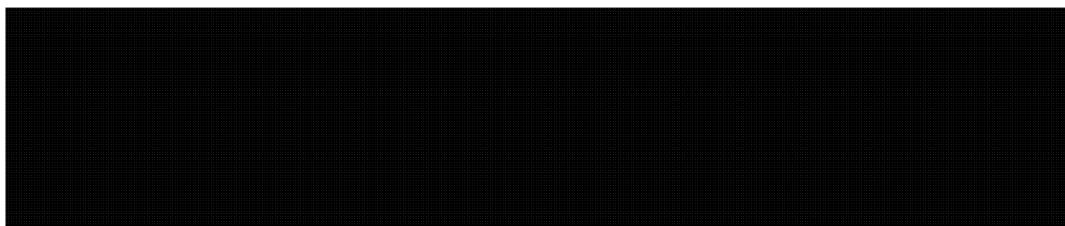
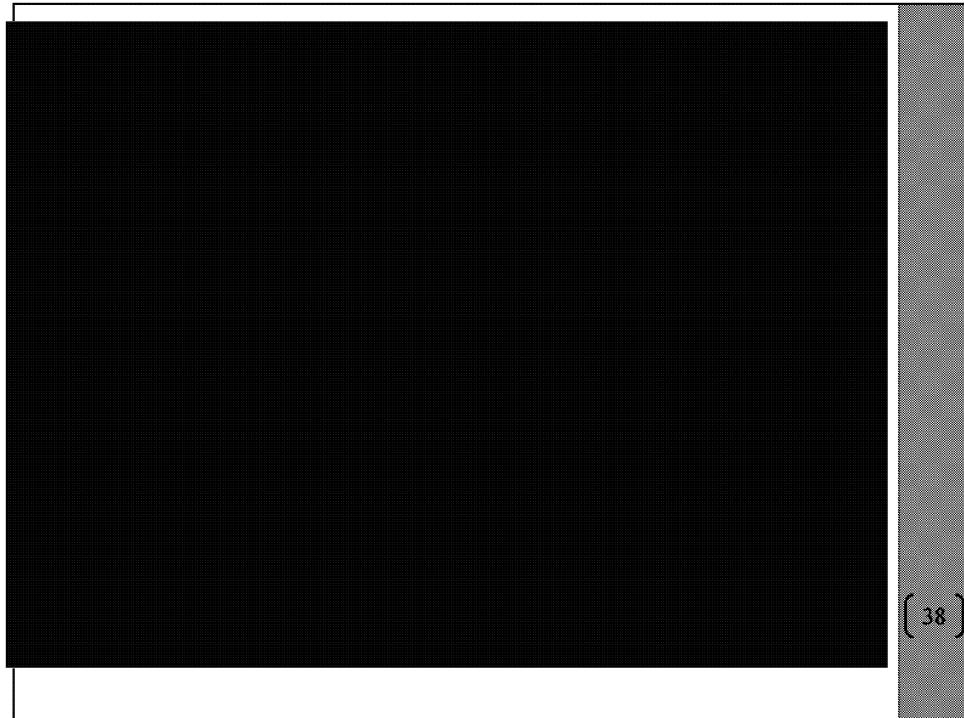
[36]

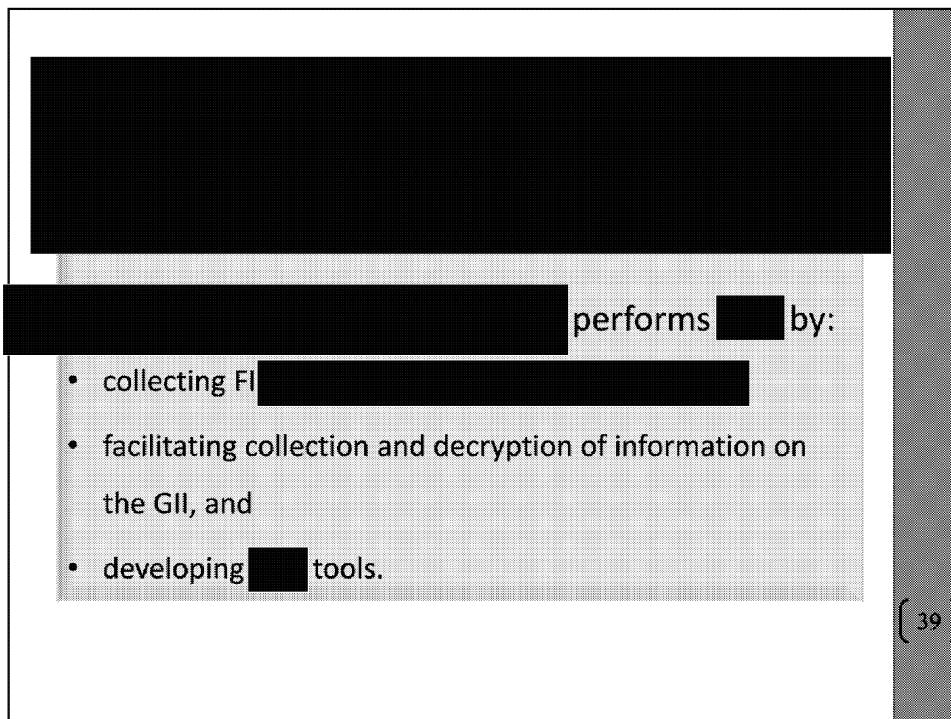
IRRELEVANT



TALENT KEYHOLE = [REDACTED] special clearance  
required







Collect Foreign Intelligence

[redacted]

facilitate collection and decryption

[redacted]

develop tools for [redacted]

[redacted]

IRRELEVANT

## Legal and Policy

[REDACTED] helps to ensure the legality of tasking / targeting.

SPOC helps to ensure compliance with policy.

### Canadian Guidelines

OPS – 1

- [REDACTED] IRRELEVANT
- One-end Canadian communications

### Guidelines

OPS 3-1

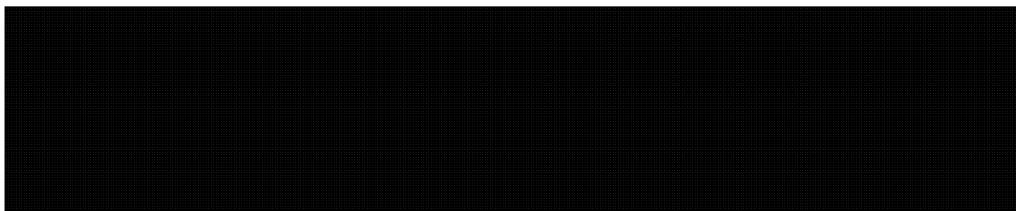
- Procedures for [REDACTED] Operations

### 2<sup>nd</sup> Party Guidelines

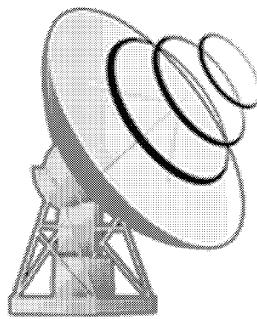
- US SIGINT Intelligence Directive (USSID-18)
- Human Rights Act (HRA) - UK
- Intelligence Services Act (ISA) - Australia

(40)

- Analysts are ultimately responsible for the legality of their tasking, GCRC is only a second set of eyes
- OPS 1 = guidelines produced by CSE policy department based on applicable law



## TERMINOLOGY EXERCISE



(4)

Match the:

Collection information on the left with the corresponding information on the right

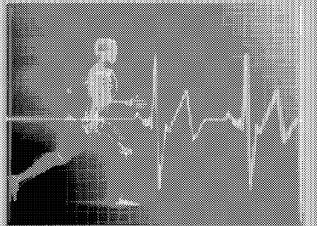
OR

Numbered items on the left with the letters on the right.

## Module 3: Research and Analysis

There are no hard and fast rules on what makes a good analyst, but definite assets are:

- thoroughness,
- organization,
- clarity of thought, and
- speed.



Good research is therefore worth the time because it will help make the analysis as accurate and complete as possible.

(42)

Page 23

Thorough:

What to include/leave out

Don't make value judgements (biases?)

Organization:

Lots of info must be **readable** or **consumable**

Clarity:

Highlight **key** info

Leave out window dressing (bogs down)

Speed:

Timeliness vs skipping steps

## Scanning

To augment their reporting, analysts will scan a variety of sources on a daily basis, including:

- End-Product Reports (EPRs) in [REDACTED]
- Open source resources
- Traffic databases

## Other scanning sources

**Requirements:** NSPL, GCRs, RFIs, feedback

**SIGINT reporting:** CSE and allied partners' [REDACTED]

**Policies:** reporting, tasking, naming, government, etc.

**Current events:** newspapers, magazines, journals

**Other sources:** CTSN (=Mandrake)

What analysts scan for in EPRs:

- for CSE and the 5-Eyes reporting -- especially on their targets
- for new and updated requirements (RFIs)
- to verify that any reports they issued are in [REDACTED] with no errors
- for feedback on reports

Open Source:

- to better understand a topic
- to follow recent developments
- to determine the urgency of reporting
- eliminate or effectively use material already in the public domain.

Traffic databases

- Traffic in CTR (Consolidated Traffic Repository) accessed through [REDACTED] for reportable foreign intelligence (FI) – see p. 24 in manual
- for CIR reportable information
- for tasking and target development

In addition to looking at the content of intercepted communications, analysts should look at the metadata [REDACTED] for tasking and target development information. For example, [REDACTED] Was

[REDACTED] This could lead to targeting of new selectors.

## Determining reportability

- GCR
- New intelligence or Open Source (OSINT)
- Foreign intercept
- Enough intelligence to warrant a report
- Traffic clearly understood
- Need for [REDACTED]?

[+]

These are some **questions an analyst could ask** himself/herself to determine if an item is reportable.

- There should be a **stated requirement** for the information.
- Foreign intelligence is **new information** not already available in **open source**.
- **One end foreign**. If one communicant is a Canadian, we would report the information from the foreign angle.
- If the information is **not time sensitive** and the analyst is aware that more information is forthcoming (e.g., [REDACTED], then it might be worthwhile to **wait for that second piece of intelligence**.
- It might be useful to search for **similar reports** in [REDACTED] and see what kind of feedback they got.

## Approved Abbreviations, Acronyms and Initialisms

Abbreviation	Expansion	Usage Notes
ADM	Assistant Deputy Minister	CEO reports only (expand in other records)
ADS	acquired immune deficiency syndrome	
AIS	Automatic Identification System	
a.k.a.	also known as	
Aka	Alberta	CEO reports only (expand in other records)
AM	amplitude modulation	
AWACS	airborne warning and control system	
AWOL	absent without official leave	
bbl.	buckets	
B.C.	British Columbia	CEO reports only (expand in other records)
Btu	British thermal unit	

Note that some of these terms do require expansion in 5-eyes reporting (they are only approved for CEO reports).

