What's the worst that could happen?

This document contains examples of specific risk which may affect operations and which may need to be considered when writing submissions. This is not an exhaustive list: any operation could involve new risks. It is also not a pick and mix list. It is here to help you think about the sorts of risk that might need to be included in a submission to ensure that the Secretary of State has all the relevant information available when deciding whether or not to approve the submission.

Are you the most appropriate person to assess the risk of your operation? Are you capable of looking at all the areas of risk (eg, reputational, technical, legal)? If not, ask someone who is (eg, an IPT expert, PTD, OPP-LEG respectively).

Risks to Personnel

- discovery/compromise of personnel involved in installation
- risks to personnel associated with housing operation if operation is compromised
- risk to collaborators / enabling agents
- adequacy of plausible cover leading to compromise of individuals
- Risk of false attribution and dire consequences (if there were a risk of reprisals against SIS agents or Embassy staff, then an assessment from the relevant SIS Controller or Ambassador might be appropriate)

Technical Risk

Appropriate technical colleagues are best placed to provide this information, eg PTD, NDIST, GTE, JTRIG.

- Compromise of technique leading to loss of capability
- Definite technical attribution leading to loss of capability
- Compromise of equity leads to loss of capability and discovery of other operations (eg by FIS)
- Novel capabilities have unknown effects outside of lab testing conditions

Political or Reputational Risk

If you think that any of the following risks are <u>significant</u> in your operation, you should consider whether or not you have adequate operational planning and mitigation in place.

- attribution to HMG
- attribution to UK
- attribution to GCHQ
- presumed attribution to UK (the target knows it's been the subject of an attack and assumes the UK is responsible)
- mistaken attribution (the target mistakenly blames a UK ally, who in turn attributes an effect to the UK)

- Political fallout with foreign governments or intelligence partners
- Media exposure
- Compromise of commercial partners

Humint

- *Talk to Humint partners if you think you have a significant Humint risk.*
- Risk of false attribution and dire consequences (if there were a risk of reprisals against SIS agents or Embassy staff, then an assessment from the relevant SIS Controller or Ambassador might be appropriate)
- Vulnerability of collaborators and enabling agents

Risks to Relationships

- Discovery or attribution could adversely impact on working relationships and/or sharing arrangements with sister agencies and/or second parties
- Discovery or attribution could adversely impact on working relationships with commercial suppliers and ultimately restrict GCHQ's sigint cability
- Potential to compromise a partner's operation
- See also Political or Reputational Risk section

Operational Phase

- See also Discovery
- Compromise of operation during installation, the course of the operation itself or egress of traffic
- Inadequate personnel security controls
- Operation does not succeed because the installed hardware/software does not function as planned
- Operation does not success because the installed hardware/software works, but is neutralized (eg because the target network/system is upgraded or replaced)
- Operation does not succeed because the target system is not used in the expected way (eg expected commercial usage does not occur)
- Operation does not succeed because of reliance on an uncertain supply chain or other risky dependence.
- Proportionality – the operation is not specific in its targeting
- Who will have direct access to the data resulting from the operation and do we have any control over this? Could anyone take action on it without our agreement, eg could we be enabling the US to conduct a detention op which we would not consider permissible?

Discovery

Discovery is a risk itself, which can lead to almost all of the other risks featured here. What follows is a list of circumstances which can lead to discovery.

- Compromise of operation during installation

- Inadequate personnel security controls and subsequent information leak
- Discover of installed hardware (including post-operation)
- Forensic discovery of installed software
- Discovery of a suspicious audit trail/logs/registry
- Discovery of suspicious RF energy
- Suspicious profile caused by hardware/software malfunction
- Discovery of egressed traffic
- Discovery through other IT leakage
- Vulnerability to HIS or other monitoring
- Inadequate monitoring of profile generated by operation
- Inadequate review of risks during the lifetime of the operation
- Reliance on an uncertain supply chain or other risky dependencies
- Failure by operators to cover tracks, including clearing logs/changing read status of emails
- Novel capabilities and techniques having unknown effects outside of lab testing conditions
- Unforeseen changes to hardware or software leading to compromise of techniques or installation
- Hardware/software malfunctions leading change in target behaviour, potentially including forensic investigation (and potential discovery) and/or loss of target access

Legality

Any risks relating to legality of operation or of subsequent actions enabled by the operation will usually be addressed by lawyers in legal section of submission, but may include the following issues:

- liability of enabling commercial partners
- the principle of non-intervention in a sovereign country's affairs
- Could the Law of Armed Conflict apply?
- Who will have direct access to the data resulting from the operation and do we have any control over this? Could anyone take action on it without our agreement, eg could we be enabling the US to conduct a detention op which we would not consider permissible?