Home Office

Home Office

The response to the Parliamentary and Health Service Ombudsman investigation into a complaint by Mrs A and her family about the Home Office

January 2015

Table of Contents

Table of Contents 2
Foreword by the Permanent Secretary 4
Executive summary 5
Summary of recommendations 6
Background to the PHSO Report 9
Current Home Office structure 10
The PHSO Report 10
Section 1: PHSO Recommendation 1 13
Overview of Section 1 13
The visa issuing process – self declaration and criminal history 13
Procedures when a criminal record is declared 13
Current procedures for checking statements made in visa applications 14
Current mandatory checks 14
Further checks 15
Audit and assurance of the visa checking process 15
The Risk and Liaison Overseas Network (RALON) 15
Checks on visas at entry 15
Bilateral and multi-lateral arrangements 16
Options for checking criminality of visa applicants 16
Which countries use Police Certificates? 17
Police Certificates issues in the UK 17
Foreign nationals in registered activity 18
The viability of Police Certificates in the UK 20
Taking account of Mrs A experience and the PHSO finding of maladministration 20
Section 2 – PHSO Recommendation 2 21
Overview of Section 2 21
How the allegations system worked in 2010 for Mrs A's case 21
How allegations works in the Home Office now 22
Allegations received electronically 22
Allegations received on the e-form and sent to the IMS system 22

Other allegations received electronically 23
Prominence of the e-form on the Home Office website 23
Using the email instead of the e-form 24
Routing of allegations received via the IMS system 24
Variation in working hours 24
Mrs A allegation of November 10 2010 received now 25
Testing the public use of the eform 26
Visibility of warnings 27
How allegations are dealt with once they are received 27
National Allegations Team 27
The Border Force National Intelligence Hub 27
Border Force Intelligence Heathrow 28
Immigration Enforcement (IE) - Regional intelligence 30
Dealing with allegations that are received via the public enquiry mailbox or complaints email addresses 31
The Command and Control Unit 32
Access to the Warnings Index 33
Watchlist & Information Control Unit 34
Allegations received by telephone 34
Checks on foreign national arrested in the UK 35
ACPO Criminal Records Office (ACRO) 35
Operation Nexus 36
Schengen 37
Summary 37
Section 3 – PHSO Recommendation 3 38
Overview of Section 3 38
Types of correspondence received by the Home Office 38
How correspondence is organised in the Home Office 39
Direct Correspondence Unit 39
UKVI - Central Point of Receipt (CPR) 40
Complaints handling by CPR 41
Handling of correspondence by CPR 42
Receipt of correspondence 42
Mrs A's dealing with the Home Office between May 2011 and November 2012 44
Glossary 45

Foreword by the Permanent Secretary

The Parliamentary and Health Service Ombudsman (PHSO) report to which this review relates found serious failings in the then UK Border Agency's handling of this case which amounted to maladministration. Institutional failings of this kind are clearly unacceptable and in the light of the PHSO report we have made significant changes to our processes and systems to reduce the likelihood of this kind of incident occurring again.

I am pleased that this review has found that significant gains have been made in handling intelligence and that specific improvements in our processes and procedures have been made, many in direct response to this case. However, as this review highlights there is still more to do and my Executive Board and I will consider the recommendations in full in the coming weeks and oversee an implementation programme.

In the years since these events took place we have made significant changes to the organisational structure of the border and immigration system. These changes allowed clearer focus on key areas of the system and have undoubtedly allowed us to make some of the improvements highlighted by this review. They also put us in a good position to make the further changes necessary.

Despite the improvements, the fact remains that this case highlighted significant failings on the part of the UK Border Agency and the Home Office, and I am sorry for the serious implications this had for Mrs A and her family. Our job is to keep our citizens safe and on this occasion we failed Mrs A and her family. I am determined that we learn the lessons from their case and I hope that the action that has been taken by the Home Office so far, and the further improvements that we intend to make, assure Mrs A, her family and the public that we are committed to addressing the maladministration highlighted in the Ombudsman's report.

Mark Sedwill
Permanent Secretary

Executive summary

This review came about as a result of the Parliamentary and Health Service Ombudsman (PHSO) finding in July 2014 of maladministration by the Home Office between November 2010 and December 2012. The PHSO report was instigated by a complaint by a member of the public Mrs A who, along with her family, had suffered serious harm resulting from the crimes of a Canadian national who had obtained a visa to enter the UK.

The finding of maladministration was based on failings in systems and processes for visa issuing, handling of allegations, sharing of intelligence and dealing with correspondence by the former UK Border Agency and the Home Office.

The PHSO recommended that compensation be paid to Mrs A's family and that the Permanent Secretary of the Home Office make an apology to Mrs A. The PHSO further recommended a review of the processes and systems that are currently in place in the context of the findings of maladministration and the experience of Mrs A's family.

In the light of the PHSO recommendation, this review looked at how the Home Office currently checks the criminal history of those that apply for visas and the processes that are in place for sharing information. It examines the means by which allegations from the public are handled by the Home Office and the current arrangements for accessing the Home Office watchlists. It reviews the current processes for receiving and dealing with correspondence and it makes recommendations for change.

This review found many cases of improvement to the processes that led to the PHSO finding of maladministration. The Home Office UK Visas and Immigration command's operating mandate, though not requiring individual checks on criminal history in the home country, has formalised the visa checking process and there is an audit and assurance process aimed at ensuring checks are done correctly. Additionally the Government is examining the feasibility of Police Certificates for some migration routes to test if this would provide additional border security. Further progress has been made in handling allegations which now have a central database that enables digital submissions by the public, with automatic routing so that performance standards can be tracked and allegations dealt with more quickly.

Issues do remain. Multiple routes by which the public can contact the Home Office are confusing and allegations that should be dealt with promptly can be missed when they are submitted through indirect routes. A disparity in working hours between units that deal with allegations and correspondence also means that information and allegations that should be regarded as urgent can take too long to action. Large amounts of correspondence are neither logged nor tracked and there are significant disparities between the ways that different units in the Home Office categorise and deal with correspondence.

The systems that deal with allegations and correspondence are structured in accordance with the previous configuration of the UK Border Agency and Home Office. As such, there is no overarching system that shows when allegations and correspondence are actioned. The result is that even when staff in individual units adhere to systems, there is still the capacity for information to 'fall through the cracks.' This is what happened in Mrs A's case.

The review makes a series of recommendations to address the issues that it found. The PHSO recommended that following publication of this review, the Home Office should monitor progress against its recommendations and publish a progress report within 12 months.

Summary of recommendations

Recommendation 1

That the Home Office introduce a means of sampling or the retrospective audit of information given by visa applicants on criminal history. The information should be assessed to see if further checks on self declared criminality are necessary.

Recommendation 2

That the Home Office work with the Department for Education and Department of Health to gather additional information on the system of Police Certificates to establish the benefits and disadvantages of using the system for migration purposes.

Recommendation 3

That the Home Office web page on gov.uk contains a link to 'reporting an immigration crime' and that the email links make it clear that the online reporting form should be used to report a crime or make an allegation. In the longer term the Home Office should consider one single contact point on the gov.uk website.

Recommendation 4

That the routing for immigration allegations be modified to ensure that cases that are high risk or time critical are routed to a 24/7 unit.

Recommendation 5

Immigration Enforcement management should ensure that as part of the monthly evaluation of the intelligence management system, they maintain information on the proportion of allegations that need to be rerouted manually. Cases of high harm among those incorrectly routed should be specifically highlighted.

Recommendation 6

The Home Office 'report an immigration crime' web page, should allow the warning to the public at the bottom of the form to be clearly visible when the web page opens.

Recommendation 7

That consideration be given to allowing the Border Force National Intelligence Hub to put entries directly onto the watchlist system.

Recommendation 8

That clear instructions are given to all staff who have requested a watchlist entry, as to what their responsibilities are in terms of following up on that information to ensure that relevant actions are taken.

Recommendation 9

That all intelligence staff in the Home Office be made aware of the practice and procedure for obtaining overseas criminal records checks and that instructions be issued for when this should be requested and how the information should be handled.

Recommendation 10

The Home Office should carry out an assessment of how intelligence systems are joined up to satisfy itself that information held cannot be overlooked.

Recommendation 11

That staff in both Border Force and Immigration Enforcement intelligence units be issued with clear instructions on how to deal with an allegation of a visa obtained by deception.

Recommendation 12

The Home Office should ensure that Border Force consider tracking action taken on all allegations in a similar way to Immigration Enforcement if there are sound business reasons for doing so.

Recommendation 13

That all units listed on the website that receive electronic communications from the public have a 24/7 service that is able to screen correspondence for time critical or high harm allegations to enable these to be actioned promptly.

Recommendation 14

That Border Force and Immigration Enforcement have some means of checking that allegations received via the public enquiries mailbox or complaints emails get to the appropriate unit in an acceptable time.

Recommendation 15

That a further investigation be made of the benefits of giving watchlist access to the Command and Control Unit. This should include analysis of a sample of CCU cases but should also look at the costs of implementation.

Recommendation 16

That a pilot is carried out that checks visa applicants against the Intelligence Management System to see if there is value in doing this on a larger scale.

Recommendation 17

That the findings of this review are incorporated into the Home Office lessons learned programme and offer a series of seminars to staff outlining the issues and direction for how such a case can be avoided in future.

Recommendation 18

That the Home Office examines existing service level agreements for correspondence to ensure that the correct response times are adhered to.

Recommendation 19

The Home Office should review the options for accurately logging and tracking all correspondence received.

Recommendation 20

The Home Office should ensure that where it is acknowledged that a member of the public has a genuine and serious issue with the Home Office they are allocated a single point of contact who can deal with their case.

Background to the PHSO Report

1. Mr M is a Canadian national. At the end of June 2012 he was given an indeterminate sentence with a tariff of at least six years for several offences including arson, theft, harassment, perverting the course of justice, possessing an offensive weapon and criminal damage.
2. Mr M had entered the UK with a visa applied for in 2009 and obtained under the points based system. At the time of application when asked if he had a criminal record, he declared that he did not. In reality he had several convictions in Canada including some for violence.
3. When in the UK, Mr M began a relationship with Mrs A's daughter; Ms. Q. Mrs A became suspicious of Mr M and contacted a private investigator to look into his background.
4. When Mr M was out of the UK in November 2010, Mrs A contacted the then UK Border Agency by email to inform them that Mr M was due to re-enter the UK via Heathrow and that he had 'an extensive criminal record for violence and use of weapons in Canada.' The email gave his flight number and passport number.
5. Although the information submitted by Mrs A did eventually reach the Heathrow Intelligence Unit and was circulated to Border Force Officers, this action was too late to prevent Mr M re-entering the UK.
6. Beyond circulating the information to stop Mr M at the Border, no action was taken against Mr M by the UK Border Agency until Mr M's arrest six months later, by which time the crimes against Mrs A's family had been committed.
7. Realising Mr M had been readmitted to the UK, Mrs A wrote once to UKBA and once to the Home Office, repeating and expanding upon the information she had given about Mr M. Both letters were ignored and neither have ever been traced.
8. Mr M began a campaign of harassment against Mrs A and her family.
9. Mr M was arrested three times. On the second arrest in April 2011 the police contacted the UKBA Command and Control Unit in Manchester to check what information was available on Mr M. Despite having access to the watchlist, but in keeping with the procedures extant both now and at the time, the operator who took the call did not check the watchlist and confirmed to the police that Mr M held a valid visa. Mr M was released on bail.
10. Two days later Mr M set fire to Mrs A's house. Mrs A and her husband Mr B were on holiday at the time and police airlifted them to a place of safety. Mr M was finally intercepted and arrested at Ms Q's place of work posing as a doctor. When he was arrested he was found to be in possession of a loaded crossbow, a serrated knife, two cans of petrol, gloves, hat and goggles.
11. Mr M was convicted in February 2012 and was remanded to await sentence. During this time prison staff learned that Mr M has attempted to arrange to kill one of the women in the case. This was assumed to be Mrs A or Ms Q and the family were returned to protective custody.
12. From May 2011 to the end of 2012 there was extensive correspondence between Mrs A and the UK Border Agency and Home Office about the case. Her letters were responded to by different officials and on occasions were not responded to at all. No central record was kept of Mrs A's case. On 21 November 2012 Rob Whiteman, then Chief Executive of the UK Border Agency, wrote to the family in response to their letter to the Prime Minister of 17

August 2012. The PHSO concluded that his letter was based on incomplete briefing by officials and that it was inappropriate and completely insensitive.

Current Home Office structure

13. The maladministration found by the PHSO took place when the UK Border Agency (UKBA) was a separate organisation from the Home Office. In February 2012, Border Force was split from UKBA and brought back into the Home Office. In March 2013, in the interests of increased transparency and accountability, the UKBA was abolished and its functions were also brought back into the Home Office.

14. To assist in reading the review the current structure of the Home Office as it relates to this review is shown below, highlighting in blue those units that are directly relevant. From this point onward the review uses the term Home Office.

