Independent Chief Inspector of Borders and Immigration

An Inspection of the Intelligence Functions of Border Force and Immigration Enforcement

November 2015-May 2016

David Bolt
Independent Chief Inspector of
Borders and Immigration

An Inspection of the Intelligence Functions of Border Force and Immigration Enforcement

November 2015-May 2016

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

July 2016

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
United Kingdom

Print ISBN 9781474136693
Web ISBN 9781474136723
ID 19071601 07/16

Printed on paper containing 75% recycled fibre content minimum

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

Our purpose

To help improve the efficiency, effectiveness and consistency of the Home Office's border and immigration functions through unfettered, impartial and evidence-based inspection.

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

Email us: chiefinspector@icinspector.gsi.gov.uk

Write to us: Independent Chief Inspector
of Borders and Immigration,
5th Floor, Globe House,
89 Eccleston Square,
London, SW1V 1PN
United Kingdom

Contents

Foreword

It is common for operational agencies, particularly those in the law enforcement field, to describe themselves as 'intelligence led' when referring to the way in which they determine their priorities and decide on where and how to deploy their resources. Being 'intelligence-led' is at a premium where the latter are stretched and choices have to be made about what gets done and what gets dropped.

What constitutes intelligence, and how this is gathered and used, differs from sector to sector. However, at its simplest, being 'intelligence-led' requires trained staff and functioning processes and systems, to collect relevant information, to evaluate it, and to ensure that it reaches those who need to know it and act upon it in a usable form and in good time.

Border Force, Immigration Enforcement and UK Visas and Immigration (UKVI) all aim to be 'intelligence-led'. This inspection therefore looked at the efficiency and effectiveness of the intelligence functions within Border Force and Immigration Enforcement (the latter services the intelligence needs of UKVI). In doing so, it reflected on the findings from previous inspections in this area, and other relevant reviews, and on the progress made in implementing earlier recommendations. It also noted the various projects and initiatives that were underway within the Home Office aimed at transforming these intelligence functions.

The inspection found that Border Force and Immigration Enforcement had made considerable efforts to develop and improve their intelligence functions, and had made significant progress towards becoming truly 'intelligence-led' by implementing the key components of the National Intelligence Model (NIM), adapted to suit the particular circumstances and challenges of Borders and Immigration.

However, as both directorates recognised, a lot remains to be done, practically in terms of systems and processes, and culturally in terms of 'hearts and minds'. The big transformation projects promise a great deal, and it is important that the momentum behind these is maintained. However, there is also a need to find solutions in faster time to some current inefficiencies and inconsistencies. In particular, both need to ensure that staff have access to and make full use of relevant IT systems; that operational priorities are aligned nationally, regionally and locally; and that information and knowledge acquired by frontline staff is fed back so that the intelligence picture is as complete as possible.

The report makes seven recommendations for improvements. It was submitted to the Home Secretary on 16 June 2016.

1. Purpose and scope

1.1 This inspection examined how efficiently and effectively Border Force (BF), Immigration Enforcement (IE) and UK Visas and Immigration (UKVI) processed, assessed, developed and shared intelligence with one another and with others, specifically:

- the extent to which BF, IE and UKVI are meeting their aim to be 'intelligence-led';
- the extent to which BF, IE and UKVI have responded to recommendations made in previous inspections and reviews dealing with intelligence;
- the efficiency and effectiveness of key stages of the intelligence 'cycle'; and
- the sharing of intelligence between BF, IE and UKVI, in particular any joint working or processes which allowed intelligence to flow and develop between the three directorates.

