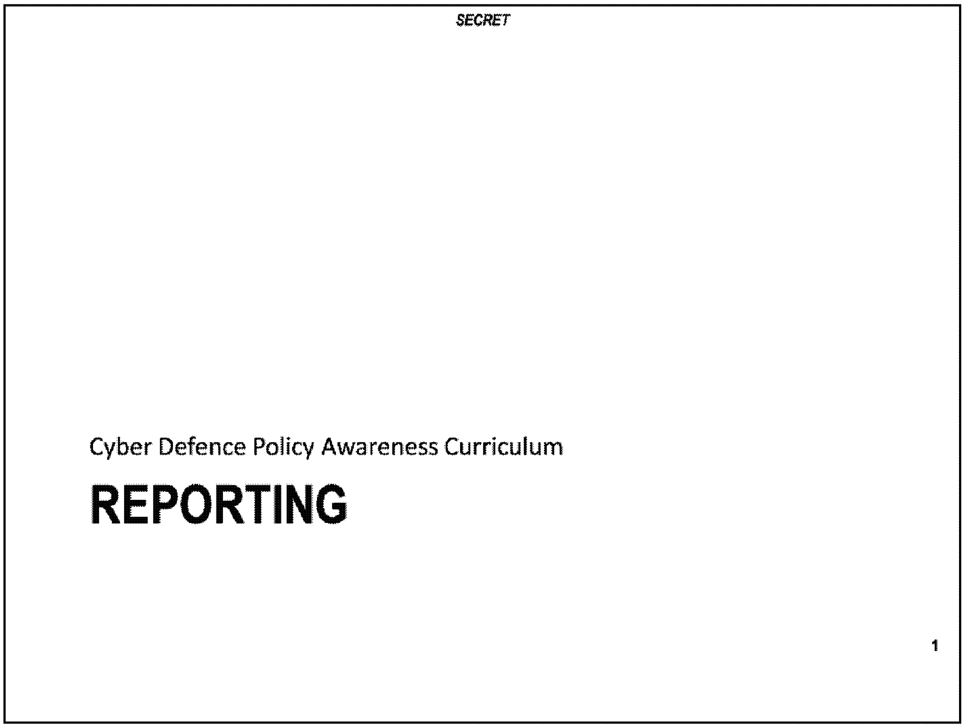
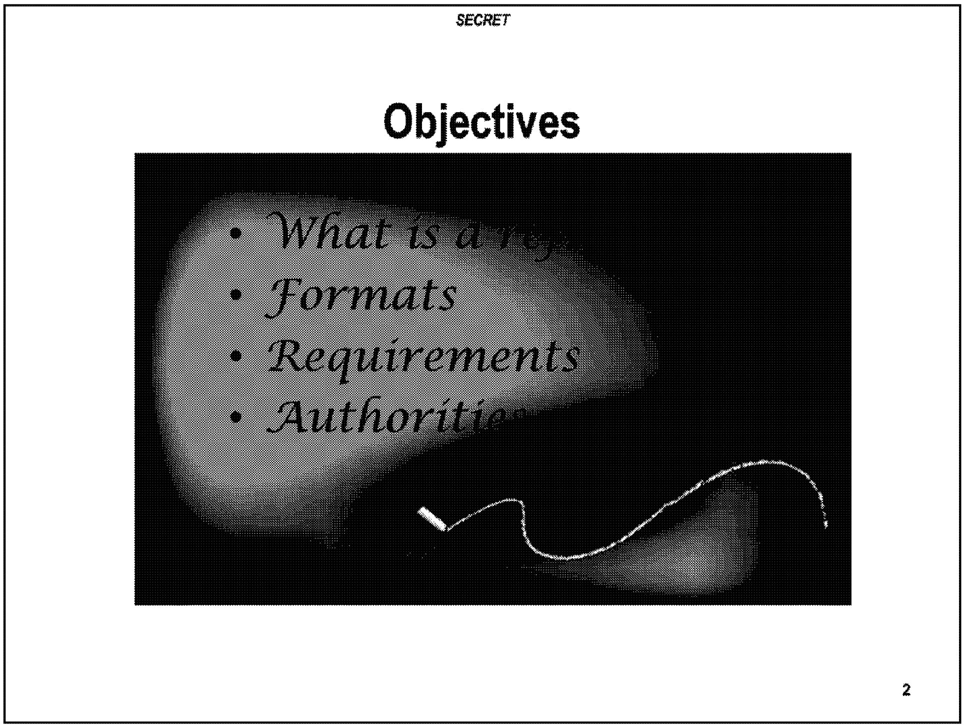


