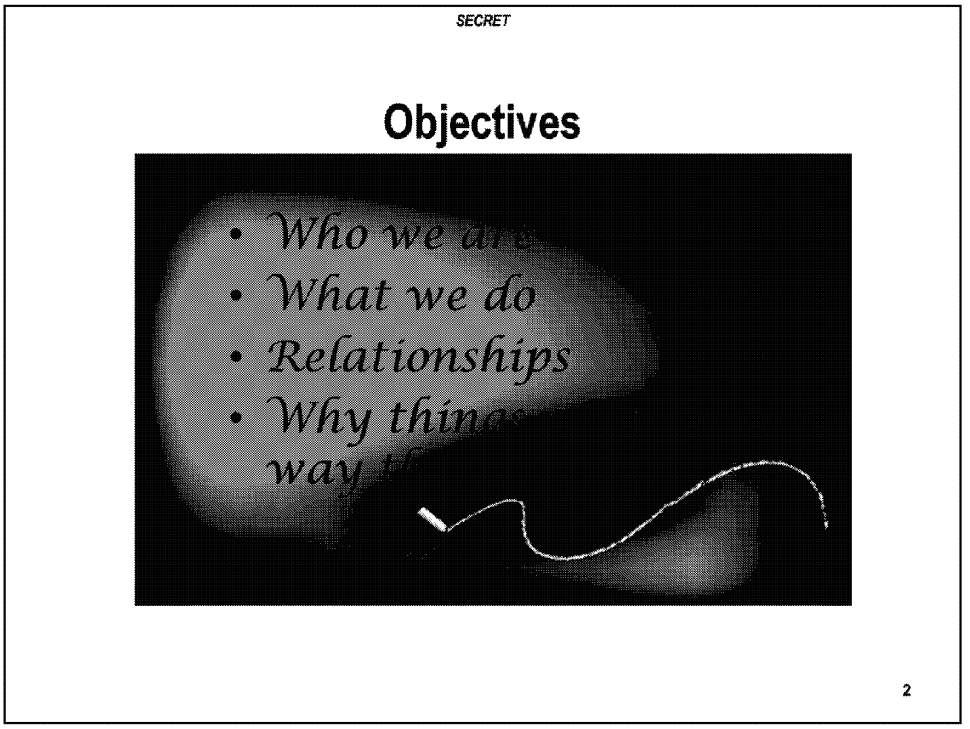
Cyber Defence Policy Awareness Curriculum