## Guidelines for Analysis

- Isolate the intelligence
- Determine inclusions/exclusions
- Highlight important points of intelligence and organize
- Brainstorm and conduct analysis
- Check your biases
- Determine context
- [REDACTED]
- Check for consistency

(46)

- Being **thorough** means **evaluating everything** in the traffic for **reportability**,
- remember that a **decision not to report** a point or piece of traffic is just as important as is a decision to report it.
- Do not include information (either SIGINT or collateral) just because it is available.
- Users need the pertinent facts and amplifying details, **not every piece of information**

## Biases & Assumptions

Be aware of your mental **biases** when analyzing intelligence

- Availability bias
- Mirror imaging
- Overconfidence bias
- Bias towards causal explanations
- Tunnel vision
- Information imbalance bias
- Anchoring bias

Examples:

- **Availability bias** – 9/11; Airplanes had been hijacked in the past, but usually the planes usually landed and hostages were kept for ransom. We didn't imagine a scenario like 9/11 where the hijackers would intentionally fly a commercial airplane into an office building.
- Mirror imaging
- **Overconfidence bias** – a person who thinks their sense of direction is better than it actually is. They demonstrate their overconfidence by going on a trip without a map or GPS.
- Bias towards causal explanations
- **Tunnel vision** – in a criminal investigation, the police may focus on an individual in the area with a prior criminal record
- Information imbalance bias – a.k.a. “sampling bias”.
- **Anchoring bias** – exercise on next slide. This bias is used in the retail industry quite often – ex. You see a great leather jacket in a store and fall in love with it. The price tag says \$1000 so you start to put it back on the rack. The salesperson tells you it's 60% off and only costs \$400 that week. “What a deal!” you think and you buy the jacket.

Question #1:

*Is the population of [REDACTED] greater than or less than 65 million?*

Question #2:

*What do you think is the population of [REDACTED]*

[48]

Example of Anchoring Bias

[REDACTED] population = approx. [REDACTED] million

The number 65 million in question #1 influences how you answer the second question.

It gives you a frame of reasonability when you have nothing else to go on, you fixate on the information at hand – it's your anchor.

## Report Research

- Research enough to understand the story and provide context for the report
- Ascertain what is already known
- Verify official titles and name spellings
- Expand acronyms (check the list of *Approved Abbreviations, Acronyms and Initialisms* on the SIGINT Reporting Working Aids page)
- Verify translations of specific terminology

[ 49 ]

### Page 26

**Performing research** is important for the analyst throughout the report writing process in order to:

- understand the story
- provide context for the end-product report
- ascertain what is already known
- verify official titles and name spellings
- expand acronyms (see: Approved Abbreviations, Acronyms and Initialisms)
- verify translations of specific terminology

## Research Tools

[REDACTED] for background information and current developments

for selectors and background information

CTSN / Mandrake [REDACTED] to review reports

[REDACTED] collaboration and social networking

[REDACTED] and [REDACTED]

### Other Resources:

- **Intranet** (Library, [REDACTED])
- **Internet** (via [REDACTED]),
- CSE library, and
- area **specialists**.

(50)

CTR = Consolidated Traffic Repository – the traffic database for [REDACTED] fax [REDACTED]

[REDACTED]  
fax, [REDACTED]

[REDACTED]

# RESEARCH EXERCISE



Resources: Unless otherwise indicated, all resources can be found on the [redacted] page

(Use [redacted] as your browser, you will need your [redacted])

Use [redacted] as your browser (you will need [redacted]): [redacted]

#1 [redacted]

#5 [redacted]

#6 [redacted]

#7 [redacted]

## Module 4: SIGINT Reports

### What is SIGINT?

COMINT – voice, data communications

ELINT – radar, navigation, jamming systems

FISINT – telemetry, beacon signals, arming, fusing & firing systems

[32]

Page 33

Signals Intelligence: Interception/analysis of Foreign signals and is comprised of:

Communications Intelligence (COMINT) [REDACTED]

Electronic Intelligence (ELINT)

Foreign Instrumentation Signals Intelligence (FISINT)

These products

- contain foreign intelligence (FI) or security intelligence (SI)
- are intended for customers with appropriate clearances
- follow the format outlined in CSOI-4-1 *SIGINT Reporting Procedures*
- can incorporate unclassified collateral and analyst comments, when properly identified as such

## Types of SIGINT Reports

End Product Reports (EPR)

Electronic Intelligence (ELINT) Reports

Cryptologic Information Reports (CIR)

Gist Reports

Summary Reports

[33]

ELINT reports are generally classified SECRET.

## Canadian Sensitivities



If the information could ...	Then issue it...	Examples
Cause embarrassment to the Canadian government	RESTRICTED	
Cause personal embarrassment to a Canadian Cabinet minister, MP or federal government official	RESTRICTED	
	CEO	
Be detrimental to Canada's security and intelligence community	CEO	
Be detrimental to Canada's national interest in ways other than those described above	CEO	
	CEO	

Full list on page 35-36 of manual

### Canadian sensitivities

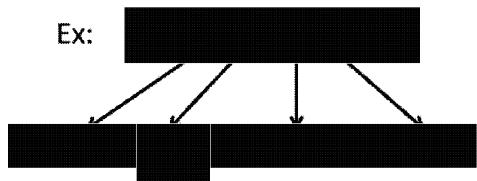
The main categories of Canadian sensitivities, and how the information should be reported (RESTRICTED or CEO), are listed in this table.

**These instructions are only guidelines, not hard and fast rules.**

Under special circumstances, information that does not meet the criteria below may have to be reported in the CEO series; this decision should be made in consultation with the Team Leader or Production Manager.

## Report Serial Numbers

Ex:



System-generated upon release of product [REDACTED]

[REDACTED] (35)

[REDACTED] (see page 37)

[REDACTED] (See page 38)

Does anyone know what the [REDACTED] represents?

[REDACTED]

## SIGINT Report Distribution Controls

CEO - Canadian Eyes Only (see Canadian sensitivities)	C [REDACTED]
R-series – CEO Restricted	R [REDACTED]
IRRELEVANT	

SIGINT Community (COM) reports are shared with one or more 2<sup>nd</sup> Party SIGINT agencies. The above reports are restricted to various levels of Canadian readers.

(36)

Additional letters at the front of the Serial Number to indicate distribution controls (C, R, [REDACTED])

SIGINT reports are divided by the two main types of distribution: COM and CEO

**Canadian Eyes Only (CEO)** reports contain intelligence that is of a sensitive nature either to Canada or to a Second Party country; therefore, such reports are limited to a Canadian readership and must not be released to Second Parties.

**Restricted (R)** reports are likewise sensitive and for this reason have a named distribution. R-series reports are always CEO Even if you are an actor of an R-series report, you may not be able to view it once released unless you are also a recipient.

Note any Special Reporting Conventions related to your targets

**SIGINT Reporting Working Aids**

Quick Reference type: General Reference

Policies and Procedures	<ul style="list-style-type: none"><li>• CSOI-4-1: SIGINT Reporting</li><li>• CSDG-102: The SIGINT Classification System</li><li>• CPS-1: Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities</li><li>• QPS-1-7: Operational Procedures for Naming in SIGINT Reports</li><li>• QPS-1-7 List of Blatant Identification Approvals</li><li>• QPS-1-7 List of Naming Authorizations</li><li>• QPS-5-3: Write-to-Releas (WTR) Procedure</li><li>• QPS-5-3 List of WTR Approvals</li><li>• Special Reporting Conventions</li><li>• Rules on reporting identities</li><li>• Privacy of Canadians</li><li>• Approved Abbreviations, Acronyms and Initialisms</li><li>• Canadian Surnames</li></ul>
SIGINT Reporting Standards Updates	<ul style="list-style-type: none"><li>• Gists and advance reports</li><li>• Military operations and sensor-checking</li><li>• Correction or cancellation of "actionable" reports</li><li>• Update on [REDACTED]</li><li>• Transliteration guidelines for Arabic names</li></ul>
Editing	<ul style="list-style-type: none"><li>• A Guide to Editing</li><li>• Report Editing Checklist</li><li>• SIGINT Style Sheet</li></ul>

[ 57 ]

SRWA can be found under “Quick References” on the DGI webpage.

Check to see if there are any special reporting conventions for your area, look at the SRWA webpage for a link to SRC.

## Special Reporting Conventions

Table 1

IRRELEVANT

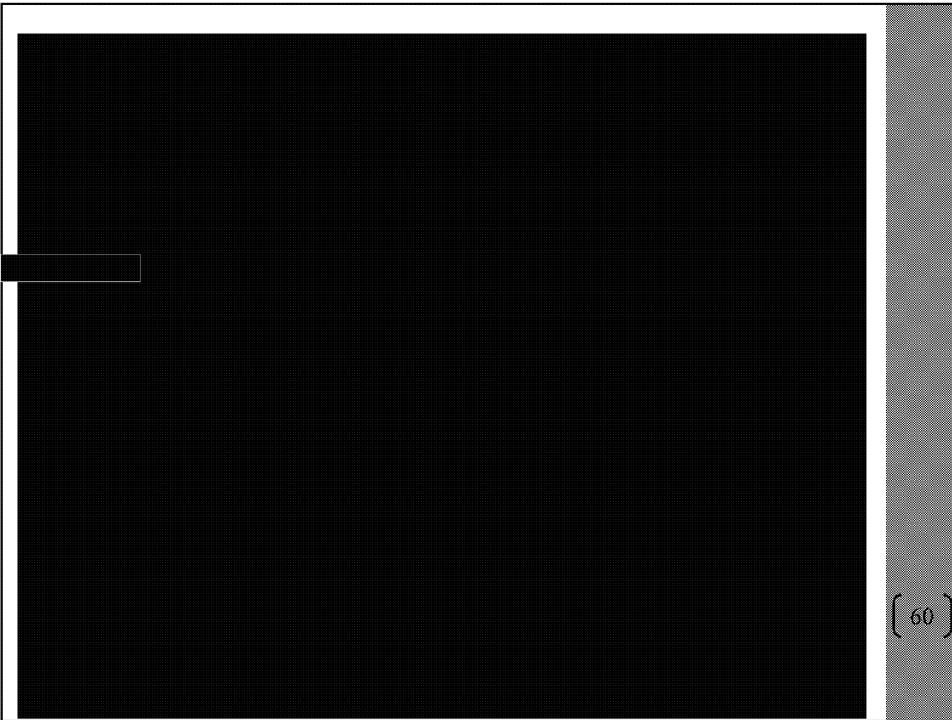
## Special Reporting Conventions

Table 2

IRRELEVANT

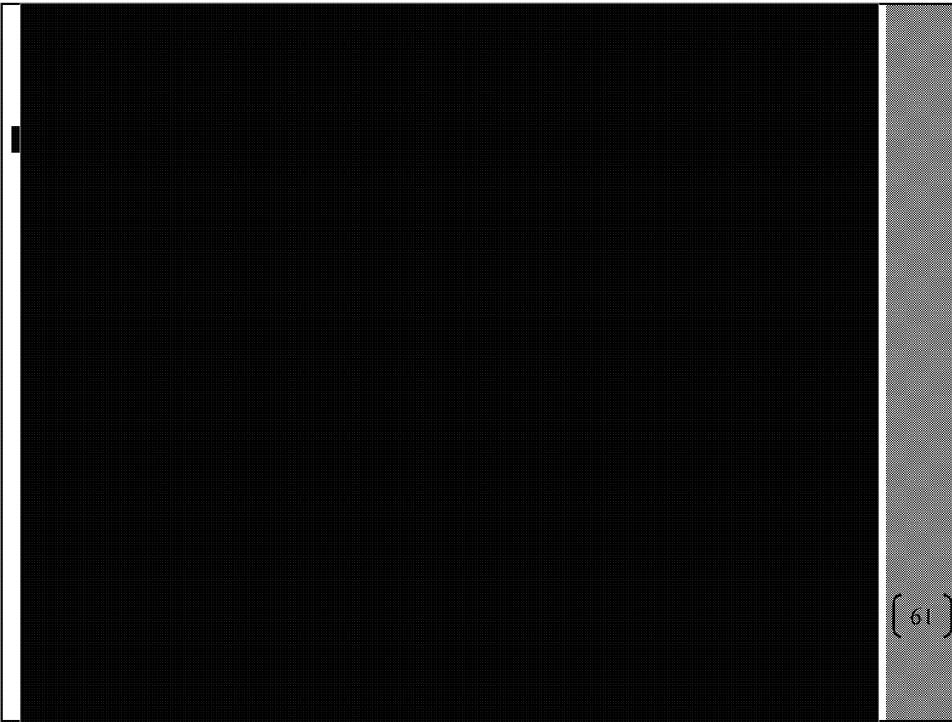
(36)

