Compliance Improvement Review

To note: for national security reasons, some sections have been replaced with a gist and some names of specific teams and programmes have been removed. Sections which have been replaced by a gist are in bold and underlined - these are in recommendations 8 and 12.

Summary of key findings

1. It is clear that **MI5 is a consistently high performing organisation**, with a growing number of committed and professional staff working under sustained pressure to keep this country safe. The priority staff give to MI5's operational mission is accompanied by a deep-seated commitment to respect and work within the law.

2. However in recent years MI5 has **failed to respond sufficiently rapidly and comprehensively** to the legal compliance issues created by its expanding reliance on data, particularly within the specific IT environment.

3. **Potential compliance risks have been identified** since the specific IT environment was **originally accredited in 2010**. A 2011 review made a number of recommendations including mandatory training for users, and implementation of a retention and deletion policy.

4. The rapid **growth of available data** and improved IT systems led to a massive and sustained increase in the number of users in the specific IT environment. Efforts to improve compliance did not keep up with the growth in size and complexity of data use.

5. In May 2013 the MI5 Management Board discussed a paper setting out **serious information management risks** within the organisation, which clearly had implications for legal compliance. Some progress was made to scope and resolve these issues. But the work was under-resourced given the scale of the problem, and lacked urgency.

6. Over this period, **MI5 as an organisation was under considerable pressure** dealing with a growing range of national security challenges. These included an evolving cyber threat, the rise of ISIL terrorism, attacks in the UK, Hostile State Activity, and a persistent threat from Northern Ireland related terrorism.

7. There was a **focus on implementing the 2016 Investigatory Powers Act effectively**, through a change programme. Improvements were made, including the formation of a new team responsible for the compliance function, and some additional resources were provided. But this programme did not consider the compliance of all existing IT systems, since **the IPA**

did not substantively change the existing legal provisions with regard to warranted data handling.

8. MI5's focus **remained on its operational activity** to keep the country safe. The resource-intensive work needed to review proactively all IT systems to check they were fully compliant with requirements for data copying, storage and eventual destruction never became a mission-critical priority for the senior leadership, nor therefore for MI5 staff; and consequently was not properly resourced.

9. It was not until **late in 2018 that the Board began to focus more urgently** on solving the outstanding compliance issues which had been highlighted in general terms over previous years.

10. **Legal input over this period on warrantry tended to focus on specific requests** for advice. Some advisers did express concerns about the robustness of the wider process. MI5's focus was on satisfying the RIPA Intelligence Services and Interception Commissioners and then from September 2017 with maintaining the confidence of IPCO in MI5 procedures.

11. **MI5's lack of urgency in reducing the legal risks** being run was partly due to the expansion of IT systems needed for operational reasons. This was compounded by a **lack of urgency in communicating continuing concerns** about compliance to the Home Office Secretary of State.

12. There was **no attempt by MI5 to hide information**. MI5 followed the working practices set out in the Protocol governing relations with the Home Office. However the information shared was insufficient to highlight the increasingly urgent problems caused by continuing compliance difficulties.

13. **The Secretary of State's legal responsibility for the approval of warrants**, consistent with the terms of the relevant legislation including section 53 of the IP Act, should have been fully taken into account. MI5 was too slow to appreciate the significance of this compliance risk for Ministerial decision making in its communication with the Home Office.

14. The problem was compounded by a **lack of structured contact** between MI5 and HO lawyers. There was not a culture of working together towards a single government legal view on issues such as compliance which were not directly operational. MI5 legal advisers provided advice to their own organisation; professional contact with Home Office lawyer colleagues tended to be informal rather than structured.

15. **Resource constraints** and other operational priorities meant that the small **Home Office team** directly engaged with MI5 in preparing quarterly review meetings and subsequent meetings with Ministers **did not have the bandwidth or the legal background** needed to engage proactively with all the information provided.