IPOC

1

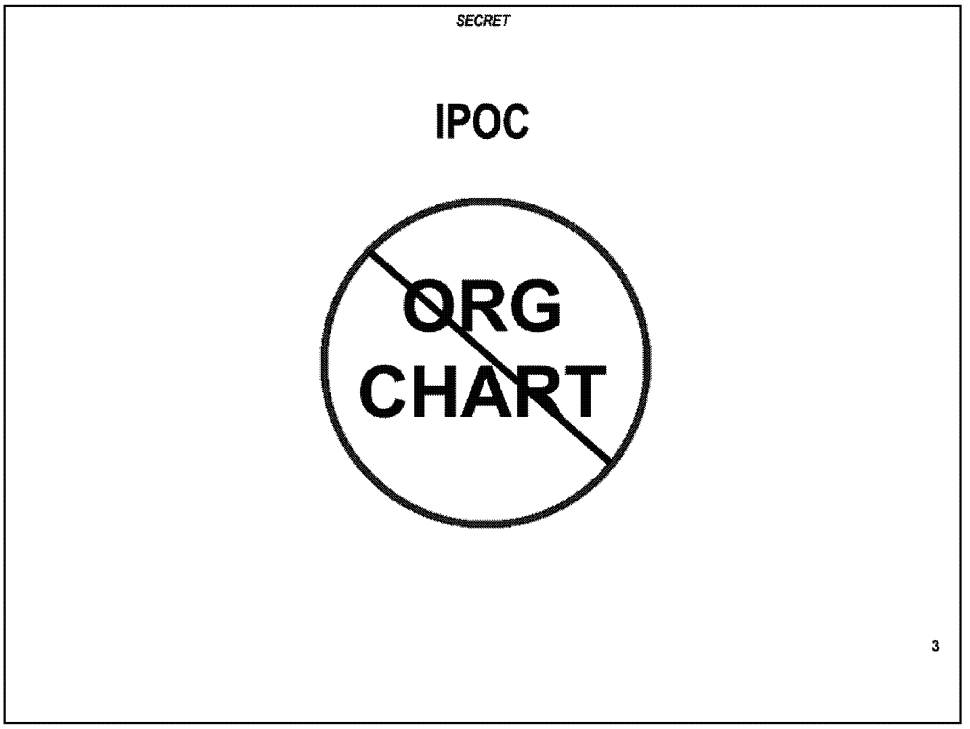


Introduction and Background to the Cyber Defence Policy Awareness Curriculum Workshop

FACILITATOR NOTES:

-Welcome participants to the class then…

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

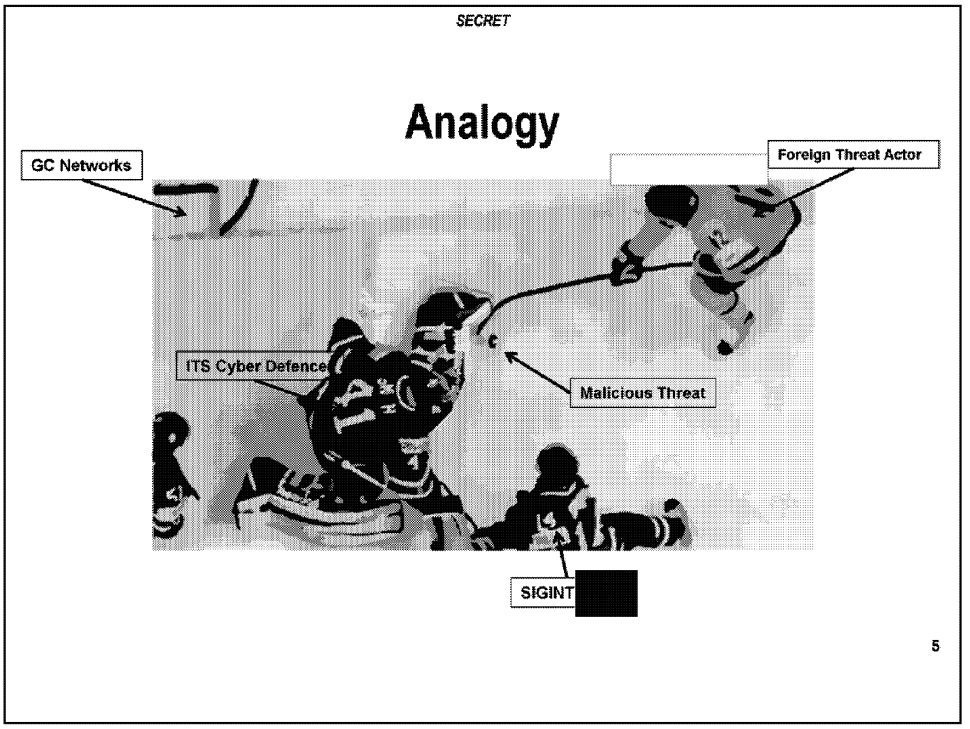


What I'm going to do is explain to you who IPOC is, what we do, and how we support you, without using any org charts. Why? Because it doesn't matter for you. All you need to know is, contact IPOC, doesn't matter who. We'll figure out internally who's best suited to handle the issue.

In the grand scheme of things, we sit in PMO and our director reports directly to DCITS.