IRRELEVANT



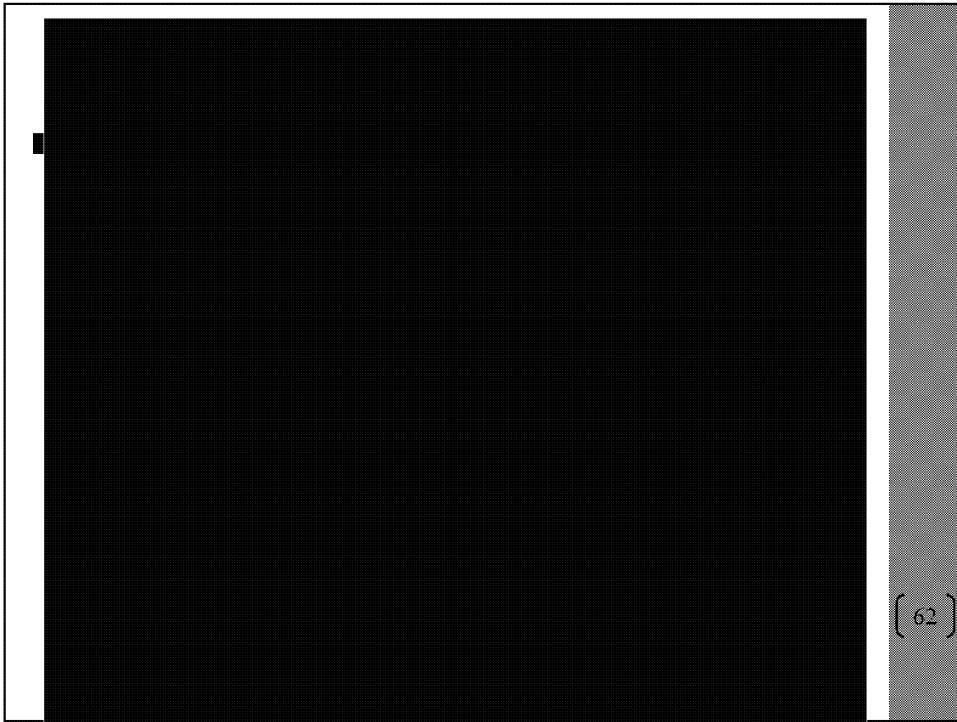
[REDACTED] indicates that this report is

1. Not derived from enciphered/decrypted material
2. Not from sensitive source (probably from [REDACTED])
3. Contains no reference to TS reporting



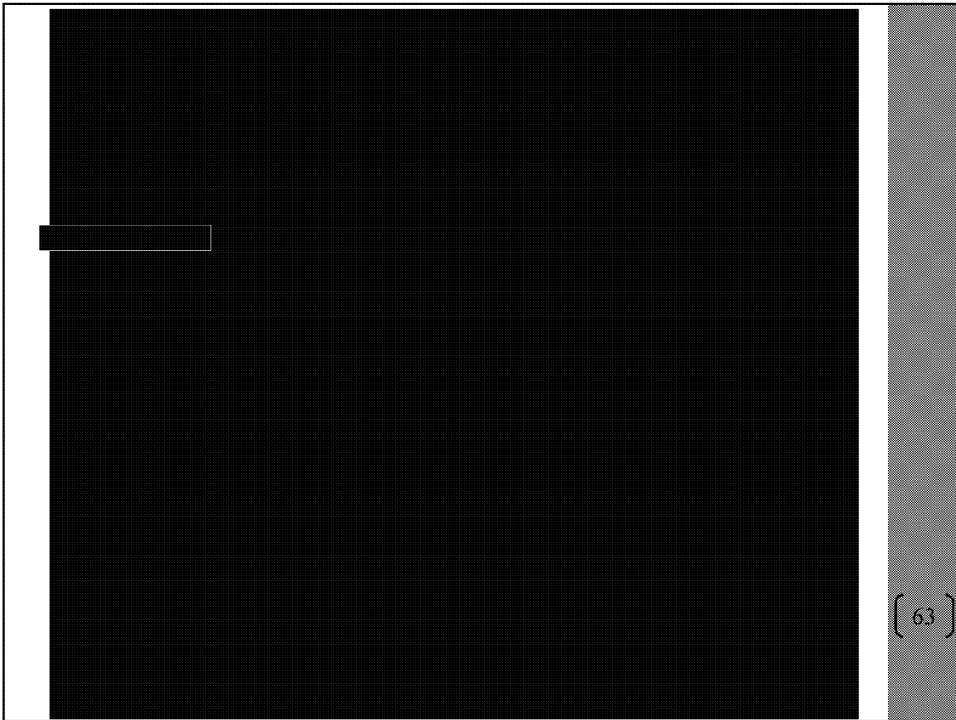
[REDACTED] indicates that this report is

Secret Elint report



[REDACTED] indicates that this report is

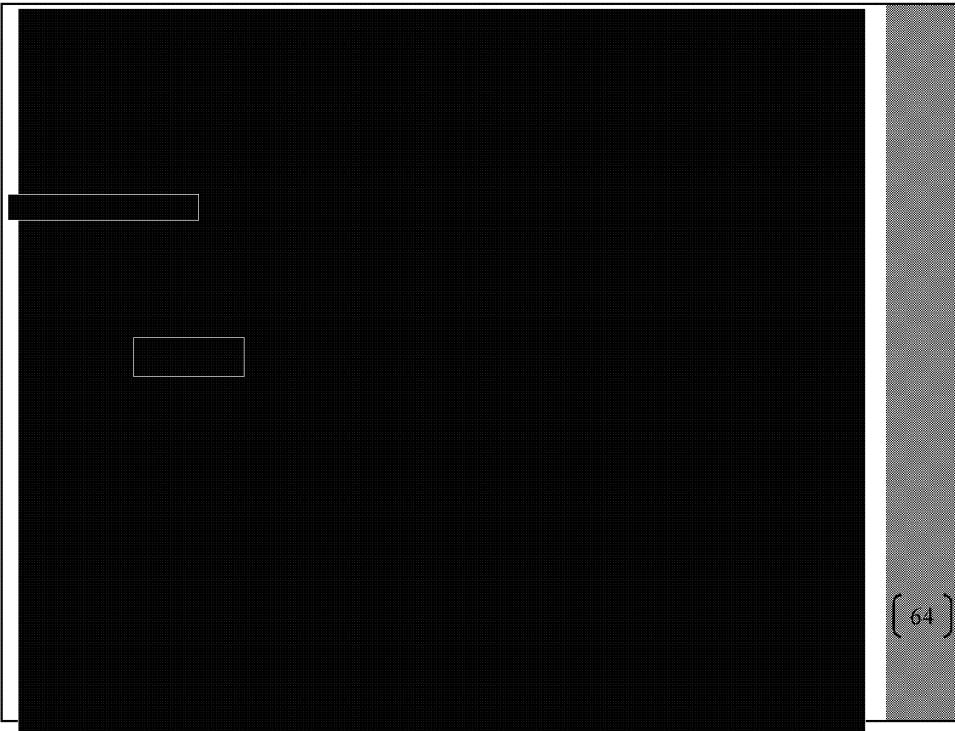
1. Derived from [REDACTED] enciphered material or
2. Derived from sensitive source collection [REDACTED]  
[REDACTED] IRRELEVANT
3. May contain references to other TS//SI reporting (footnotes)



[REDACTED]  
Indicates a summary report at the top secret level.

Report is an accumulation of previously issued reports on the same issue.

Used to identify and analyse trends.



[REDACTED]  
Derived from a gist, mostly used by the [REDACTED] team to provide timely turn around of gisting while still maintaining accountability through serialized product.

## Cryptologic Information Reports

CIRs are SIGINT reports that:

- contain cryptologic communication
- contain [REDACTED] information
- distributed to COMINT producers only, not to GC clients
- are not subject to the same restrictions as EPRs (no need to suppress [REDACTED])

They are:

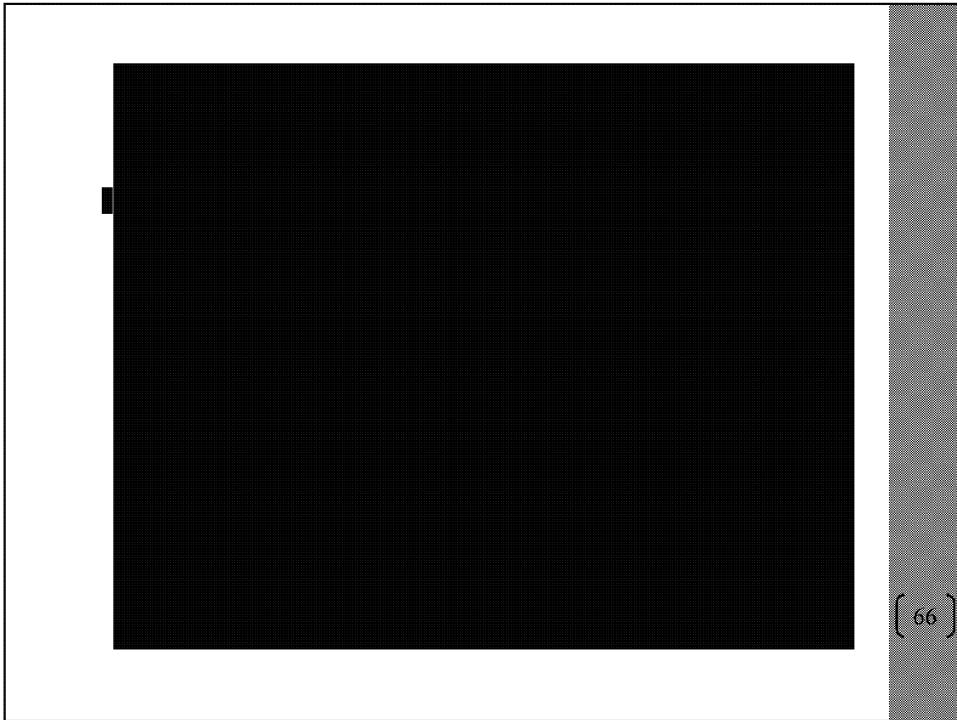
distributed only to COMINT producers

do not provide information about CSE/CFIOP's capabilities

no need to suppress [REDACTED]

meets CIR and regular reporting criteria will be issued in two reports

If you have traffic containing both information that meets CIR reporting requirements and information that meets regular reporting criteria, issue two reports (a CIR and an EPR).



