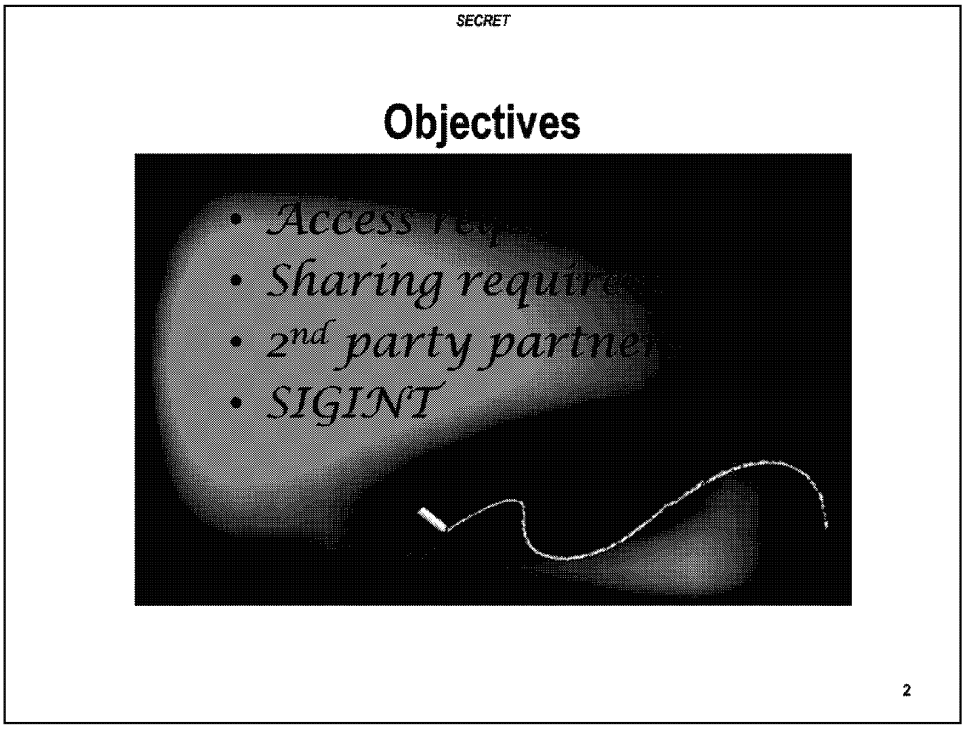
Cyber Defence Policy Awareness Curriculum

ACCESS AND SHARING

1

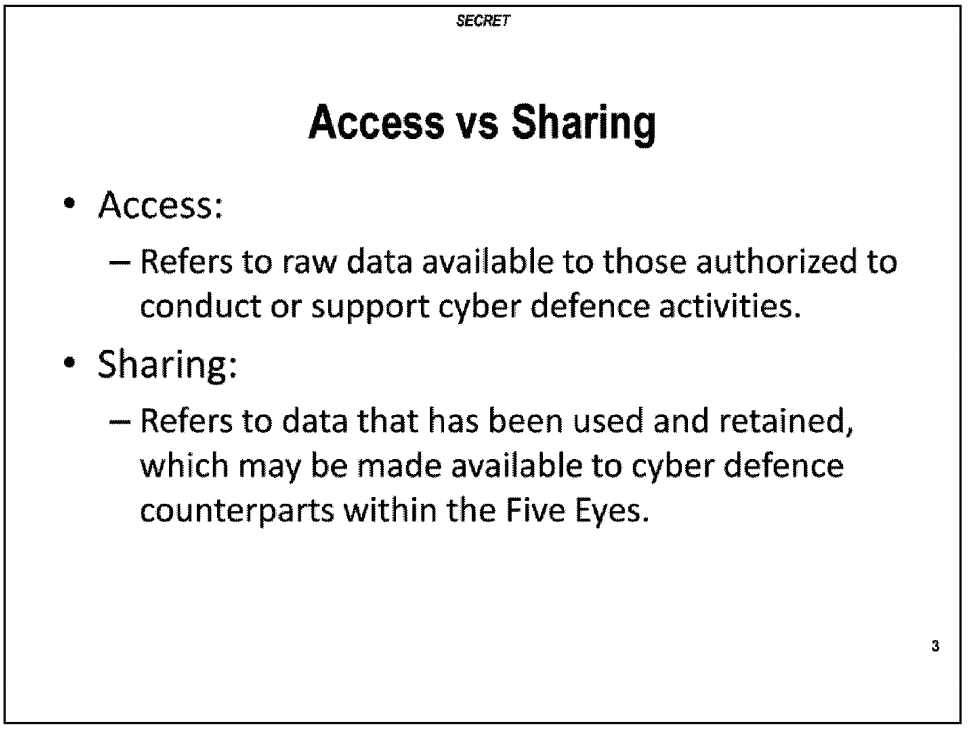


Introduction and Background to the Cyber Defence Policy Awareness Curriculum Workshop

