Independent Chief Inspector of Borders and Immigration

An inspection of the Intelligence Management System

February-April 2014

John Vine CBE QPM

Independent Chief Inspector of Borders and Immigration

An inspection of the Intelligence Management System

February-April 2014

Presented to Parliament pursuant to Section 50 (2) of the UK Borders Act 2007

October 2014

This publication is available at www.gov.uk/government/publications
Any enquiries regarding this publication should be sent to us at

Independent Chief Inspector of Borders and Immigration,
5th Floor,
Globe House,
89 Eccleston Square,
London, SW1V 1PN.

Email: chiefinspector@icinspector.gsi.gov.uk

All Independent Chief Inspector of Borders and Immigration inspection reports can be found at:
www.independent.gov.uk/icinspector

Print ISBN 9781474111638
Web ISBN 9781474111645

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

ID 15101403 10/14

Printed on paper containing 75% recycled fibre content minimum

Our Purpose

We provide independent scrutiny of the UK's border and immigration functions, to improve their efficiency and effectiveness.

Our Vision

To drive improvement within the UK's border and immigration functions, to ensure they deliver fair, consistent and respectful services.

Contents

Foreword from John Vine CBE QPM	2
1. Executive Summary	3
2. Summary Of Recommendations	5
3. The Inspection	6
4. Inspection Findings – Operational Delivery	9
5. Inspection Findings – Safeguarding Individuals	21
6. Inspection Findings – Continuous Improvement	25
Annex 1 - Role & Remit Of The Chief Inspector	27
Annex 2 - Glossary	28
Acknowledgements	30

Foreword from John Vine CBE QPM
Independent Chief Inspector of Borders and Immigration

My 2011 report[1] looked at the way in which the then UK Border Agency used intelligence to prevent and detect immigration and customs offences. I was pleased to find that, in response to this, the Home Office had developed and implemented an Intelligence Management System to record and process these allegations. In 2013, over 75,000 allegations were added to this system, which by the end of February 2014 had resulted in over 4,000 arrests and almost 1,000 removals.

This system already provides clear benefits by enabling the collection and analysis of allegations to develop intelligence, inform strategy and direct operational enforcement and caseworking activity. However, I found that more could be done to improve the quality of data entry and to make better use of the advanced search facility, which would result in improved case management and lead to better results. There were also issues around the timeliness of the initial assessment of an allegation, with over a third of cases missing the Ministerial target of two days.

I was concerned to find that opportunities to prevent or identify offences may have been missed. A number of the allegations in my file sample could have been investigated but were wrongly categorised as being of no value. In other cases, I identified that ineffective communication between teams and across Home Office Directorates had resulted in valuable intelligence not being used appropriately. The Home Office must ensure that the value of information contained within allegations to various parts of the business is recognised and that any action taken is appropriate.

I have made four recommendations for improvement.

John Vine CBE QPM
Independent Chief Inspector of Borders and Immigration

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

1. EXECUTIVE SUMMARY

1.1 The Intelligence Management System (IMS) is a Home Office database used for recording and processing allegations concerning immigration or customs offences. These allegations may originate from the public, through stakeholders such as Crimestoppers, or from Home Office staff.

Positive Findings

1.2 Until the introduction of the IMS in September 2012, there was no system in place to centrally record allegations from the public and assess their value in terms of combating immigration and customs offences. The IMS now provides a centralised database for all incoming allegations, which can be accessed by users nationwide. Its creation is a positive step and in line with recommendations from my 2011 report on intelligence.

Its creation is a positive step and in line with recommendations from my 2011 report on intelligence

1.3 In 94% of cases in our sample (15), where the Home Office took action after receiving an allegation, we considered that the action taken was appropriate. In the small number of cases where operational activity led to an arrest (three), we found that the allegation had contributed to the Home Office targeting individuals whom they had a realistic prospect of removing.

1.4 IMS users were able to take action quickly when necessary, once an allegation had been initially assessed. This resulted in effective operational work, such as the disruption of a sham marriage ceremony and checking an incoming flight manifest for the arrival of an alleged offender.

1.5 After completing relevant background checks on Home Office systems, IMS users were able to identify that seven of the alleged offenders in our sample of non-actionable cases had valid leave to remain and to correctly close the case.

1.6 Regular upgrade work has improved the functionality of the IMS. In August 2013 an advanced search function was added, enabling users to search within the system for allegations which might be connected and might enhance the overall intelligence picture. Furthermore, the public could submit allegations directly (via an online form) for the first time. Planned upgrade work during the summer and autumn of 2014 will further enhance IMS functionality. This will include making the public on-line form more user-friendly and will enable IMS managers to produce more accurate performance reports from the system.

Areas for Improvement

1.7 In order for the information contained within the IMS to be of real value, it is important that, after it is disseminated to the relevant team, appropriate action is taken. However, we found examples where the receiving team had failed to act appropriately on IMS information. The Home Office therefore needs to put more effective processes in place to support joint working across teams and Directorates.

However, we found examples where the receiving team had failed to act appropriately on IMS information

1.8 We found that the details of allegations were not being routinely cross-checked against the information already on the IMS. In one category in our file sample (NFA[2] actionable cases), we found that almost a quarter were duplicates of others already on the system, but this had not been identified by the IMS user.

1.9 Management information taken from the IMS was limited and produced unreliable performance reports. For example, over a third of actioned cases in our sample had been categorised incorrectly. In another category (NFA actionable cases), we found that only four out of 25 cases (16%) had been categorised correctly, which in turn produced unreliable and inaccurate management information regarding case outcomes.

Management information taken from the IMS was limited and produced unreliable performance reports

1.10 A substantial number of the 125 allegations we sampled contained such limited information that there was little the Home Office could do to progress them. This affected half of the cases in the NFA non-actionable category in our sample (25 cases). However, in almost half (12) of the remaining 25 cases in this category we found no evidence that any background checks had been conducted on Home Office systems, despite the fact that either an address or full name of the alleged offender had been provided. This needs to be addressed promptly to ensure that informed decisions are made as to whether or not to progress received allegations in all cases.

1.11 Once again, we found significant issues with data quality. The information contained within allegations must be added to an electronic form in order to generate results via an advanced search on the IMS. This electronic form had not been completed correctly in 35 cases (28% of our overall sample). Furthermore, in 14 of 38 cases (30%) where the source of the allegation submitted their details, these details were not added to the electronic form and again would not be identifiable through this search function. This could seriously undermine the ability of the National Source Unit (NSU) to mitigate source risks, as associated cases from the same source would not be identified.

1.12 A Ministerial target of two working days exists for the initial processing of all allegations. We found that the Home Office had failed to adhere to this in over a third of the cases in our overall sample of 125 cases (39%). This led to some time-critical allegations not being assessed until it was too late to take preventative action.

1.13 Although we were told that all cases were checked by a compliance officer prior to an outcome being prescribed, we only found evidence that any management assurance process took place in 14% of our sample (18 cases). Quality assurance processes are crucial in ensuring that allegations are processed effectively and progressed in appropriate circumstances and that the information retained on the IMS is complete and recorded correctly.

We only found evidence that any management assurance process took place in 14% of our sample

1.14 In general, staff demonstrated limited knowledge of the relevant guidance and legislation that affected their area of work regarding managing source risks. This led to inconsistent practices in relation to contacting sources for further information and referring potential source risks to the National Source Unit.