Page 33

This is what a [redacted] serial number looks like.

[redacted] reports are shared strictly between 2<sup>nd</sup> party agencies [redacted] that assist in ITS activities.

They are always classified TS//SI and the serial number will always contain the trigraph [redacted]

[redacted] draw from a **special set of DDI** (Delivery Distribution Indicators) – Section 9

## SERIAL NUMBERS EXERCISE



Resources [REDACTED]

[REDACTED]

Please provide the serial number of each of the following four reports

See [REDACTED]

If link is still down, use [REDACTED]

## Organizational Strategies

IRRELEVANT

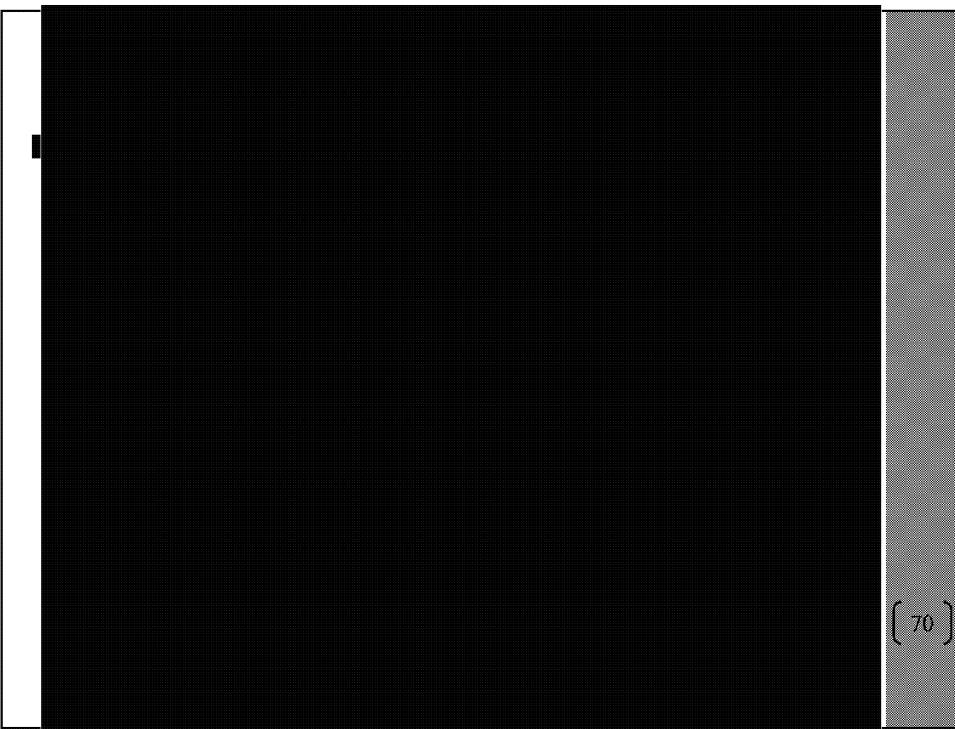
[ 68 ]

## Inverted Pyramid

IRRELEVANT

[ 65 ]

IRRELEVANT



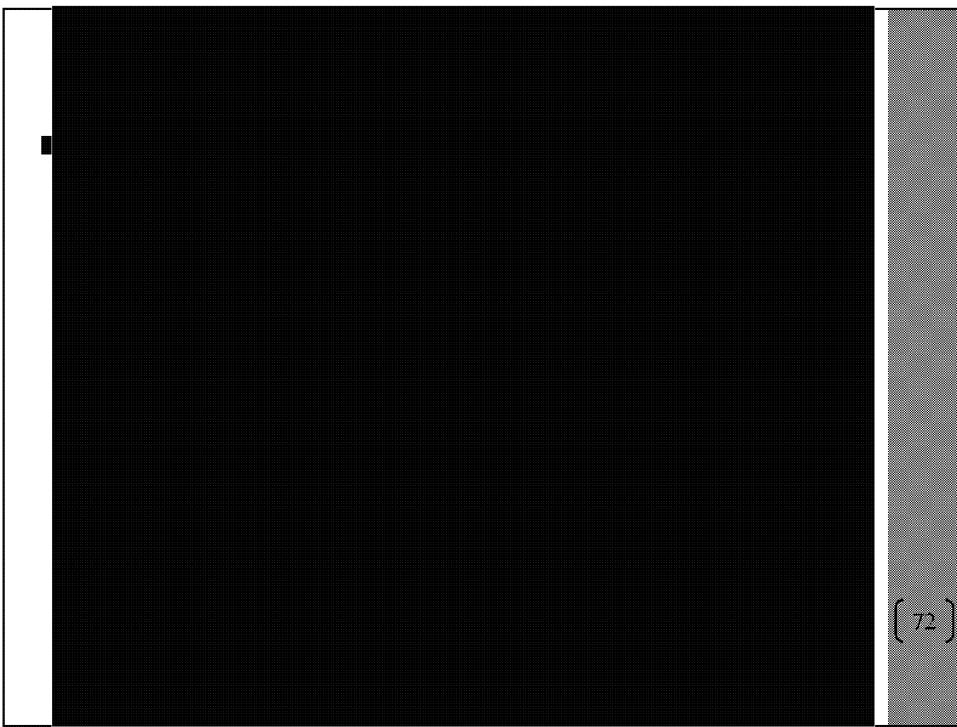
Page 43

70

## Lead Plus Equal Facts

IRRELEVANT

(v)



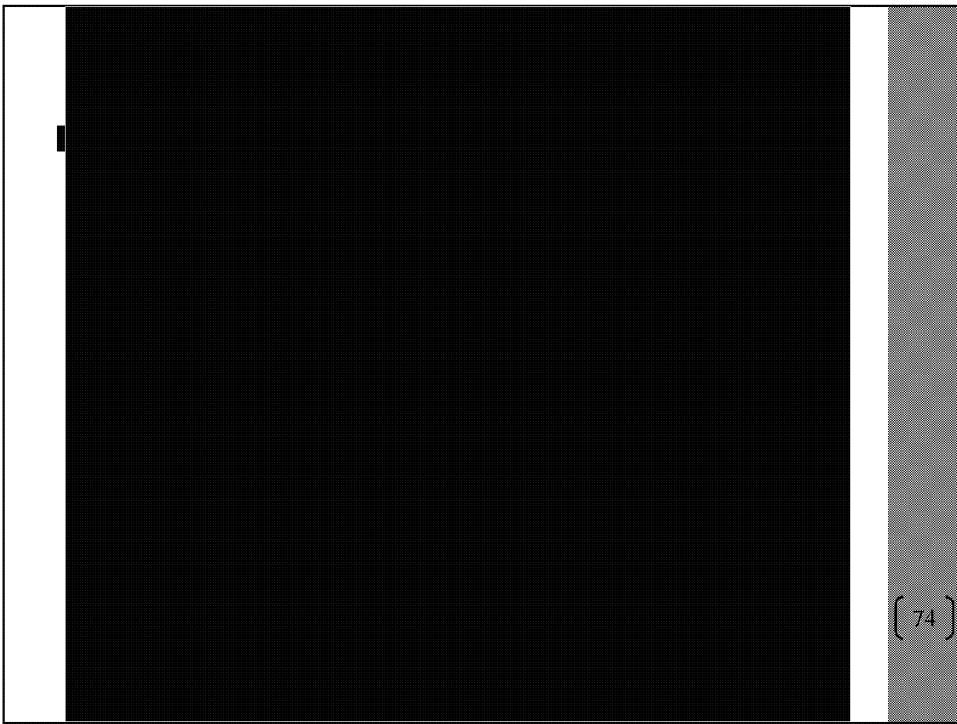
Page 45

72

## Chronological Account

IRRELEVANT

[redacted]



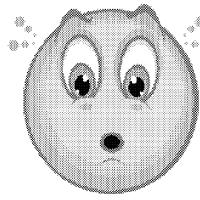
Page 47

74

## Module 5: Report Structure

IRRELEVANT

## Attribution



- identifies the intelligence source
- identifies the recipient
- helps readers assess the importance or reliability
- is repeated only if needed to maintain clarity



AVOID: a back-and-forth conversational style

DO NOT REVEAL: [REDACTED]

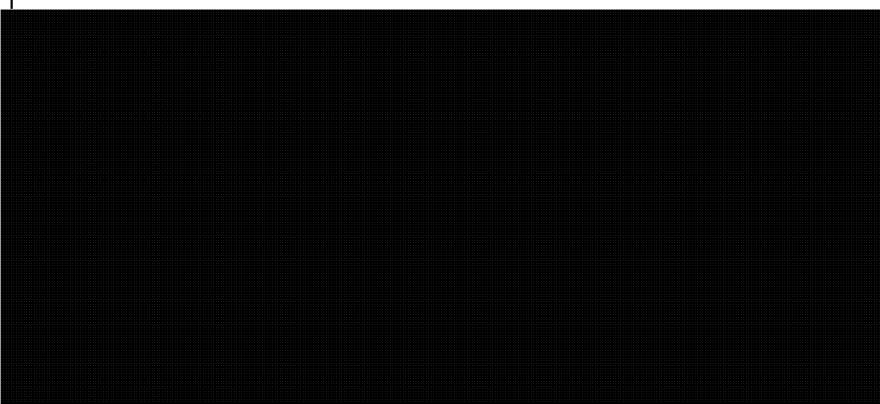
[REDACTED]

[REDACTED]

- identifies the intelligence **source** (who revealed the information)
- identifies the **recipient** of the information when the source cannot be revealed for policy reasons
- helps readers assess the importance or **reliability** of the information
- is repeated only if needed to maintain clarity; vary the style used to identify the source  
(e.g. [REDACTED])

- Avoid a back-and-forth conversational style
- Indicate that reporting was [REDACTED] when based on [REDACTED] traffic  
(see section **4.2.1.6** of CSOI-4-1)

## **Attribution in the Title**



(General attribution is in the title, details are in the body of the report.)

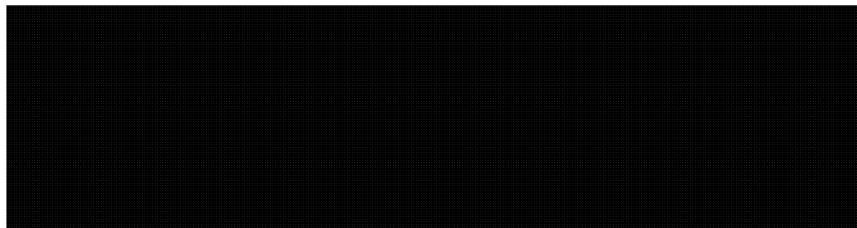
## **Attribution in the Body**

[78]

Source: [REDACTED]

Reliability: High

## Attribution Block



[79]

(General attribution is in the title, details are in the body of the report.)

Details (U)

Context (U)

## Block Headings

[REDACTED]

IRRELEVANT

[REDACTED]

[REDACTED]  
[REDACTED]

IRRELEVANT

[REDACTED]

## Block Headings

IRRELEVANT

[3]

IRRELEVANT

## The Lead

IRRELEVANT

**The Lead**

IRRELEVANT

## Key Points & Analysis

- Key points highlight SIGINT information to **senior readers** and help them to:
  - understand the most pertinent points
  - determine if the report is worth reading
- Each key point should capture an essential fact.
- The Analysis delivers the report's strategic significance or the trend that the report illustrates within the reporting line.