16. Organisationally **the MI5 risk register proved insufficient** to produce the level of response needed to resolve legal compliance issues. These were flagged up as red from October 2016, and compliance failure risk had been reported to the Management Board as early as 2010. Management focus was primarily on operational issues, and the Home Office did not challenge this sufficiently in the quarterly review process.

Conclusions

Overall, there was a **lack of urgency** and insufficient resourcing of MI5's work to assure warrantry compliance within its data management systems; and **limited communication** with the Home Office about the extent of the compliance problem. These are serious shortcomings. But they did not reflect either individual negligence or a deliberate intention to mislead; rather a sustained organisational failure to appreciate the extent of the compliance problem and its consequences.

Poor management of legal compliance within the specific IT environment posed **risks for the continued effective operation** of the organisation, including the signing of warrants. This must now be resolved in a way which ensures that no such problem can occur again within MI5 as it modernises its IT systems.

In parallel there must be **a commitment to achieve greater openness** between MI5 and the Home Office so that Ministers can be confident that they will be made aware of legal and other risks at an early stage.

My recommendations therefore focus on achieving lasting improvements in the areas of compliance, openness and legal assurance. Their effectiveness depends on MI5's leadership delivering the lasting change in organisational culture which will ensure that, when such issues arise in the future, they are handled as a management priority and properly resourced.

Individual improvements, while needed, will not be sufficient without a sustained focus on compliance.

I therefore recommend that the implementation process should be treated as a mission critical change project to be led by the Deputy Director General personally, and delivered in full no later than end June 2020.

Recommendations

A. Improved Compliance

In order to support an effective compliance culture across all parts of MI5, I recommend that:

Recommendation 1:

There should be an urgent programme to provide staff including contractors with tailored **best practice training on MI5's statutory obligations in respect of handling warranted data**. This should draw on experience elsewhere in the UK Intelligence Community (UKIC), with input from the Investigatory Powers Commissioner's Office's (IPCO) inspectorate on the level of detail required. The training should include specific modules appropriate to technical staff, approved by MI5 legal advisers. An effective, rigorous process for confirming learning, including through online tests and regular retesting, should be implemented. Satisfactory completion of training should be linked to the annual appraisal process.

Recommendation 2:

Effective implementation of this **enhanced training should be regularly reviewed** by the Audit, Risk and Assurance Committee and by the Management Board, given its responsibility for governance of MI5 activities. Completion of the training should be a precondition for analysts and technical staff to work on any IT systems which hold warranted data.

Recommendation 3:

Successor IT environments **must retain robust control of compliance** at all stages, signed off by the programme owner, MI5's head of compliance and the relevant legal advisor. These processes should ensure that:

a) The legal requirements for the management of the data processed by MI5 IT systems are understood by all programme staff involved in the IT build.

b) Appropriate governance systems (e.g. Gateway Reviews) are put in place to ensure that those requirements are met/ built at each stage of the development, including audit, Retention Review and Disposal procedures (RRD), confidential material management or other requirements.

c) Sufficient resource is allocated to business change and user training to ensure that all users understand their compliance obligations under the law.

d) Continuing proactive checks are made regularly to ensure that the system is used compliantly.

Recommendation 4:

Resources for **MI5's compliance function need to be increased substantially**, particularly in their Policy, Compliance, Security and Information team. There should also be an expansion of the compliance hubs within different departments, appropriately skilled lawyers to support the compliance function, and more proactive monitoring of compliance behaviours across the organisation.

Recommendation 5:

The Deputy Director General should be given responsibility for ensuring MI5 implements all these structural changes no later than the end of June 2020, including identification and sourcing of the required financial and human resources.

The satisfactory **delivery of this change programme should be independently verified** by the end of June 2020.