2 No further action.

2. SUMMARY OF RECOMMENDATIONS

We recommend that the Home Office:

1. Ensures that all allegations are properly assessed, by:
   - adding all the information contained within allegations (including in attachments) to the electronic form on the IMS;
   - conducting relevant background checks on Home Office systems;
   - cross-checking the details of allegations using the advanced IMS search facility; and
   - classifying them appropriately by attributing the correct outcome.
2. Ensures that IMS users recognise the value to other parts of the business of information contained within allegations and take appropriate action to communicate this effectively.
3. Conducts the initial assessment of all allegations within the target timescales agreed by Ministers.
4. Provides all intelligence staff with adequate training in handling sources.

3. THE INSPECTION

Purpose

3.1 This inspection examined how effectively the Intelligence Management System (IMS) captured and recorded information relating to allegations made about immigration or customs offences (such as residing in the UK without valid leave to remain or drug-smuggling). It considered how this information was then progressed to inform operational activity, specifically examining whether the IMS:

- • effectively captured and recorded all allegations;
- • was administered effectively and cases were processed correctly;
- • was utilised successfully to inform intelligence packages and operational activity; and
- • handled information responsibly and protected the personal details of individuals providing information (commonly referred to as the source).

Background

3.2 The Intelligence Management System is a tool for recording and processing allegations concerning immigration or customs offences. One of the key drivers for the development of the IMS was our previous inspection report entitled 'Preventing and detecting immigration and customs offences: A thematic inspection of how the UK Border Agency receives and uses intelligence', published in May 2011.[3] In this report, the Chief Inspector recommended recording the outcome of allegations and assessing how often they led to the development of intelligence and subsequent operational activity to prevent or detect immigration or customs offences.

3.3 As a result, an Allegation Management System (AMS) was launched in September 2012, allowing all allegations from the public, as well as referrals from staff across the Home Office and other partners such as local authorities and other government departments, to be recorded centrally. The AMS was upgraded and re-released in August 2013. This upgrade included an online form for the public to use to report allegations directly. Its name was changed to the IMS to more accurately reflect the types of information received, as not everything related specifically to an allegation of an offence.

Process

3.4 Submissions to the IMS can be made by a number of communication methods. Those entered via the online form are automatically routed to the appropriate Regional Intelligence Unit (RIU),[4] based upon the postcode in which the alleged offence is taking place. However, the exception to this was London, where, due to the volume of work, a specialist team assesses the information prior to dissemination to one of the five Intelligence Units based in London.Allegations received by post or using the online form that do not contain sufficient detail regarding the location of the alleged offence are sifted by the National Allegations Team (NAT), added to the IMS and forwarded to the appropriate RIU. Submissions by post, telephone, email or fax are also accepted by the IMS. These allegations can be received directly into the RIU who will handle the case, who will either action or

3 http://icinspector.independent.gov.uk/wp-content/uploads/2011/02/Preventing-and-detecting-immigration-and-customs-offences.pdf
4 There are 19 of these throughout the UK divided into four regions: North, South, London and Central (including Scotland and Northern Ireland).

reallocate to a more appropriate RIU if required.

3.6 Information exists within the IMS on an electronic form, which mirrors the online form used by the public to submit information. Therefore, regardless of how the information is received, everything is stored electronically and there is no requirement for paper files.

Outcomes

3.7 Guidance for IMS staff states that every IMS case must be concluded into one of three categories. They are:

- Actioned – referred to an intelligence team to progress;
- No further action (NFA) actionable – enough information has been provided to action the case, but there is not sufficient priority to justify any further action; and
- No further action (NFA) non-actionable – often due to duplication or not enough information provided to progress the case further.

Service Standards

3.8 The IMS has a Ministerial target to initially assess all incoming information within two working days. In addition, differing service standards exist for the processing and development of this information, depending on how it has been prioritised. All incoming information is assessed and assigned a rating, dependent on risk. These ratings are set out in a Service Level Agreement and require appropriate action[5] to be taken:

- immediately;
- within four hours;
- within 48 hours; or
- within 30 days (the majority of ratings are set at 30 days).

3.9 In 2013, over 75,000 allegations were added to this system, which by the end of February 2014 had resulted in over 4,000 arrests and almost 1,000 removals.[6]

Methodology

3.10 This inspection measured the performance of the Home Office against three of the Independent Chief Inspector's inspection criteria under the themes of:

- Operational Delivery – Customs and immigration offences should be prevented, detected, investigated and where appropriate, prosecuted;
- Safeguarding Individuals – Personal data of individuals should be treated and stored securely in accordance with the relevant legislation and regulation; and
- Continuous improvement – The implementation of policies and processes should support efficient and effective operational delivery.

3.11 To aid the on-site phase of the inspection, we conducted:

- a familiarisation visit to the National Allegations Team in Croydon to observe how it processed allegations onto the IMS system;

5 Research to be conducted and the development of the information.
6 Further arrests and removals may arise as a result of ongoing operational work.

- an examination of documentary evidence including management information, performance figures, guidance, targets and risk registers; and
- a file sample of 100 cases added to the IMS in September 2013, broken down into the following categories:

– 50 NFA non-actionable;

– 25 NFA actionable; and

– 25 Actioned;

- a further file sample of 25 cases added to the IMS in January 2014 in the category: NFA non-actionable.[7]

3.12 The file sample contained a greater number of cases from the NFA non-actionable category because the vast majority of allegations received this outcome. In addition, the inspection intended to explore whether all potentially useful information from these allegations was being developed appropriately and taken forward by the Home Office when necessary.

3.13 The on-site phase took place between 24 February and 6 March 2014. We undertook inspection visits to South London, Central London and Solihull to observe administrative processes and assess how Regional Intelligence Units in these locations progressed IMS cases. We conducted interviews and focus groups with a range of staff at these locations, as set out in Figure 1.

Figure 1: Home Office staff interviewed (by grade)	
Director (Grade 5)	1
Deputy Directors (Grade 6)	1
Assistant Directors (Grade 7)	3
Senior Executive Officer (SEO/HMI)	2
Higher Executive Officer (HEO/CIO)	6
Executive Officer (EO)	4
Administrative Officer (AO)	6
Administrative Assistant (AA)	1
Total	**24**

3.14 We provided feedback on high-level emerging findings to the Home Office on 18 March 2014. The inspection identified four recommendations for improvement.

3.15 The final version of this report was submitted to the Home Secretary on 30 May 2014.

7 We undertook an additional file sample because we established that the IMS had only been introduced very recently during the time period of our original sample.

4. INSPECTION FINDINGS – OPERATIONAL DELIVERY

Customs and immigration offences should be prevented, detected, investigated and where appropriate, prosecuted

4.1 The Home Affairs Committee, in its March 2014 report into the work of the immigration directorates,[8] questioned why less than 3% of allegations recorded on the IMS led to a removal. The committee noted that, as an entire unit was in place to process these allegations, it considered these results were poor. We assessed how effectively the Home Office was processing cases added to the IMS (hereafter referred to as allegations). We achieved this by undertaking a random file sample of 125 allegations in order to examine:

The Home Affairs Committee questioned why less than 3% of allegations recorded on the IMS led to a removal

- how efficiently these were processed and concluded;
- the quality of the information retained on the IMS and how this contributed towards building an overall intelligence picture; and
- whether or not the allegation was processed correctly, leading to a reasonable outcome.

Actioned Cases

4.2 The Home Office advised us that most of the cases in the 'Actioned' category would have been actioned and concluded within three months of the receipt of the allegation. We therefore randomly selected 25 allegations made in September 2013, on the basis that any actions taken on these cases should have been completed by the time of our inspection in February 2014. Staff guidance describes the five outcomes that result from an allegation being identified as actionable – Figure 2 refers.