SECRET

Cyber Defence Policy Awareness Curriculum

REPORTING



SECRET

Objectives

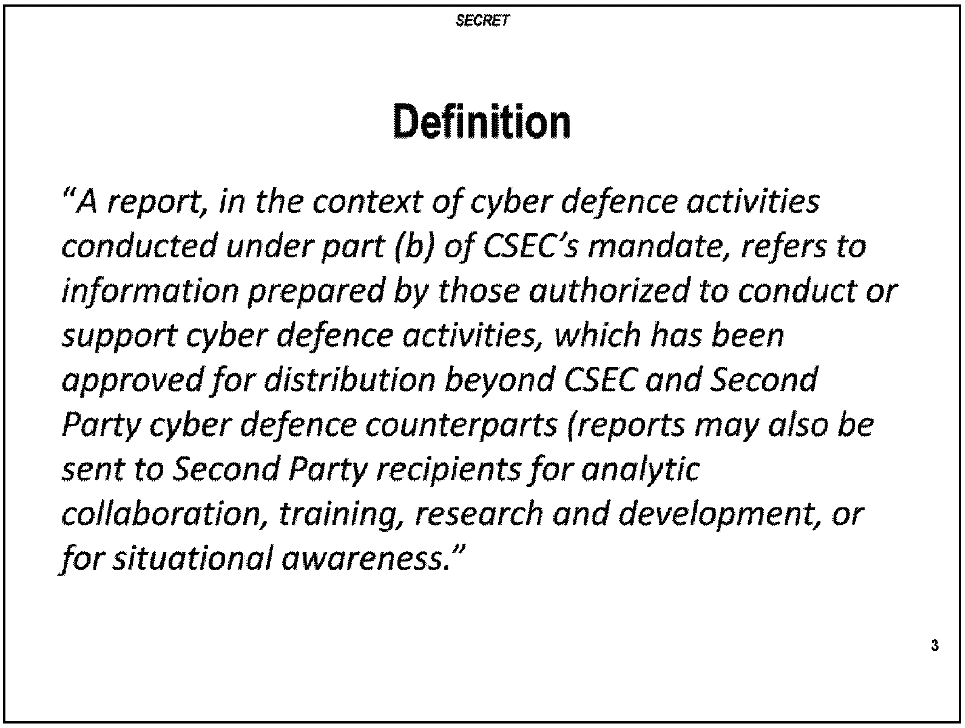
- *What is a re*
- *Formats*
- *Requirements*
- *Authoritie*

Introduction and Background to the Cyber Defence Policy Awareness Curriculum Workshop

FACILITATOR NOTES:

-Welcome participants to the class then…

-use a graphic , or bullet points to explain why participants need to attend this training



SECRET

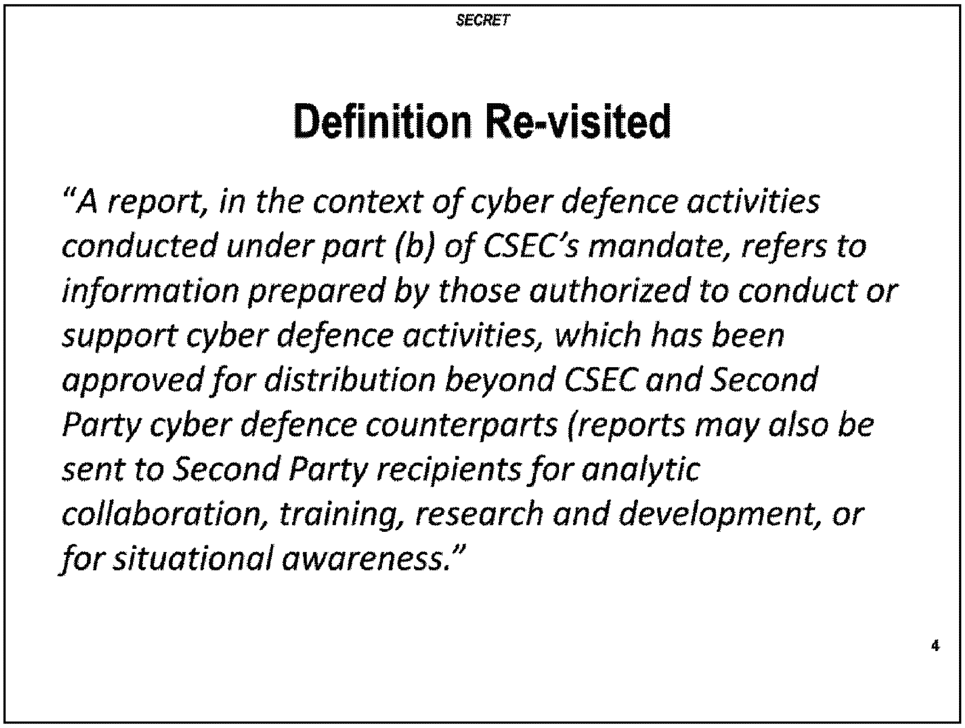
Definition

"A report, in the context of cyber defence activities conducted under part (b) of CSEC's mandate, refers to information prepared by those authorized to conduct or support cyber defence activities, which has been approved for distribution beyond CSEC and Second Party cyber defence counterparts (reports may also be sent to Second Party recipients for analytic collaboration, training, research and development, or for situational awareness."