IPOC Mission

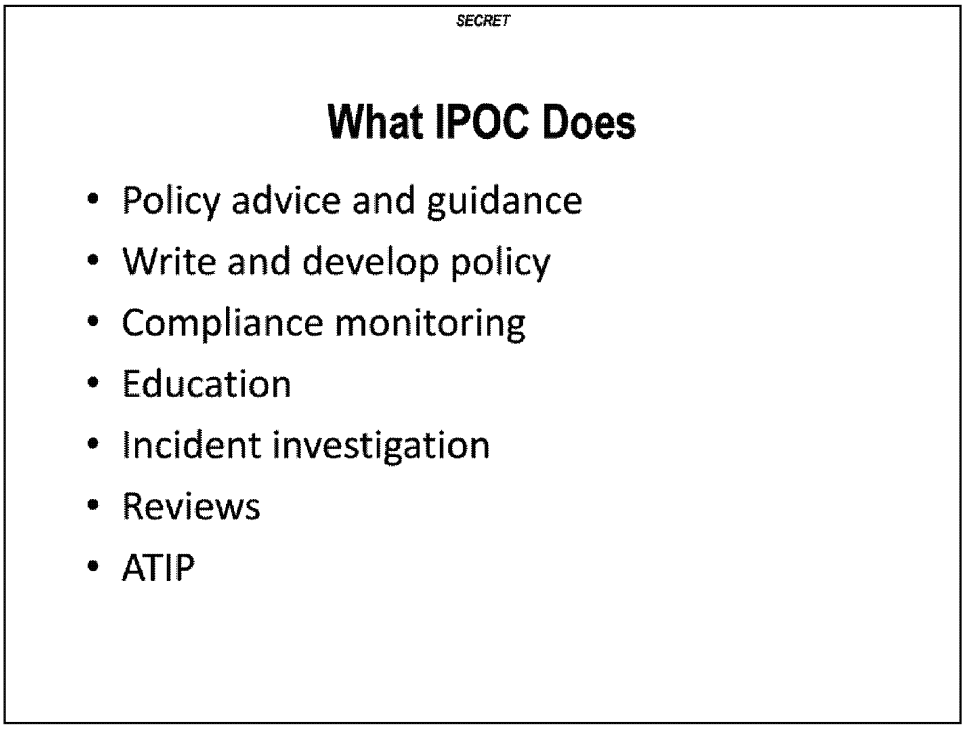
The purpose of ITS Policy Oversight and Compliance (IPOC) is to enable the development and delivery of IT Security cyber defence operations to external federal institutions by coordinating associated governance, compliance, policy and legal requirements.



Some of you may have seen or heard this analogy before

ITS Cyber Defence is like being the goalie in a hockey match. Our role is to keep the puck out of our net as it comes to us. We don't focus on the opposing player, SIGINT handles that, our only concern is keeping our net free from pucks.

IPOC, we are the equipment team. We get your pads and stick ready. Ensure your helmet is secure. Basically, we enable you to do your job of stopping that puck in accordance with league regulations.



We interpret the policy to give you advice for any questions or concerns you may have while conducting operations. To go along with that, we also apply the spirit of the legislation and policy to provide guidance when gaps are identified.

We write policy. Even though DGPC controls the OPS policies, we play a huge role in assisting them to write sections of the policy that apply to the cyber defence team. We also write our own ITSOIs.

We provide oversight on the cyber defence activities. We have plan and each quarter we check on some activities/tools to ensure that everything is compliant and provide reports to higher.

Education is somewhat a new function in IPOC. We've always organized and coordinated info sessions, but now we are getting involved with the OCS faculties.

The "dirty" part of the job is the incident investigations. Often incident investigation, be they for privacy or compliance reasons, draws fear into the heart of even the bravest of people, but don't fret. We are actually the "good guys" here. The aim of the investigations is not only to find out what happened, but to document it all and to provide recommendations on ways to ensure that it does not happen again. We

have the responsibility to report privacy incidents to the Minister, so it's always better to self report incident, including measures taken to prevent it from happening again.

Reviews, this is the best part of the job! We basically coordinate an initial info brief, pull hundred of documents to satisfy requests for information (RFIs) and coordinate interviews. Tons of fun! Seriously though, this is once of the most important part of the job. We try to gather as much documentation as possible so operators don't have to, but be aware that you may be required to either find or review documents for RFIs. OCSEC is the main review body we deal with.

Finally, we coordinate the ATIP request to come to ITS. By coordinate, we are more than just a mailbox. We push back on request, seek clarifications and try to make your lives easier when it come time to actually do the search or recommend redactions. Remember, ATIP is everyone's responsibility.

SECRET

Relationships

- SPOC
- B Group
- D Group
- OCS
- Second Parties

I'm not going to talk about our relationship with the Cyber Defence Team because that should be pretty obvious, the CDT is pretty much the reason for IPOC's existence. But, there are groups, like ATA, that we deal with because they require report access. I'm not going to list groups that have report access, because it really is a business decision who gets access, with certain policy restrictions that we will get into more detail during this course.