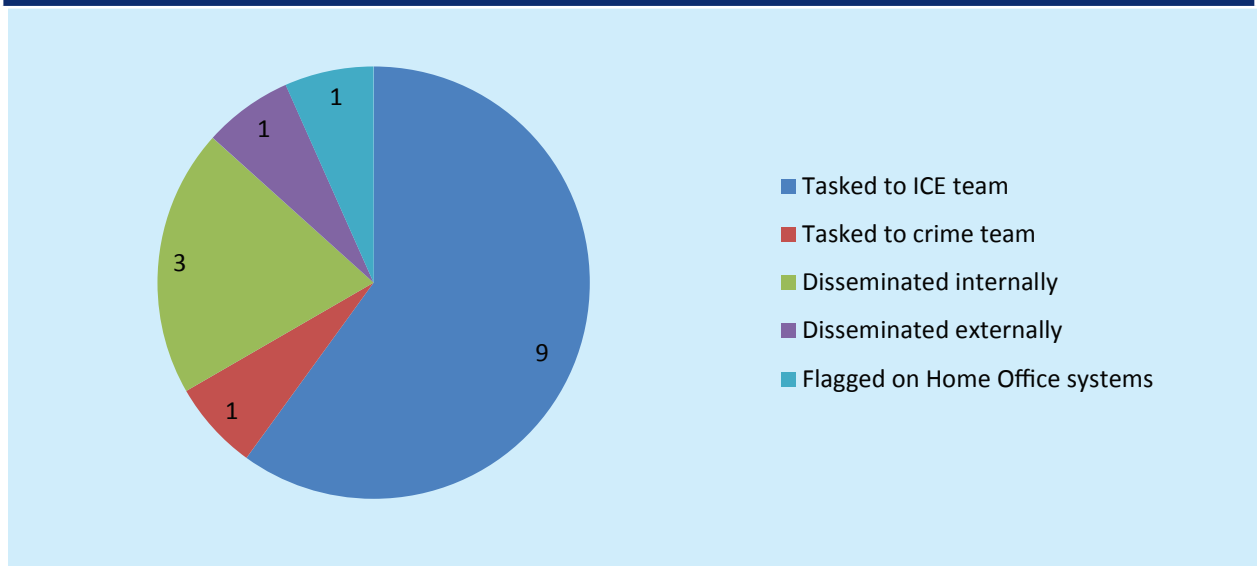
8 http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/820/82004.htm#a12

Figure 2 – Guidance – Actioned cases	
Action taken	**Description**
Tasked to ICE[9] team	Case created on the National Operations Database (NOD)[10] and presented at tasking and/or pre-tasking.
Tasked to crime team	Case created on NOD and presented at tasking and/or pre- tasking.
Disseminated internally	Information shared with another part of the Home Office, e.g. Casework.
Disseminated externally	Information shared with another organisation, intelligence report (IR) created, e.g. Police.
Flagged on Home Office systems	Marker placed on internal system, such as CID,[11] CRS,[12] or WI.[13]

4.3 In just over a third of the cases we sampled (nine cases – 36%) we found no evidence that any of these outcomes had taken place, primarily because the allegations should not have been assigned to this category. This reflected the poor quality of management information which was being provided by the IMS at the time of our inspection. We deal with this issue in greater detail in the section on Continuous Improvement.

4.4 In 15 (94%) of the remaining 16 cases, the actions taken by the Home Office were appropriate. Figure 3 provides a breakdown of the actions taken in these cases.

Figure 3: Actioned cases – breakdown of actions



4.5 Of the nine cases tasked to an ICE team, four resulted in enforcement activity being carried out, which led to three arrests. As of April 2014, none of those arrested had been removed. However, we do not consider that the true value of allegations contained within the IMS should be judged solely on whether or not they contribute directly towards a removal. In these three cases, the Home Office targeted appropriate cases with a good prospect of removal, but were unable to follow this through

9 Immigration, Compliance and Enforcement – operational teams responsible for locating and arresting immigration offenders.
10 Database used to record all enforcement operations undertaken by the Home Office.
11 Case Information Database – Home Office system to manage immigration casework in the UK.
12 Central Reference System – Home Office system used to manage all UK visa applications.
13 Warnings Index – database used to ascertain whether passengers are of interest to the Border Force, the police, or other government departments.

due to circumstances outside its control. For example, two of the arrested persons claimed asylum and the third made an application to remain under the EEA regulations, due to the existence of a relationship that the Home Office was unaware of. Figure 4 details one of these cases.

The Home Office targeted appropriate cases with a good prospect of removal

Figure 4: Case study – Circumstances outside of Home Office control

Background:

- An allegation was received from a member of the public regarding an individual who had allegedly remained in the UK almost six years beyond the expiry of their visa.
- Upon receipt of this information an enforcement visit was undertaken which led to their arrest.
- The individual was detained while a travel document could be obtained.
- Six weeks later, they claimed asylum; ten days prior to the travel document being issued. Their case was accepted into the detained fast-track process.
- The asylum decision was drafted and ready to serve before the applicant submitted an application to the Medical Foundation and was subsequently released from detention.
- Both the asylum decision and the medical report remain outstanding.

Chief Inspector's comments:

- The information obtained through the IMS was effective in this case and led to a successful enforcement visit where the target was arrested and detained.
- A travel document was obtained within a reasonable time period and the Home Office did everything within its power to progress the case to removal.
- Removal action was not possible due to circumstances outside the Department's control.

4.6 The IMS is a system which depends on other teams and departments within the Home Office taking the information forward and carrying out the required action in order to produce tangible outcomes. Any action taken by IMS users must be communicated effectively to ensure that other relevant teams are made aware of the information within the IMS. We found an example where the IMS case had been actioned correctly and the record closed, but the necessary action by the receiving team had not been carried out appropriately. While this is not a criticism of the IMS, intelligence teams working in different parts of the business need to ensure that relevant information is transferred seamlessly to produce effective outcomes – Figure 5 refers.

The IMS case had been actioned correctly, but the necessary action by the receiving team had not been carried out

Figure 5: Case study – Ineffective joint working across Immigration Intelligence

Background:

- Information was received alleging that a named person had applied for a UK visit visa but their true intention was to settle permanently in the UK.
- It was alleged that the individual had lied on their visa application form (VAF) about their current employment status.
- The IMS team liaised with the entry clearance post and a note on the IMS record indicated that a local alert was to be put on CRS[14] in order to ensure that this information was available to the Entry Clearance Officer (ECO) when considering the application.
- However, the local alert was not added to CRS until one month later. The decision to issue the visa was made three weeks earlier (one week after the original allegation was received by the IMS) and there is no evidence that any subsequent consideration was given to this information.

Home Office Response:

- The information was passed to the visa issuing post in New Delhi within 24 hours of receipt and assurance given by them that a local alert would be raised.
- The responsibility for updating local records and issuing the local alert rests with the visa issuing post.

Chief Inspector's comments:

- The IMS team handled the allegation promptly and determined the correct course of action.
- The visa post failed to add the local alert in a timely fashion. As a result, a UK visa was issued that might not have been had the ECO been aware of the information on the IMS.
- No action was taken to update the WI.[15] Had this action been taken at the outset, the individual could have been questioned on their arrival into the UK. This was relevant, as even though the visa had been issued, the individual's intended date of travel (recorded on their visa application) had not yet elapsed.