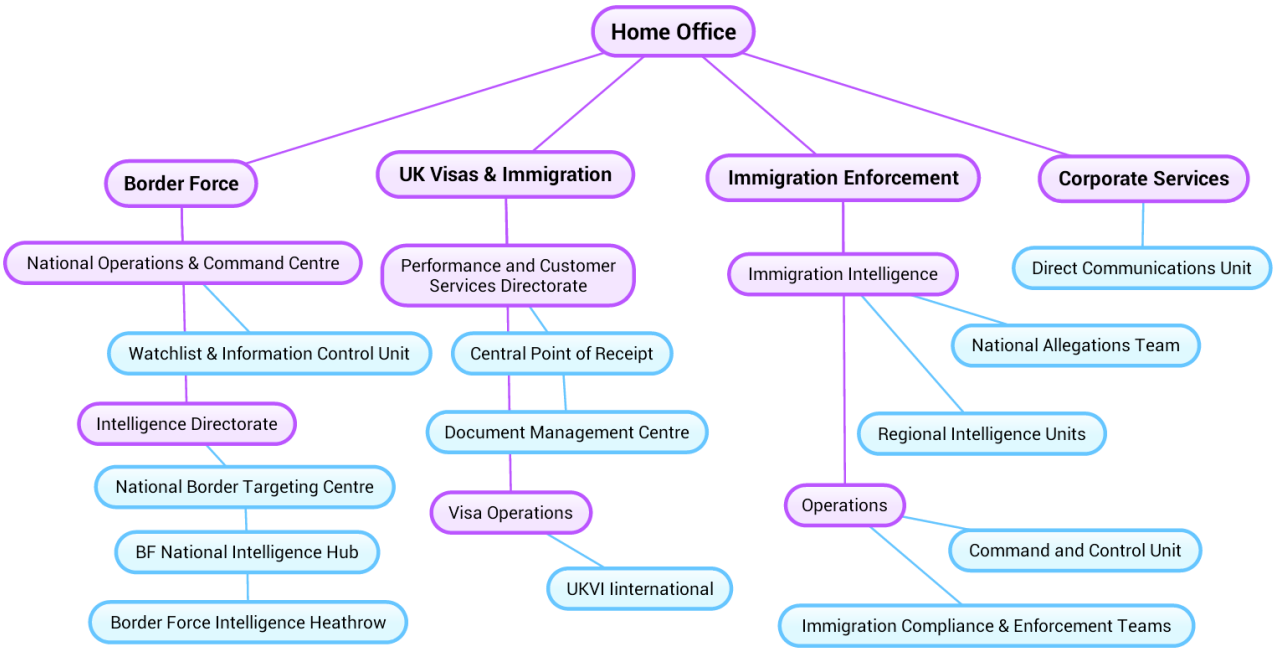

Figure A – Home Office Structure regarding this review

The PHSO Report

15. Mrs A complained to the PHSO in February 2012 and their findings were published in July 2014. The PHSO concluded that;

- The Home Office did not have adequate measures to test the information that Mr M gave them about his visa history, criminal convictions and good character.
- The Home Office logged Mrs A's email of 10 November 2010 too late for any action at Heathrow Airport when Mr M re-entered the UK.
- After Mr M re-entered the UK without being stopped the Home Office did nothing to follow up Mrs A's allegation.
- The Home Office lost Mrs A's two follow-up letters about her allegations.
- The Home Office failed to ensure that they gave police officers all the available relevant information about Mr M after his arrest.
- After Mr M was in prison, Mrs A asked the Home Office to explain how they had failed to deal with her information or to protect her and her family. The Home Office accepted they

could have acted faster in responding to her email, but took no further responsibility for what had happened.

- The Home Office mishandled Mrs A's complaint.

16. In order to remedy the injustice the PHSO made nine recommendations.

Recommendations one to four

The Permanent Secretary of the Home Office should appoint a senior official, with knowledge of immigration, to review urgently;

- the effectiveness of the Home Office's approach to and systems for testing the statements made about visa history, criminal convictions and good character on visa applications; and their systems for verifying and sharing intelligence information for their handling of visa applications.
- the effectiveness of the Home Office's processes for handling allegations including their systems for giving access to the watchlist to people with a legitimate need to use it and the systems and rationale for funding this work.
- the effectiveness of the Home Office's current processes for capturing correspondence on receipt; for acknowledging correspondence; for sending it to the relevant team for action; for tracking the action taken in response to correspondence; for ensuring that the action is complete and good enough; and for retrieving the correspondence for later queries or investigations.

The three reviews should take explicit account of Mrs A's family's experience and of the PHSO findings of maladministration. The Home Office should give the review appropriate funding and publish its outcome, including its recommendations for action, within six months of the PHSO report.

- The Home Office should promote and support the implementation of the reviews' recommendations and monitor progress against them and publish a progress report within 12 months of its publication.

Recommendation five

The Home Office should take steps to demonstrate to Mrs A and her family that they have a grip on the next stages in their dealings with Mr M. These steps should include a written statement to the family of the measures the Home Office are taking to monitor his detention and to take the appropriate action when Mr M leaves prison in the UK. The Home Office should confirm in writing to Mrs A and her family that, in line with existing arrangements, she and the family will have an opportunity to make representations to the Home Secretary before the Home Office reach any agreement to transfer or release Mr M to the Canadian authorities.

Recommendation six

The Home Office should pay Mrs A, on behalf of her family, £10,184 for the costs they incurred. They should also pay interest calculated from the dates the family incurred the costs.

Recommendation seven

The Home Office should pay Mrs A, on behalf of her family, £100,000 in recognition of the effect of the maladministration on her, her husband and her daughter's well being and livelihood.

Recommendation eight

The Home Office should pay Mrs A, on behalf of her family, £20,000 in recognition of the effect of the maladministration on the rest of the family's well being and livelihood.

Recommendation nine

The Permanent Secretary should apologise to Mrs A as the representative of her family.

17. At the time of publishing the report recommendations five to nine had been met. This report deals with recommendations one to four.

Section 1: PHSO Recommendation 1

18. The Home Office should review its approach to and systems for testing the statements made about visa history, criminal convictions and good character on visa applications and their systems for verifying and sharing intelligence information for the handling of visa applications.

19. The review should take explicit account of Mrs A's family's experience and the PHSO findings of maladministration. The Home Office should give the Review appropriate funding and publish its outcome, including its recommendation for action, within six months of the date of the final report on this investigation.

Overview of Section 1

20. In the context of this review the finding of maladministration largely related to the visa application process that relies on self declaration of criminality history.

The visa issuing process – self declaration and criminal history

21. Mr M applied for a visa under the tier 2 points based system. When applying for the visa he was asked if he had any criminal convictions in any country and Mr M answered no. In reality he had been convicted of several criminal offences in Canada, which included violence and he had received a suspended sentence and probation of two and a half years along with 22 days in custody. He also answered no to a question as to whether he had engaged in any activities that might indicate he was not of good character and to the question of whether or not he had been refused a visa to visit any other country. It subsequently transpired that Mr M was refused entry into the United States on 8 July 2009, as he was using a fictitious letter of employment. Mr M has a lifetime inadmissibility to enter the United States.

22. Mr M was subsequently issued a visa and entered the UK where he began a relationship with Ms Q. The visa also allowed him to re-enter the UK in November 2010 following a period abroad.

23. Mr M's application in 2009 was dealt with in accordance with the procedures extant both now and at that time. Visa applicants are asked to self declare whether they have a criminal conviction. If they do not declare criminality and this is subsequently found to be false, the visa should be refused and the applicant will be subject to a 10 year ban for future applications. If the applicant had already entered the UK and is found to have lied their leave to enter may be curtailed. The self declaration is relied upon in the visa issuing process and although there are procedures in place to mitigate the risk of false declarations, including bulk checking against the Police National Fingerprint Database (IDENT1), there are no routine checks of criminal activity in foreign jurisdictions.

Procedures when a criminal record is declared

24. Declaration of a criminal record does not automatically mean that a visa should be refused. The General Grounds for Refusal (GGFR) are contained in Part 9 of the Immigration Rules[1] and the thresholds for mandatory refusal for entry clearance applications are outlined in 320 (2) which states that entry clearance to the United Kingdom is to be refused if the person seeking entry to the UK:

    2a) is currently the subject of a deportation order; or

[1] https://www.gov.uk/government/publications/immigration-rules-part-9

2b) has been convicted of an offence for which they have been sentenced to a period of imprisonment of at least 4 years; or

2c) has been convicted of an offence for which they have been sentences to a period of imprisonment of at least 12 months but less than 4 years, unless a period of 10 years has passed since the end of the sentence; or

2d) has been convicted of an offence for which they have been sentenced to a period of less than 12 months, unless a period of 5 years has passed since the end of the sentence.

25. A further set of general grounds list the circumstances when a person should normally be refused and in terms of criminality this is defined as;

18a) Within the 12 months prior to the date on which the application is decided, the person has been convicted of or admitted an offence for which they received a non-custodial sentence or other out of court disposal that is recorded on their criminal record;

18b) in the view of the Secretary of State:
(a) the person's offending has caused serious harm; or
(b) the person is a persistent offender who shows a particular disregard for the law.

19 The immigration officer deems the exclusion of the person from the United Kingdom to be conducive to the public good. For example, because of the person's conduct (including convictions which do not fall within paragraph 320 (2)), character, associations or other reasons, make it undesirable to grant them entry.

26. The GGFR rules were amended in December 2012 and would not therefore have applied to this case. At the time Mr M applied there were no mandatory refusals for criminal offences and Entry Clearance Offices (ECOs) and officers at the Border worked within a discretionary framework where convictions that would have resulted in a sentence of 12 months imprisonment had they been committed in the UK, could have led to a refusal. Had Mr M declared his criminal convictions at the time he applied, the ECO would have either refused the application or made further checks. These may have included calling Mr M in for an interview, contacting local law enforcement agencies or obtaining further intelligence.

Current procedures for checking statements made in visa applications

27. The current process of checking information given by visa applicants is a two step process. The first set of checks are mandatory, following which staff will carry out a series of further checks where they obtain any additional information that may be deemed necessary.

Current mandatory checks

28. The UK Visas and Immigration (UKVI) operating mandate, which was launched on 1 November 2014, sets out formally the minimum mandatory checks that must be made on those seeking to come to or stay in the UK. The mandate has not changed the checks or the way that they are conducted, but consolidates the processes that are to be followed into a single document. The mandate will be reviewed every six months. The checks vary depending on the migration route that is being applied for but for entry clearance all applicants are checked against the UK Warnings Index and the UKVI Central Reference System (CRS). Those aged 5 and over are also subject to biometric checks and are checked against the immigration fingerprint system (IABS) and the UK police criminality database (IDENT1). Additional checks can also be made with sponsors or employers who have provided supporting documentation.

Further checks

29. Further checks conducted on applications would not routinely include a check with the home country on undeclared criminal history. UK Visas and Immigration are generally unable to check a foreign national criminal record. The availability of overseas criminal record certificates, their coverage and reliability, vary widely internationally. The ability to access foreign national criminal records directly is also very limited due to lack of infrastructure (outside of the European Union) for doing so, restrictions on the use of the data and the reliability of the information obtained. Where criminality is declared, secondary checks would seek to obtain the detail from the relevant authorities but there is no guarantee the information could be obtained or where it could be that it would be accurate.

Audit and assurance of the visa checking process

30. The audit and assurance process has introduced checks by UKVI Managers overseas to ensure that there are no breaches of the procedures set down in the UKVI Operating Mandate and to ensure that visa checking processes are being followed correctly.

31. The systematic checking of applications is clearly an improvement that will assist UKVI in ensuring that checks are carried out robustly. Nonetheless the PHSO report highlighted that there was no evidence that the Home Office tested some of the assertions that visa applicants made about their criminal history. Given the harm done to Mrs A's family, the findings of the PHSO should be given further consideration.

Recommendation 1

That the Home Office introduce a means of sampling or the retrospective audit of information given by visa applicants on criminal history. The information should be assessed to see if further checks on self declared criminality are necessary.

The Risk and Liaison Overseas Network (RALON)

32. In addition to the checks outlined in the UKVI operating mandate there are a range of processes that increase the security of visa issuing and reduce the risk of visas being issued based on false information. The Home Office maintain intelligence systems which are used to generate risk profiles that encourage closer examination of groups of individuals who are deemed to be a higher risk. An application from an individual who meets the profile may trigger additional checks such as interviews and verification of documents.

33. RALON is the unit providing intelligence for visa checking and it maintains good relationships with local law enforcement agencies overseas and may be able to verify criminal histories through those connections if there are specific concerns about an individual.

34. Detailed discussion on risk profiling is restricted for security reasons.

Checks on visas at entry

35. A further check is made on passengers when they enter the UK. At the UK Border all passengers, including British Citizens, are checked against the WI. The WI does not contain information on criminal records abroad, although it does contain some criminality information, including alerts for those wanted for serious crimes.

36. A passenger in possession of a valid visa would also have his or her fingerprints verified against the fingerprints he gave at the time of application.