1.2 It did so using eight of the Independent Chief Inspector's inspection criteria.[1]

1.3 The inspection involved:

- familiarisation visits to a Receipt, Evaluation and Development (RED) Team Operational Intelligence Unit (OIU) and Analyst Team (Sheffield), Border Force National Intelligence Hub (Dover), Strategic Intelligence Centre (Folkestone) and Border Force Intelligence South East & Europe (Folkestone);
- examination of management information and documentary evidence, including staff guidance and operational instructions, workflow processes, terms of reference for national and regional boards and bodies, and continuous improvement reports;
- sampling of records received between 1 July and 30 September 2015, comprising:
  - 78 IE records with only one action recorded on the Intelligence Management System (IMS), 39 of which were marked for 'no further action';
  - 99 IE records where an OIU 'package' was presented to a Tasking & Coordination Group to consider action;
  - 50 records from the BF National Intelligence Hub;
  - 125 BF records (25 from each BF region); and
- interviews and focus groups involving over 200 BF, IE and UKVI staff.[2]

1 The criteria used in this inspection are detailed at Appendix 2 of this Report. The full set of inspection criteria can be found on the Independent Chief Inspector's website at: http://icinspector.independent.gov.uk/inspections/inspection-programmes/.
2 Locations visited and numbers and grades of staff seen are given at Annex.

2. Key Findings

2.1 Both IE and BF have developed and implemented the key components of the National Intelligence Model (NIM), adapted where necessary to suit their particular circumstances and needs. Therefore, to the extent that NIM compliance is the measure of being 'intelligence-led', both have largely achieved this.

2.2 However, at the detailed level some elements are either missing or not working effectively. This is particularly true of 'systems products' (relevant IT systems and data enabling information/ intelligence to be stored, retrieved, researched, developed etc.). For example, while the Intelligence Management System (IMS) provides the functionality to record information received and to track what is done with it, BF is not using this system except for allegations submitted via the online reporting form, and is instead using local spreadsheets which are not accessible to BF staff in other offices and regions, or to IE.

2.3 Access to certain IT systems, required to be able to check whether new information connects to what is already known, is limited and uneven. It is dictated more by history (they are mostly legacy systems), geography (terminals are where they were needed under old organisational structures) and the cost of making changes (additional licences and new installations), than by any sense of current business needs, although a review of licence holders for Centaur and Semaphore was underway at the time of the inspection. For operational (frontline) staff the duplication of effort required to update two or three non-integrated systems with the same information acts as a powerful disincentive to feeding the intelligence function.

2.4 IE, BF and HM Passport Office had been collaborating on a new Single Intelligence (IT) platform that will better meet their intelligence related business needs. The incremental approach to development and roll out of new SIP functionality was prudent, and over time SIP will provide significant improvements to the Home Office's search and data-matching capabilities. In the short term, the planned switching off of ATHENA (at the end of May 2016) had caused inconsistencies in how intelligence reports were being created and stored.

2.5 IE and BF both have NIM compliant Tasking & Coordination processes in place to identify operational priories and determine resource allocations at strategic and tactical levels, and both produce a range of intelligence products to feed these processes, with intelligence analysts in attendance at Tasking & Coordination Group meetings. Both IE and BF allow for regional and local differences (threats and opportunities) in terms of how national priorities are interpreted and implemented on the ground. However, the inspection revealed that local TCGs were rejecting 'packages' that met national and regional priorities on the basis that they did not meet local priorities, and some intelligence staff complained that operational staff were more 'opportunity-driven' than 'intelligence-led'.

2.6 Ostensibly, the primary knowledge product used for guidance by both IE and BF intelligence staff is the Immigration Intelligence Manual (IIM). This was produced by IE in 2013 and last updated in 2014, since when both IE and BF have undergone significant structural changes and changes to processes. In practice, IIM is a high-level statement of principles rather than a 'how to'

manual, and both IE and BF intelligence issue separate detailed operational instructions relating to specific processes and changes. The IIM and operational instructions are available to staff via the Home Office intranet. Searching for specific guidance sometimes requires several attempts, and it is not easy to know whether the results are the latest version or whether there is other relevant guidance. However, the IIM is to be replaced in 2016 by a Professional Practice Manual (PPM) and a BF Intelligence Manual (BFIM).

2.7 IE and BF have both demonstrated their commitment to learning and improvement in relation to their management and use of intelligence. Two previous inspections, including one of the then UK Border Agency in 2011, identified a number of key areas where improvements were required, and IE and BF have either implemented or were making progress with all of these.