3

That's a pretty heavy definition to digest, but the key take away from this are that reports:

- Authored by cyber defence team members
- Meant for distribution beyond CSE
- Authorized



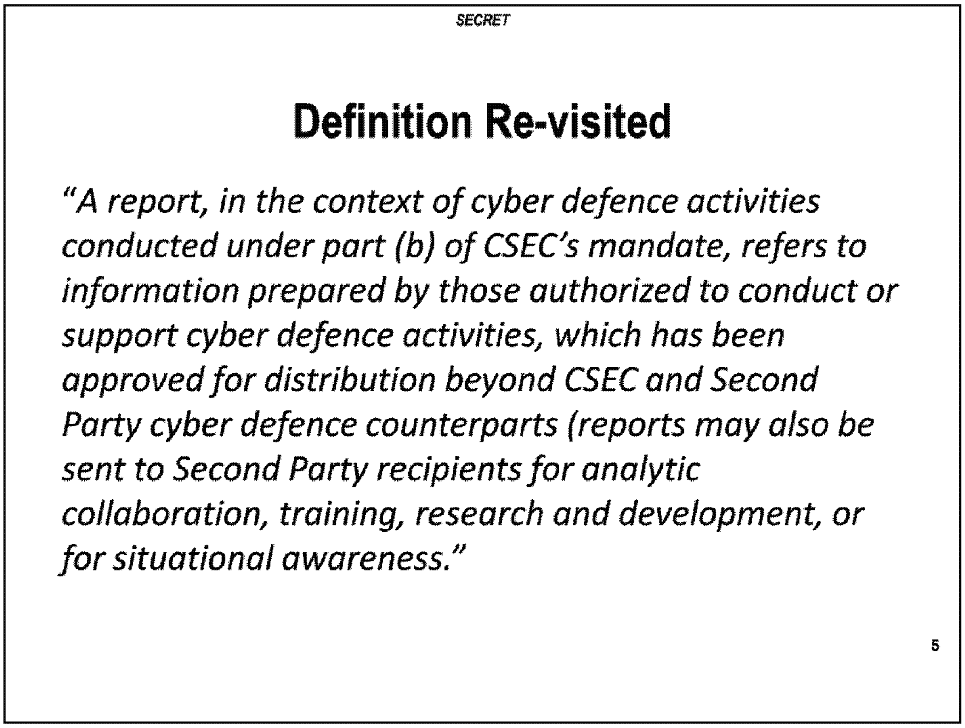
SECRET

Definition Re-visited

"A report, in the context of cyber defence activities conducted under part (b) of CSEC's mandate, refers to information prepared by those authorized to conduct or support cyber defence activities, which has been approved for distribution beyond CSEC and Second Party cyber defence counterparts (reports may also be sent to Second Party recipients for analytic collaboration, training, research and development, or for situational awareness."

4

This is what a report is: Information prepared by the cyber defence team for distribution beyond CSEC for Mandate B purposes.