B. A stronger, more open MI5-HO Relationship

Maintaining Ministerial trust in MI5 requires more effective sharing of information to identify emerging issues. I recommend that:

Recommendation 6:

The HO-MI5 Quarterly Review meetings, should, with the agreement of the Home Secretary, normally be **chaired by the Security Minister** to strengthen the link between MI5 and Ministers. The DG OSCT will continue to attend, and be responsible for preparing the meetings with MI5. When the Minister is unavailable, the DG OSCT should chair the meetings. Outcomes should be reported to the Home Secretary by the Minister, copied to the MI5 Director General.

Recommendation 7:

The papers provided to support the quarterly review meeting should also include the **minutes of the MI5 Executive and Management Board meetings** occurring during the relevant quarter.

Recommendation 8:

In order to increase knowledge and information flows, there should be **greater engagement, closer working and co-location between** MI5 and Home Office staff.

Recommendation 9:

OSCT in the Home Office should **take a more proactive approach** to their oversight role in respect of MI5, through:

1. **An increase in staff resources** to ensure the team has sufficient capacity to develop additional expertise and engage more proactively with MI5 on legal, political, and other risks that the Home Secretary may be exposed to as a result of accountability to Parliament for MI5 activity. Advice to the Home Secretary on MI5 non-operational risks should normally be given in conjunction with MI5.

2. **Reviewing and updating the protocols** governing MI5's relationship with the Home Office to reflect the recommendations in this report, while maintaining MI5's operational independence.

The required increase in resources for this purpose should be provided before the end of 2019.

C. Increased legal input and closer joint working

There can only be **one Government view on legal compliance** with statutory obligations. The Home Secretary has statutory responsibilities with regard to MI5 activities and warrants. The MI5 legal team and Home Office legal advisors should collaborate closely in confirming all legal requirements are being met, keeping Ministers informed of any emerging issues. I recommend that:

Recommendation 10:

MI5's **Legal Director should become a full member of the MI5 Management Board** to provide an authoritative legal voice on all governance issues in Board discussions. The Legal Director should help to ensure that due diligence on all potential legal risks is being carried out; that legal issues are properly resourced; and **that actions to remove any identified legal non-compliance are carried out urgently**.

Recommendation 11:

The **MI5 Legal Director** should provide a **quarterly report agreed with the Home Office Chief Legal Advisor** to the Home Office Permanent Secretary and the Director General MI5 on issues relating to MI5's compliance with its statutory obligations and key legal risks, including litigation and disclosure risks. This report should also be considered at the quarterly review meetings.

Recommendation 12:

MI5 legal advisors should be expected to **work more closely and co-locate with other government departments' legal departments** and there should be regular joint training with Home Office legal advisors.

Recommendation 13:

The Cabinet Office should undertake a wider review of relations between the three Intelligence Agencies' legal advisors and central government, looking at how best to build a shared culture of legal support, shared training and promotion opportunities, and to facilitate and expand the joint working already underway.

Recommendation 14:

Longer term, MI5 should work with the Home Office to identify **potential amendments to the terms of the IP Act** that may be required as new digital systems develop, **to maintain the appropriate balance between operational needs and effective oversight**. These should be considered by Ministers before the IP Act is next reviewed.

Achieving Rapid Change: the Challenge Ahead

A sustained improvement in compliance requires **a step change in MI5 awareness of the issues** and early engagement with future risks from technical developments to data handling.

This will only be securely achieved through a **continued MI5 Board level commitment** to ensure that **full legal compliance** with the protection of warrantry data is understood by all across the organisation to be **a mission critical responsibility,** requiring continued vigilance by staff.

MI5 must ensure that all its data can be shown to be held in accordance with legal compliance requirements by June 2020. It is their responsibility to do so through a properly resourced initiative, led at Board level, working closely with Home Office officials and Ministers. A similar effort is needed, working with the Home Office, IPCO and the wider UKIC, to ensure that future data management systems can be shown to be fully compliant with the law.

The degree of change required is ambitious in a short timescale. **It is also necessary** if MI5 is to continue to carry out its vital operational functions legally and sustainably. Achieving it must be a Board priority, as a key part of MI5's wider commitment to keep our country safe.

June 2019