2.8 In 2014, Deloitte was commissioned by both IE and BF to conduct a review of intelligence. While their specific objectives differed, IE and BF were both looking to Deloitte to identify potential improvements in their structures, processes and impact. Each produced a detailed response to the review, setting out their respective visions for the intelligence function. These involved major transformation programmes, which both IE and BF have been pursuing, applying continuous improvement principles and on occasion seeking input from the Home Office Continuous Improvement Unit.

2.9 A significant element of transformation is the Intelligence Professionalisation Programme (IPP), which was due to go live in March 2016, and through which intelligence staff would be able to gain accreditation from a national organisation (the IPP Board) which will be recognised by other law enforcement agencies.

2.10 The intelligence 'cycles' in IE and BF involve a number of detailed processes and 'handoffs'. Two are particularly important to overall efficiency and effectiveness of the intelligence function. The first concerns the receipt, initial evaluation and distribution of new information. The second concerns how well frontline staff engage with and support the intelligence function. This has often been a challenge for law enforcement agencies.

2.11 Based on the evidence provided to this inspection, both IE and the BFNIH make a correct and timely (within the target time of 48 hours for II and a maximum of 24 hours for BFNIH) initial evaluation of the vast majority of the information they receive. IE relies on its Intelligence Handling Model (IHM) to achieve its aim of 'providing the right information to the right people, on time.' However, IHM is regarded as immigration-centric and therefore not used by BF. BFNIH's task is essentially to move any credible and actionable information on to a BF region to action, which it does efficiently. However, based on file sampling, it is less clear to what extent BF regional intelligence teams are efficient in terms of the 48 hour target or effective in the action they take, since there is no consistency to regional record keeping and the records sampled contained many gaps.

2.12 Between August 2014 and July 2015, two thirds (c.50,000) of all allegations recorded on IMS were from members of the public, which as the 2014 Deloitte review recognised were 'not the most efficient way for IE to direct its activity'. Referrals from IE, UKVI or BF frontline staff were potentially more valuable, as these staff should be more aware of what is of organisational interest or concern. However, numbers of internal referrals were low, either because frontline staff failed to understand the importance of making referrals, were misdirected regarding how to make them, or did so in ways that were non compliant and therefore difficult to audit.

2.13 Within IE the risk that ICE teams were not making use of IMS to make referrals had been recognised and changes had been made to the training and guidance provided to ICE Team staff. In the case of UKVI, IE structures and processes dealing with UKVI related intelligence (e.g. regarding temporary and permanent migration) changed in 2015, but guidance for UKVI caseworkers, available on the Home Office intranet, had not been updated since November 2014. Meanwhile, despite up to date guidance requiring them to use IMS, BF front line staff were using emails and telephone calls to refer allegations of immigration and customs abuse.

2.14 There was a similar picture with feedback, including any new intelligence, from operational teams acting on the intelligence 'packages' they received, despite the teams completing operational debriefs. This was largely due to the fact that reporting arrangements were unclear (BF) or involved the duplication of effort (IE). While the IE and BF Field Intelligence Officers (FIOs) were a potential solution, they were weighed down with administrative office based duties and did not have the capacity to get 'into the field' and collect feedback and newly acquired intelligence from frontline staff to pass back to intelligence colleagues.

Overall picture

2.15 Overall, IE and BF have made considerable efforts to develop and improve their intelligence functions, and both have made significant progress towards being 'intelligence-led'. However, as both recognise, a lot of work remains to be done, practically in terms of systems and processes, and culturally in terms of 'hearts and minds'. It will be important for both to keep up the momentum behind their big transformation projects, in particular the Single Intelligence Platform (SIP), Programme Professional Practice Manual (PPM) and BF Intelligence Manual (BFIM), and Intelligence Professionalisation Programme (IPP). However, there is also a need to find solutions in quicker time to some of the current inefficiencies and inconsistencies, for example the failure to make best use of IMS.