SECRET

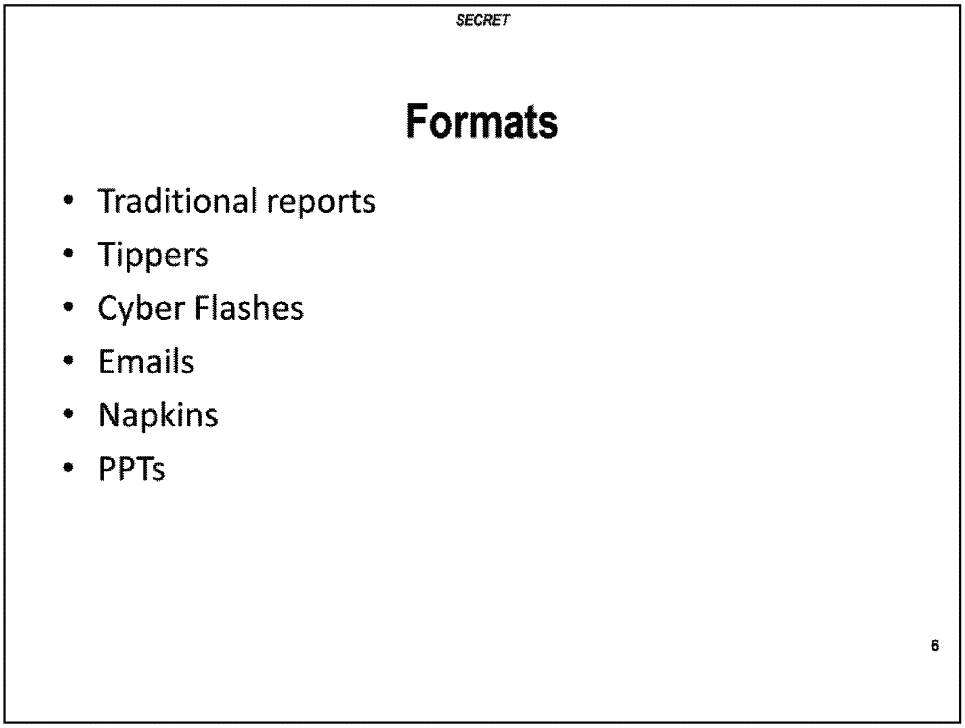
Definition Re-visited

"A report, in the context of cyber defence activities conducted under part (b) of CSEC's mandate, refers to information prepared by those authorized to conduct or support cyber defence activities, which has been approved for distribution beyond CSEC and Second Party cyber defence counterparts (reports may also be sent to Second Party recipients for analytic collaboration, training, research and development, or for situational awareness."

5

And this is the requirement.

Basically, any information (data) you send for Mandate B purposes is a report and you must get the proper authorization before distribution.



SECRET

Formats

- Traditional reports
- Tippers
- Cyber Flashes
- Emails
- Napkins
- PPTs

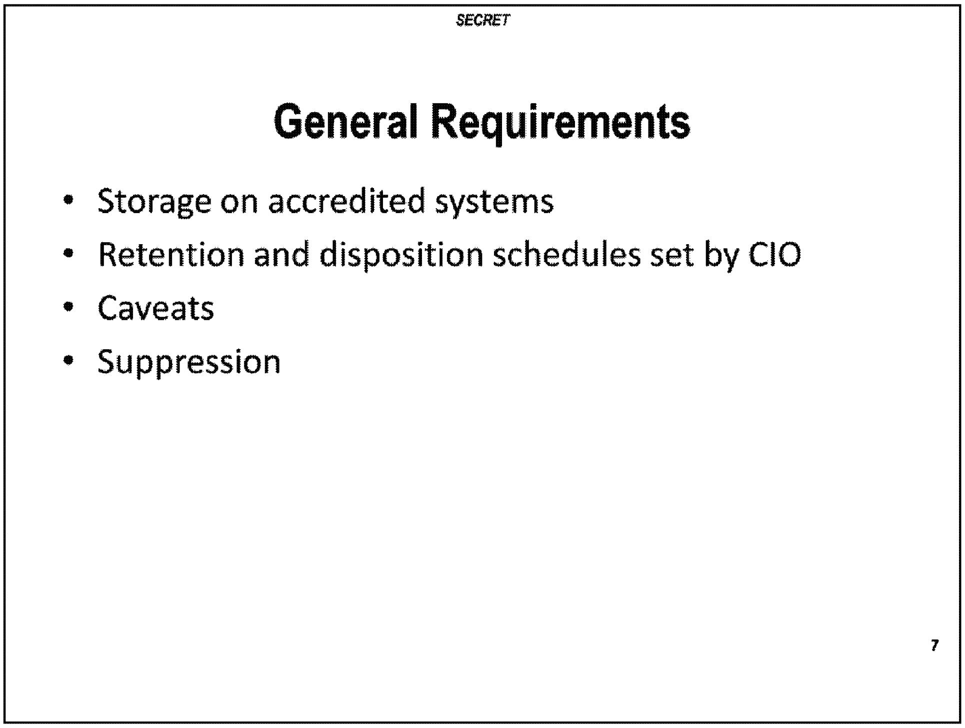
6

Report can come in different formats. So your traditional reports are things like [redacted] etc.

Tippers and cyber flashes also count

Any other e-mails also count. So if you want to send some malware samples, or provide rapid mitigation advice via email, you still need to get the proper approvals.

Napkins? Seriously, if you want to provide mitigation advice on a napkin, feel free. But you still need to meet all the report policy requirements before you give the client your napkin. So really… don't….



SECRET

General Requirements

- Storage on accredited systems
- Retention and disposition schedules set by CIO
- Caveats
- Suppression

7

Speaking of report requirements…

All reports must be stored on accredited systems and retain in accordance with CSE's retention and dispositions schedules set by CIO/Information Holding Services, which currently ranges from 5 - 20 years, depending on the type of report, then transfer to Library and Archives Canada. So if you want to write a report on a napkin…

Remember we are talking about reports here, not raw data. The base authority for the retention of reports comes from the Library and Archives of Canada act, whereas the authority for the retention of Raw Data comes from the Ministerial Authorizations.