The way CSE is organized right now, we have cyber activities being conducted under both the SIGINT and the ITS business lines. That naturally leads to questions about sharing and joint activities for operations. IPOC and SPOC meet on a regular basis to discuss cyber issues, as well as ad hoc to discuss important issues as they arise. As CSE cyber grow and develops, so will the relationship between IPOC and SPOC.

B Group is strategic policy. For IPOC, anytime anything has to be sent to the Minister of National Defence, we deal with B Group. So reports, MOUs, Mas, MDs, etc.

D Group:

- D1 for disclosures. Anytime CSE information could be used as evidence in legal

proceedings and inquiries. Or requests under the Access to Information Act or the Privacy Act.

- D2 for anything to do with the Operational policies. This includes action on for suppressed identities.
- D3 for all external reviews. Generally speaking, the bulk of our relationship with D3 is for OCSEC reviews and studies.

OCS is a relatively new relationship. Our manager is the co-chair (along with SPOC) of the [redacted] and we hold meeting to discuss learning initiatives.

Finally, Second Parties. We deal with them on many policies issues related to sharing of data and idents.

That list does restrict use from dealing with other teams/groups, it's just the main groups we deal with.

SECRET

Why things are the way they are

- The great shutdown of 2006
- [redacted] report, 8 June 2007
- IPOC stood up August 2007

It wasn't always like this, IPOC is a relatively young group as it was only stood up in August of 2007. So what happened?

The great shutdown of 2006… Basically, with the passage of the Anti-Terrorism Act, , ITS was granted the authorization by the MND to conduct activities that may risk intercepting PC through MAs. Unfortunately, through a series of unfortunate circumstances that we won't delve into on this course, ITS did not receive the required support it needed for its MA governed operations.

Which led to: October 2006, when ITS shut down it's cyber defence activities due to non-compliance with the MAs in effect during the period of June 2005 to October 2006.

DGAEE conducted two investigations (initial and detailed) and produced the [redacted] report in 8 June 2007.

The report contained a number of recommendations that needed to be done in order for cyber defence activities to resume. Some of those recommendations included:

- Develop and revise ITS-related operational policy at the pace of

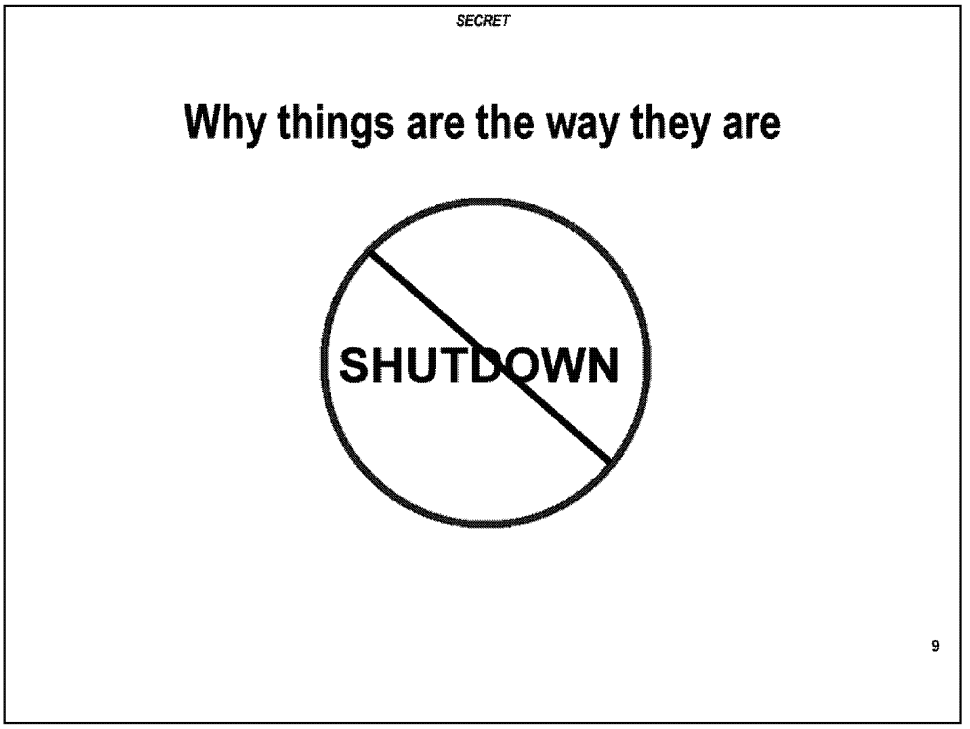
evolution of ITS' technological expertise