3. Summary of recommendations

The Home Office should:

1. Ensure that the Intelligence Management System (IMS) is being used to its full potential, specifically that BF uses IMS to record all allegations it receives and not just those received via the online reporting form, and desists from using local spreadsheets.
2. Pending the development and implementation of full Single Intelligence Platform (SIP) functionality, review IE and BF user access to IT systems that support key intelligence functions, in particular the receipt, evaluation and checking of information for links to what is already known, and where necessary reallocate or extend licences and system availability.
3. Ensure that the Professional Practice Manual when produced is readily accessible and searchable via the Home Office intranet, and that future amendments to it identify what has changed (and why) and are clearly marked with the operative date. In the meantime, cleanse the Home Office intranet of intelligence related material that is no longer valid, and collect extant operational instructions in one place for ease of reference.
4. Conduct a stock take in relation to the implementation by IE and BF of their 'visions' for intelligence set out in response to the 2014 Deloitte review, and identify and prioritise those elements that require further work.
5. Set and enforce (through clear guidance and quality assurance) appropriate standards for the receipt, initial evaluation and distribution, including for record keeping, giving consideration to whether the Intelligence Handling Model (IHM) used by IE could be adapted for BF use.
6. Ensure that all 'frontline' staff in IE, UKVI and BF are fully aware of their obligations with regard to referring and reporting information, intelligence and feedback to intelligence colleagues, and that the processes and mechanism for doing this are clearly set out.
7. Review the responsibilities and workloads of field intelligence officers with a view to reducing their time spent on office based administrative duties and enabling them to get 'into the field' to collect feedback and new intelligence from frontline staff.

4. Being 'intelligence-led'

Definition of intelligence

4.1 The Home Office defines intelligence as 'assessed information'.[3] Information becomes intelligence when evaluated by an intelligence officer, who will normally have conducted research and background checks using Home Office and other systems, including open sources, to confirm or add further details about the 'entities'[4] contained in the original information.

Intelligence structures

4.2 The Home Office's borders and immigration functions are supported by two intelligence structures, one within the Immigration Enforcement (IE) Directorate and another within Border Force (BF). UK Visas and Immigration (UKVI) does not have its own intelligence structure. Its intelligence functions are delivered by IE.

4.3 During 2015, IE's Immigration Intelligence Directorate (II) was restructured to create four regional RED (Receipt, Evaluation & Development) teams, located in Croydon, Solihull, Sheffield and Glasgow. The RED teams triage and assess any information received and, where appropriate, refer it to II's Operational Intelligence Units (OIU) for further research and development into 'packages' for potential enforcement activity or criminal investigation.

4.4 II's Risk and Liaison Overseas Network (RALON) delivers three main functions: support to the overseas visa operations managed by UKVI; preventing inadequately documented passengers from reaching the UK by air; and the investigation of organised crime groups facilitating the abuse of visa and air routes. RALON is supported in the UK by the Immigration Intelligence Centre (IIC), The IIC provides a 24/7 capability for II, including out of hours cover for the RED teams, specifically to ensure incoming intelligence is assessed as soon as possible. The IIC also manages requests for support from IE and UKVI in relation to the investigation of organised immigration crime, and acts as the single point of contact for IID with external partners, such as the National Crime Agency (NCA).

4.5 BF Intelligence Directorate (BFID) consists of four geographical areas: North; South; South East & Europe; and South & Heathrow and Central. It also includes the Border Force National Intelligence Hub (BFNIH), a central unit with responsibility for conducting the initial evaluation and recording of incoming information before referring it on to one or more of the four BF regions, the National Border Targeting Centre (NBTC), Cargo Targeting, or BF International.

4.6 BFNIH assesses the information it receives to determine whether it is time critical.[5] It does the same for intelligence received from partner agencies. Where there is an immediate threat to the border, BFNIH will typically send an alert directly to the affected ports. Where information is not time-critical, BFNIH allocates ownership to the most appropriate regional intelligence unit for further development and action.

3 In response to scoping questions sent out to BF and IE by ICIBI.
4 The Home Office defines 'entities' as 'People, Offences, Locations, Events'.
5 Border Force defines 'time critical' as border activity occurring within three hours of receipt of information by BFNIH.