Caveats: Any classified or protected cyber defence reports must have a caveat stipulating how the reported info may be used, and any other restrictions as appropriate. IPOC can help you construct a caveat, if there are specific concerns you want to address.

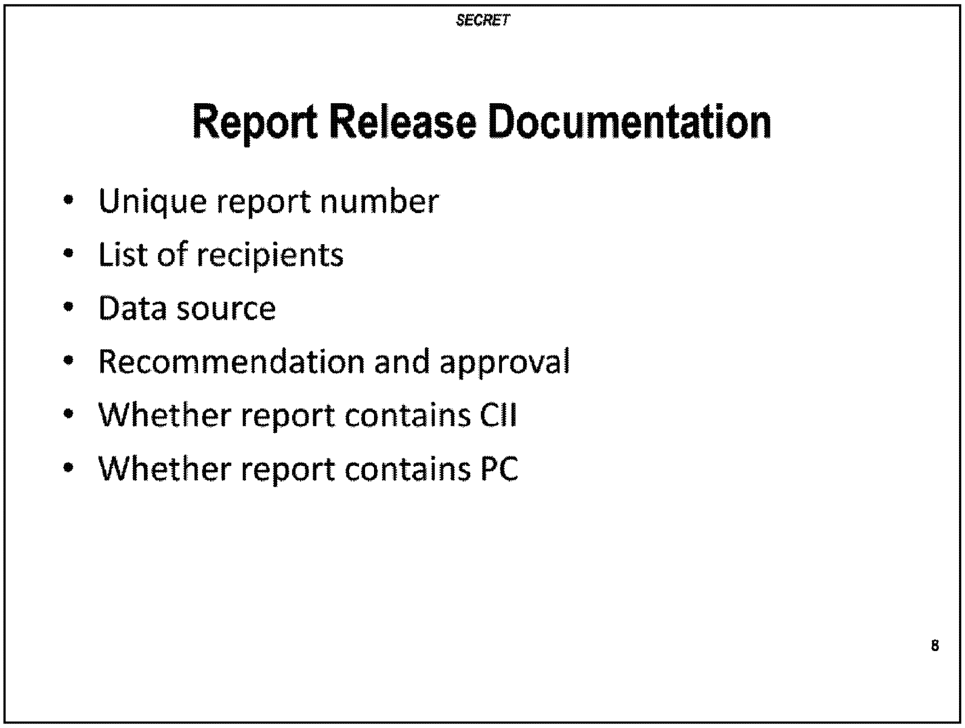
Suppression: Remember the common theme throughout this course, protecting the privacy of Canadians. There is where suppression comes in. So, the general rule is, You can send unsuppressed CII back to the institution from which the data was obtained because it is their data. They have it already, they own the data, they can see it unsuppressed, so there is no requirement for us to suppress in this case. We are not compromising the privacy of any Canadians by releasing their identities to those who do not already have access/ownership of it. On the other hand, you must suppress CII in any reports that are being distributed beyond the institution from which the data was obtained, including non-cyber defence team members of CSE.

There are some exceptions of course. CII may be unsuppressed beyond the institution from which the data was obtained if:

- The information is necessary in order for recipients to use the mitigation advice to protect their own networks, or
- CII has been compromised by, or is the target of, a malicious foreign actor.

Honestly, the wording in the policy is not the greatest. What it is meant for is: You [redacted]

Please consult IPOC if you ever encounter a situation like this.