37. Passengers both with and without visas are also checked through the use of Advance Passenger Information (API). API acts as an early warning that checks passengers on route to the UK against the WI. Again, criminal activity in foreign jurisdictions would be not part of API data.

38. Non-EU passengers are questioned by a Border Force Officer. The Immigration Rules grant powers to Border Officers to curtail leave to enter or remain if they believe that leave may have been obtained through false representation or failure to disclose material facts.

Bilateral and multi-lateral arrangements

39. The UK Government has a series of agreements and arrangements that allow sharing of data and intelligence that allow further checks on criminality to be made.

40. The Five Country Conference Protocol is a data sharing agreement signed in 2009 between the UK, United States, Canada, Australia and New Zealand. These countries share a limited number of immigration fingerprint records (approximately 3,000 for each country every year) for matching against the other countries' immigration databases. The Protocol is generally used to check fingerprints of asylum seekers to counter immigration fraud and asylum shopping. Additionally, the UK and New Zealand also share details about foreign national offenders deported from their territories where the primary reason for deportation was their criminal conviction.

41. The Home Office is working to improve data sharing on criminality with other countries. Recent visits to Pakistan and Nigeria by senior Home Office officials have initiated a dialogue about how these processes can be improved. Criminal Records Information Sharing Agreements have recently been signed with Ghana and a number of British Overseas Territories in the Caribbean – that will mean that conviction information should be provided in the same circumstances and timescales as the EU exchange under European Criminal Records Information System (ECRIS), which is looked at later in the review. These arrangements would not directly affect current visa processing since they are aimed at foreign nationals already in the UK but they do enrich the overall intelligence picture.

Options for checking criminality of visa applicants

42. A number of checks are made on visa applicants as set out earlier in this report. The UKVI operating mandate formalises the mandatory checks and an assurance framework ensures compliance. Possession of a visa does not guarantee entry and further checks are made on visa holders at the Border. Mr M went through all of these checks, but nonetheless was able to enter the UK on a visa despite making a false declaration about his criminal history.

43. During the course of this review we met with Mrs A and Mr B (her husband) on three occasions and each time they argued strongly in favour of introducing individual checks on applicants' criminal history in their home country. The PHSO were also critical of the reliance on self declaration and believe that this undermines the visa process.

44. If all visa applicants are to be checked, or even certain groups of applicants, (eg: those applying for settlement) then there are two options; either direct access to the home country's criminal data or requesting from the applicant that they produce the information. Neither option is without flaws.

45. Direct access would involve the Home Office in setting up systems with all countries whereby they could either access their data directly or request the home country to do it on the Home Office's behalf. Either way would be expensive and would take many years to implement fully. Additionally, many countries would refuse direct access to their data by a foreign jurisdiction.

46. Alternatively applicants could be asked to produce the information for the Home Office as part of the visa application process. This could take the form of Police Certificates that summarise the applicant's criminal history. Some countries would not have the infrastructure to produce a recognised certificate and in these cases the applicant could make the equivalent of a subject access request asking their own police force to give them a statement

of their criminal history which they then produce for their visa application. Again, not all countries would facilitate this.

47. Police Certificates are already requested by some countries for settlement and citizenship applications, and in others for work or study applications. It is not always easy to establish the veracity of the documents; since some countries have no centralised records and only have local systems. This means that a certificate may be obtained in one state or region that won't reveal criminal activity in another state or region.

48. Fraud is also a major issue particularly where police forces are localised, since in those circumstances one country may have many variations of Police Certificates.

49. Security is also a concern since some individuals may not wish their home country to know that they are applying for a visa and a request for a Police Certificate may put them at risk. There are also complications relating to the use of criminal data for immigration purposes which many countries will not agree to.

50. Although some countries do not have the infrastructure to produce Police Certificates and those produced could be subject to the fraud and security concerns highlighted above, other countries do have the capability to produce certificates securely. Canada falls into this latter category.

Which countries use Police Certificates?

51. The UK is the only member of the Five Country Conference (Australia, Canada, New Zealand, UK, USA) not to require Police Certificates from migrants applying in any immigration routes. No country requires the certificates for every route and visitors are not routinely required to present this evidence.

52. The PHSO report fell short of saying that had it not been for Home Office maladministration Mr M would not have been able to enter the UK on a visa and the review agrees with this. Had Mr M applied for a visa in Australia for example, he would not have to produce a Police Certificate, since that is only required for permanent migration. It also needs to be considered that had Mr M declared his criminal record to the Home Office, then under the procedures that were extant at the time, there can be no automatic assumption that he would have been refused. Mrs A's family claim that Mr M's level of criminality was much higher than the official records the Home Office has seen suggests. The Home Office has not been able to verify this, possibly because Mr M may have used several aliases. To some extent this reinforces the point that official police records can paint a partial picture that can mislead. This is not to suggest that Police Certificates cannot be useful, simply that they are not a panacea.

Police Certificates issues in the UK

53. ACRO produce certificates for British nationals, or foreign nationals who have previously resided in the UK, who are asked to provide Police Certificates when they travel to other countries for certain purposes. In 2008-09 ACRO produced 62,000 Certificates and in 2012-13 this rose to 110,000 The vast majority of Certificates that ACRO issue relate to four countries. Figure B, taken from the ACRO Annual Report (2012-13), summaries their use.

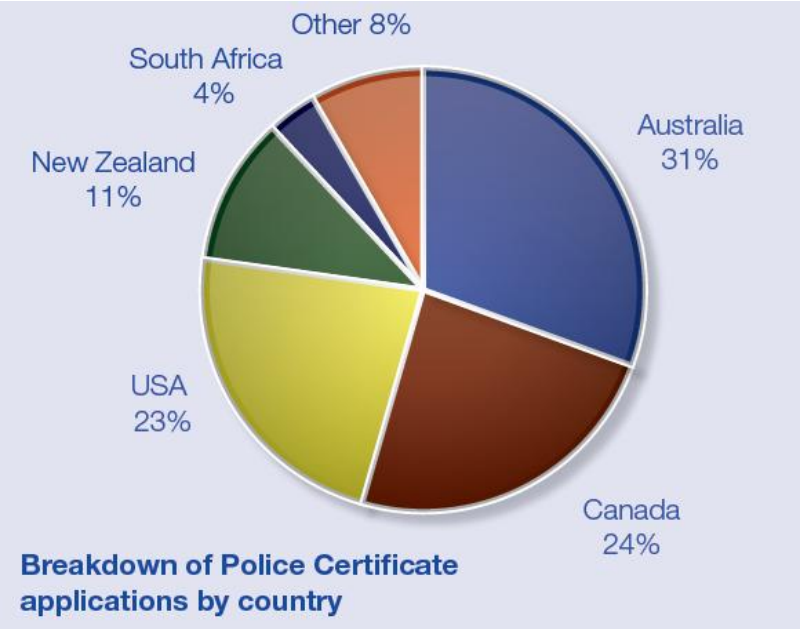

Figure B: ACRO 2012-13 Police Certificate data

Foreign nationals in registered activity

54. Although the UK Government does not currently request Police Certificates for those applying for visas there is a system for requesting Police Certificates for foreign nationals (and UK nationals who have lived abroad for a significant period of time) who apply for certain jobs in registered activity e.g. NHS, teaching or security industry posts. Guidance is available to support these recruitment practices, which provides contact details for each country explaining how to apply for certificates, cost, estimated time to process applications and examples of certificates. The process is outlined below.

Step 1	Migrant applies to relevant overseas records authority for a Police Certificate
Step 2	Overseas records authority gives certificate to migrant
Step 3	Employer applies to the Disclosure and Barring Service (DBS) for a check on the migrant
Step 4	DBS issue the certificate to the migrant (having checked against PNC)
Step 5	The migrant gives the employer both the overseas Police Certificate and DBS check
Step 6	The employer, content the migrant has been adequately checked, applies for a “Certificate of Sponsorship” (COS) from the Home Office
Step 7	The Home Office issue the COS
Step 8	The employer gives the COS to the migrant
Step 9	The migrant uses the COS to apply for a visa
Step 10	The Home Office issues a visa (having checked against PNC)

Table 1 – Process for applying for a Police Certificate

55. These types of checks are carried out in the following circumstances.

UK Agencies requirements for overseas workers

Agency	Workers requiring Police Certificate	Time period	Countries that the certificate should cover
Teaching Agency	Trainee and new teachers will require a DBS check No formal requirements for overseas checks – up to each institution. NB School Employment Regulations require adequate checks to be done (see below)	n/a	n/a
Security Industry Authority	Anyone applying for a license who lives overseas (including EU) or has lived overseas for 6 months or more (continuous) in the past 5 years.	5 years prior to application	Residing country if outside the UK or any country lived in for 6 months or more.
NHS	Strongly recommended to do overseas checks on applicants that would be require checks in UK. Eligibility for checks is based on an assessment of roles & responsibilities to dictate level of check required by DBS (basic, standard, enhanced)	Not specified	Not specified

Table 2 – UK Agency requirements for overseas workers

56. Although there is no specific statutory requirement for organisations to carry out such checks it is widely considered best practice to do so. The Department for Education has published guidance that sets out the responsibilities of all local authorities, schools and further education (FE) colleges in England to safeguard and promote the welfare of children and young people. It sets out recruitment best practice, some underpinned by legislation, for the school, local authority, and FE education sectors.

57. Specifically the law says that in the case of any such person for whom, by reason of having lived outside the United Kingdom, obtaining an enhanced DBS certificate is not sufficient to establish the person's suitability to work in a school, the governing body must make such further checks as it considers appropriate, having regard to any guidance issued by the Secretary of State.

58. The review was not able to comment on whether employers are following the guidance that is laid down for making overseas checks for those in registered activity. Given that this body of work could provide evidence to the Home Office of how well the system of Police Certificates works and may provide information on timescales, benefits and disadvantages of the system it should be examined in more detail.

Recommendation 2

That the Home Office work with the Department for Education and Department of Health to gather additional information on the system of Police Certificates to establish the benefits and disadvantages of using the system for migration purposes.

The viability of Police Certificates in the UK

59. Most foreign nationals entering the UK do not require a visa. They are either EEA nationals who are covered by the free movement directive or non-visa nationals. A non visa national does not need a visa to come to the UK for less than six months, unless it is a requirement of the immigration category under which they are entering.

60. Since EEA nationals and non-visa nationals make up the majority of those entering the UK, this means that a check on criminality in the home country would, for the large majority of those entering, have to either take place at the Border or be carried out prior to entry by a check on API data. Within current infrastructure this is not possible.

61. Police Certificates could be considered for the minority of passengers who are visa holders but that would impact heavily on visitors in terms of time, cost and bureaucracy. A Police Certificate costs between £20-30 on average and takes around 10 days turnaround time. It would be detrimental to visa processing for the 2.2 million visitor applications and a disproportionate response for the majority of law-abiding visitors.

62. Police Certificates could be requested for certain groups of migrants, such as those applying for settlement and nationality applications and options for this are currently being discussed in the Home Office.

Taking account of Mrs A experience and the PHSO finding of maladministration

63. The PHSO finding of maladministration relied significantly on the failure of the Home Office to test the statements given to them by applicants on their criminal history. In our meetings with Mrs A and Mr B they also felt that had Mr M's criminal record been checked then his visa would have been refused. We cannot know whether this would have been the case or not. Equally we cannot assume that Mr M would have been deterred from applying had there been a system of Police Certificates in place. The level of Mr M's criminality may not have reached the criminal threshold for refusal that was extant at the time and it is feasible that had he declared his criminal record in 2009 he would still have been issued with a visa. That would equally apply today and although the general grounds for refusal are more prescriptive than they were when Mr M applied, the level of his criminality would have not reached the threshold for automatic refusal had he declared it.

64. Although the PHSO and Mrs A's family see value in introducing Police Certificates, there are no guarantees that they would prevent a case of this nature happening again. Police Certificates could not be introduced for all visitors to the UK and given that only a minority of those entering the UK require a visa, many of whom are visitors, the minority coverage would leave scope for a similar case to occur. Additionally, although reliable certificates could be obtained from some countries, such as those signed up to the five countries protocol, there are many others where fraud and reliability of certificates would undermine the value.

65. The Government is currently considering the feasibility of introducing Police Certificates for a limited number of migration routes.

Section 2 – PHSO Recommendation 2

66. Review of the Home Office's processes for handling allegations, including their systems for giving access to the watchlist to people with a legitimate need to use it and the systems and rationale for funding this work.

67. The Review should take explicit account of Mrs A's family's experience and of the PHSO findings of maladministration. The Home Office should give the Review appropriate funding and publish its outcome, including its recommendations for action, within six months of the date of the final report on this investigation.

Overview of Section 2

68. In terms of this section of the report, the finding of maladministration against the Home Office was based on;

- Heathrow Intelligence Unit logging the allegation by Mrs A too late.
- Heathrow Intelligence Unit did nothing to follow up Mrs A's allegation.
- The Command and Control Unit failed to ensure that they gave police officers all the available relevant information about Mr M after his arrest.

In terms of allegation handling, the PHSO report also found maladministration in the handling of allegations submitted by mail. The handling of post is examined in section 3.