4.7 We also found an example where the action taken by the IMS user was not appropriate and resulted in a breakdown of the supply of information between different Home Office Directorates. In this case, a member of staff added a warning marker to CID simply identifying that an allegation had been received. The allegation indicated that an applicant had provided false information that was fundamental to their asylum claim. However, the individual had been granted asylum three months earlier, so there was no reason for a caseworker to re-visit this case without being prompted. In this case direct contact with the casework team was required, but as this did not occur, no further action was taken.

4.8 The Chief Inspector of Borders and Immigration has emphasised the importance of the different parts of the Home Office working together effectively, most recently in his 2012/13 annual report.[16] The Chief Inspector noted the challenge of ensuring that the different facets of the immigration system do not operate in isolation

The successful operation of the IMS requires an effective flow of information to other parts of the business

14 Central Records System – Home Office system for managing visa applications.

15 Warnings Index – A database of names available to Border Force staff of those with previous immigration history, those of interest to detection staff, police or matters of national security.

16 http://icinspector.independent.gov.uk/wp-content/uploads/2013/12/Annual-report-2012-13-FInal-Web-Version.pdf

and has made assessing how effectively these areas worked together an area of particular focus for his 2014-15 inspection plan.[17] As highlighted by the examples above, the successful operation of the IMS is one that requires not only effective joint working between intelligence teams but also an effective flow of information to other parts of the business.

4.9 Aside from the cases which had been incorrectly allocated to this category, we found that the majority of allegations in our sample had been actioned correctly by the IMS user. However, the results of these actions were not being retained on the IMS and there was no system in place to monitor the eventual outcomes if they were referred to other teams. The Home Office told us that this function is satisfactorily addressed by data-matching with other systems such as CID or NOD and a further system upgrade during the summer and autumn of 2014 will allow for better recording of intelligence outcomes on IMS. We therefore make no further recommendation here.

NFA Actionable Cases

4.10 We sampled 25 allegations (added to the IMS in September 2013) where the Home Office had established that there was enough evidence to progress the case, but due to tasking priorities no further action was taken. We therefore expected that background checks carried out in these cases had determined that they were suitable to be allocated this outcome. However, we found no evidence that any background checks had been completed in over half of these cases (14 – 56%).

We found no evidence that any background checks had been completed in over half of these cases

4.11 We also determined that the outcome 'NFA actionable' had been attributed correctly in just four of the 25 cases we sampled (16%). This was because there was no discernable difference between the vast majority of cases in this category and those considered to be NFA non-actionable. This was caused by IMS staff entering the incorrect outcome on IMS, which in turn produced unreliable and inaccurate management information regarding case outcomes. Managers assured us that the accuracy of case outcomes would be reviewed and improved as part of ongoing improvement work.

4.12 We were concerned that duplicate cases were not always identified by IMS users. For example, in a quarter of the cases in this category (six cases - 24%), a duplicate of the allegation was already on the system under a different reference number. This was easily observed when checking the details of the case using the advanced search function on the IMS. However, it was clear that the details of these cases had not been checked using this search tool. As a result, IMS users were duplicating work unnecessarily because they were carrying out research which was not needed.

IMS users were duplicating work unnecessarily

4.13 The IMS does not link associated allegations or allow staff to link these manually; therefore duplicate information is retained in separate IMS records. Managers advised us that it was not desirable for the system to automatically link cases, as they were wary of the system making mistakes and linking cases incorrectly. It was therefore the responsibility of staff to identify duplicate case records and take appropriate action. In the light of this, IMS staff should use the advanced search function in all cases to either identify or rule out the possibility that the information had already been received and actioned elsewhere. We therefore make the following recommendation.

17 http://icinspector.independent.gov.uk/wp-content/uploads/2014/04/Inspection-Plan-2014-15-FINAL.pdf

We recommend that the Home Office:

Ensures that all allegations are properly assessed by:

- conducting relevant background checks on Home Office systems;
- cross-checking the details of allegations using the advanced IMS search facility; and
- classifying them appropriately by attributing the correct outcome.

NFA Non-actionable Cases

4.14 We initially examined 50 cases which were added to the IMS in September 2013, in order to assess how the Home Office had determined that they could take no further action. At the outset, we noted the poor quality of the information contained within half of these referrals (25 cases). This meant that there was little the Home Office could do to progress the case because:

The poor quality of the information contained within half of these referrals meant that there was little the Home Office could do to progress the case

- the alleged offence was not clear;
- the case was a duplicate of a pre-existing allegation that was identical;[18] or
- the allegation contained insufficient information.

4.15 Although no action was taken as a result of the information in these cases, the details of all allegations were retained on the IMS under a unique case reference number. This helped the IMS to build an overall intelligence picture, as information could be received cumulatively, which meant that action could be taken once connections between associated allegations had been identified. This was a positive step towards enabling the IMS to provide an effective data management process for the handling of all incoming allegations.

4.16 In the remaining 25 cases there was sufficient information within the allegation to enable the IMS user to conduct research and properly assess the case. We observed some positive work in terms of how these allegations were progressed. We found that in seven cases (14%), checks carried out on Home Office systems by IMS users revealed that the subject of the allegation had valid leave to remain in the UK. In another case, substantial checks were carried out and recorded on the IMS regarding the business address of an employer allegedly using illegal workers. It was identified that an enforcement visit had recently been carried out, which found nothing of interest, and therefore there were insufficient grounds to act upon this recent allegation. This was good practice and the standard of research we expected to be reiterated in all IMS cases, regardless of the quality of the information received.

4.17 However, in almost half (12) of the remaining 25 allegations we found no evidence that any background checks had been conducted prior to the decision to categorise the allegation as 'NFA non-actionable' and close the case. In each of these cases, the alleged offence was clearly outlined and at least a full name or address had been provided. Details of these 12 cases are as follows:

- seven contained both the full name and full address of the alleged offender;
- two contained the full name of the alleged offender; and
- three contained a full address of the alleged offender.

18 Or the content of the allegation was already known to the Home Office by other means.

4.18 We then sampled a further 25 cases in this category that had been added in January 2014, in order to consider whether recent system enhancements improvements had had any impact. We noted that performance had improved, but still found that no background checks had been carried out in four (17%[19]) of these cases. This was despite the alleged offence being clearly outlined and either a full address or full name of the alleged offender being present.

4.19 Due to the absence of adequate background checks in a number of these cases, it was not possible to determine what proportion of allegations in this category could have been actioned. We do not consider that the Home Office could be confident that such information is of no further interest without first conducting mandatory checks against its own IT systems. We therefore reiterate our earlier recommendation concerning the importance of conducting relevant background checks in all appropriate cases prior to deciding the outcome.

Due to the absence of adequate background checks in a number of these cases, it was not possible to determine what proportion of allegations in this category could have been actioned

4.20 We also identified four allegations (8%) where we believe action should have been taken if they had been properly assessed. One should have been actioned by a Border Force embarkation team, as it concerned outbound smuggling. The remaining three all concerned information that would have been useful to caseworking teams. However, no attempts were made to contact the caseworking teams and no warning markers were added to CID. The information provided in these three cases was as follows:

- a report of a marriage breakdown for an individual with no other valid leave to remain;
- an allegation of illegal working and document abuse for an individual with an outstanding application where their conduct would be a consideration; and
- a potential address for a long-term absconder[20] with no address listed on CID.

We also identified four allegations (8%) where we believe action should have been taken if they had been properly assessed

4.21 We understand that all operational activity must be carefully considered and approved by tasking processes. However, the action required in these cases was simply to notify the relevant team that information that might be of interest to them existed within the IMS.