FACILITATOR NOTES:

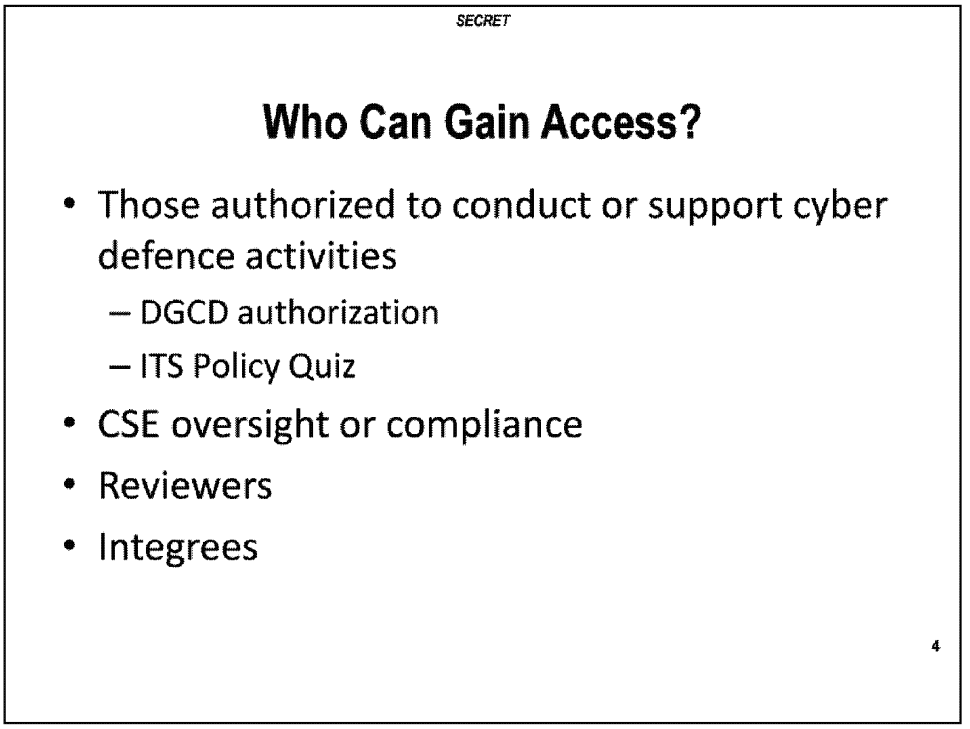
-Welcome participants to the class then…

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



The big difference here is the type of data. Remember back in the data handling lesson we out lined the difference between raw data and used and retained data? Well, we give access to raw data, we share used and retained data.

Why is there a distinction? Simple put, there are restrictions depending on who can access raw data and who you can share used and retained data with.



"Those authorized to conduct or support cyber defence activities" is how it is worded in the policy, but what it really should say is "Those authorized to conduct or support cyber defence activities **AND** have a need to query/use/retain and manipulate raw data".

In ITS, employees in CDO, CTEC and IPOC fall into this category.

Additionally there are "specialists" from [redacted] that also fall into this category.

To gain access, you need to have a cyber defence team manger sponsor you and request authorization from DGCD. After that, you need to complete the ITS Policy Quiz to demonstrate you understand the applicable policies. If you are part of the aforementioned groups, once you receive authorization from DGCD the first time, you do not need to do so again unless you leave your group and then come back. But you still need to revalidate your understanding of the policies yearly by passing the ITS Policy quiz.