How the allegations system worked in 2010 for Mrs A's case

69. In 2010 the public could make an allegation by email, letter or telephone. An email allegation was made via the public enquiries inbox which was manned during office hours. The public enquires team would forward all allegations to the evidence and enquiry unit who would forward the allegation to the appropriate unit, which in this case would have been Heathrow Intelligence Unit. This is the route that Mrs A's allegation of 20 November 2010 took. The result was that the information contained in the allegation was circulated to Officers at the border too late to prevent Mr M re-entering the UK.

70. Since November 2010 there have been significant changes to the way allegations received from the public are handled.

How allegations works in the Home Office now

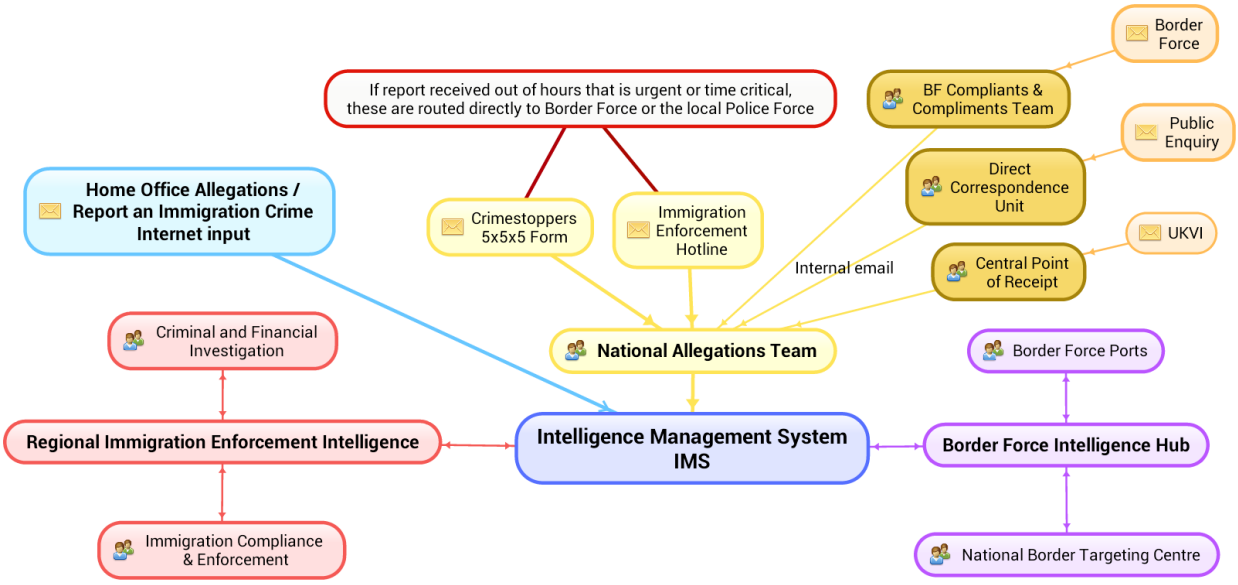

Figure C – Allegation routing

71. As shown in figure C an allegation to the Home Office can be made by e-form, email, face to face (reporting centre), fax, letter or by telephone. An allegation by letter is dealt with in section 3 which deals with handling correspondence, since the handling procedure for letters is the same whether the correspondence is an allegation or some other matter. This section looks at the handling of allegations that are received electronically or by telephone.

Allegations received electronically

72. There are several ways that a member of the public can submit an allegation to the Home Office electronically. They can submit information online by searching on 'report an immigration crime' and then filling in the electronic form (e-form) which is sent for inclusion in the intelligence management system (IMS). Alternatively they can use the main Home Office contact on the gov.uk webpage and send their allegation via the public enquiries inbox in the same way that Mrs A did in 2010. They could also use the complaints procedure. There are three separate links on the Home Office website for complaining on immigration matters, one for the Home Office and one each for Border Force and UKVI.

73. The Home Office prefers to receive allegations on the e-form to IMS. The layout of the website however does mean that allegations are also received via the other two routes and in this case they are re-routed by staff to the appropriate unit dealing with the allegation.

Allegations received on the e-form and sent to the IMS system

74. In May 2011, following a recommendation in a report by the Independent Chief Inspector of Borders and Immigration[2], the Home Office introduced the intelligence management system (IMS) as a means of handling and managing allegations and intelligence received from the public and partners. The IMS now provides a centralised database for all incoming allegations received via the e-form which are routed for action to an appropriate part of the Home Office.

75. The IMS system is auto-populated via the gov.uk website under the heading of 'Report an immigration crime.'

[2] http://icinspector.independent.gov.uk/wp-content/uploads/2011/02/Preventing-and-detecting-immigration-and-customs-offences.pdf

76. The latest statistics available for use of the system are shown below.

- In 2013-14 the IMS system received 75,000 pieces of information of which approximately 30% was not usable since it did not contain sufficient information to progress the allegation further.
- Of the 75,000 allegations received 58,000 were received by email or online and 9,000 by hard copy. (Allegations received in hard copy are looked in the next section of the review.) The remaining 8000 were received by fax, telephone or face to face.
- The IMS team monitor use of the website and collect information and analyse that information so that it can be used to improve the system. The latest release of IMS was made in November 2014 and this made some updates, including simplifying the form and reducing the amount of time taken to complete it.
- The team processing the allegations have a service level that requires all allegations to be actioned within 2 working days of receipt. In this context 'actioned' means that the allegation is assessed against risk and priority then allocated to the appropriate business unit for them to progress. There are plans to reduce the SLA to 24 hours in the early part of 2015.
- The target for compliance with the 2 day SLA is 100%. Performance against this standard has risen steadily since September 2013 and is currently in the region of 95%.

Other allegations received electronically

77. As an alternative to the e-form, a member of the public may send an email containing an allegation to one of the three relevant addresses listed on the website. These would go to different inboxes depending on the email address used;

- An allegation received via the public enquiry email address will go to the Home Office Direct Correspondence Unit.
- An allegation sent in the form of a complaint to UKVI will be sent to the Central Point of Receipt in Croydon.
- An allegation received in the form of a complaint to Border Force will be sent to Border Force Complaints and Compliments Team in Croydon.

78. When in receipt of an allegation by email the section receiving it should re-route the allegation to the National Allegations Team in Croydon who should create a case in IMS, attach the correspondence to it and then route it to the most appropriate team. This procedure is not fail safe because it relies on the staff receiving the email reading it and correctly identifying it as an allegation. The majority of email received into the three inboxes highlighted are not allegations and would be primarily complaints or questions and consequently allegations can be overlooked. Additionally there are emails that contain both complaints and allegations. Possibly for this reason the review found cases where allegations were incorrectly routed and took many days before they were recognised as allegations and routed accordingly. This is looked at in further details below.

Prominence of the e-form on the Home Office website

79. The online form for use by the public to make an allegation that auto-populates the IMS system can be found on the Home Office page of gov.uk. The link is not immediately obvious on the web page, but a search on the page and on Google of 'report an immigration crime' immediately brings up the electronic form used to make the allegation. The form was refreshed on the 1st November 2014 and is simple to use, taking between ten and twenty minutes to complete when tested by the author of this review. The form is in English.

80. Although the link to the online form is not on the front page of the Home Office gov.uk website two other links to contact the Home Office are. Scrolling down on the webpage links the user to the address to use for the public enquiry mailbox should they wish to contact the Home Office. There is a further link to an email address that the public can use to make a complaint. Neither of these two email addresses link directly to the IMS system, only the 'reporting an immigration crime' does that. Information received via either of these units needs to be rerouted manually.

Using the email instead of the e-form

81. Members of the public who wish to make an allegation or give information to the Home Office may not make a distinction between reporting a crime, contacting the Home Office and making a complaint, so may use email to make an allegation instead of the e-form, unwittingly slowing down receipt of the information.

82. The gov.uk website may be inadvertently encouraging this since the email addresses are more prominent than the online reporting form. Given that in the case of Mrs A's allegation the time that it took for the information to reach Heathrow Intelligence Unit was a factor that contributed to Mr M being allowed to re-enter the UK unhindered, it would be better if it was made clearer to the public which route should be used when making an allegation.

83. The review noted that the front Home Office gov.uk web-page lists frequently used pages in the top right corner, for example applying for a passport or getting a criminal records check. It may encourage the use of the online reporting to make allegations if a link to the form for reporting immigration crime is also included in this space. Alternatively, and possibly in the longer term, there should be only be one link on the front page with an automatic routing behind that so that the public are not asked to distinguish between an allegation, complaint or contact.

Recommendation 3

That the Home Office web page on gov.uk contains a link to 'reporting an immigration crime' and that the email links make it clear that the online reporting form should be used to report a crime or make an allegation. In the longer term the Home Office should consider one single contact point on the gov.uk website.

Routing of allegations received via the IMS system

84. Once a member of the public gives information to the Home Office by using the e-form it is automatically routed to the appropriate unit within the Home Office to deal with. The automatic routing means that regardless of the time of day that the allegation is made, the information can be forwarded promptly and correctly to the appropriate business unit for action. Should the information allege that a migrant is here illegally for example and gives the postcode where they believe the person is living, then the IMS system automatically routes that to the regional intelligence unit covering that post code. Similarly, if the allegation indicates that the matter relates to smuggling or to a person in the process of travelling, then the allegation is routed to the Border Force National Intelligence Hub.

85. Automatic routing only takes place once and if an allegation is routed incorrectly it then needs to be rerouted manually and this may cause delays. The current number of manually routed allegations is averaging 200 per week (10,400 per year). The number of manually routed allegations is important because it is these allegations that can become subject to delays.

Variation in working hours

86. The process diagram in figure C above shows how the routing of allegations works. Not all of the units that receive allegations work on a 24/7 basis and working hours are as follows

Route	Hours worked	Days
Border Force National Intelligence Hub (BFNIH - The Hub)	24 hours coverage	Monday to Sunday
National Allegations Team (NAT)	9am to 5pm	Monday to Friday
Immigration Enforcement Regional Intelligence Units	7am to 9pm 10am to 4pm	Monday to Friday Saturday and Sunday
Border Force Intelligence Heathrow	Redacted	Redacted

87. Given that the IMS does have an automatic routing system the vast majority of allegations will be delivered correctly in the first instance. All Border Force allegations are automatically routed to the Border Force National Intelligence Hub (BFNIH – the Hub) which has 24/7 coverage. We visited the Hub and were satisfied that they were fully aware of the hours worked by Ports and of their responsibilities in providing the one 24/7 capability for Border Force. The staff we spoke to at the Hub were clear on the action that they needed to take on allegations, such as making sure the information was available to Border Force Officers or phoning control desks when Port Intelligence Units were closed. This automatic routing and 24/7 coverage means that the situation that arose with Mrs A's allegation would not happen now if the e-form was used to submit the allegation. Since Mrs A included in her allegation travel details, her allegation would be automatically routed to the Border Force Hub. In Port working hours they would forward the allegation to Heathrow intelligence Unit who would ensure the allegation was actioned. If the Heathrow Intelligence Unit was closed, the Hub would ensure the allegation was actioned themselves.

88. Outside of Border Force there is no 24/7 coverage for allegations, although in regional intelligence offices there is 14 hour cover on weekdays and six (core) on weekends. This means that the vast majority of allegations routed to Immigration Enforcement should be actioned within service standards, but nonetheless there is scope for an allegation to 'fall through the net'. This could impact most when an allegation is either high harm or time critical. For example, allegations relating to human trafficking, since this is largely seen as an in-country issue, generally auto-route to the National Allegations Team (NAT). If the allegation included details of travel it would instead be routed to the Border Force 24/7 facility. If it did not include the travel details however and even if the subjects were on route to the UK, it would go to NAT. Since NAT is only 9am to 5pm Monday to Friday, an allegation received after close of business on a Friday, that alleged people were being trafficked through Heathrow on Saturday morning, would not be actioned until Monday. Although a different crime, it was the re-routing issue that partly contributed to the delay in Mrs A's case.

Recommendation 4

That the routing for immigration allegations be modified to ensure that cases that are high risk or time critical are routed to a 24/7 unit.

Mrs A allegation of November 10 2010 received now

89. The two figures below demonstrate what would happen with Mrs A's allegation if it were received now. Figure D shows the scenario if she had used the e-form and figure E if she used the email address for the public enquiry office or complaints.