4.22 Information-sharing between Home Office departments is a fundamental role of intelligence teams. We consider that in all instances where information received into the IMS can be attributed to an active case, this should be brought to the attention of the caseworker. The Home Office must ensure that IMS teams recognise the value of information contained within allegations to other parts of the business so that cases can be better identified for further action. We therefore make the following recommendation.

We recommend that the Home Office:

Ensures that IMS users recognise the value to other parts of the business of information contained within allegations and take appropriate action to communicate this effectively.

19 One of the 25 cases was not applicable.

20 A person with no valid to leave to remain in the UK who is not complying with a requirement to report to the immigration authorities.

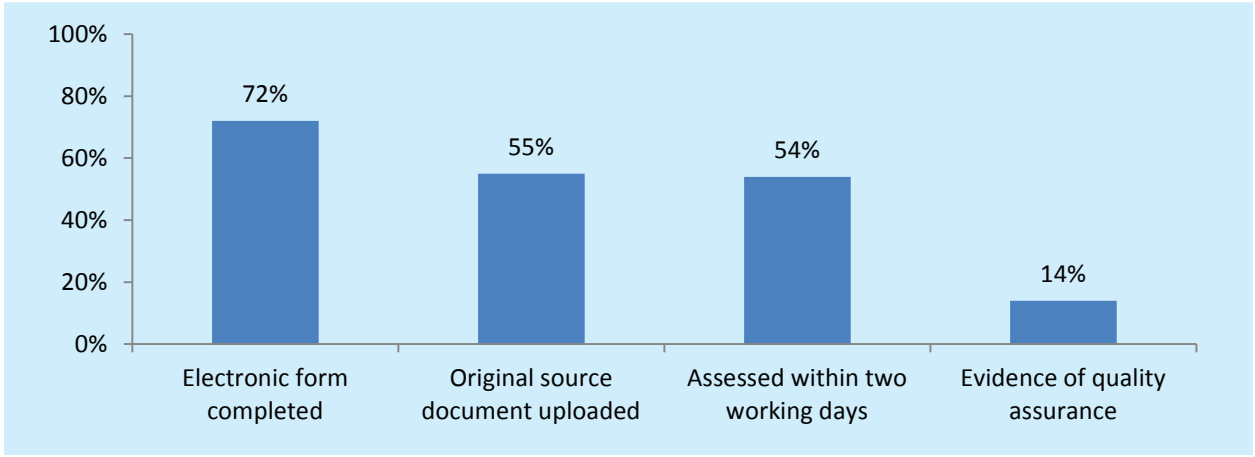
General Findings – Data Quality

4.23 There was substantial room for improvement in terms of the quality of the data retained by the IMS. Some of this was due to technical limitations of the system itself and was beyond the control of system users. For example, although separate fields existed to record how an allegation had been received (letter, fax, telephone or email), there was no way of recording whether or not it was initially received using the online form. This was because all incoming information that was received either via the online form or by email was recorded on the IMS as having been received by email. It was therefore not possible to identify whether the electronic form had been completed by a member of the public or by a member of staff upon receipt of information from the public.

4.24 Our file sampling also found that the quality of the information retained on the IMS needed to be improved significantly by staff adopting a more robust approach. We found substantial room for improvement in terms of data quality, timeliness and quality assurance processes. Figure 6 demonstrates overall performance in our sample in these areas, which are discussed in further detail below.

The quality of the information retained on the IMS needed to be improved significantly

Figure 6: Data quality, timeliness and assurance



Completion of the Electronic Form

4.25 In September 2013, work to upgrade the IMS was completed. This allowed users to utilise an advanced search on the system, enabling them to identify allegations that might be connected to the same offence and to build an intelligence picture in cases where individual pieces of information were not sufficient for action to be taken. This was an important enhancement. However, for this process to be effective, information stored on the individual case records must be stored in the correct location on the IMS (i.e. in the relevant areas of the electronic form).

4.26 This was because the advanced search tool only examined information that had been entered on the electronic form and would not identify information that had been left in an attachment. This problem was identified during our file sampling, when details contained within the IMS case record had not been added to the electronic form in over a quarter of the 125 cases we sampled (35 cases – 28%).

Details contained within the IMS case record had not been added to the electronic form in over a quarter of the 125 cases we sampled

4.27 This meant that the data could not be cross-checked using the advanced search function within the IMS. This was significant, as it meant that intelligence staff were unable to identify associated cases which could have either:

- helped to determine that action was not appropriate; or
- strengthened the overall intelligence picture and resulted in actionable intelligence being passed to operational teams for enforcement action.

4.28 Furthermore, failing to add details of the allegation onto the electronic form can result in important information being overlooked by intelligence staff, as Figure 7 illustrates.

Figure 7: Case study – Failure to complete electronic form

Background:

- An allegation was received of outbound drug smuggling.
- The electronic form detailed a named offender who was said to be carrying 'a lot' of a Class A drug on a specific date and time from a named airport in the UK.
- An attachment on the IMS contained a scanned itinerary of the flight details, including the destination airport.
- Research was completed by the IMS user, but then the case was determined as being of no further action by the receiving intelligence unit; in part because there were four flights leaving the named airport at that particular time and the correct flight could not be identified.

Home Office Response:

- In this particular instance, when the both the case officer and the compliance officer attempted to review the details via the search facility on IMS, both were unable to see the attachment.

Chief Inspector's comments:

- Critical detail in this case was missed by both the IMS user and the compliance officer because it was contained within an attachment and not within the electronic form.
- This case could have been actioned if all of the details of the allegation had been entered on the electronic form and might have resulted in a drug smuggler being apprehended.

4.29 During our focus groups with staff, we discovered differing practices between teams using IMS that may have contributed to failures to act on intelligence. In some teams, staff admitted that no attempt was made to improve the quality of the information on the electronic form prior to the case being assessed and disseminated. However, in other teams, a designated member of staff would review all allegations upon receipt and would ensure that all relevant fields on the electronic form were completed with the information from the attachments. We consider this to be good practice and believe the Home Office should adopt this process nationwide to ensure that all information retained on the IMS is identifiable using the advanced search function. We therefore make the following recommendation.

We recommend that the Home Office:

Ensures that all allegations are properly assessed by adding all the information contained within allegations (including in attachments) to the electronic form on the IMS.

Original Source Documents

4.30 When information was received by the IMS via letter or fax, we were told that a scanned version of the original document would always be attached to the allegation on the IMS before the document was securely stored or posted to the appropriate Regional Intelligence Unit (RIU). Although staff demonstrated that they were aware of the correct procedures in relation to the storage of original documents, our sampling found that the process of scanning and attaching the original document to the allegation was not being consistently followed. For example, where the source of the information had been recorded as either letter or fax, the original document was attached to the allegation in only 11 of 20 cases (55%). Furthermore, there was no explanation on the IMS as to why these documents had not been uploaded in the cases where they were absent.

4.31 We were concerned that, due to the limited content of the electronic form in such a substantial number of cases, the failure to attach the original document to the allegation may have led to crucial information not being brought to the attention of intelligence staff when the allegation was assessed. This may have affected the outcome of some referrals to the IMS.

Failure to attach the original document to the allegation may have led to crucial information not being brought to the attention of intelligence staff

Timeliness

4.32 We considered how the Home Office had performed in relation to its target of initially assessing all incoming information within two working days. Of the 100 allegations we sampled that had been added to the IMS in September 2013, over a third had not been assessed within this two-day target (39%), while one allegation was not assessed for 73 days. We found that in the January 2014 allegations we sampled, performance was even worse, with over half taking three working days or longer before being assessed (13 cases – 52%). The longest delay before assessment in the January cases was 15 days. Figure 8 illustrates performance against this two-day target.