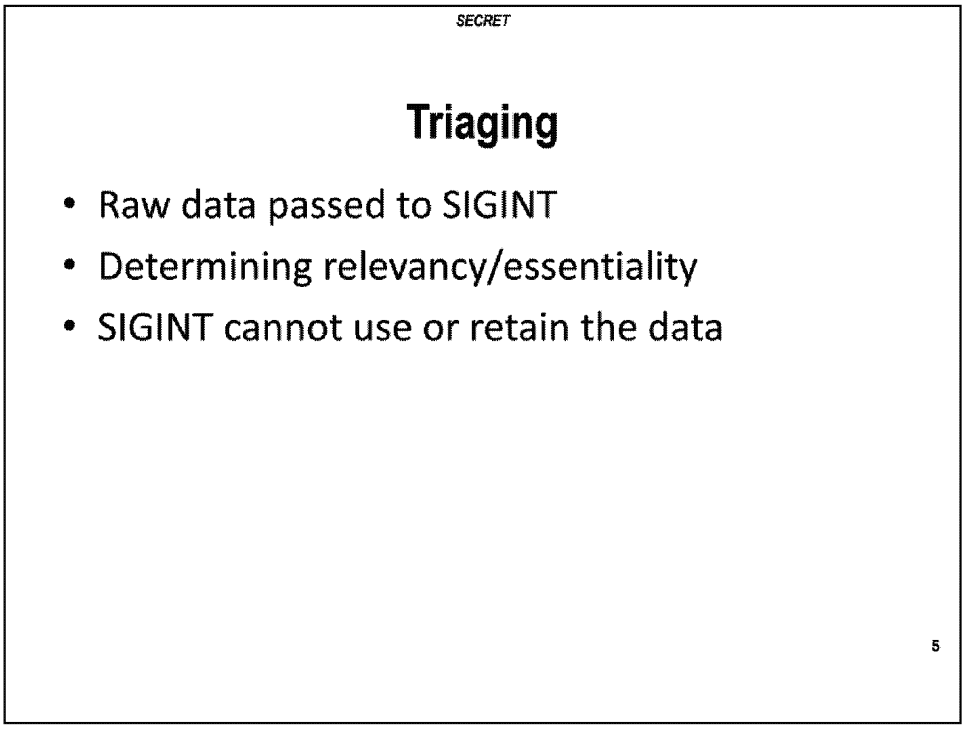
Note – This quiz is NOT the same as the SIGINT OPS-1 Quiz. And by annual, it means every year, not a year after you've just done it. i.e. you join in Nov, you'll

have to do it again the next Spring.

It is also possible to obtain access to raw data for a temporary/short period of time. For example, R&D projects, BIGDIG, workshops, etc. The same process is followed, except DGCD's authorization is for a limited amount of time. Also, the ITS Policy quiz may be focused on the issues particular to the temporary access request. i.e. if you are not reporting, there will likely not be many/any reporting questions on the quiz.

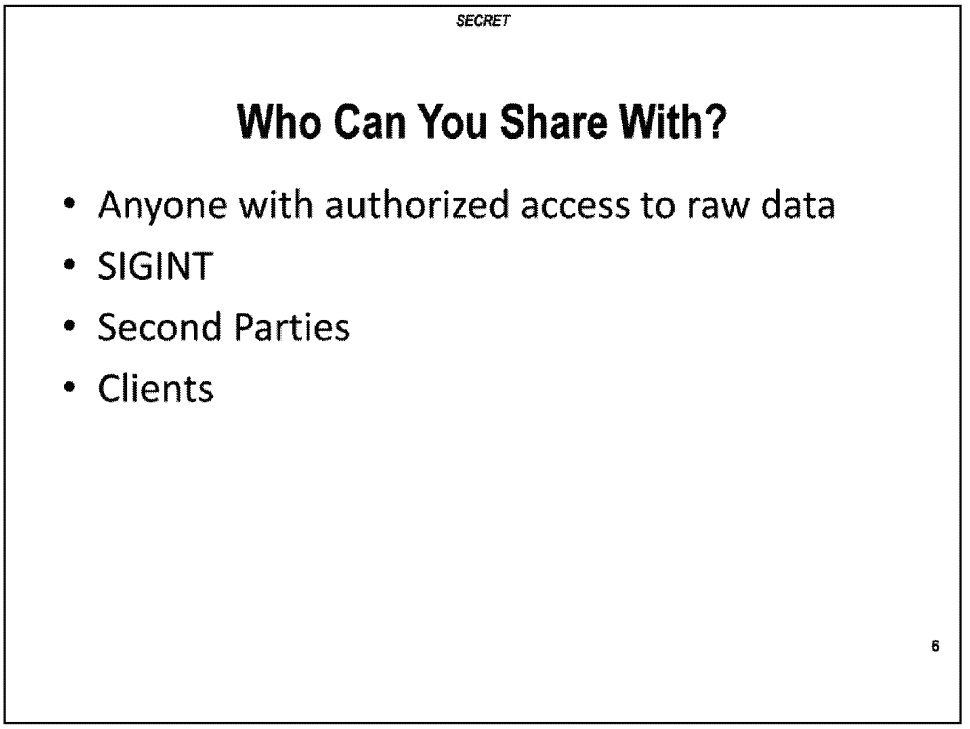
[redacted] second party partners are NOT allowed access to raw data [redacted]