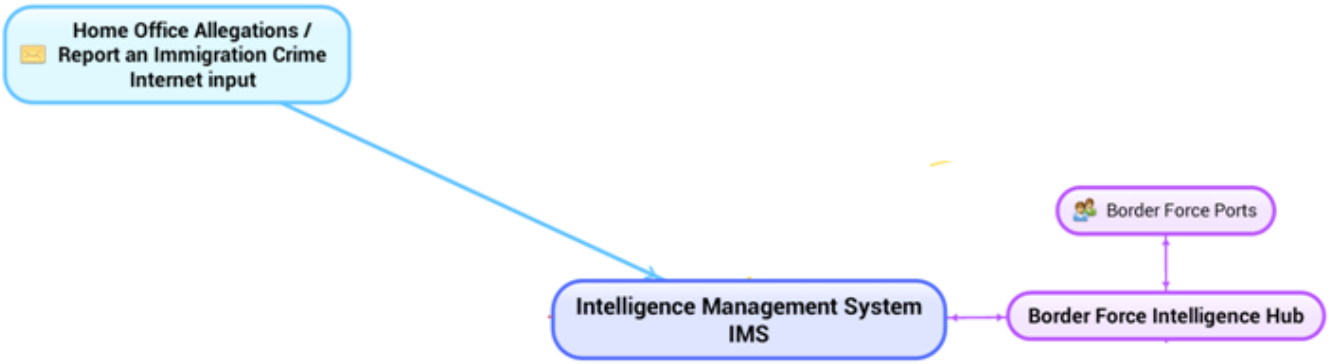

Figure D – Allegation via the e-form

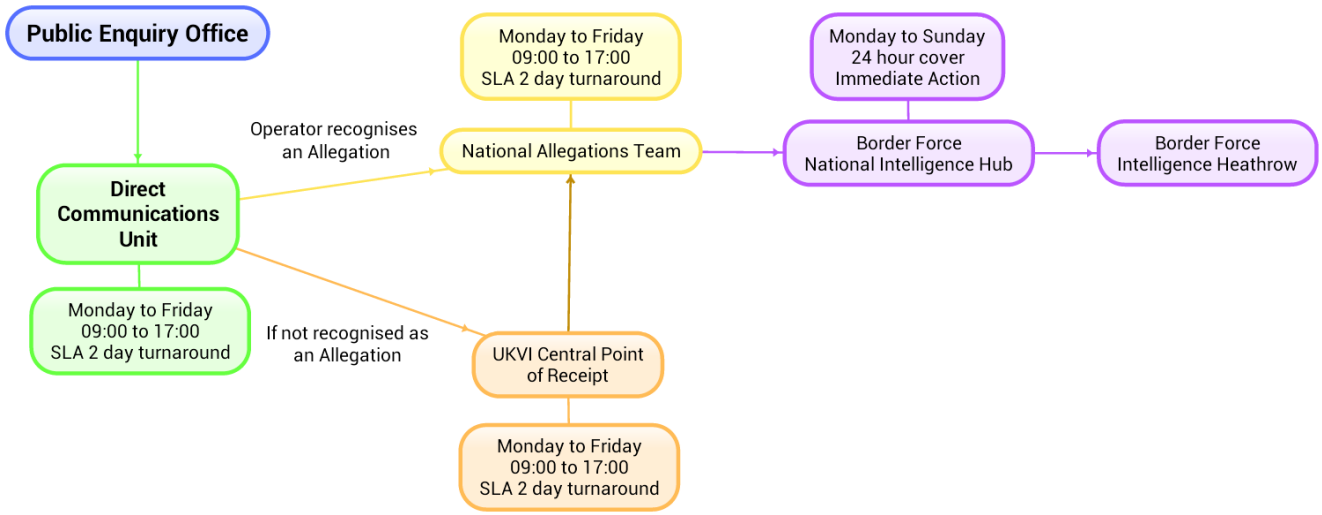

Figure E – Allegation via the Public Enquiry Office or Complaints process

The above show that although the e-form provides significant improvement, use of the email address means that the allegations could be delayed in reaching the appropriate unit for action.

Testing the public use of the eform

90. The form that the public use to make an allegation was refreshed on 1 November 2014 and it is hoped that the form is simpler to use and that the time taken to complete it has been reduced. Given that the new form was put in place during the review we are not able to comment on how well it is working but the review were assured that it will be evaluated on a monthly basis. It is important in the context of the PHSO Review, that the system is evaluated with regard to allegations which need to be rerouted.

Recommendation 5

Immigration Enforcement management should ensure that as part of the monthly evaluation of the intelligence management system, they maintain information on the proportion of allegations that need to be rerouted manually. Cases of high harm among those incorrectly routed should be specifically highlighted.

Visibility of warnings

91. The web page containing the 'report and immigration crime' link contains a warning on the bottom of the page that if a crime is in progress or someone is in danger then the police should be called. The bottom of the page also gives links for Crimestoppers and the confidential-anti terrorist hotline. The warning is not visible on some browsers or on some ipads and smart phones but the 'start' button is. This may encourage users to begin to complete the form without having seen the warning that they may need to contact the police.

Recommendation 6

The Home Office 'report an immigration crime' web page, should allow the warning to the public at the bottom of the form to be clearly visible when the web page opens.

How allegations are dealt with once they are received

92. As the process in Figure D above show, allegations received through the IMS system are routed to the relevant section of the business to deal with. This section of the review outlines how allegations are handled within each of those units.

National Allegations Team

93. The National Allegations Team (NAT) is the unit that receives all allegations made using the e-form that do not route automatically to either Immigration Enforcement or Border Force. They also receive email allegations that come via Crimestoppers using 5x5x5 intelligence forms and from other parts of the business. NAT's role is to reroute e-form allegations that have not routed automatically. Allegations received in other formats such as email or by mail are also routed to NAT who create a case in IMS and manually route it to the appropriate business area. In an average week, NAT deal with between 600-700 allegations[3] of which 200 are received by mail. Although their official hours of work are 9am to 5pm on weekdays they do in fact have cover from 7.30am to 5.30 pm. There is no cover at weekends.

The Border Force National Intelligence Hub

94. The Border Force National Intelligence Hub, known as the Hub, runs 24/7, 365 days a year. One of its roles is to receive information from the IMS system. When an allegation is received into the Hub, staff will forward to the relevant unit during working hours. Out of hours the Hub make relevant checks against other Home Office databases that they have access to. Following evaluation of the information they have received they will inform ports that an individual should be stopped or that some other action needs to be taken. The Hub informed us that if they received an allegation that was time critical and a person was, for example, about to enter the UK, they would phone through to the Control Unit at the relevant port.

95. One issue raised by the Hub was that although the Hub have access to the watchlist system, they are unable to place entries on directly and need to send them through to a separate data entry team. If an entry is urgent, the Hub telephone through to get the entry prioritised. The Hub felt it would be quicker if they could put a WI entry on themselves. The need to ensure data quality of watchlist entries is critical however, since poor quality entries generate 'noise' on the watchlist, which risks the integrity of the system. Without further evidence the review cannot recommend either course of action but nonetheless the issue should be considered further based on the appropriate evidence.

[3] Confirmed in an email from NAT Manager (Average of allegations over a six month period)

Recommendation 7

That consideration be given to allowing the Border Force National Intelligence Hub to put entries directly onto the watchlist system.

96. We asked the Hub for their assessment of how they would action the allegation from Mrs A if it was received by them now. They confirmed that given the information contained in the email they would have forwarded the allegation to the Border Force Intelligence Heathrow Team (BFIHT), if it has been during their working hours. If it was outside of BFIHT working hours they would ensure that the information was circulated to Border Force Officers at the airport, together with the correct action to take.

97. The Hub also informed us that they have the capability to check if a passenger was actually on a plane and on route to the UK, through use of the API. This would be useful in cases where the allegation was serious but did not include specific details of the flight the passenger was on.

Border Force Intelligence Heathrow

98. Allegations received by the BFIHT come via the Border Force Hub, Crime Stoppers and Custom hotline. On receipt, the BFIHT will check the allegation against intelligence databases that contain information about immigration and customs. If it is considered appropriate after checking the allegation, the BFIHT would ensure that the information was circulated to Border Force Officers at all ports.

99. The BFIHT work [REDACTED] Monday to Sunday. We spoke to both the Hub and BFIHT and are confident that both understood their responsibilities in terms of dealing with allegations. The Hub knew they had to action time critical allegations when the BFIHT was closed and the BFIHT knew that it was important to check allegations at the start of shifts to ensure that nothing had been missed.

100. The PHSO outlined that they were told by BFIHT (at the time called Heathrow Intelligence Unit) and the relevant part of Border Control that in a case such as Mrs A's, when they had requested a watchlist entry, they would expect the port to contact them when the subject was stopped. If this did not happen then the BFIHT would contact the Canadian Embassy to check on Mr M's convictions and would then request immigration enforcement to intervene.

101. We asked the BFIHT about Mrs A's case and whether or not they would have taken the time to phone the Canadian Embassy to check whether or not the allegation about Mr M was true. They felt that this was primarily the responsibility of the Border Officer at the control once Mr M had been stopped at the Border. They would not have expected to do this themselves. There was no dispute that checking the record with the Canadian Authorities would be best practice but there were conflicting views within BFIHT as to whether or not a Border Officer who stopped Mr M would have gone so far as to check his record once Mr M had been detained. The exact procedure is not set out in policy or local practice and subjectivity is understandable, since Border Force Officers must be given discretion to act as they see fit. Additionally it could not be guaranteed even if the request was made that the Canadian Authorities would have provided the necessary information within a tight deadline, particularly given that the information was being requested for immigration and not criminal purposes.

102. What was also not clear is whether a unit that requests a watchlist entry is responsible for following it up. The PHSO report implied that they were told that they were, but the review was not convinced that this was the accepted practice and there was nothing that could be found in the operating instructions that indicated that it was.

Recommendation 8

That clear instructions are given to all staff who have requested a watchlist entry, as to what their responsibilities are in terms of following up on that information to ensure that relevant actions are taken.

103. We found in all of the Units we visited (with one exception) that in terms of dealing with allegations there was an attitude of 'when it's gone it's gone.' This is not a criticism of individuals, all of the staff we met were clearly committed and all saw the value of their work but nonetheless there was an attitude, even among fairly senior managers, that once an allegation was forwarded that was the end of it. This attitude was very closely linked to the design of the systems that encouraged this mentality. The one exception we found to this was the Border Force Hub who displayed a much greater end to end understanding of the allegations process and the consequences of not following up.

104. Where there is no follow up to a watchlist entry, then as the PHSO pointed out the intelligence can in a case like Mrs A's remain 'hidden'. The intelligence is held on the watchlist if the suspect has entered the UK but the chances of this intelligence being seen is limited, since this system is used primarily for border security and control. This issue is looked at it more detail in the section relating to the Command and Control Unit.

105. Given the current focus across the Home Office a request to check on the overseas criminal histories of subjects arrested, Border Force may wish to consider in their operating practices a note to intelligence staff that checking of overseas criminality is now an option. ACRO checks do currently take some time, depending on the co-operation of the receiving country, but there is no reason why a local intelligence hub such as the one at Heathrow could not ask for an ACRO check and put the information onto IMS or the watchlist at a later stage. Immigration Enforcement and UKVI have both adopted the practice of making ACRO checks when it is appropriate to do so.

Recommendation 9

That all intelligence staff in the Home Office be made aware of the practice and procedure for obtaining overseas criminal records checks and that instructions be issued for when this should be requested and how the information should be handled.

106. The BFIHT raised with us some of the anomalies that exist between the way IMS delivers information and the way other immigration and customs intelligence systems deliver it. Whilst some intelligence systems are checked against the watchlist, others are not.

107. The review was also surprised that sections of the Home Office did not have access to the IMS system, and in particular the Command and Control Unit (CCU) and UKVI who may need access to the information on it. That said, it is accepted that as an intelligence system there must be some restrictions on access.

108. We were not able to investigate the rationale for these anomalies and there may be good reasons for them. Nonetheless the Home Office should be satisfied that it cannot be in a position where they are in possession of information that could have been used to prevent harm and that it has failed to act upon it because it is on the 'wrong' system.

Recommendation 10

The Home Office should carry out an assessment of how intelligence systems are joined up to satisfy itself that information held cannot be overlooked.

109. The BFIHT did inform us that they do sometimes receive allegations in letter form. When this happens they put the allegation onto IMS for appropriate routing.

110. Like the other units we spoke to the BFIHT also informed us that allegations can be wrongly routed to them. In those cases they will re-route manually to the most appropriate business unit.

Immigration Enforcement (IE) - Regional intelligence

111. Time did not permit visiting all of the regional intelligence units. There are nineteen units in England and the review visited one of them based at Sandford House in the West Midlands that serves the central region.

112. The SLA for allegations received from the public via the e-form is that they must all be actioned within 48 hours, although in the West Midlands there is a local target of 24 hours.

113. The IE Intel Unit confirmed that should they receive an allegation that is time critical, such as Mrs A's case, they would telephone the Port. An Operational Instruction was issued to this effect in October 2014

114. As with Border Force, the IE intelligence unit staff check at the beginning of the shift for anything in the inbox that is high priority or high harm and they deal with this first. Staff were conscious of the need to do this since important allegations could come through when the office is closed.

115. As with Border Force, once an allegation is received it is checked against the relevant databases, which in the case of IE are the Central Reference System (CRS), the Warnings Index (WI) and the Case Information Database (CID). Once all relevant information is obtained from the databases it is sent to a triage officer who decides if allegations should be researched further to determine if action could potentially be taken. All information received is graded using the Intelligence Handling Model which rates the information based on risk and priority. Priorities are set by the Strategic Tasking Board for Immigration Enforcement and UK Visas & Immigration and the Tasking Coordination Group for Border Force, the priorities are reviewed monthly. The decision therefore as to what is investigated is based on the level of risk and the priority of the abuse type.