SECRET

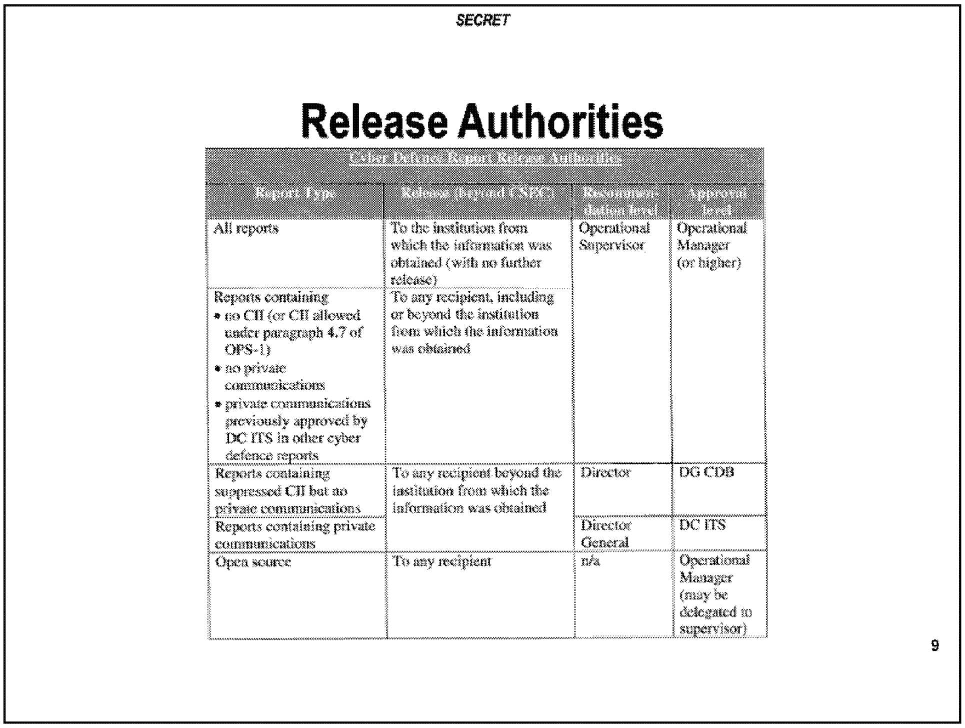
Report Release Documentation

- Unique report number
- List of recipients
- Data source
- Recommendation and approval
- Whether report contains CII
- Whether report contains PC

8

Here's what you have to document for all reports. So, if you are using traditional report dissemination methods [redacted] this should all be part of the mandatory fields you need to fill out.

But, if you are using "non-traditional" report disseminations formats, make sure all of this information is captured and stored in an easily retrievable method. You should check with your supervisor/manager, as the documentation should be saved in a central location for easy retrieval.



SECRET

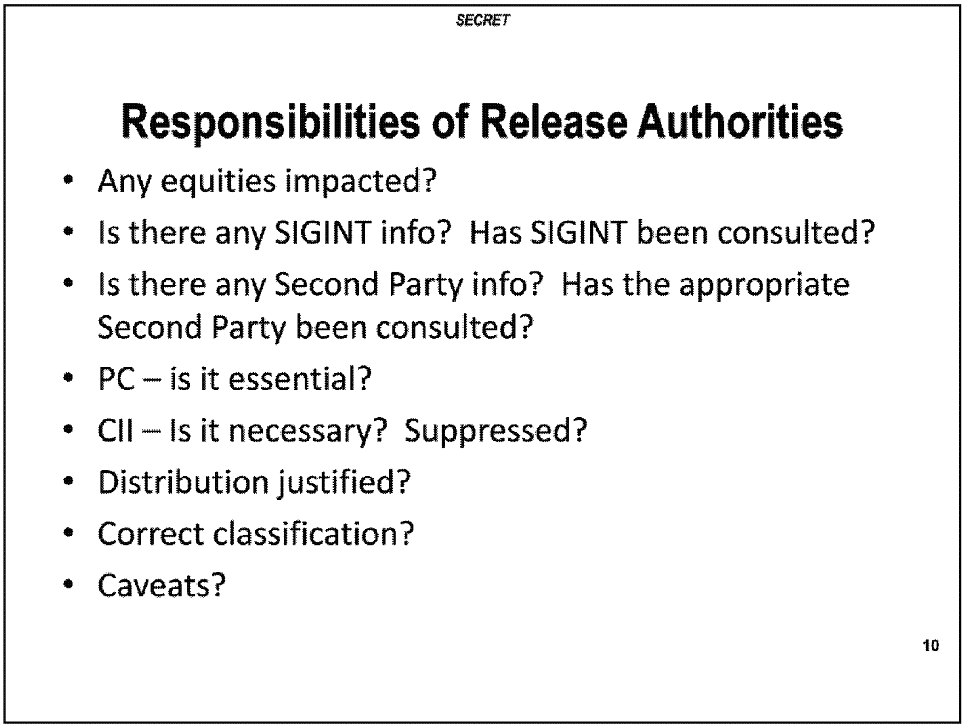
Release Authorities

Cyber Defence Report Release Authorities			
Report Type	**Release (beyond CSEC)**	**Recommendation level**	**Approval level**
All reports	To the institution from which the information was obtained (with no further release)	Operational Supervisor	Operational Manager (or higher)
Reports containing • no CII (or CII allowed under paragraph 4.7 of OPS-1) • no private communications • private communications previously approved by DC ITS in other cyber defence reports	To any recipient, including or beyond the institution from which the information was obtained		
Reports containing suppressed CII but no private communications	To any recipient beyond the institution from which the information was obtained	Director	DG CDB
Reports containing private communications		Director General	DC ITS
Open source	To any recipient	n/a	Operational Manager (may be delegated to supervisor)

9

This is the release authorities table from ITSOI-1-2 and based on OPS-1. It shows what the recommendation and approval levels are depending on what type of information is contained in the report (CII and/or PC).