Figure 8 – Timeliness – Performance against two-day target

Days until assessment	September Cases	January Cases
0-2	61	12
3-5	10	5
6-8	3	4
9-11	16	2
12-14	3	1
15+	5	1
Not known	2	0
Total	100	25

4.33 When the Home Office did adhere to the two-day initial assessment target, it was able to process cases very quickly when time-critical aspects were identified. This enabled staff to conduct appropriate research and, where applicable, take action to prevent offences taking place, including:

- disrupting a sham marriage ceremony;
- checking a flight manifest for incoming passengers suspected of visa abuse; and

- liaising with overseas colleagues to provide evidence to be taken into account regarding a visa application.

4.34 In some cases the information contained in the allegation received will be time-critical and a failure to act in a timely manner may render it ineffective. In one case we sampled, the information received made it very clear that the alleged offender was moving house in three days' time and therefore, any action must be taken before that date. Unfortunately, the Home Office failed to assess the case until over two weeks later, rendering the information irrelevant by the date of assessment. Figure 9 details another example from our sample that highlights the importance of conducting the initial assessment within two working days.

In some cases the information contained in the allegation received will be time-critical and a failure to act in a timely manner may render it ineffective

Figure 9: Case study – Time-critical case

Background:

- The information was time-critical, as it related to an immigration appeal hearing which was due to take place three days after the allegation was received into the IMS.
- The allegation concerned issues central to the appellant's credibility at the imminent appeal hearing.
- However, the case was not assessed until five days later. No action was taken and the case was later closed as 'resolved'.
- The appeal was allowed and the individual was granted a five year UK residence permit.

Chief Inspector's comments:

- This information could have materially affected the outcome of the appeal.
- The failure of the Home Office to process the information within its target timeframe may have resulted in an individual being granted leave to which they were not entitled.

4.35 The Immigration Intelligence Manual provided guidance on cases where the content indicated that they were time-critical. Staff were instructed to refer these cases immediately to the duty intelligence manager, who would determine their priority. Any subsequent action should be taken within 24 hours. However, as evidenced in the case study above, this guidance is ineffective if time-critical cases are not identified promptly upon receipt of the information.

4.36 In all the locations where we conducted on-site activity, we observed staff assessing allegations on the same date that they were submitted. We were told that this was normal practice and that although delays had occurred historically, these were due to resourcing issues that had now been resolved. While this has been taken into account, the lack of improvement in the cases we assessed from January 2014 indicates there is still substantial room for improvement in this area.

4.37 It is therefore important that the Home Office takes steps to ensure that the initial harm assessment is carried out in all cases within the timescales set out in the Ministerial target. We therefore make the following recommendation.

We recommend that the Home Office:

Conducts the initial assessment of all allegations within the target timescales agreed by Ministers.

Quality Assurance

4.38 The Home Office acknowledged that management assurance of records kept by staff on the handling of allegations needed to be improved. However, despite this, managers working with the IMS told us that satisfactory assurance did routinely take place, as several different members of staff would consider each case prior to its closure and cases could only be closed on the IMS by a compliance officer.[21] While our file sample did identify that cases were accessed several times by multiple users, there was little evidence of what quality assurance activity had taken place.

4.39 Managers also told us that compliance officers were responsible for checking every IMS case prior to its outcome being determined, regardless of whether or not action was to be taken. However, of the 125 cases we sampled, we only found specific evidence that compliance activityhad been carried out in 18 cases (14%). Due to the issues concerning data quality which we have addressed above, we were not satisfied that adequate management assurance processes were being carried out to make sure that the IMS was being administered effectively.

We were not satisfied that adequate management assurance processes were being carried out

4.40 Effective quality assurance is important in ensuring that guidance is being followed correctly by staff using the IMS and that the information retained on the system is being recorded and progressed in a consistent way. The importance of effective quality assurance has been highlighted in a number of our previous inspections, including the recent inspection report concerning Stansted Airport, published in January 2014.[22] Many of the issues we noted in relation to data quality during this inspection would have been identified by managers, had more robust quality assurance processes been in operation.

4.41 Senior managers told us that, although management assurance had not been undertaken in a consistent or coordinated manner, this was to be addressed by a new Business Assurance Framework for Immigration Intelligence, which was in the development stage during our inspection. We welcome this development, as it was clear from our file sample that improvements at the basic level would significantly improve the quality of the information retained on the IMS and the consistency of how cases were progressed.

Improvements at the basic level would significantly improve the quality of the information retained on the IMS

21 A member of staff with a superior user status on the IMS which enables them to carry out additional system functions.

22 http://icinspector.independent.gov.uk/wp-content/uploads/2014/01/An-Inspection-of-Border-Force-Operations-at-Stansted-Airport.pdf

5. INSPECTION FINDINGS – SAFEGUARDING INDIVIDUALS

Personal data of individuals should be treated and stored securely in accordance with the relevant legislation and regulations.

5.1 In 2013, nearly three-quarters of all allegations received by the IMS were made directly by members of the public. Figure 10 provides a breakdown of the sources of the information in these cases.

In 2013, nearly three-quarters of all allegations received by the IMS were made directly by members of the public

Figure 10: 2013 – Source of allegation

Source of allegation	Number	%
Member of the public	54,894	73%
Other (e.g. internal staff, police etc)	12,070	16%
Crimestoppers	8,315	11%
MP's	115	0.2%
Total	**75,394**[23]	-

5.2 We examined what safeguards had been put in place to manage any risks to personal data which may have arisen from the submission of information to the IMS. We also assessed how the Home Office ensured that staff were aware of their data handling responsibilities.

Identifying Risks to Individuals Who Provide Information

5.3 The Home Office provided us with its published guidance in relation to the protection of sources (i.e. individuals who have provided information about alleged immigration or custom offences). Figure 11 is extracted from the document entitled 'Guidance, Policy and standards: debriefing and human intelligence' and outlines the principles behind the need for source protection.

23 These figures are provisional and subject to change, as they have been derived from management information. This information has not been quality assured under National Statistics protocols.

Figure 11 – Guidance – Source Protection

It has long been acknowledged that human intelligence sources must be protected. The Swinney judgement of 1996 (Swinney v Chief Constable Northumbria Police (1996) 3 All ER 449) confirmed a clear legal duty of care on Law Enforcement Agencies to protect individuals who provide information to them … **Where a source divulges their identity it is our responsibility to take all reasonable steps to ensure that this personal data is kept securely and is accessible only to those with a need to know.**

5.4 The National Source Unit (NSU) was established in September 2010. It is responsible for developing and implementing human intelligence source policy and procedures. The IMS has no automated method by which it identifies potential source risks; such as repeat referrers of information, and relies entirely upon staff identifying appropriate cases and referring these to the NSU to take forward. We found that this process relied upon staff recalling from memory the details of sources who had provided multiple referrals to IMS and might have been of interest to NSU, rather than cross-referencing source details through IMS advanced searching. We were surprised that cross-referencing was not standard practice as a means to identify potential source risks.

This process relied upon staff recalling from memory the details of sources who had provided multiple referrals to IMS

5.5 We found that not all staff were clear about how this process worked. Some, for example, believed that the NSU monitored IMS and identified sources of interest through their own checks, even though this was not the case.