[redacted]



Triaging is a special form of access, whereby you (someone authorized to conduct or support cyber defence activities) can pass raw data to a SIGINT employee who is NOT authorized to conduct or support cyber defence activities for the sole purpose of determining if that data is relevant or essential to Mandate B.

SIGINT is not allowed to use or retain that data for their own purposes, and it is the responsibility of the person seeking assistance to ensure that the recipients are aware of that.



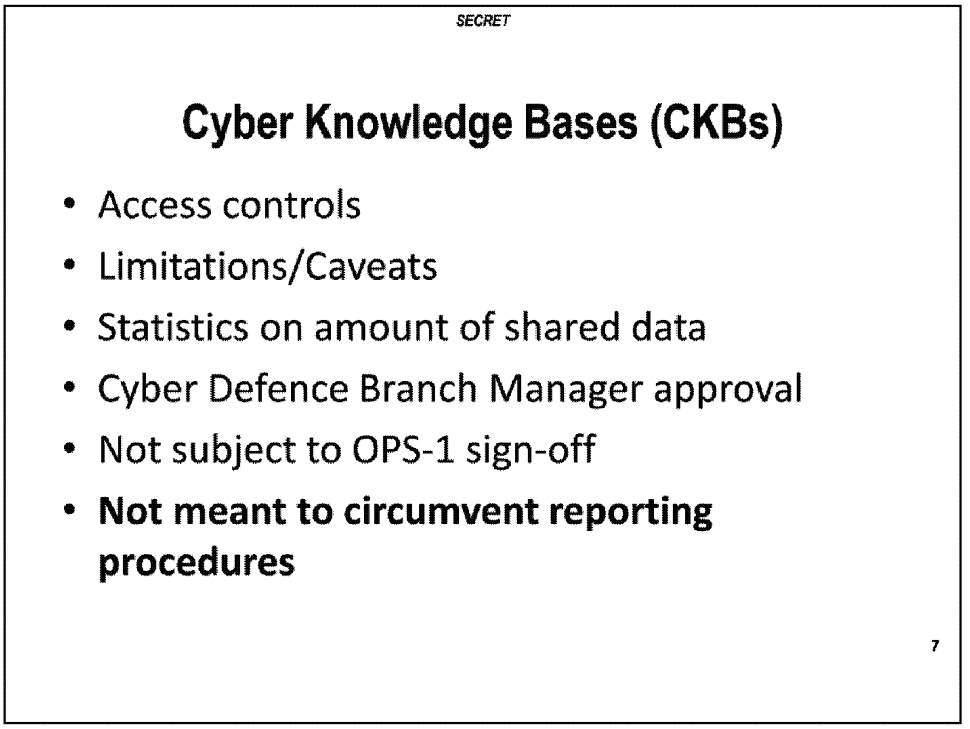
Sharing is normally done in the form of a report, but there are other means of sharing data, mainly through Cyber Knowledge Bases (CKBs) with second party partners.

Even though it is only used and retained data being shared, you must ensure that proper access controls are in place as well as appropriate caveats. Remember, everything must be auditable, so we have to be able to know what was shared and to whom.

Also, just because we can share used and retained data, doesn't mean we can share it all. CII, still must be suppressed.

Sharing outside of CSE and Second Party Partners must be in the form of a report.

Raw data is not "shared" beyond CSE.



Sharing is normally done in the form of a report, but there are other means of sharing data, for example, through Cyber Knowledge Bases (CKBs) like the malware repo.