[ 84 ]

## Key Points & Analysis - Exercise

### **Study finds evidence of first human-to-human transmission of H7N9 bird flu**

By **Jethro Mullen**, CNN  
updated 7:06 AM EDT, Wed August 7, 2013

Until this week, no cases of human-to-human transmission of the deadly bird flu virus that broke out in China this year had been reported. But now, researchers say they believe a woman in the eastern Chinese city of Wuxi probably caught the H7N9 virus from her father.

The woman, 32, most likely became infected when she was looking after her father at his bedside in the hospital in March, according to a study published Tuesday in the British Medical Journal. Both patients eventually died. The woman had no known exposure to poultry, the study said.

"Our findings reinforced that the novel virus possesses the potential for pandemic spread," the study's authors wrote. But in the case they studied, they said "the transmissibility was limited and non-sustainable."

In April, the World Health Organization warned the H7N9 virus was "one of the most lethal" that doctors and medical investigators had faced in recent years. The virus has caused 132 human infections resulting in 43 deaths since February, Chinese state media reported last month. The rate of infections seen earlier this year has dropped off dramatically.

1. Read through report
2. Highlight any Key words or phrases (these will be used to identify key points) – 5-10 min
3. Discuss with a neighbor
4. Take up as a group (para by para)
5. Reveal answers

## Key Points & Analysis - Answer

### Study finds evidence of first human-to-human transmission of H7N9 bird flu

By Jethro Mullen, CNN  
updated 7:05 AM EDT, Wed August 7, 2013

#### Key points

- New evidence from China finds that H7N9 may be transmitted between humans.
- A woman in China, with no known exposure to poultry, contracted the virus from her father; both have since died.
- The virus possesses the potential for pandemic spread, but its transmissibility is limited and non-sustainable.
- The rate of infection has declined dramatically.

#### Analysis

If human-to-human transmission of the H7N9 virus is confirmed, the rate of infection may increase dramatically.

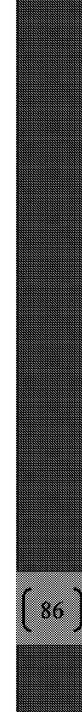
#### Details

Until this week, no cases of human-to-human transmission of the deadly bird flu virus that broke out in China this year had been reported. But now, researchers say they believe a woman in the eastern Chinese city of Wuxi probably caught the H7N9 virus from her father.

The woman, 32, most likely became infected when she was looking after her father at his bedside in the hospital in March, according to a study published Tuesday in the British Medical Journal. Both patients eventually died. The woman had no known exposure to poultry, the study said.

"Our findings reinforced that the novel virus possesses the potential for pandemic spread," the study's authors wrote. But in the case they studied, they said "the transmissibility was limited and non-sustainable."

In April the World Health Organization warned the H7N9 virus was "one of the most lethal" that doctors



These were put together by four of us when Key points was first introduced.

We didn't modify though like a lot of the studnets' ones better

Discuss what the "decline in rate of infection might mean". Has it declined since this outbreak or leading up to it?

## Key Points

### Format:

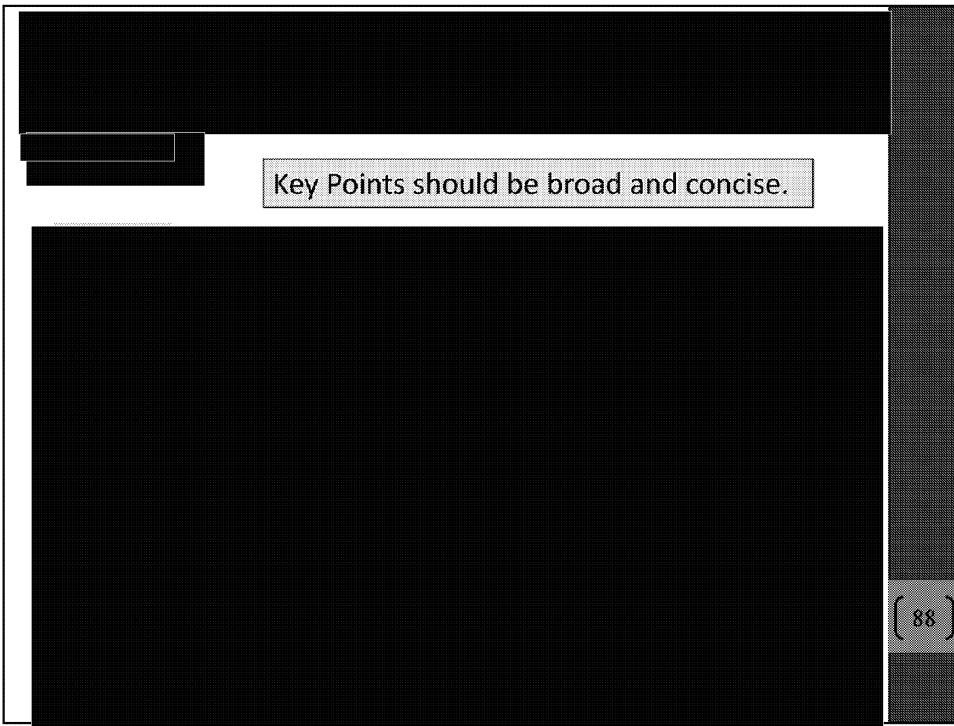
- Use full sentences (NOT headline-style).
- Key points are preceded by the stem:

***"The essential elements in this report are as follows:"***

### Tense:

- Present or future tense unless events occurred in the distant past.

[ 8 ]



Broad – use general identifiers rather than specific names (eg: [REDACTED])

Concise – pick out only the highlights of the report

## CSE Analysis

### **Format:**

- Should not exceed a couple of sentences.
- May include well-known acronyms
- May include well-established information
- Uses assumptive wording
- May include footnotes to additional information or reporting.

### **Tense:**

- Present tense where appropriate.

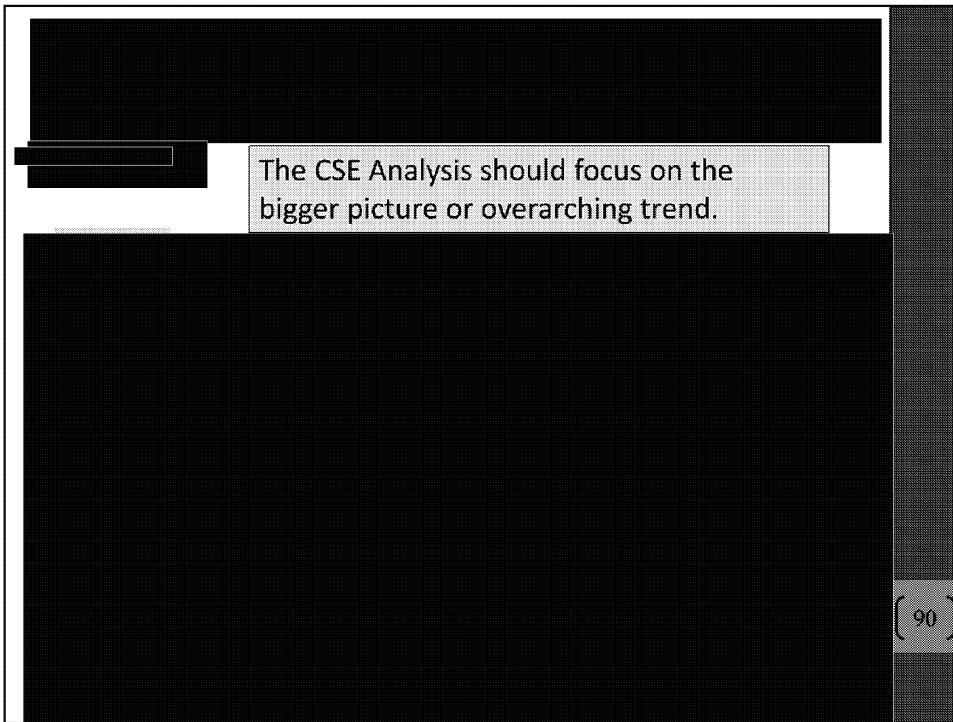
[ 89 ]

May include well-known acronyms (outside of the approved acronyms)

May include well-established information not strictly supported within the body of the report (e.g.: [REDACTED])

Typically uses terminology such as: "suggests", "implies", "provides evidence that", "may demonstrate".

May include footnotes to additional information or reporting.



The Analysis should focus on the bigger picture and not just analyse the facts of an individual report.

## **KEY POINTS & ANALYSIS EXERCISE**



Have flipcharts ready in advance

Separate group into 3's or 4's and have them construct Key points and an Analysis for the provided report (30 min).

Present in groups and critique eachother's work

# The Title

IRRELEVANT

IRRELEVANT

## Title Punctuation: Comma (,)

IRRELEVANT

## Title Punctuation: Semicolon (;)

IRRELEVANT

## Title Punctuation: Colon (:)

IRRELEVANT

# Title Slug

IRRELEVANT

## TITLES EXERCISE



[ ]

## **Module 6: SIGINT Style**

Why do we need a style guide?

Who updates the style guide?

Who owns the report?

[ 98 ]

Page 57

To ensure a standard of reporting is followed

Affords our clients a common-look-and-feel to all CSE reporting (predictability)

Style guides contributed to by all users

Updated by [REDACTED] and members of [REDACTED] on behalf of DGI

Reports are owned by CSE not the individual authoring them.

## Abbreviations & Acronyms

IRRELEVANT

## Dates in SIGINT Reports

IRRELEVANT

100

## Dates - Examples

IRRELEVANT

## Currency

IRRELEVANT

## Currency – Examples

IRRELEVANT

## Numerals

IRRELEVANT

## Lists

IRRELEVANT

## Lists (short)

IRRELEVANT

## **Lists (long)**

IRRELEVANT

## Lists (sentences)

IRRELEVANT

**Analytic Comments**

IRRELEVANT

## Analytic Comments (embedded)

IRRELEVANT

## Analytic Comments (paragraph)

IRRELEVANT



## **Footnotes**

IRRELEVANT

## Footnotes (bad example) ..

IRRELEVANT

## Footnotes (better example)

IRRELEVANT

## **Footnotes**

IRRELEVANT

## Collateral

### Purpose:

- is information not derived from SIGINT
- puts the SIGINT in context or contributes to the understanding of the SIGINT information

### Format:

- must be clearly flagged and delimited, using the flag **(End of collateral)**,
- must be classified according to the source
- should be included in the traffic metadata

[ 116 ]

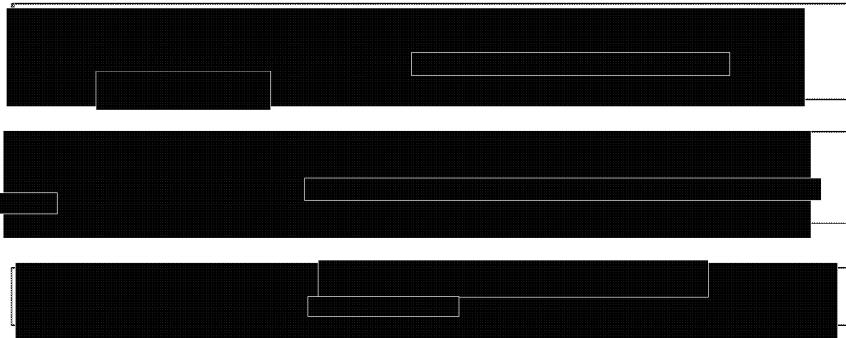
## Collateral (example)

[117]

117

## Point of Contact (POC)

The minimum classification for this section is S//SI



[118]

## STYLE EXERCISE



[ 119 ]

Edit the provided report.