4.7 The BF regional intelligence teams[6] are responsible for the dissemination of all intelligence material to other agencies operating within their region and serve as points of contact for these agencies.

The National Intelligence Model

4.8 Since they replaced the UK Border Agency[7] , IE and BF have been engaged in business change programmes aimed at becoming 'fully intelligence-led', based on the principles of the National Intelligence Model (NIM)[8]. NIM was created by the National Criminal Intelligence Service (NCIS)9 in 2000, and is an 'intelligence-led' business model used by law enforcement agencies, principally police forces, to set their strategic direction, to prioritise and risk manage resourcing decisions, to formulate tactical plans, and to task and coordinate actions. NIM has four components:

Figure 1

Component	Description
The tasking and coordinating process	Tasking and Coordination Groups exist at various levels, e.g. Strategic/Tactical, National/Regional/Local, and meet as often as required. Strategic TCGs set an agency's overall priorities ('control strategy'), including for intelligence, crime prevention and enforcement, and allocate resources accordingly. Tactical TCGs meet more frequently, and are normally chaired by a senior manager with the authority to deploy the operational resources needed to complete the tasks the TCG has endorsed.
Four key intelligence products	Strategic assessments: longer term, high level pictures of issues, how they are changing and might change in the future, to assist with overall planning and policy making. Tactical assessments: shorter term issues, where prompt action can prevent a situation from deteriorating or developing, to assist management of current operations and plans, including resource reallocations. Target profiles: detailed pictures of an offender or offenders, to assist operational managers to select targets for action, including for further intelligence collection. Problem profiles: identifying established or emerging 'hot spots' or patterns of offending, to assist resourcing decisions.
Knowledge products	Manuals, guidance, codes of practice, intelligence training and any other products that define the operating rules and best practice.
System products	Provision of access to relevant IT systems and data enabling information/intelligence to be stored, retrieved, researched, developed etc.

6 Border Force refers to these as Border Force Intelligence Teams (name of Region), or BFIT (Region).
7 Border Force became a separate organisation from UKBA in 2012. IE was created following the abolition of UKBA in 2013.
8 http://www.intelligenceanalysis.net/National%20Intelligence%20Model.pdf.
9 A former non-departmental body of the Home Office which formed part of a merger to become the Serious and Organised Crime Agency (SOCA) in 2006 and latterly, the National Crime Agency (NCA) in 2013.

Tasking & coordination in IE and BF

4.9 IE and BF run national and regional tasking & coordination processes, through which operational priorities are set, resources allocated, and the intelligence requirement defined.[10] The Tasking & Coordination Groups (TCGs) receive regular threat assessments, as well as business performance and operational capacity data.

IE TCGs

4.10 IE has a National Tasking Board (NTB), Regional Tasking Boards (RTB), and local Immigration Crime & Enforcement (ICE) Team[11] TCGs. These set the priorities for operational activity. In addition, there is a National Intelligence TCG, which meets to ensure that intelligence staff know the NTB and RTB priorities and that intelligence resources are deployed in line with these priorities.

4.11 The NTB meets monthly and produces a 'priority matrix'. This sets out the types of offences considered a priority for IE. These are known as 'threat categories'. The 'priority matrix' also sets out under what circumstances and how IE will respond to certain offences committed under each of the threat categories. For example, the September 2015 'priority matrix' identified 'sham marriage' as a particular priority under the threat category of 'abuse of legitimate entry and leave to remain'.

4.12 RTBs also meet monthly and decide which of the national priorities will be regional priorities for the month ahead. Regional priorities vary, reflecting the nature of immigration crime taking place in that region, e.g. in the South East, which covers Dover, clandestine entrants is a priority, while it is not in the North West.

4.13 Local ICE Team TCGs meet weekly and make decisions about how local resources will be used in the week ahead, and sometimes beyond. They review existing operational commitments, but also discuss intelligence 'packages' created by regional OIUs and decide whether or not to adopt them. Adoption should result in enforcement activity by an ICE team.