To purpose of sharing data with Second Party Partners in order to:

•Increase analytic coverage and efficiency

•Allow analytic collaboration, training and R&D

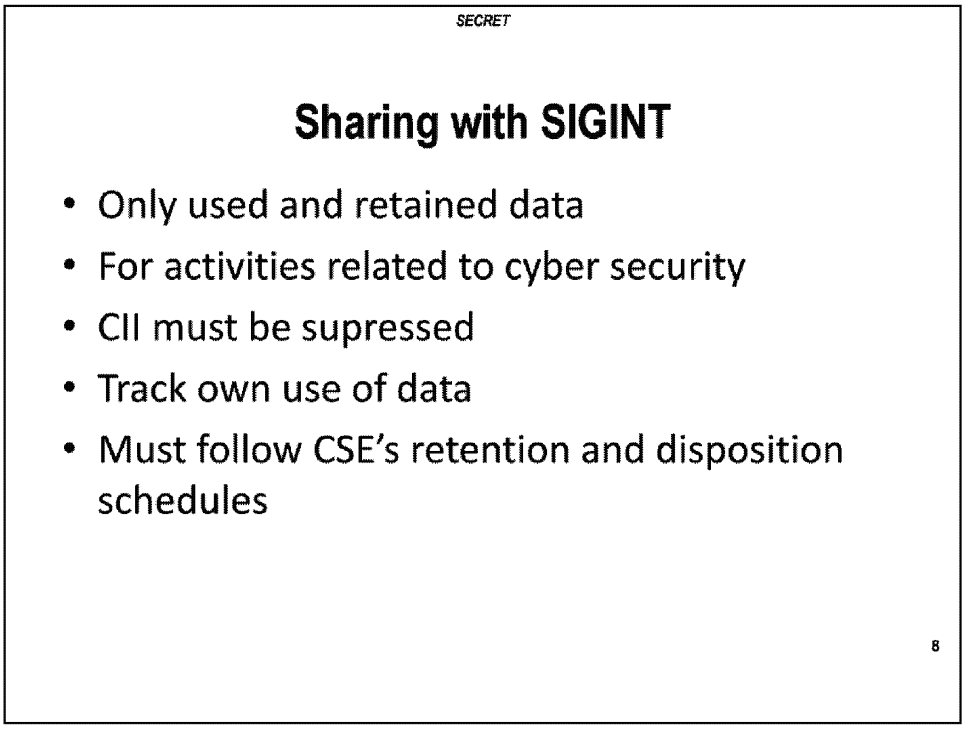
•Allow CSE to receive data from Second Parties

[redacted]

Even though it is only used and retained data being shared, you must ensure that proper access controls are in place as well as appropriate caveats. Remember, everything must be auditable, so we have to be able to know what was shared and to whom.

Also, just because we can share used and retained data, doesn't mean we can share it all. CII, still must be suppressed/access restricted.

CKBs are not subject to OP-1 sign-offs… Although it's not explicitly written, CKBs are meant for sharing with Second Party Partners and within CSE only, so you can't use a CKB to avoid sign off for reports/mitigation advice to clients. CKBs are not meant for mitigation.



None of this should really be a surprise and it's pretty straight forward.

Remember, this is referring to used and retained data, not raw. SIGINT is allowed to use ITS shared data for part (a) of the mandate, but only if it's related to cyber security. Once data has been shared, it now "belongs" to SIGINT, so it must be tracked in accordance with SIGINT's applicable policy and oversight instructions.

Reminder – CII must be supressed if it is sent outside of the cyber defence team at CSE. This includes used and retained data as well as reports.