5.6 It was reassuring that, if the IMS record led to an intelligence report being created, staff responsible for creating these were aware of the need to sanitise the source details; as required by the guidance. Once completed, these intelligence reports would be uploaded onto Athena[24] and source details were suitably protected.

Source Details on the IMS

5.7 The IMS was equipped with a restricted source page on the electronic form, where personal and contact details of the individual providing the information were securely stored. Only staff who were working on that particular case at that time could access this page. Furthermore, when staff attempted to open the source details page, a warning message was displayed indicating that an audit entry for the Security and Anti-Corruption Unit (SACU)[25] would be created which would enable security staff to view who had attempted to access the source details.

5.8 When an allegation was received directly from the public using the online form, any source details provided would be automatically entered onto this restricted page. In our file sample, 38 of the 125 cases we reviewed contained source details (30%). Of these 38 cases, source details were visible, without the need to access the restricted screen, in over a third of cases (14 cases – 37%). This was because the information had been received in either a letter or an email and a scanned version had been uploaded without any of the personal details of the source being sanitised. However, a further system safeguard was in place which ensured that these details were only accessible by staff who had been specifically allocated to work on that particular case. Furthermore, the IMS recorded the details of all users who had been granted access to this information.

5.9 Staff told us that there was no requirement to sanitise source details on original documents prior to uploading onto the IMS or to ensure these were only retained on the restricted page on the electronic

24 A system for managing and developing intelligence reports.
25 An internal body responsible for monitoring the activity of Home Office staff.

form. This was supported by guidance, as we noted that a desk aid, produced to assist staff in entering details onto IMS, did not describe how to process attachments or to ensure that a source's details were added to the restricted page on the electronic form.

5.10 Home Office managers advised us that it was important for all IMS users working on a specific case to be able to access the source details, in order to assess the reliability of the source and to contact them if necessary – a practice which they actively encouraged. Furthermore, the IMS was only accessible by intelligence staff, all of whom had the required security clearance to view this data. They added that this approach to information handling was consistent with other law enforcement organisations.

5.11 We accept that system safeguards were in place to limit access to source details to only those users who were working on specific cases. However, we were concerned that the failure to add the source details to the restricted page on the IMS would render this important information inaccessible under an advanced search. Therefore, if the case were to be referred to the NSU due to the identification of potential source risks, the NSU would not be able to identify any associated cases, as the data would not have been entered into the searchable fields on the IMS. This could seriously undermine the effectiveness of the NSU's work to identify and mitigate source risks in IMS cases. It is therefore important that the Home Office takes remedial action to ensure that source details are always recorded on the restricted page in order to enable NSU to identify source risks effectively.

Contacting Sources

5.12 We found that the source had been contacted in just one of the 125 cases we sampled. We explored this further during the on-site phase of our inspection and identified that staff had an inconsistent understanding of their role in relation to contacting sources for further information. Some teams appeared confident and willing to contact sources if necessary in order to clarify information already received or make follow-up enquiries. However, in other teams, staff were extremely wary of contacting sources, indicating that they were unaware of the relevant legislative provisions that governed this type of activity. This inconsistency was reiterated by the NSU, who told us that most referrals to them were of very poor quality and related to the need to contact a source for further information about the allegation, rather than due to any potential source risks.

The source had been contacted in just one of the 125 cases we sampled

5.13 The issue of intelligence staff awareness regarding contacting sources had been highlighted in previous inspection reports. Most recently, the 2010 HMIC[26] report entitled 'Handling of Human Intelligence Sources – Revisited'[27] considered that staff were dissuaded from acquiring information from the public due to confusion over how to handle the information – many believed they could only receive the information given and did not seek further clarification (paragraph 3.52).

5.14 All staff working in the intelligence sphere should at least be aware of the relevant provisions of the legislation that affect their area of work, such as the Criminal Procedure and Investigations Act 1996 (CPIA) and the Regulation of Investigatory Powers Act 2000 (RIPA). In addition, IMS staff who have the authority to contact sources must be aware of the wider risks that this activity can entail. For example, it was clear that knowledge of basic principles such as how to define a 'CHIS[28] relationship' and 'status drift'[29] had not been communicated to all staff working with the IMS.

26 Her Majesty's Inspectorate of Constabulary.
27 http://www.hmic.gov.uk/publication/hmrc-handling-of-human-intelligence-sources-revisited/
28 Covert Human Intelligence Source as defined in RIPA.
29 Where sources who submit information move from being a non-CHIS to a CHIS. It is vitally important for intelligence staff to be able to identify this, to ensure that anyone whose activity falls under the statutory definition of a CHIS is authorised as such and subsequently properly managed and controlled.

5.15 We consider that if managers are content for all intelligence staff working with the IMS to be granted access to source details and to be encouraged to engage in contact with sources directly, then they must be provided with adequate training to ensure that they:

Knowledge of basic principles such as how to define a 'CHIS relationship' and 'status drift' had not been communicated to all staff working with the IMS

- do not jeopardise the integrity of the information they are seeking to obtain; and
- are able to identify activity that could lead to a potential unauthorised CHIS relationship being formed.

5.16 The Home Office needs to ensure that consistent national practices exist in relation to contacting sources. Guidance must be issued to all staff responsible for this function and adequate training provided to ensure that they are aware of the relevant legislative provisions that underpin this activity. We therefore make the following recommendation.

We recommend that the Home Office:

Provides all intelligence staff with adequate training in handling sources.

Retention – Disclosure under CPIA

5.17 Chapter 17 of the Immigration Intelligence Manual requires that Immigration Intelligence staff retain all original documents, whether used or unused, that are gathered during an investigation. Unused material may include emails, minutes and results of checks which did not form part of the case against the accused. The guidance explains that all written material, including information as informally recorded as on a post-it note, is disclosable under CPIA and must be retained. We were therefore disappointed to find that staff working with the IMS demonstrated an inconsistent level of understanding of this principle.

Staff working with the IMS demonstrated an inconsistent level of understanding of this principle

5.18 In some teams, the level of understanding was excellent, with processes in place to ensure that all material produced was filed and retained securely in line with this guidance. However, other teams explained that all hand-written notes would be shredded or placed into confidential waste promptly after use.

5.19 Although the majority of staff indicated that they rarely wrote paper notes and did the bulk of their research exclusively by electronic means, there was an acknowledgement that sometimes written notes were produced in the course of an intelligence investigation. It is important that staff are aware of the relevant guidance relating to this issue, as failures to retain and disclose relevant material could have far-reaching connotations for the development of future investigations.

6. INSPECTION FINDINGS – CONTINUOUS IMPROVEMENT

The implementation of policies and processes should support efficient and effective operational delivery.

System Improvements

6.1 An extensive improvement project to upgrade the functionality of the IMS was ongoing at the time of our inspection. These changes were expected to be operational by autumn 2014. This upgrade work represented the third release of the IMS since its inception in September 2012 and demonstrated that steps were being taken to improve the system.

User-testing

6.2 Public user-testing had been carried out to inform the new release of the IMS. Plans included an improved online form for submitting allegations, designed to make the process more streamlined and user-friendly. Furthermore, plans were in place to make the electronic form accessible via smart phones, tablets and for those who use screen-readers. These were positive developments, as ease of access and simplicity of navigating the system would encourage more people to submit allegations and improve the quality of the information received directly from the public.

6.3 In addition, staff told us that they had been consulted and given an opportunity to contribute their ideas towards how the system could be improved. As a result, improvement plans included a case summary sheet and an enhanced internal search engine that would identify information placed anywhere on the electronic form within its search parameters; including the free text and notes fields for the first time.