4.14 However, the inspection revealed a disconnect in the way that OIU 'packages' were handled, with 'packages' containing allegations that met NTB, RTB and NITCG priorities being rejected by local TCGs because they did not meet the latter's priorities.

4.15 Of the 99 cases sampled, 37 were rejected, either prior to the local ICE TCG meeting (nine) or at the meeting (27). Figure 2 shows the reasons given.

Figure 2: reasons for rejection of intelligence packages	
Did not meet current priorities	13
Lack of resources	10
Inappropriate	4
Practical constraints	3
Adverse intelligence found	2
Quality of intelligence	2

10 The Intelligence Requirement sets out the types of information/intelligence that should be sought or collected.
11 ICE teams are located around the UK and conduct compliance and enforcement visits, and arrests of immigration offenders where appropriate. ICE Teams come under the management of Regional Enforcement Directorates, which are separate from IID.

Evidence of legitimate relationship	1
Intelligence too old	1
Not known	1
Total	**37**

4.16 Figure 3 shows the alleged offences recorded for the 13 cases deemed not to meet current priorities.

Figure 3: offences alleged not meeting current priorities	
Illegal working (employee)	6
Sham marriage	3
Illegal working (employer)	1
Fake documents	1
In the UK illegally	1
No permission to stay in the UK	1
Total	**13**

BF TCGs

4.17 The BF Strategic TCG is responsible for setting the priorities and direction for BF at a national level, in line with the BF control strategy. The BF Tactical TCG is a decision making forum that uses outputs from the Strategic TCG, the BF Control Strategy, intelligence products, performance information and ongoing regional activity, to ensure that BF resources are deployed appropriately.

4.18 The purpose of the BF Tactical TCG is to ensure that BF capitalises on opportunities to maximise its performance by driving 'intelligence-led' tasking at the national level. It also co-ordinates and prioritises tasking requests from partners. National taskings can be modified by regional and/or local tasking. The latter will take account of location specific knowledge and regional risks, for example the types and volumes of traffic at particular ports.

4.19 BF Strategy Delivery Groups (SDGs) review intelligence, performance and operational activity at both national and regional levels in relation to the themes identified in the Control Strategy, looking to identify 'intelligence-led' or other opportunities for future activity. The SDGs consider and agree proposed national tasking activities prior to their submission to the Tactical TCG for consideration.

4.20 A detailed and thorough evaluation is required for all activity in response to any national taskings. Each evaluation is reviewed by the relevant SDG before being submitted to the Tactical TCG, who will decide whether further activity is appropriate having considered the SDG's comments.

IE (UKVI) and BF Intelligence Products

Strategic assessments

4.21 In 2015, in relation to becoming 'intelligence-led', the director of the BF intelligence directorate wrote *'the Annual Threat Assessment and the ensuing Control Strategy are key tools to support that ambition*.'[12] IE and BF work with the NCA and other partners to produce strategic assessments of the borders and immigration threats facing the UK. The following strategic documents are produced annually:

- National Borders Strategic Assessment (NBSA) - produced in conjunction with the NCA, and providing a strategic assessment of criminality and other threats at the border;
- Border Force Annual Threat Assessment (BFATA) - detailing the main threats to the UK border from a thematic perspective, covering immigration, commodities and National Security at the border;
- Border Force Control Strategy (BFCS) - describing how BF will prioritise its efforts in respect of each of the identified threats[13]; and
- Immigration Intelligence Annual Threat Assessment (IIATA) - assessing threats across the immigration system and designed to complement the NBSA and *'provide the foundation for a deliverable control strategy to inform prioritisation and tasking across IE and UKVI*.'[14]

Other intelligence products

4.22 IE and BF analysts produce numerous intelligence products, under various titles, that perform most of the functions of the NIM's tactical assessments, target profiles, and problem profiles.