Use Annex 4 (page 89-91). I have 21 edits. Who can identify all the ones I have (prizes for top three participants). ---30 min

119

## Module 7: Naming policy

④ Suppress the Canadian and Second Party identity info.

④ NEW: Suppress anyone's name in Canada. (as of April 2014)

④ Enter the actual name and corresponding alias into [REDACTED]

④ Use generic terms:

④ "a named Canadian person/company"

④ "a [department name] official"

"a named person in Canada"

(See [REDACTED])

④ If identity info is not known, make that clear:

④ "an unnamed/unidentified/unspecified Canadian entity"

(See OPS-1-7 SIGINT Naming Procedures for complete details)

[REDACTED]  
120

Page 61

What to do when you receive incidental collection on CA

- OPS-1-7 SIGINT Naming Procedures

**LEGALLY – can't name CA**

As part of a **REFLEXIVE AGREEMENT** - don't name 2<sup>nd</sup> party entities

- Suppress the names and **identifying information** of Canadian and Second Party citizens, companies, and organizations.
- The actual name is entered into [REDACTED] with the corresponding alias.
- Use generic terms

Reader must formally request suppressed information (this is done through D2).

- When traffic refers to an unnamed Canadian entity, state this to indicate that CSE is not suppressing the name.

This would indicate there is nothing suppressed (no additional info) and therefore

120

no request for information would be made.

## Naming policy (cont'd)

- ◎ When there is doubt about the nationality, err on the side of caution with validity wording
  - ◎ "a possible Canadian citizen"
- ◎ Beware of **contextual identification**.  
(see page 64 in manual)
- ◎ If geographic references reveal the identities of provincial or municipal government officials or private citizens or organizations, they must be replaced with generic terms.



[12]

- EG: mayor of Toronto
- Lower level officials have a higher expectation of privacy
- If a CAN is named (overtly or contextually) you must
  1. Contact D2
  2. Cancel report
  3. Reissue if necessary

## Naming policy

### Exceptions for Canadian entities\*

An exemption may be granted if the subject:

- ◎ is in immediate/life-threatening danger
- ◎ is being held hostage by any foreign group, or imprisoned by an unfriendly government
- ◎ has or plans to commit a life-threatening act, or
- ◎ is outside Canada acting in an official capacity as an agent of a foreign organization or government; their citizenship should not be revealed

\* approval by D2 required

[122]

4. Dual citizens can be named but their citizenship not revealed

Eg: [REDACTED]

Eg: [REDACTED]

Expectation of privacy ends with death: [REDACTED]

(name)

## Naming policy Exceptions

IRRELEVANT

- ④ Foreign-registered subsidiaries and affiliates of Canadian corporations may be named (e.g.)
- ④ Current Cabinet ministers and federal public servants acting in their official capacities may be identified **by title** provided their identification is necessary to understand the foreign intelligence
- ④ Federal Crown Corporations may be named (next slide)

[123]

IRRELEVANT

If a company is registered in CA it can not be named

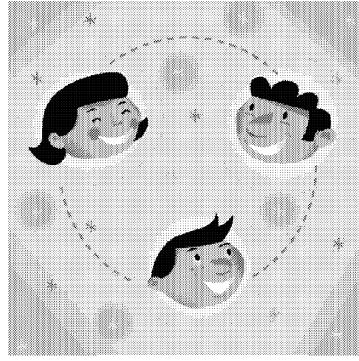
123

## Federal Crown Corporations

Atlantic Pilotage Authority	Enterprise Cape Breton Corporation
Atomic Energy of Canada Limited (AEC)	Export Development Canada (EDC)
Bank of Canada	Farm Credit Canada
The Blue Water Bridge Canada	Freshwater Fish Marketing Corporation
Business Development Bank of Canada	Great Lakes Pilotage Authority
Canada Council for the Arts	International Development Research Centre
Canada Deposit Insurance Corporation	Laurentian Pilotage Authority
Canada Development Investment Corporation	Marine Atlantic
Canada Lands Company Limited	National Arts Centre Corporation (NAC)
Canada Mortgage and Housing Corporation (CMHC)	National Capital Commission (NCC)
Canada Pension Plan Investment Board	National Gallery of Canada
Canada Post Corporation	Old Port of Montreal Corporation Inc.
Canada Science and Technology Museum Corporation	Pacific Pilotage Authority Canada
Canadian Air Transport Security Authority (CATSA)	Parc Downsview Park Inc.
Canadian Broadcasting Corporation (CBC)	PPP Canada
Canadian Commercial Corporation	Public Sector Pension Investment Board
Canadian Dairy Commission	Ridley Terminals Inc.
Canadian Museum of Civilization	Royal Canadian Mint
Canadian Museum of Nature	Standards Council of Canada
Canadian Race Relations Foundation	Telefilm Canada
Canadian Tourism Commission	VIA Rail Canada INC
Defence Construction Canada	see <a href="http://canada.gc.ca/depts/major/depind-eng.html">canada.gc.ca/depts/major/depind-eng.html</a>

124

## NAMING POLICY EXERCISE



Resources in Annex 5 (pages 93-97); also available online (in SRWA under Policies and Procedures).

## Module 8: Write-to-Release (WTR)

- WTR involves sanitizing (to the **non-SI**, usually **SECRET** level) all key information in a SIGINT report that can be released outside COMINT channels...
  - ... **without** compromising COMINT sources, methods or techniques.
- The WTR report contains SI and non-SI paragraphs.

[126]

Page 67

Once adopted allowed us to release to non-SI readers by weighing the gains of wider distro against possible risk of exposure

126

## Why?

- It's CSE policy: *OPS-5-3 Write-to-Release Procedures*
- Most intelligence users are not indoctrinated for COMINT.
- If intelligence isn't used, the money spent producing it is wasted.
- **It's what the clients want.**

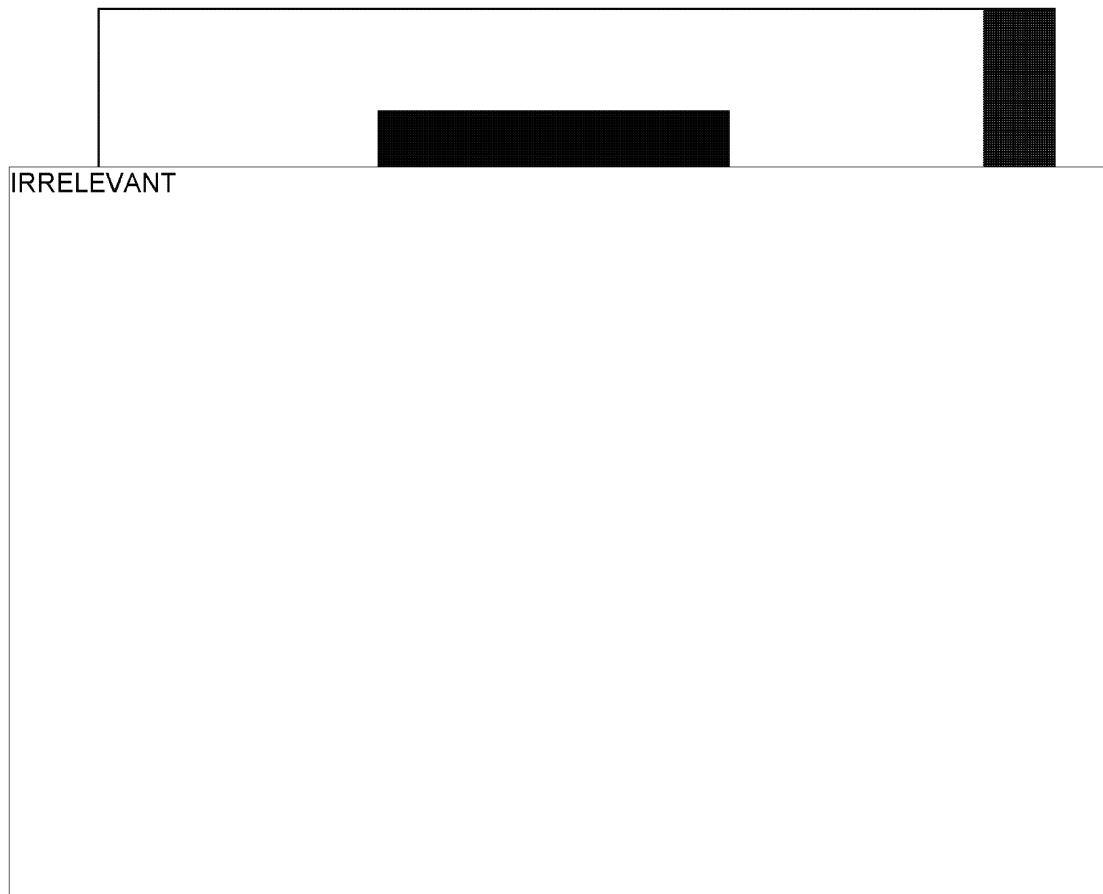
[12]

Allows us to get our reporting to the widest audience with a need to know

Eg: border agents who are not SI cleared - [REDACTED] distributed at S level

## Prerequisites for WTR

IRRELEVANT



Exemptions	
See WTR Exemption List (on the Operational Policy website)	
Category	Details
Targets	[REDACTED]
Sources	[REDACTED]
Subjects	<ul style="list-style-type: none"><li>• law enforcement-related info with a Canadian angle</li><li>• Information related to communications characteristics</li></ul>
Other	<ul style="list-style-type: none"><li>• R-series reports</li></ul>

Page 69

Targets

ECI reporting lines (formerly [RELEVANT])

Sources

[REDACTED]

Subjects

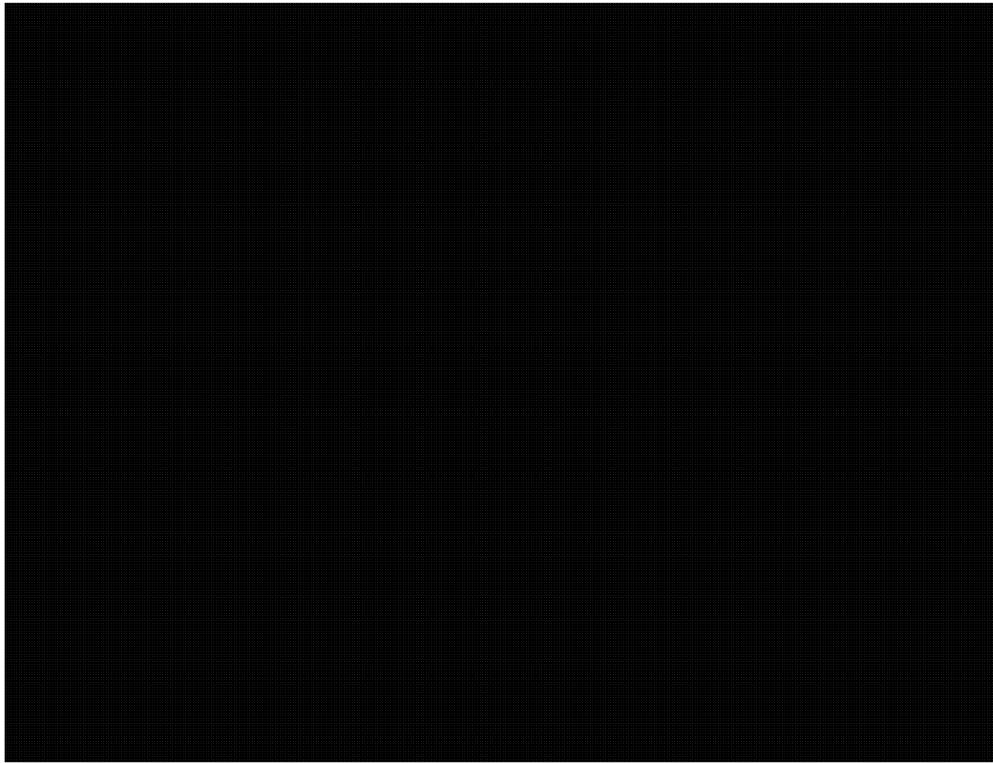
CEO

[REDACTED]