What I want to highlight though is what the recommendation and approval authorities should actually be looking for before signing off on a report.



SECRET

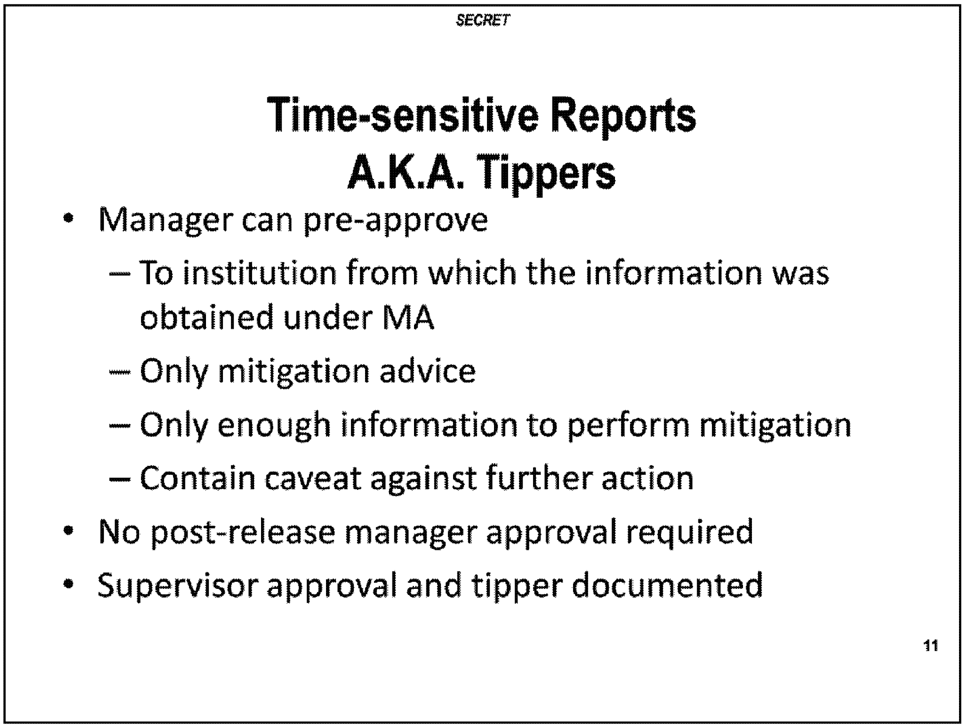
Responsibilities of Release Authorities

- Any equities impacted?
- Is there any SIGINT info? Has SIGINT been consulted?
- Is there any Second Party info? Has the appropriate Second Party been consulted?
- PC – is it essential?
- CII – Is it necessary? Suppressed?
- Distribution justified?
- Correct classification?
- Caveats?

10

Here are some of the questions that the recommending and approving authorizes should be asking before they sign off a report.

Release authorities have the responsibility of not only making sure the report meets the operational requirements, but also the policy requirements as set out in the policies.



SECRET

Time-sensitive Reports A.K.A. Tippers

- Manager can pre-approve
  - To institution from which the information was obtained under MA
  - Only mitigation advice
  - Only enough information to perform mitigation
  - Contain caveat against further action
- No post-release manager approval required
- Supervisor approval and tipper documented