4.23 IE analysts sit on national and regional TCGs, feeding the results of their analyses directly into decisions about operational priorities, including in relation to prospective national campaigns, for example the targeting of illegal workers in a particular industry. UKVI also makes use of analysis when considering 'pilot' schemes targeting particular types of immigration abuse, for example individuals who have entered the UK legally under the points-based visa system and have gone on to claim asylum.

4.24 Periodically, IE produces *'intelligence analysis - products delivered by month & customer group'*. This provides details of all products completed for internal and external customers. The 1 April to 30 September 2015 version listed more than 200 products including *'Country Briefings'*, *'Contributions to Nationality Assessments'*, *'Research on Deportation Orders'*, *'Global Air Threat'* updates, and a *'EuroMed[15] Air Threat Assessment'*.

4.25 UKVI's October 2015 '*Threat Assessment Update'*, produced by IID, set out the the overall threat levels in relation to UKVI operations and individual areas of concern. The document contained an analysis of all information about abuses by applicants, broken down by the various immigration routes to the UK. The document also had a global 'risk by region' section, which detailed the different types of risk that individual overseas posts might encounter.

12 Part of the foreword to the BF Annual Threat Assessment 2015 issued 6/2/15 (page 4).
13 BF also had targets set by Her Majesty's Revenue & Customs relating to the identification of goods being imported into the UK without the required duty having been paid.
14 Stated on page 1 of the 2015 Annual Threat Assessment published September, 2015.
15 A UKVI region covering Europe and the Mediterranean.

4.26 The '*Threat Assessment Update'* document was evidence that UKVI and BF exchanged intelligence, linking risks identified overseas to possible resultant risks in the UK. There was also evidence of BF and IE working together to produce analytical products, for example products outlining trafficking profiles.

4.27 BF analysts produce analytical products to inform staff of the current intelligence picture as well as tactical threats at the border. Some are produced monthly on a regional basis, entitled *'Intel Update'* or *'Intel Picture'*. These monthly reports, also referred to as *'Intelligence Assessments'*, identify threats by commodity and risk level (e.g. Very High, High, Medium etc.) and outline successes or emerging trends. They also cross refer to ongoing operations. They were used by the regional TCGs to determine how resources should be directed.

4.28 BF analysts also produce quarterly *'Tactical Threat Update'* reports for the whole of Border Force, with assessments of all of the thematic areas contained within the BF Control Strategy, and whether the threat was 'emerging', 'new', 'renewed', or 'increasing', and detailing specific methods being used by people trying to evade border controls. One example of the type of issue covered in this report was a section with detailed statistics on the routes taken and nationalities of people encountered during 2015's mass migration across the Eastern Mediterranean. This section of the report drew on information from Frontex[16], overseas intelligence networks (RALON) and known results from the UK.

4.29 The *'Tactical Threat Update'* included the 'intelligence requirement' for certain threats. This gave clear instructions on the type of information that BF staff should be looking to collect when involved in operational activity against specific threats.

BF targeting

4.30 BF uses trade and carrier data to target people (e.g. known criminals or immigration offenders) and goods (illicit, prohibited and those liable for duty) arriving into the UK. Targeting teams dealing with specific themes (e.g. air passengers, air freight, container traffic etc.) create 'rules' by which to filter data obtained from travel documents and manifests etc., and identify potential threats.

4.31 BF was able to evidence that monthly tasking boards, attended by managers from targeting teams and NBTC, used analysis to review and update the targeting 'rules'. However, the Freight Targeting System (FTS), which had been in place for 10 years and is leased to the Home Office, could not be amended as its 'rules' were 'hard coded' into the system and any change required a software developer, for which there was a cost. Consequently, FTS 'rules' were not changed.

4.32 Managers reported that FTS was due to be replaced during 2016 with a system known as Advanced Freight Targeting Capability (AFTC). The new system would allow BF immediate access to change its 'rules' to improve the quality of the targets being identified. It was also expected to deliver efficiency savings.