116. In a similar vein to Border Force, staff were not entirely clear what they would do if there was an allegation of a visa obtained using deception. The reasons for this may largely relate to organisational structure in that visa issue has traditionally been, and remains, a separate part of the organisation. Regardless of the reason it would, given the harm caused in the case, be worthwhile issuing a clear instruction to intelligence staff outlined what to do in the event of an allegation of a visa obtained by deception.

Recommendation 11

That staff in both Border Force and Immigration Enforcement intelligence units be issued with clear instructions on how to deal with an allegation of a visa obtained by deception.

117. The majority of tasked cases (those where there is a follow up action) that arise from allegations are referred to Immigration Compliance and Enforcement (ICE). Local Intelligence track and then monitor the tasked cases to see what action has been taken and then update IMS with this information. Tasked cases are monitored through a weekly tasking process and outstanding cases are discussed routinely. This would have been useful in Mrs A's case and clearly illustrates improvements made in the IMS system.

118. When an IE intelligence unit forwards an allegation to Border Force or another part of the business they do not employ the follow up procedure that they employ within Immigration Enforcement as highlighted in the paragraph above. Border Force may also wish to introduce

tracking of its IMS allegations in line with IE. It is recognised that IMS does not form the entirety of Border Force intelligence systems and there may be operational reasons why this does not happen.

Recommendation 12
The Home Office should ensure that Border Force consider tracking action taken on all allegations in a similar way to Immigration Enforcement if there are sound business reasons for doing so.

Dealing with allegations that are received via the public enquiry mailbox or complaints email addresses

119. The IMS system has enabled real improvements in the handling of allegations received from the public. It has allowed auto-routing and tracking and provided a simple way for the public to submit information to the Home Office. Problems occur however when allegations are received by other parts of the business and in particular when allegations are received via the public enquiry mailbox or the complaints route. This was raised with us several times and we were shown two examples where an allegation with time critical information did not reach the Border in time. The first had come in via the Home Office private office mailbox and the Home Office public enquiry mailbox. The allegation, warning of the imminent arrival of a passenger who posed a risk, took the following route and demonstrates that even though all units acted within the two day SLA, there was a delay in the information reaching the Border.

Date / Time received	Who	Action
Saturday 20 September 2014 22:07	Private office (External) and public.enquires@homeoffice.gsi.gov.uk	No action. The public enquiries inbox is managed by Direct Communications Unit (DCU). DCU is not an operational team and is staffed Monday – Friday.
Sunday 21 September 2014		No Action (as above)
Monday 22 September 2014		No Action (this is first day that DCU would have been forwarding cases received from public enquiries inbox).
Tuesday 23 September 2014		No Action
Wednesday 24 September 2014	DCU	Forwarded to DMC (Croydon) "*The email below is forwarded from our mailbox for your attention*."
Thursday 25 September 2014		No Action
Friday 26 September 2014 13:32		No action
Friday 26 September 2014 13:32	DMC (Croydon)	Central Referral Team

Date / Time received	Who	Action
Friday 26 September 2014 14:16	Central Referral Team	Border Force National Intelligence Hub Cc DMC (Croydon) "*This does not mention any aspect of fraud and corruption relating to HO staff.* *Forwarded to BF intel for info.*"

Table 3 – Processing an allegation

120. We were also shown an example where the complaints email address was sent an allegation on 30 October (Thursday) at 09.37 with details of travel. This was not forwarded until 31 October at 10.49 despite having 'allegation' in the title box.

121. Both of these examples are very similar to what happened in Mrs A's case and highlight the need for all units that receive electronic communications from the public to have some 24/7 capability and also to have systems in place that forward time critical allegations promptly.

Recommendation 13

That all units listed on the website that receive electronic communications from the public have a 24/7 service that is able to screen correspondence for time critical or high harm allegations to enable these to be actioned promptly.

122. A further issue with electronic correspondence is that although there is an audit trail for its receipt and an audit trail showing when it is forwarded, there is no way of telling when an allegation is NOT forwarded. There needs to be some mechanism for checking that allegations are being forwarded. A secret customer approach could be one means of doing this.

Recommendation 14

That Border Force and Immigration Enforcement have some means of checking that allegations received via the public enquiries mailbox or complaints emails get to the appropriate unit in an acceptable time.

The Command and Control Unit

123. The purpose of the CCU is to service police forces or other law enforcement agencies when they have inquiries relating to the immigration status of arrested persons. The command and control unit is the only 24/7 IE capability dealing with live information sharing with police forces and other law enforcement agencies on the status of foreign nationals encountered during operational activity. The unit have been in existence since 2006 and are contacted by one national number that is known to police and other law enforcement agencies. The unit does not take calls from the public.

124. Operators have access to a range of databases including immigration case working (CID) and visa and passport systems among others. CCU does not have access to the IMS system and only have limited access to the WI.

125. The CCU service is a real time service that takes between 4000 and 5000 enquiries per week, primarily from police forces and immigration enforcement staff. Approximately 20% of the police calls that they receive are from the police at the roadside. Most police calls will come from custody suites but CCU will also take emails from police and other law

enforcement agencies pursuing investigations where the subject has not been detained. They deal with calls immediately on a call centre basis and handle slower time email requests in between calls. All calls are logged and recorded. There is a quality assurance process in place and all staff have their calls listened to at least five times per month. Staff receive training in immigration enforcement as well as port and casework issues. Training and mentoring can take up to 12 weeks, but it can take up to a year for a member of CCU staff to be experienced in all facets of their role.

Access to the Warnings Index

126. The PHSO made a finding of maladministration because CCU did not pass the information that was on WI to the police. This was looked at earlier in the review and it was acknowledged that in the absence of follow up on watchlist entries, information on the WI could remain hidden, when it could in fact be useful for other purposes. In Mrs A's case the information was critical.

127. Issue of access to WI in the CCU is a contentious one. The PHSO Report was clear that they felt the failure of the CCU to pass to the police the information that was on held the WI about Mr M was a serious omission - and that is accepted. The CCU in particular felt that given that Mr M was in custody, access to the information on the WI about his deception to obtain a visa would have prompted the police to contact their local immigration unit. We were assured that because Mr M was in custody it is likely that the ICE team would have attended the police station and may have been able to establish that Mr M had lied. This could quickly have led to his removal. Instead Mr M was released and although we cannot be certain that he would not have been released had the WI information been passed to the police, it was nonetheless at this point that his criminal behaviour escalated.

128. The reason for the CCU not checking the WI was that they only had access to one (now two) WI terminals. Given the immediate nature of the service provided by CCU this would not allow each operator to check WI - which is usually only checked for refusal/removal, detention and counter terrorism cases. As already outlined, a significant number of calls received in the CCU are from police at the roadside and the separate WI check would mean that the transaction time would be too long and other calls might be missed. The call abandoned rate in the CCU is currently 11% and rising as police referrals continue to grow. (For most of 2013 the call abandoned rate was less than 2%) This is because there are less staff and an increase in the number of calls and their overall complexity. Consideration is currently being given to how best to respond to this increased demand. This needs to be considered in the context of the WI because if staff took more time on calls by accessing the WI, the call abandoned rate would increase even further. It has been suggested that CCU make WI checks on all calls which would mean all operators having access to the WI from their own desk tops.

129. There are however issues with this that will need to be considered. First is cost and space. The WI cannot be run through an existing terminal and that means that all operators will need to have a separate WI terminal on their desks. Secondly, should access to the WI be given to CCU, the information cannot always be passed to the police without a check. For reasons that are outside the scope of this review, information from the WI often cannot be passed to a third party without checking first with the data owner. The workload for CCU staff would significantly increase if they had to do this.

130. In order to assist in this decision CCU managers looked at 1000 random sample of cases which CCU dealt with during October 2014 to see how many of the cases did have information about them on the WI. The sample identified that a quarter of the cases did have WI entries. Despite this, since much of the WI information was duplicated on CID/CRS which CCU operators have access to no decisions made would have been changed if CCU operators accessed the information on the WI. This does suggest that the costs of making WI

more widely available and the impact on transaction time in completing individual checks would not merit its installation. Given the impact in Mrs A's case however, and the finding of maladministration by the PHSO, further investigation of the issue is warranted.

Recommendation 15

That a further investigation be made of the benefits of giving watchlist access to the Command and Control Unit. This should include analysis of a sample of CCU cases but should also look at the costs of implementation.

Watchlist & Information Control Unit

131. The Watchlist & Information Control Unit is the central until that controls the use of the WI. It also houses the cross check facility (run by Immigration Checking and Enquiry Services) which is the process by which visa applicants to the UK are checked against the WI.

132. For reasons that are outside the scope of this review the number of staff who can make an entry on the WI directly is limited to ensure that the data being input is entered correctly and does not impact any other data owners entries. Should an intelligence or other unit wish to put an entry on the WI they must fill out a template form and submit it for manual entry onto the system.

133. In Mrs A's case a template was completed by the Heathrow Intelligence Unit, but key pieces of information provided by Mrs A were not included on the form. Additionally Heathrow Intelligence Unit did not telephone the port to alert them to Mr M's imminent arrival. Despite incomplete details on the template, the information relating to Mr M was circulated to the border 30 minutes after it had been received. It was unfortunate that this was too late to stop Mr M re-entering the UK.

134. The WI will be the main barrier to Mr M returning to the UK once he has been deported. There is a link between CID, the immigration data base, and the WI which means that where a foreign national is imprisoned in country or served with illegal entry papers and CID is updated, there is an automatic update to the WI. In the case of Mr M, this means that all his conviction data and the fact that he was served illegal papers is now on the WI. If he tried therefore to come to the UK (either with or without a visa) he would be flagged at the border and refused entry. Any visa application would be automatically refused. Additionally, his biometrics would be matched against IDENT1 which would provide a further reason for visa refusal.

135. Currently WI checks are performed at the Border on all passengers entering the UK.

136. In terms of cross-check, one noticeable omission was that visa applicants are not checked against the IMS system as visa issuing centres do not have access to IMS. The IMS contains a range of information that might, if used correctly and carefully, be useful to ECOs in making their decision.

Recommendation 16

That a pilot is carried out that checks visa applicants against the Intelligence Management System to see if there is value in doing this on a larger scale.

Allegations received by telephone

137. There are three telephone numbers that the public can use to make an allegation to the Home Office. These include the Immigration Enforcement hotline, Crimestoppers, and the Customs Hotline.

138. The Customs Hotline is currently manned by HMRC National Co-ordination Unit (NCU) as part of a shared service agreement with Border Force. Border Force rely on HMRC NCU identifying information relevant to Border Force and entering it onto an Intelligence Report that is passed to them.

139. Both Crimestoppers and the Immigration Enforcement hotline operate the same system. Information they take from the public is entered onto an intelligence report that is routed to the NAT who create a case on IMS.

Checks on foreign national arrested in the UK

140. When Mr M was arrested on 7 April 2011 by police they did not check if he had a criminal record in Canada. They contacted the CCU and were told by them that he had a valid visa. The family claim, not unreasonably, that this gave Mr M a legitimacy that would not have been afforded to a British Citizen whose criminal record and fingerprints would have been checked on arrest.

141. At the time of Mr M's arrest it would not have been common practice for police to check the overseas criminal records of foreign nationals arrested in the UK. Since 2011 however there have been significant improvements in this area through the work of ACRO and Operation Nexus.

ACPO Criminal Records Office (ACRO)

142. ACRO was established in 2006 to help organise the management of criminal record information and improve the links between criminal records and biometric information.

143. ACRO manages the International Criminal Conviction Exchange (ICCE) Portfolio which is aimed at exchanging criminal conviction information with other countries. In terms of the EU this means that notifications are sent to other EU Member States by ACRO when their nationals are convicted of criminal offences in the UK. Similarly, ACRO receives notifications when UK nationals are convicted of criminal offences in other EU states.

144. ACRO will also respond to requests from other EU Member States, with criminal convictions of UK nationals who are subject to criminal proceedings in other EU Member States, so these can be taken into account on sentencing. Information is exchanged via the European Criminal Records Information System (ECRIS) which was established in April 2012 to achieve an efficient exchange of information on criminal convictions between EU countries. The system gives judges and police access to comprehensive information on the offending history of any EU citizen, no matter in which EU countries that person has been convicted in the past.

145. Outside of the EU, ACRO conducts similar criminal record exchanges with non-EU countries via INTERPOL. It is however much more limited.

146. In 2012-13, 16% of the 200,000 foreign nationals arrested in the UK were subject to requests for ACRO checks. In 2013-14 this had risen to 31%. Of the EU requests, which ACRO estimates at about 4,500 a month, approximately 30% are returned with one or more convictions when the EU Member State is able to successfully identify the individual (requests would also include requests for victims and witnesses and recidivists and persons subject to non-criminal proceedings). Police check significantly fewer non-EU arrestees than EU (23% as opposed to 37% nationally) but ACRO have indicated to us anecdotally that they believe the hit rate in percentage terms would be the same for EU and non EU once the individual is successfully identified.