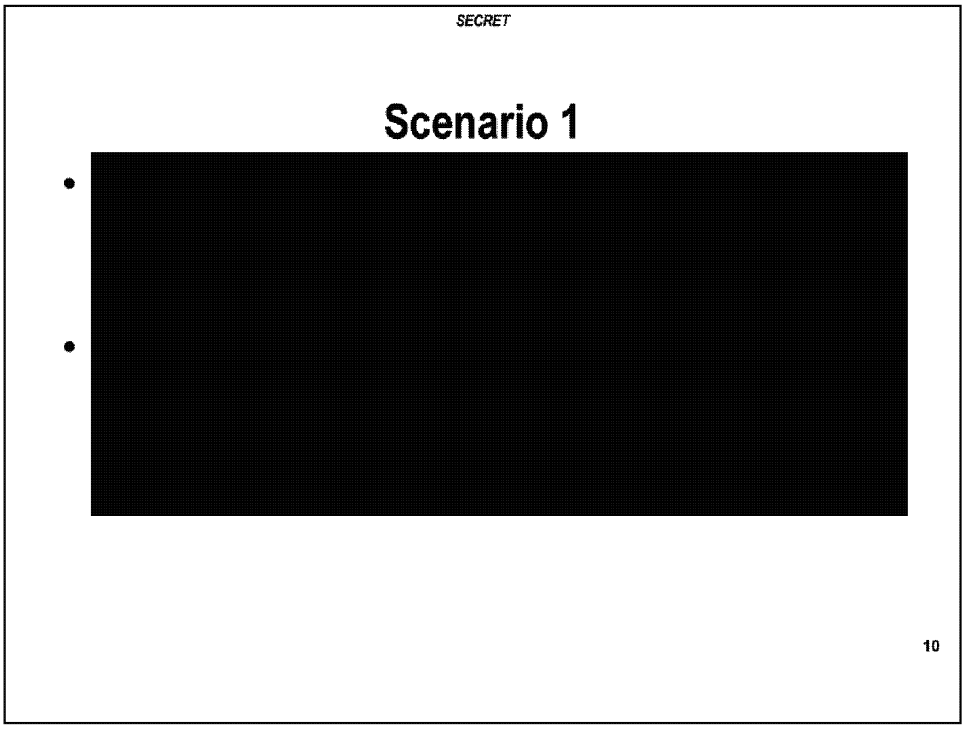
Different sharing mechanisms are: CKBs, [redacted] etc.

Exercise - YOU ARE IPOC

- You are members of IPOC
- You have been asked to provide any policy considerations that need to be taken into account for scenario
- Suggest ways forward

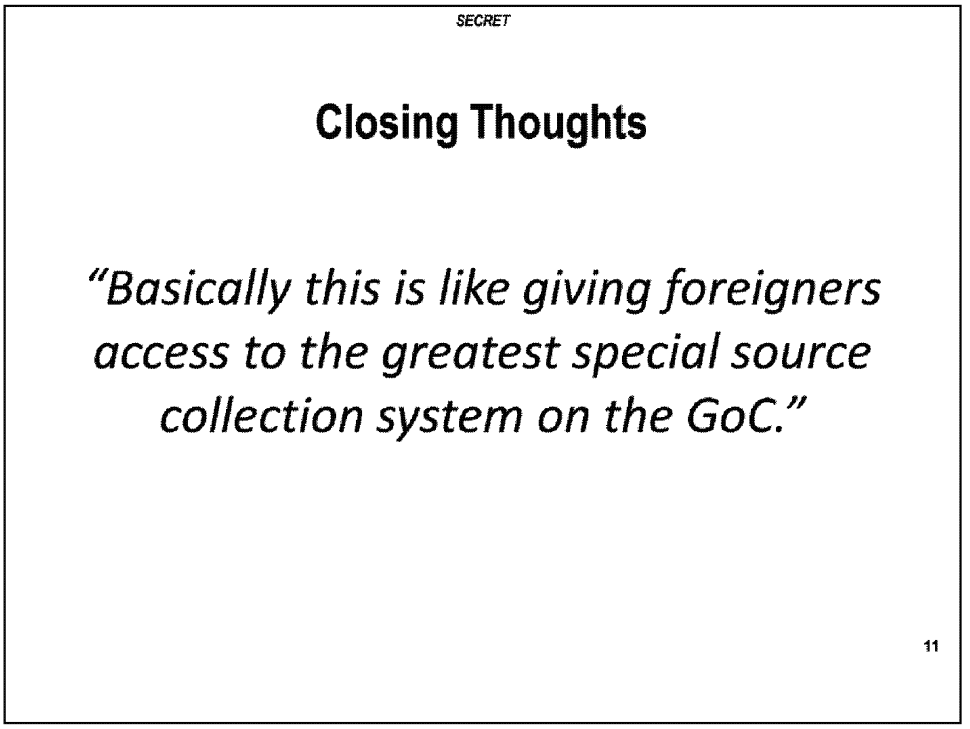
9

Have class split into groups.



10 mins group discussion

10 mins class discussion



So why does any of this matter?

A very wise man once said: *"Basically this is like giving foreigners access to the greatest special source collection system on the GoC. Before I'll grant that I'd like to understand the research objectives, the controls around the data, what interaction they would have with the data, what systems will they be working on, will the data ever be sent to systems in the US, etc."*

Or another quote "*With great power comes great responsibility."*

The point is, we must be careful what we give and to whom. Because once it's out of our hands, all we have left are our policies and procedures to show that we've done everything legally and in compliance with our regulations.