Other

Named distro for R-series (can't expand receivership)

May be embarrassing if details of a [REDACTED] are shared broadly; hard to come up with [REDACTED]



## Disguising COMINT

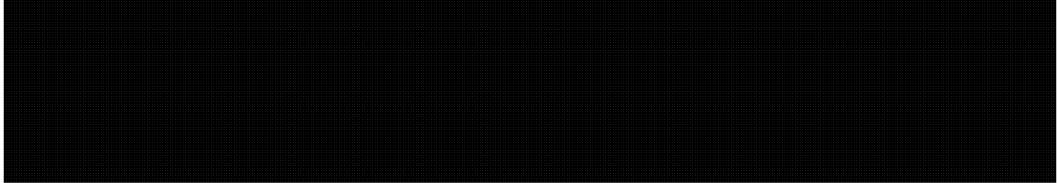
Certain types of information must **not** be included in the WTR paragraphs.

**AVOID:**

- COMINT markings and terminology (including collateral statements and comment flags and phrases such as "not further identified")
- Attribution (both ends of communication identified)
- Conversational words that suggest communications as the source

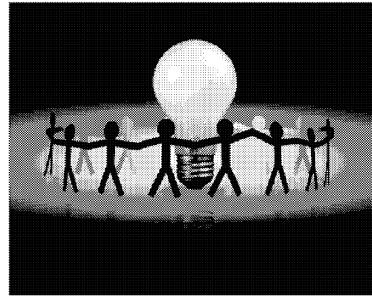
[ 132 ]

Page 68



132

[REDACTED] EXERCISE



[133]

133

## Disguising COMINT

Certain types of information must **not** be included in the WTR paragraphs.

**AVOID:**

- Direct quotes
- Exact dates and figures
- Information that might reveal analytic methods, techniques, degree of [REDACTED] success
- Suppressed identities

[134]

Mid-July rather than 15 July, round up numbers

Who was privy to the info (only two ppl in the room).

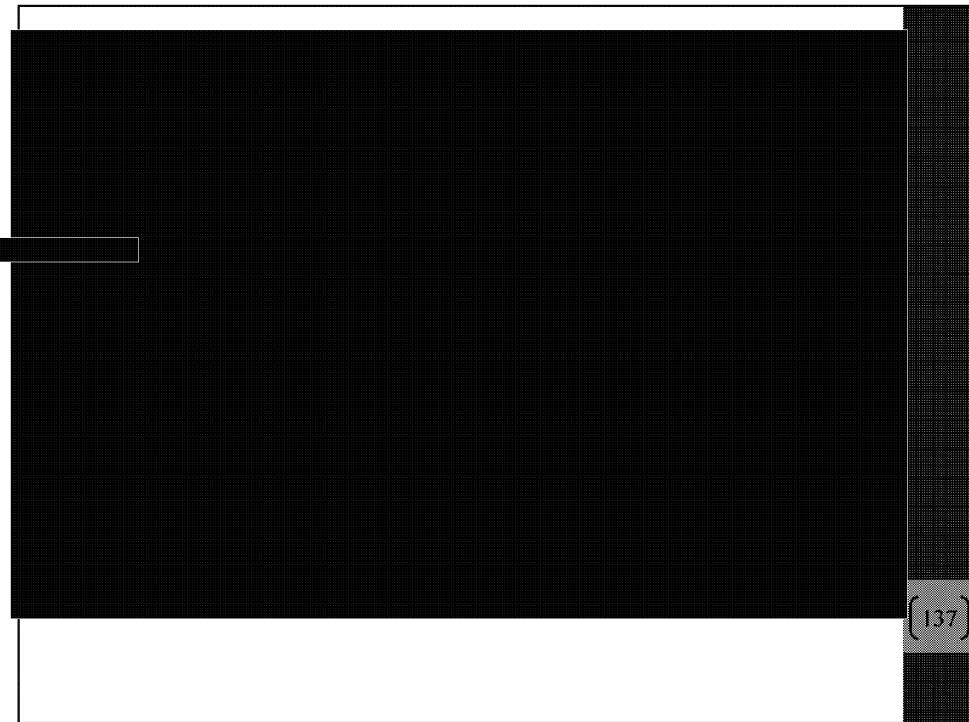
134

## **WTR Report Format**

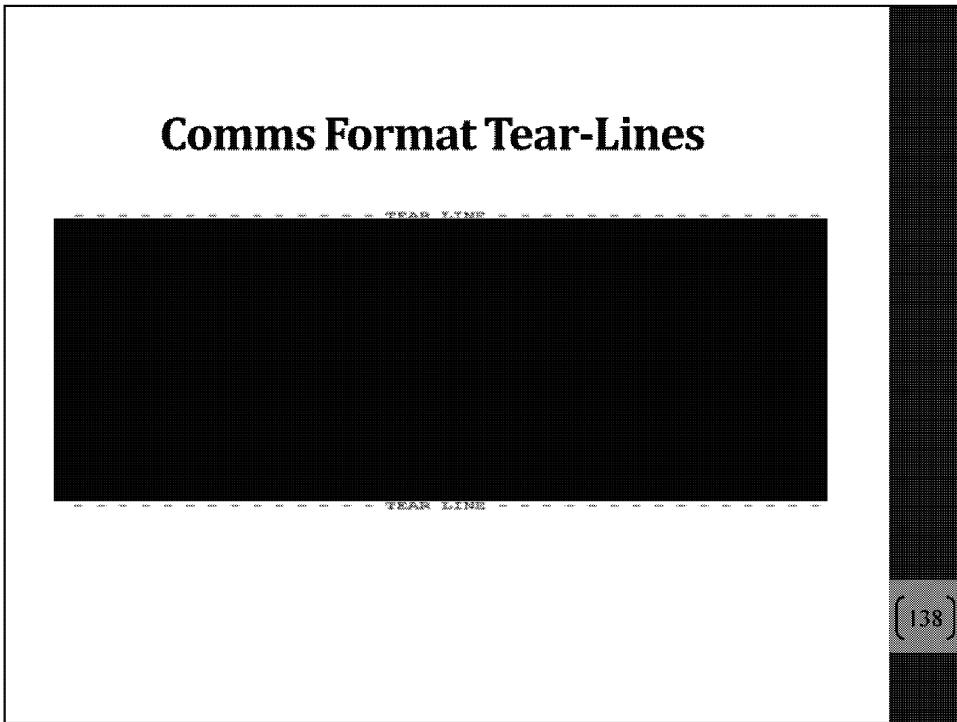
IRRELEVANT

## WTR Report Format

IRRELEVANT



IRRELEVANT



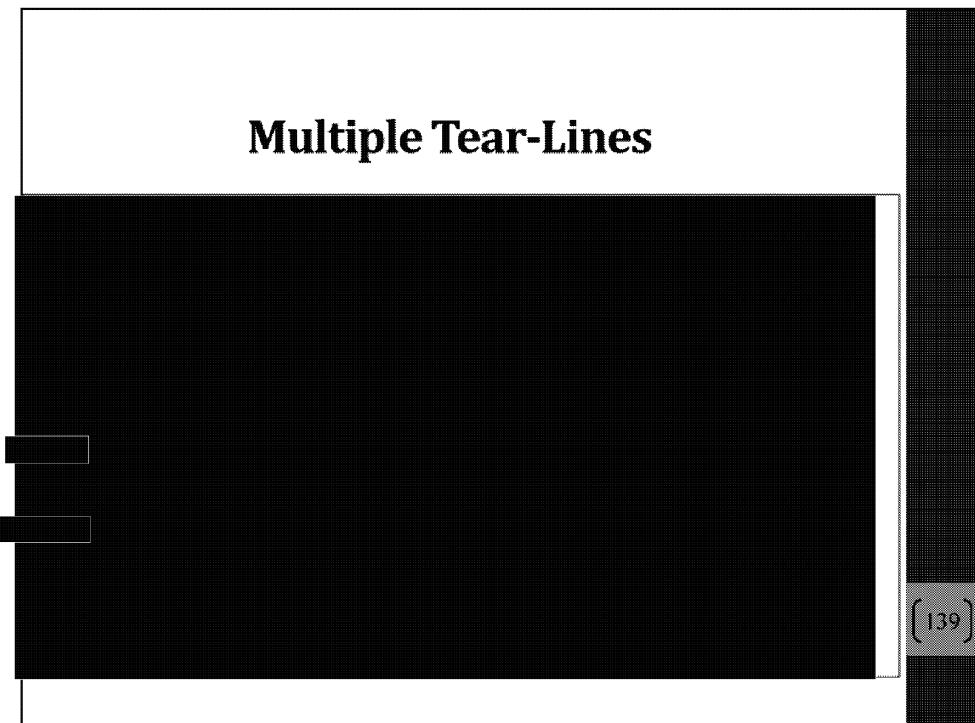
No crest

Serial # truncated [REDACTED]

SI para's removed (generally at S level)

Appears at the bottom of the print out and can physically "tear off"