147. Despite the improvements, a criminal records check is not straightforward and although much valid and important information is sent and received via this channel ACRO informed us that there are several issues with these processes. For example,

- A number of high criminality Non-EU countries have limited criminal records infrastructure and obtaining the information is therefore very difficult and unreliable.
- The purpose of the request is important and although all EU Members States are legally obligated to respond to requests for criminal proceedings they are not obliged to respond to requests for purposes other than criminal proceedings, for example immigration.
- The exchange of criminal records information between EU Member States is underpinned by EU legislation. This mandates that all EU Member States must respond to requests for conviction information for criminal proceedings within 10 days of the receipt of the request. The exchange of criminal records information between Non-EU countries is carried out through the Interpol Protocols on a Police to Police basis and there is no legislation underpinning this. Therefore countries do not have to respond to requests for criminal records information and there are no set timescales for countries to respond. ACRO and the Home Office are working very closely with high priority Non-EU countries to establish bi-lateral information sharing agreements to improve the exchange of criminal records information with the UK.

Operation Nexus

148. Operation Nexus is an operational and intelligence partnership between Immigration Enforcement (IE) and the Police Service that aims to remove offenders who are foreign nationals from the UK. Along with London, a Nexus operating model has been implemented in the West Midlands, Manchester, Merseyside, West Yorkshire, Cleveland, Cheshire, Kent and Wales forces with an adapted format operating in Scotland.

149. Since its inception, Operation Nexus has helped to enable the removal of over 3000 offenders who are foreign nationals from the UK. This Includes 191 individuals who were classed by police as being High Harm[4]. Operation Nexus has now been rolled-out in ten police forces with plans to expand across the UK. The police are now using a range of immigration interventions, including making better use of local ICE teams and the IE 24/7 Command and Control Centre. Additionally in appropriate high harm and repeat offending cases referred by police colleagues, Immigration Enforcement seek to utilise revocation of visa and deportation solutions to foreign national offending.

150. The Metropolitan Police have issued instructions to all of their Custody Suites that if any foreign national are arrested for a chargeable offence, an ACRO check must be made for overseas convictions.

151. Immigration Enforcement Officers are now assigned to 16 of the Metropolitan Police custody suites with a central function (Joint Operations Command) overseeing a hub and spoke function to cover other London Police stations. Out of core hours police are instructed to utilise the service of the Manchester based Immigration Command and Control Unit which gives coverage and response for police queries.

---

[4] **Definition of a high harm person**

A person is considered to be high harm for one or more of the following reasons. Their:

- presence in the UK increases the risk of real and immediate, significant physical harm to person(s)
- presence increases the risk of significant damage to property, or
- entry to the UK is likely to cause significant harm to the reputation of the UK and/or the Home Office.

This includes people who have, or are being considered for:

- a deportation order, or
- an exclusion order.

Schengen

152. Another crucial part of strengthening data sharing on criminality is the UK's connection to the Second Generation Schengen Information System (SIS II). This system lists all outstanding European Arrest Warrants and persons reported missing as well as other information on people and property. We expect the UK to join SIS II in January 2015 which will allow us to go live in March 2015. This will allow the UK to extradite people in the UK on European Arrest Warrants (EAW) of whom we are currently unaware. It will also allow the UK to apprehend those wanted in other EU jurisdictions. This is not relevant in Mr M's case but would be relevant to an EU national who was in the UK or was trying to enter the UK and was wanted in another EU country.

Summary

153. It was clear from our review that there have been many improvements in intelligence handling since the allegation made by Mrs A. The reports by the Independent Chief Inspector of Borders and Immigration support these findings. The staff that we spoke to where all aware of the importance of their work and the need to deal with things promptly and carefully.

154. Despite this there is still the opportunity for 'dropping the baton' when an allegation moves from within one part of the Home Office to another. Perhaps as a result of having been a separate organisation up until 2012, an attitude of 'that is not ours' was sometimes observed. This mentality contributed to the breakdown in allegation handling in Mrs A's case and although there is no empirical evidence to support the finding it should be noted that this could remain an issue.

155. The Home Office Transformation Programme recognises that these cultural problems still exist within the organisation and the need to learn from mistakes. The Transformation Programme is putting great emphasis on individuals taking responsibility, getting things right the first time and being proud of the work that they do. They emphasise consistency of performance, making sure that service standards, targets and commitments are met consistently.

156. The Home Office is also keen that the organisation learns from its mistakes and has consequently set up a series of lessons learned seminars to ensure that implications and direction from investigations and enquiries are fully understood. Given the serious harm that was committed against Mrs A's family the Home Office should incorporate the findings of this review into the Lessons Learned programme.

Recommendation 17

That the findings of this review are incorporated into the Home Office lessons learned programme and offer a series of seminars to staff outlining the issues and direction for how such a case can be avoided in future.

Section 3 – PHSO Recommendation 3

157. Review of the Home Office's current processes for capturing correspondence on receipt; for acknowledging correspondence; for sending it to the relevant team for action; for tracking the action taken in response to correspondence; for ensuring that the action is complete and good enough; and for retrieving the correspondence for later queries or investigations.

158. The Review should take explicit account of Mrs A's family's experience and of the PHSO findings of maladministration. The Home Office should give the Review appropriate funding and publish its outcome, including its recommendations for action, within six months of the date the PHSO report was published.

Overview of Section 3

159. The finding of maladministration in relation to the Home Office related to two streams of correspondence. First were the two letters that Mrs A wrote to the Home Office on 15 November 2010 and 25 November 2010. Although the Home Office had receipt of both letters, no action was taken on either. The PHSO therefore commented;

"We found it astonishing that two letters, each giving enough information for the Home Office to identify Mr M in their records, were not acted on at all. The letters vanished almost without a trace in the Home Office. With them, the Home Office lost two chances to put right their earlier mistakes. The mishandling of [the] letters undermined their ability to meet their public commitments to secure the border and pursue people who flout immigration law."

Following Mr M's arrest there was a further extensive series of correspondence which the PHSO concluded constituted maladministration. In involved various officials. Some correspondence was not responded to and some was responded to inappropriately. The PHSO commented;

"They [The Home Office] have kept no unified record of their dealings with Mrs A, but have maintained separate records in different parts of the organisation without identifying a 'single point of contact' for her and her family. Cumulatively the Home Office's complaint handling was…maladministration."

Types of correspondence received by the Home Office

160. The Home Office receives the following types of correspondence.

- MPs' correspondence (where an MP writes to a Minister of Secretary of State)
- Complaints
- Correspondence sent to the Department addressed to a named Minister or Official (Treat Official)
- Correspondence sent to the Department but which is not addressed to a named individual. (Treat Official – although UKVI use a different definition)
- Correspondence that is marked for a specific individual or unit. (This type of correspondence, which is often related to specific customer queries on applications, is not dealt with in this review.)

With the exception of the last category, Mrs A's case included all of these correspondence types.

How correspondence is organised in the Home Office

161. There are leaflets available at various locations such at airports, explaining to the public how to complain or correspond with the Home Office and there are explanations on the www.gov.uk website. The website lists three email addresses the public can contact and three addresses. The public enquiries email is given as the address for general contact and has a corresponding address in Marsham Street. A separate email is given for complaints about Border Force with an address in Dover and a third email address for complaints about UKVI gives a corresponding address in Croydon.

162. There are two IT systems that deal with correspondence. The correspondence tracking system (CTS) and the Complaints Management System (CMS).

163. The diagram below shows how the correspondence system works and shows that the Home Office has two main units for dealing with its large volume of correspondence that does not go to individual or specific units. They are the Direct Communications Unit (DCU) and the Central Point of Receipt. (CPR)

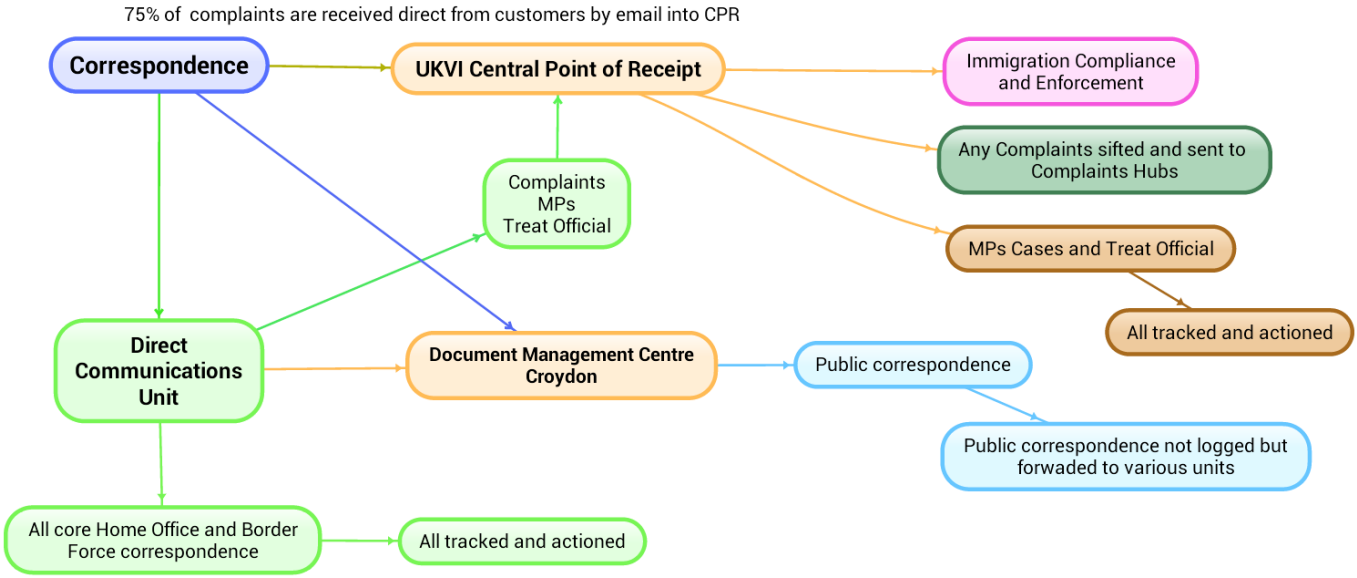

Figure F - Handling of correspondence

Direct Correspondence Unit

164. The DCU is the point of receipt for everything that comes into Marsham Street or via the public enquiries email. The DCU will record, action and track all information that relates to the core Home Office. They will forward all other correspondence received to the UKVI Central Point of Receipt in Croydon (CPR), who are responsible for logging and allocating correspondence for UKVI, IE and Border Force

165. Tracking by DCU is on the CTS. They will put on the system all correspondence received electronically or by mail (scanned in) that relates to the core Home Office. There are occasionally items of correspondence that may be sensitive that would be dealt with outside the CTS system.

166. With the exception of MPs' correspondence, DCU do not put correspondence that is forwarded to CPR on CTS. MP's correspondence for UKVI, IE and Border Force is logged

onto CTS by DCU on behalf of the UKVI team, if it is received in Marsham Street or via the public enquiries inbox.

167. Correspondence received electronically is forwarded to CPR electronically. Mail is sent on to them in hard copy via a bagging system.

168. With the exception of the correspondence that is forwarded, DCU respond to all mail. Email is responded to by email and later by letter.

169. DCU deals annually with approximately 7,000 MPs' letters and 8,000 Treat Official letters for core Home Office. In addition they scan c6,500 MPs' letters onto CTS for UKVI, IE and Border Force and forward a further c25,000 emails and 8,000 letters to the UKVI CPR.

170. A team within DCU is responsible for answering Border Force correspondence (although it is logged onto systems and allocated by the UKVI team). This may seem an anomaly. The reason DCU deals with Border Force correspondence and not other operational units is because when UKBA separated from Border Force it became part of the core Home Office. At a subsequent date the remainder of UKBA was brought into the Home Office but their correspondence remained separate and the Border Force team has remained with DCU. For this reason UKVI CPR does in fact include both UKVI and Immigration.

171. Service standards for DCU responses are 15 days, which is shorter than the standard used by UKVI CPR which is the Cabinet Office's target of 20 working days, the same as Border Force.

172. If DCU receive an allegation similar to one in Mrs A's case that related to a visa they would forward it to UKVI CPR in Croydon. DCU does not differentiate between allegations that relate to Border Force, such as a dangerous person attempting to enter the country and allegations that are for UKVI or IE. They would forward all allegations to CPR.

173. DCU works 9am to 5pm Monday to Friday. They have a 48 hour standard to log correspondence or forward it on. Calculation of the 48 hours for correspondence received over the weekend begins on Monday. This means that correspondence received after close of business on Friday could be logged or forwarded anytime up to 9am on Wednesday and remain within the service standard.

174. The CTS is ten years old and the review were told it is a good although progressively antiquated system. A new system is in its final stage of development; this will combine the CTS with the other systems that monitor Parliamentary Questions and Freedom of Information requests. Whilst the principles of answering correspondence and the channels through which it is managed remain the same, the new system will provide a modern and streamlined platform to track and manage official correspondence across a single IT system.