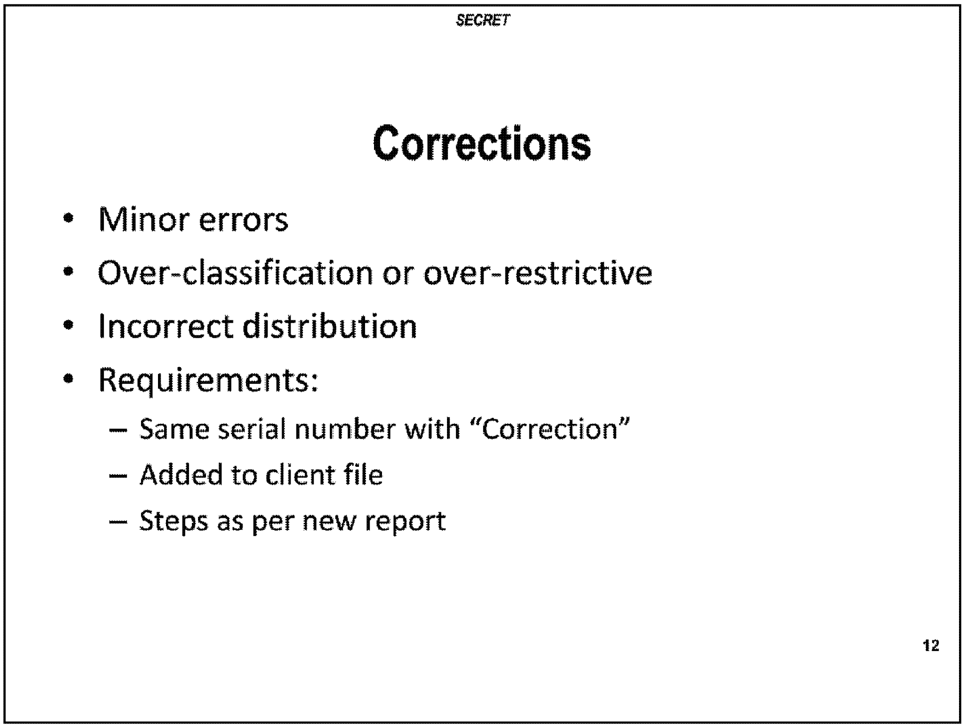
11

I want to quickly mention tippers because there are some special procedures for these types of reports.

Because we understand that some mitigation advice must be passed on as quickly as possible, there is a procedure that allows tippers to be released at the supervisor level. Basically, the manager can pre-approve all tippers that meet the above criteria. Once the manager formally pre-approves, supervisors are allowed to release tippers under their authority.

Not that you must ensure that all of this information is documented and kept for compliance monitoring.

Now approved and disseminated through [redacted]



SECRET

Corrections

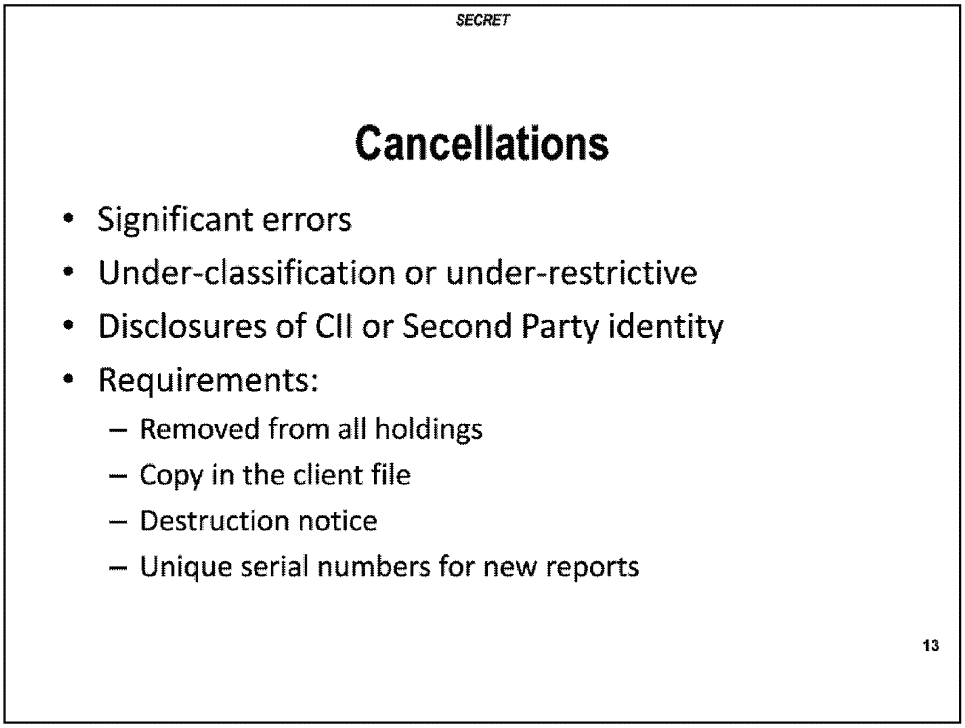
- Minor errors
- Over-classification or over-restrictive
- Incorrect distribution
- Requirements:
  - Same serial number with "Correction"
  - Added to client file
  - Steps as per new report

12

If you note any minor errors in a report that must be fixed, you can issue a correction.

Depending on the circumstances of the correction, you may have to notify recipients to destroy the original report.

Remember the 'privacy incidents' we referred to earlier…we said "Accidents happen", so remember, if we have a potential impact to privacy of Canadians, we have an established procedure we must follow. Remember – don't panic!



SECRET

Cancellations

- Significant errors
- Under-classification or under-restrictive
- Disclosures of CII or Second Party identity
- Requirements:
  - Removed from all holdings
  - Copy in the client file
  - Destruction notice
  - Unique serial numbers for new reports

13

Cancellations are meant for more serious errors.

The procedures are slightly different, in that you are required to send a destruction notice to all recipients, and any follow-on “new reports” are unique and not linked to the cancelled report.

Note that in both cases, IPOC must be informed because there may be impacts on privacy in both cases.