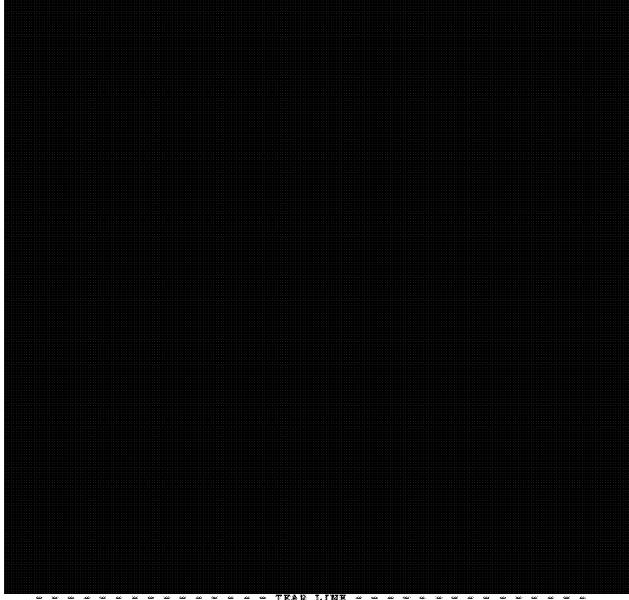
## Multiple Tear-Lines



139

## Multiple Tear-lines / Comms Format

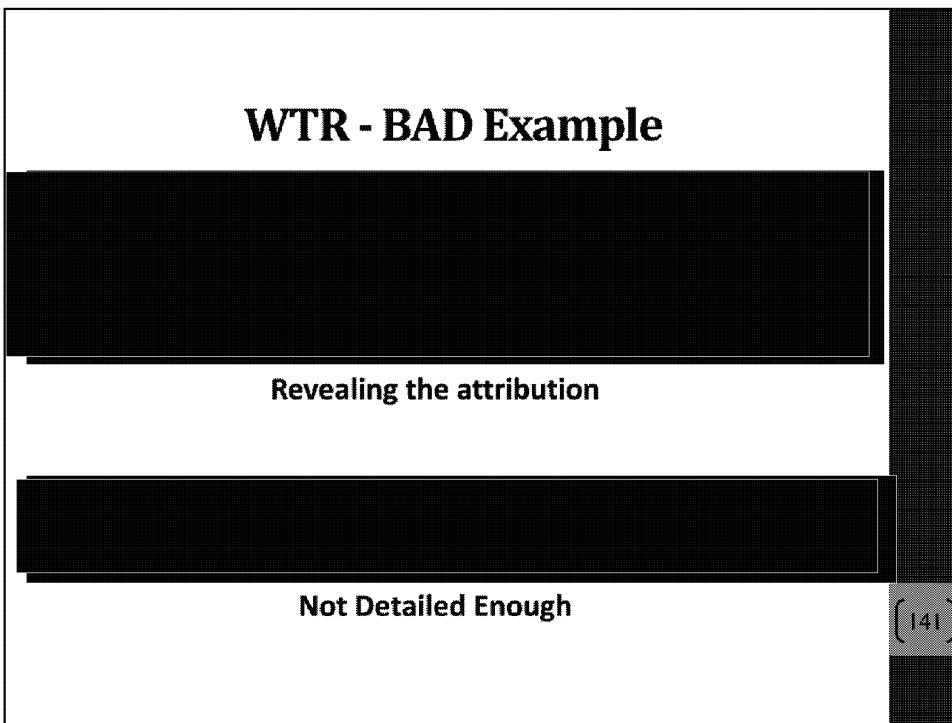
TEAR LINE CUI



----- TEAR LINE -----

140

140



Both [REDACTED] revealed

## Tips and Tricks

- For [REDACTED] think *beyond* the communicants of the traffic
- Consider how fast your [REDACTED] can deliver information
- A [REDACTED] comments can be attributed to his/her [REDACTED]  
e.g. [REDACTED]
- Confine the information to just the most relevant facts from the full report.

[142]

Take a step back



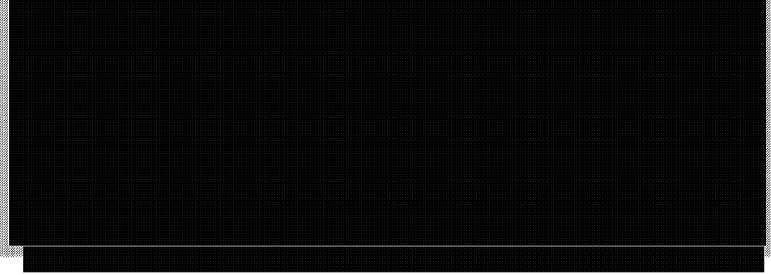
142

## Suppressed Identities in the WTR

- Do **not** include suppressed idents (e.g., "a named Canadian company") in the WTR portion, because
    - the intelligence won't be of much value to the SECRET-level reader without the name, and
    - the SECRET-level reader can't request the identity
- If the 5-Eyes identity is essential to the report's intelligence value, do **not** write a WTR report.

[ 143 ]

## Attribution in the WTR

- Some identification of the intelligence source may be required when the “who said it” is part of the significance of the intelligence.
- In these cases, **generalize** the intelligence source.
- None of these examples implies COMINT as the source:  


[144]

## Collateral in the WTR

You can use collateral in the non-SI portion as long as:

- it's not TOP SECRET
- you don't mark it as collateral in the non-SI portion
- you repeat it, properly marked, in the SI portion

[ 145 ]

Must be repeated in the details with the appropriate mark up.

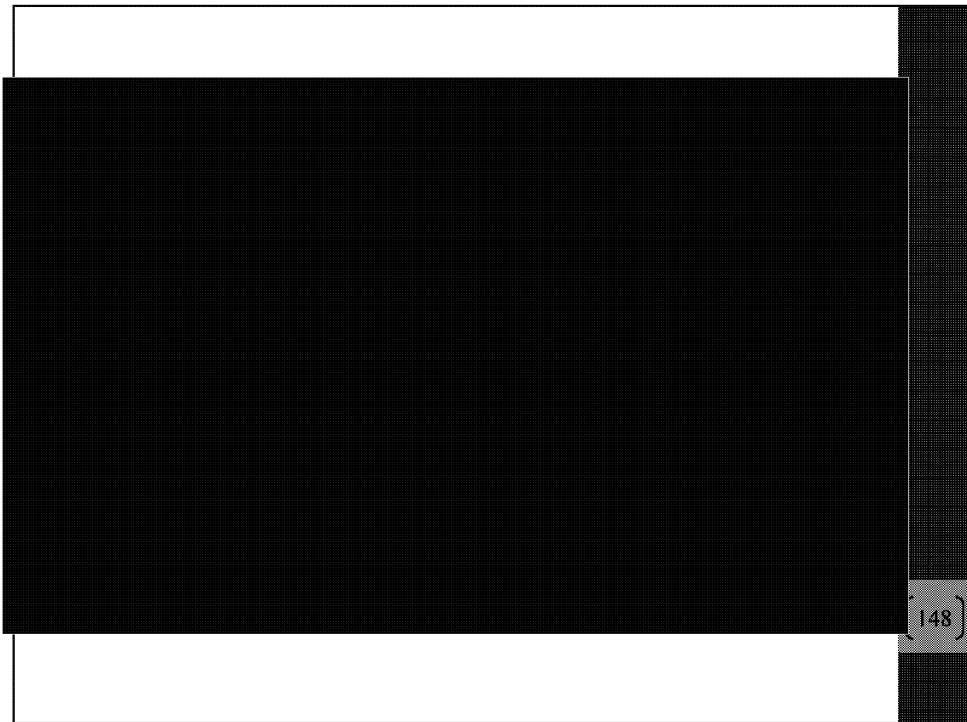


146

## Comments in WTR

IRRELEVANT

[+]



Do not mark as Comment, weave into text (probably for early July...)

148

## WTR EXERCISES



149

Three groups to individually work on WTRs for one of the examples. Discuss and pick best one for presentation.

149

## Module 9 Topic and Area Guide (TAG)

- Based on [REDACTED]
- Provides a quick summary of the intelligence source, type of information and major participants in a report
- Accessible from the [REDACTED] search on TAG

*Example:*



Page 71

150

[REDACTED]  
[REDACTED]  
[REDACTED]  
consists of three letters:

- a **country digraph** indicating the source of the intelligence
- a **function letter** which identifies the functional association [REDACTED]

*Example:* [REDACTED]

(151)

## Intelligence Source Function Letters

Letter Topic

Definition

at

(152)

## Subject/Topic Component (STC)

[ 153 ]

153



154

## Principal Component (PC)

IRRELEVANT

(155)

155

## Topic Area Guides (TAGs)

IRRELEVANT

[ 156 ]

156

156

## Topic Area Guides (TAGs)

*Example:*

IRRELEVANT

[ 157 ]

## Topic Area Guides (TAGs)

Create separate TAG lines for each [REDACTED]

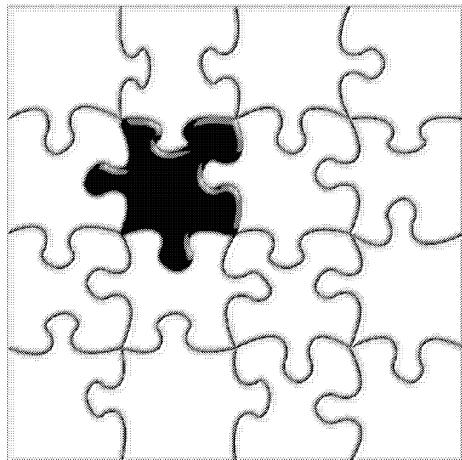
*Example:*

IRRELEVANT

[158]

158

## TAGs EXERCISE



[ 159 ]

159

## Delivery Distribution Indicators (DDIs)

- The DDI is the [REDACTED] used to permit automatic routing of a report to specific databases and elements within national SIGINT centers, primarily NSA
- There are two sets of DDIs:
  - one used exclusively for EPRs, and
  - one used exclusively for CIRs.
- Select DDIs for all [REDACTED]  
[REDACTED] in your report.

[160]

DDI [REDACTED]

Different DDIs are used for CIRs and EPRs

160

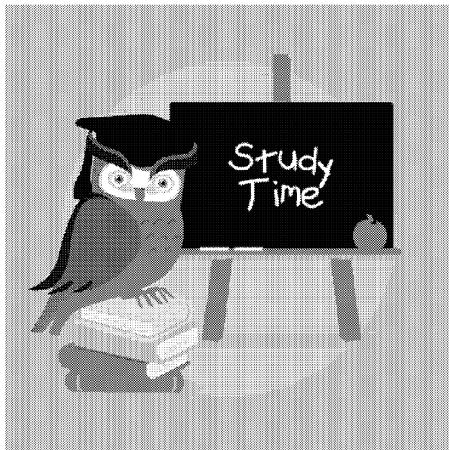
## Delivery Distribution Indicators (DDIs)

DDIs can be used on any report.

- the DDI [REDACTED] IRRELEVANT EPR templates in [REDACTED]
- the DDI [REDACTED] IRRELEVANT [REDACTED] EPR templates in [REDACTED]

[ 161 ]

## DDIs EXERCISE



( 162 )

## Correction Guidelines

IRRELEVANT

[ 163 ]

## Cancelation Guidelines

### When to CANCEL a report

- Its entire contents are found to be incorrect.
- It is underclassified or overclassified.
- It was issued CEO, but should have been shared with one or more Second Parties.
- It was sent to one or more ineligible addresses.
- It inadvertently discloses a Canadian or Second Party identity.

[ 164 ]

## References

OPS 1 *Protecting the Privacy of Canadians ...*

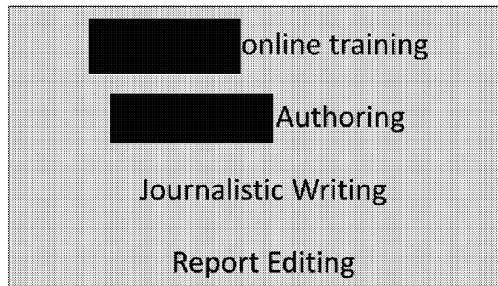
OPS 5-3 *Write-to-Release Procedures and WTR Exemption List*

OPS 1-7 *SIGINT Naming Procedures*

**CSOI 4-1 *SIGINT Reporting Procedures***

[ 165 ]

## What's Next?



*Happy Report Writing !*

( 166 )

**Before you leave, please...**

IRRELEVANT

**Thank you!**

( 167 )

167