175. Retrieval of correspondence can be done simply once correspondence is on the CTS system and can show details of action taken or outstanding.

UKVI - Central Point of Receipt (CPR)

176. All correspondence for UKVI, Immigration Enforcement and Border Force is received via the Central Point of Receipt, (CPR) based in Croydon. Correspondence into central point of receipt comes from five sources.

    a. Correspondence forwarded from DCU electronically and also mail directed from DCU by internal mail.

    b. Complaints that come directly from the UKVI complaints email address listed on the gov.uk website and complaints that come in via mail.

    c. Correspondence and emails from MPs offices to Responder Hubs and MP Account Managers in UKVI

d. Other correspondence that other parts of the business redirect using the internal mail.

e. Other mail that comes from the Lunar House post room that is not distributed to other parts of the business.

177. CPR's work is divided between MPs' correspondence/emails, complaints, Treat Official correspondence, Further Actions (following up a telephone conversation to an MPs' office), Changes of Customers' addresses and legal representatives and public correspondence.

Complaints handling by CPR

178. In terms of in-country complaints CPR enters those they receive onto the Complaints Management System (CMS) and allocate them to Responder Hubs. There are four responder hubs for dealing with complaints – Sheffield, Croydon, Solihull/London and Liverpool, reflecting the old regional UKBA picture. These hubs are then responsible for responding to these service complaints within the target 20 days. The diagram below summarises this process.

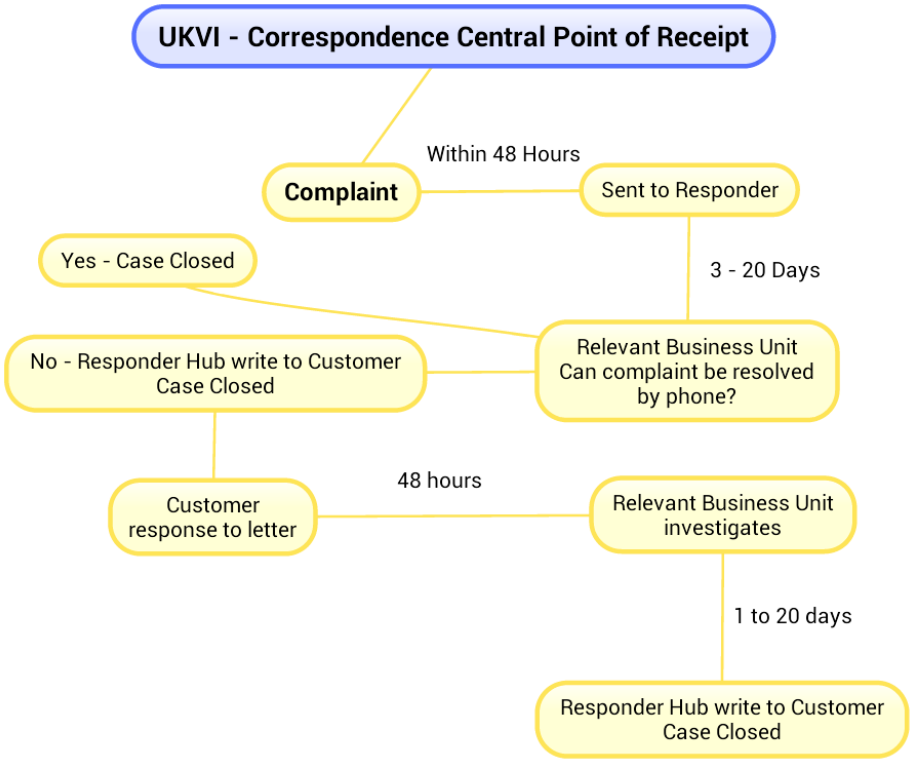

Figure G, Handling of complaints

179. In 2013 UKVI received 15,151 in-country complaints, of which
- 93% were service related,
- 6% minor misconduct and
- less than 1% serious misconduct.

The main topics were:
- delay (53%),
- admin or process errors (30%) or
- poor communication (28%).

The majority of these complaints (75% in November 2012 to October 2013) were received via email.

180. Complaints on CMS are tracked both whilst they are within the target service level and when they are out of the target service level, with backlogs being monitored.

Handling of correspondence by CPR

181. The Central Point of Receipt also receives UKVI and IE correspondence other than complaints.

182. The definition of Treat Official used by CPR is different from that used by DCU. DCU in line with other Government Departments, regard Treat Official as any correspondence sent to the Home Office from the public, regardless of whether or not it is addressed to a named person (e.g., the Secretary of State). CPR and therefore UKVI only regard Treat Official as correspondence addressed to a specific list of people, e.g., the Permanent Secretary or the Home Secretary.

183. Treat Official correspondence is logged and tracked via an excel spreadsheet. CPR are currently in the process of moving the tracking of Treat Official correspondence onto the CMS system so that it can be tracked alongside complaints. Currently CPR need to rely on those staff allocated correspondence to report whether or not they have dealt with it. Moving onto CMS will allow CPR to see the actions that have taken place, including copies of replies. At the moment they do not have that capacity.

184. Correspondence that is not a complaint and which is not designated as Treat Official is classed as public correspondence by CPR. Public correspondence is not logged by CPR or UKVI post rooms and is forwarded to other parts of the business without record. Since there is no logging it is not possible to say what the quantity of this is, but staff at CPR estimated it is probably in the region of 60,000 emails and letters per year. The one exception to this is passports and cheques, where a manual log is kept of what is forwarded and to whom.

185. It is estimated that CPR only receives about 8% of the post that comes into the former UK Border Agency (UKVI, Immigration Enforcement and Border Force) and the 60,000 figure needs to be seen in that context. The UK Border Agency was previously a regional structure and although it has now been brought under the umbrella of the Home Office many of the regional structures remain for incoming post. There are post rooms dealing with large amounts of correspondence outside of London which do not track public correspondence and they may be adopting similar practices. The figures quoted for untracked correspondence could be significantly higher.

Receipt of correspondence

186. It is clear from the review of both DCU and UKVI CPR that they are handling large volumes of correspondence and that the systems they are using are not consistent. DCU logs and replies to all correspondence whereas CPR does not use the tracking system. It also forwards large quantities of mail unlogged. The diagram below shows the difference in procedure and how they work together.

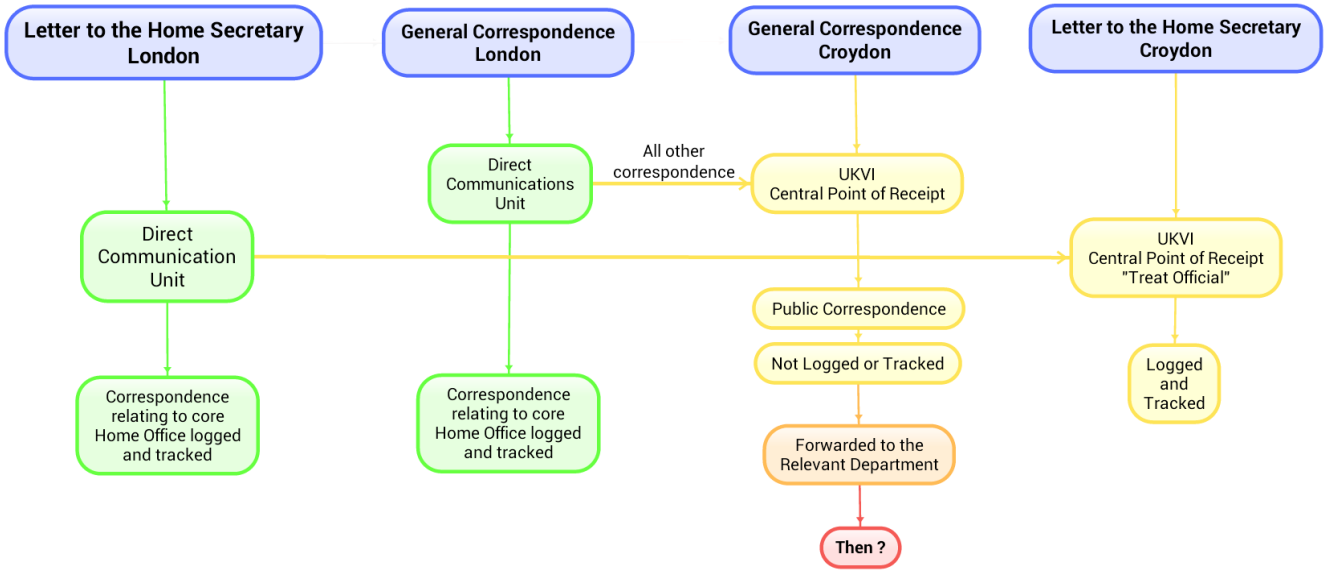

Figure H - Systems in London and Croydon for dealing with correspondence

187. The IMS system has contributed to a huge improvement in handling allegations and that was addressed with in the previous section but what the system does not do is pick up allegations that are delivered by post. An allegation received by post in the DCU would most likely be sent by hard copy to Croydon, even if it were addressed to the Home Secretary. Being addressed to the Home Secretary it would be regarded as Treat Official in Croydon which means it would be logged. An allegation that was not addressed to any particular Unit or individual and sent to London would be forwarded to Croydon. Croydon would then open it and forward it on unlogged and untracked.

188. The public cannot be expected to distinguish between an allegation, a contact and a complaint. Indeed when Mrs A submitted her allegation she headed it *Complaint that the UKBA had allowed a dangerous man to enter the country*. Whilst different avenues and systems remain for dealing with correspondence, the possibility of an allegation being lost remains.

189. Some staff in correspondence units appeared to assume that the public understood the Home Office systems. In fact one manager commented that 'allegations have their own dedicated route' to come into the Home Office, clearly unaware that the public would not know this.

190. Forwarding of mail means that a piece of correspondence can be subject to an SLA twice. Generally within the correspondence system there is a 48 hour SLA for taking action, which includes rerouting. Each time an item is rerouted, it then become subject to the SLA again.

Recommendation 18

That the Home Office examines existing service level agreements for correspondence to ensure that the correct response times are adhered to.

191. In addition to the addresses on the website, a member of the public can submit correspondence to one of many addresses dotted throughout the country. We were not able to establish what processes are in place for handling this correspondence.

192. All correspondence teams are reliant on the post room. There are many post rooms through the Home Office Estate and the review was told that none of them track mail. Mail is moved from one unit to another by sack, unlogged and untracked.

193. It was difficult for the review to make any further inroads into the issues raised about correspondence. There have been reviews in the past that have looked in detail at the issue and 'dip samples' have been carried out to establish if mail is forwarded correctly or stored as backlogs. The Home Office however should establish the current scale of unlogged correspondence and look at options for logging and tracking.

Recommendation 19

The Home Office should review the options for accurately logging and tracking all correspondence received.

Mrs A's dealing with the Home Office between May 2011 and November 2012

194. Many of the units and individuals involved in the correspondence and contact with Mrs A have either been abolished or have left the agency. The review did not feel is would serve any real benefit to revisit the decisions that were taken. Rather to avoid this situation reoccurring, it would be wise to establish a single point of contact for cases similar to those of Mrs A.

Recommendation 20

The Home Office should ensure that where it is acknowledged that a member of the public has a genuine and serious issue with the Home Office they are allocated a single point of contact who can deal with their case.

Glossary

ACPO	Association of Chief Police Officers
ACRO	ACPO Criminal Records Office
API	Advance Passenger Information
BF	Border Force
BFIHT	Border Force Intelligence Heathrow Team
BFNIH	Border Force National Intelligence Hub
BSM	Border Suspect Message
CCU	Command and Control Unit
CID	Case Information Database
CMS	Complaints Management System
CPR	Central Point of Receipt Handling correspondence and complaints for UKVI and IE
CRS	Central Reference System A database of all UK visa applications processed overseas
CTS	Correspondence Tracking System
DBS	Disclosure and Barring Service
DCU	Direct Communications Unit
DMC	Document Management Centre
EAW	European Arrest Warrants
ECO	Entry Clearance Officer
ECRIS	European Criminal Records Information System
EEA	European Economic Area
EU	European Union
FE	Further Education
GGFR	General Ground for Refusal
HMRC	Her Majesty's Revenue and Customs
IABS	Immigration Asylum Biometric System
ICCE	International Criminal Conviction Exchange
ICE	Immigration Compliance and Enforcement
IDENT1	UK National Fingerprint Database
IE	Immigration Enforcement
IMS	Intelligence Management System

MP	Member of Parliament
MPS	Metropolitan Police Service
NAT	National Allegations Team
NBTC	National Border Targeting Centre
NCA	National Crime Agency
PCP	Primary Control Point
PHSO	Parliamentary and Health Service Ombudsman
PNC	Police National Computer
RALON	Risk and Liaison Network Overseas
SIS II	Second Generation Schengen Information System
SLA	Service Level Agreement
UKBA	UK Border Agency
UKVI	UK Visa and Immigration Department
WI	Warnings Index