- Revised versions of operational policies be approved and promulgated
- Ensure ITS staff involved in MA activities receive periodic training on pertinent operational procedures and CSEC/s policy framework
- Document and implement a management monitoring regime for CND MA activities
- A Personal Information Bank be established

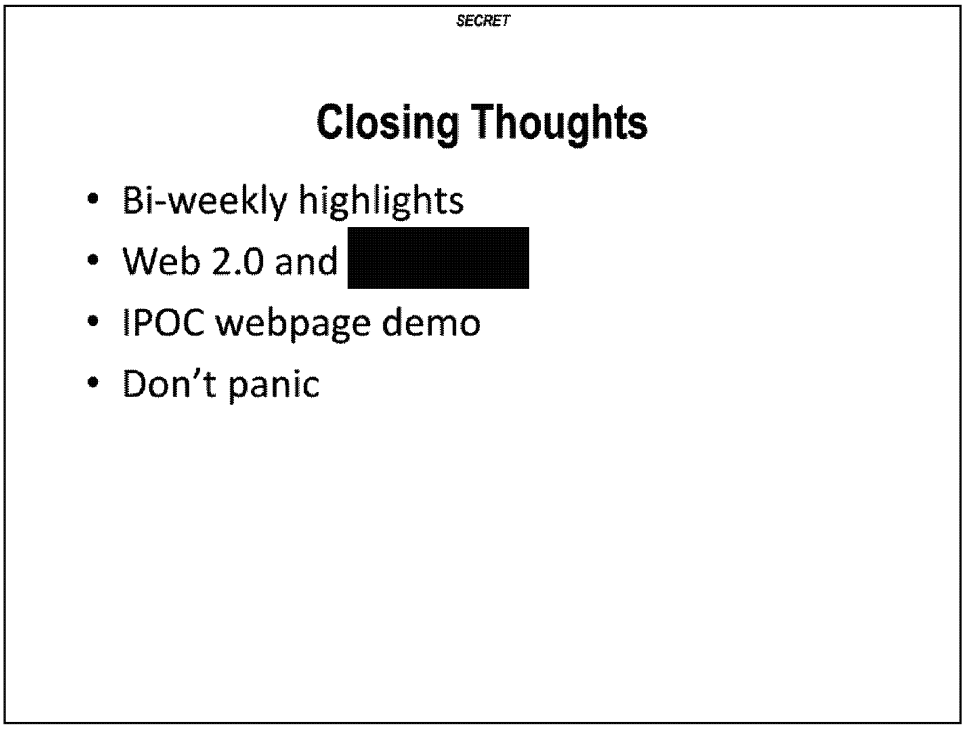
So, based on all of that, a steering group (LIBRA) was established to ensure all recommendations were implemented.

IPOC (formerly known as CDSO) was stood up in August 2007 and worked with DLS and DGPC to establish a comprehensive policy suite and compliance regime to enable the resumption of Security Posture Assessment (SPA) and CND operations.

- Onsite Technical Vulnerability Assessment (OTVA) (non-MA portion of SPA) resumed in November 2007 with Mandrake as the client
- Active Network Security Testing (ANST) resumed in January 2008 with DND as the client
- CND resumed in March 2008 with CSEC/CIO as the client



So why are things the way they are? Because we don't want them to go back to the way they were when we shut down in 2006…



So some closing thoughts.

If you are curious what we do, IPOC publishes bi-weekly highlights of what activities we have engaged in and send them out via email to level 4 and 5s. So feel free to ask your supervisor if you want to see them.

Final thing I want to mention for this lesson is "don't panic". Things happen, we know. If you discover potential incidents, just follow the procedures set out in the policies. Inform your supervisor and let us know. We have a web form to report incident. Don't just delete all traces of the incident as it could effect the investigation. We'll work with you to resolve the issue and recommend a way forward to ensure the incident does not happen again.