6.4 We consider that it was beneficial to the IMS that the Home Office were taking into account the views of its users, both from a staff and public perspective, in order to inform improvement work.

It was beneficial to the IMS that the Home Office were taking into account the views of its users, both from a staff and public perspective, in order to inform improvement work

Management Information

6.5 We were told that the upgrades to the IMS would result in far greater capability in terms of its ability to produce management information, largely due to the introduction of a report-building programme which came into operation during our inspection. This would allow managers to produce more focused performance reports from the IMS. It was not possible to comment on its effectiveness during our inspection, as it had only just been implemented. However, the steps being taken to improve management information and reporting tools were key in order to:

- ensure that case outcomes were being recorded accurately, leading to the creation of better-informed performance reports;
- conduct meaningful analysis to identify intelligence trends; and
- improve oversight to swiftly identify issues such as regional variations in case progression and put in place measures to combat this.

6.6 The quality of the management information produced by the IMS during our inspection was not satisfactory; as evidenced by the results of our file sample in which many allegations were assigned the wrong outcome. In order to be a productive tool, the IMS must be able to produce useful and accurate management information which can be used to assess performance and inform activity. We are satisfied that this issue is being addressed.

Many allegations were assigned the wrong outcome

Guidance and Training

6.7 Guidance for intelligence staff is located in the Immigration Intelligence Manual. This is a 'one-stop-shop' guide, providing consolidated and up-to-date guidance. Launched in December 2013, the guide is updated centrally whenever changes are made to standard processes, legislation or guidance. It was most recently updated in February 2014. We found this 147 page document to be a comprehensive guide for staff in terms of intelligence handling. However, many of the IMS staff we interviewed were not aware of the existence of this manual and told us that they had never received any training in relation to intelligence issues such as identifying potential source risks. We noted that e-learning courses were available on this subject, but the completion of these was not mandatory for IMS staff.

6.8 Specific guidance for processing cases on the IMS was available to staff. We found that this was sufficiently detailed and comprehensive in terms of how to navigate the system. However, we noted that it did not provide staff with a practical guide to follow in terms of what information was important for the IMS to be effective and what operations must be completed in all cases – such as adding source details to the restricted screen and utilising the advanced search function.

6.9 This view was reiterated by staff, who told us that there were only limited national instructions regarding how to consistently populate the IMS. They relied upon local procedures and as a result, felt that there were inconsistent regional practices between teams processing allegations on the IMS. An example of this that we observed was that, when allegations received by the IMS were developed, staff in some regions created intelligence reports and uploaded these onto Athena (where they would be accessible to intelligence teams anywhere in the UK), whilst in other regions, a local tasking pro-forma was used, which meant that this information would not be shared with intelligence teams across the UK.

6.10 Managers were aware of the lack of standardised training for IMS users and told us that the core intelligence training was in the process of being redesigned. The use of the IMS and the Intelligence Handling Model[30] were being incorporated into a new classroom-based course for new intelligence practitioners. This course was due to be launched to coincide with an influx of new staff in March/April 2014.

Managers were aware of the lack of standardised training for IMS users and told us that the core intelligence training was in the process of being redesigned

6.11 As we were satisfied that the Home Office were aware of, and were taking action to resolve, issues around training and guidance for IMS users, we make no further recommendation here. We consider that the positive impact of implementing system improvements to the IMS may be negated if these issues are not promptly addressed. While improving the overall capability and functionality of the IMS will help users to navigate the system and managers to produce more effective performance reports, these changes will have limited impact unless IMS users are provided with effective guidance which enables them to carry out their day-to-day roles and populate the IMS consistently.

30 A grading system used to prioritise incoming intelligence based on a harm rating.

ANNEX 1 - ROLE & REMIT OF THE CHIEF INSPECTOR

The role of the Independent Chief Inspector ('the Chief Inspector') of the UK Border Agency (the Agency) was established by the UK Borders Act 2007 to examine and report on the efficiency and effectiveness of the Agency. In 2009, the Independent Chief Inspector's remit was extended to include customs functions and contractors.

On 26 April 2009, the Independent Chief Inspector was also appointed to the statutory role of independent Monitor for Entry Clearance Refusals without the Right of Appeal as set out in Section 23 of the Immigration and Asylum Act 1999, as amended by Section 4(2) of the Immigration, Asylum and Nationality Act 2006.

On 20 February 2012, the Home Secretary announced that Border Force would be taken out of the Agency to become a separate operational command within the Home Office. The Home Secretary confirmed that this change would not affect the Chief Inspector's statutory responsibilities and that he would continue to be responsible for inspecting the operations of both the Agency and the Border Force.

On 22 March 2012, the Chief Inspector of the UK Border Agency's title changed to become the Independent Chief Inspector of Borders and Immigration. His statutory responsibilities remain the same. The Chief Inspector is independent of the UK Border Agency and the Border Force, and reports directly to the Home Secretary.

On 26 March 2013 the Home Secretary announced that the UK Border Agency was to be broken up and brought back into the Home Office, reporting directly to Ministers, under a new package of reforms. The Independent Chief Inspector will continue to inspect the UK's border and immigration functions, as well as contractors employed by the Home Office to deliver any of these functions. Under the new arrangements, the department UK Visas and Immigrations (UKVI) was introduced under the direction of a Director General.

ANNEX 2 - GLOSSARY

Term	Description
A	
Allegation	An allegation is a piece of information which brings to the attention of the Home Office a perceived breach of the immigration system, or the illegal importation of goods.
C	
Central Reference System (CRS)	A Home Office system used to manage UK visa applications.
D	
Director	A senior Home Office manager, typically responsible for a directorate, region or operational business area.
E	
Enforcement	A Home Office term used to refer to all activity that takes place within the UK to enforce the immigration rules. In addition to the work done by arrest teams, this includes areas such as asylum, citizenship, detention and removal.
Enforcement Action / Operation	Action taken within the UK (as opposed to being undertaken at the border) by trained Home Office staff to locate and process suspect or known immigration offenders.
Enforcement Team	A team of Home Office staff who conduct operations in the field, such as visits to employers of illegal workers.
H	
Home Office	The Home Office is the lead government department for immigration and passports, drugs policy, crime, counter-terrorism and police.

I	
Immigration, Compliance and Enforcement Team (ICE)	An ICE Team is a local team undertaking as many functions as practicable at a local level within an Immigration & Enforcement region. They focus on enforcement work and community engagement, although the functions of ICE Teams can vary between regions.
IMS	The Intelligence Management System is a national database used by the Home Office to manage allegations of customs or immigrations offences.
L	
LACAT	The London Area Central Allegations Team conducts the initial assessment for allegations in the London area before deciding the outcome.
N	
National Allegations Team (NAT)	An IMS team who process and disseminate internally all allegations which could not be automatically routed to the appropriate region.
National Operations Database (NOD)	Database used to record all enforcement operations undertaken by the Home Office.
R	
Regional Intelligence Unit (RIU)	A team that collates and disseminates intelligence, usually for enforcement teams.
S	
Source	An individual who submits to the Home Office information that is used to prevent or identify an immigration or customs offence.

ACKNOWLEDGEMENTS

We are grateful to the Home Office for its help and co-operation throughout the inspection and appreciate the contributions of all staff who participated in the inspection process.

Assistant Chief Inspector:	**Garry Cullen**
Lead Inspector:	**Mike Townson**
Inspection Officers:	**Foizia Begum** **Akua Brew-Abekah**

ISBN 978-1-4741-1163-8

HO_02161_ICI