4.33 Targeting teams disseminate 'alerts' to operational staff. Alerts are categorised depending on the likelihood of a successful outcome:

- **Category A**: *movements where there is strong evidence to suggest that an intervention will result in a positive outcome (for example detection of smuggled goods, identification of known target, collection of intelligence).*

16 http://frontex.europa.eu/

- **Category B**: *movements where there are specific indicators suggesting that an intervention is likely to result in a positive outcome.*
- **Category C***: movements where links to known problem routes, or to source or destination countries assessed as high risk, or other available information, provide reasonable grounds to suspect that an intervention may result in a positive outcome. BF officers should action category c alerts. BF officers must action all Category A and Category B Alerts. Category C Alerts should be actioned wherever available resources permit.*

4.34 BF provided targeting data for maritime and air freight for the 12 months up to February 2015 and up to February 2016.

Figure 4: maritime and air freight targeting data

		12 months to February 2015			12 months to February 2016		
Category		**A**	**B**	**C**	**A**	**B**	**C**
Maritime freight	Alerts	100	3,071	25,222	132	2,132	23,443
	Successes	39 (39%)	307 (10%	793 (3%)	82 (62%)	336 (16%)	840 (4%)
Air freight	Alerts	1,034	5,592	55,373	1,492	4,550	36,054
	Successes	651 (63%)	2,126 (38%)	1,698 (3%)	1,018 (68%)	1,320 (29%)	958 (3%)

4.35 This data showed an improvement in the success rate for category C targets. In 2012/13, only 505 out of over 43,000 freight consignments identified as category C resulted in a successful outcome, wasting time and effort in the selection and physical examination of these consignments, and delays to the flow of legitimate trade.[17] BF commented that it now issues significantly fewer targets (a drop from c.150,000 in 2013/14 to c.70,000 in 2015/16), but that they are of a higher quality and outcomes have been maintained.

IE and BF knowledge products

The Immigration intelligence manual

4.36 The Immigration Intelligence Manual (IIM) was produced by IE. It is available to all staff who have access to the Home Office intranet. The IIM was first published in 2013. It was last updated in February 2014, and therefore does not reflect the numerous changes IE has since made to its structures and processes. However, some of these changes are covered by separate operational instructions. IE reported that the IIM will be replaced in 2016 by a Professional Practice Manual (PPM) and the Border Force Intelligence Manual (BFIM).

4.37 The IIM sets out all basic intelligence processes and procedures. It also explains the legislation under which intelligence staff operate. The latter includes the requirement to adhere to both the Data Protection Act 1998 and the Human Rights Act 1998 when deciding about creating an intelligence record on any individual.

4.38 However, IIM does not provide explicit instructions or guidance, for example it does not mandate the minimum checks to be completed at each stage of the intelligence process, or direct non intelligence staff regarding their responsibilities for gathering and submitting

17 http://icinspector.independent.gov.uk/wp-content/uploads/2013/11/An-Inspection-of-Border-Force-Freight-Operations-FINAL-PDF.pdf.

intelligence. IE and BF Intelligence Directorates each publish operational instructions for staff relating to specific areas of intelligence work. These instructions supplement the IIM and are used to inform about changes to processes, via 'global' emails to IE and BF staff. Although instructions are normally cross referred to IIM, IIM is not updated to reflect them.

IE and BF systems products

Intelligence Management System

4.39 IE uses the Intelligence Management System (IMS) to record information (normally referred to as 'allegations') received from members of the public, crimestoppers and other government agencies, and referrals from members of staff. As well as providing a record of each allegation, IMS has work flow functionality so that information/intelligence can be tasked to different units and tracked to completion. Use of IMS is subject to the IMS Guidance document published on the Home Office intranet.

4.40 Allegations sent to BFNIH by members of the public using the online form are automatically uploaded onto IMS, which BF then uses to task and track information/intelligence in the same way as IE. However, BF does not use IMS for information received from staff, or from another law enforcement agency, or from members of the public via telephone or email. Instead, BFNIH and BF regions record this information on spreadsheets held on local shared drives, and available only to staff with access to those drives.

4.41 BFNIH maintains a system of Unique Reference Numbers (URNs) for information received. The URN is retained if the information is passed to a regional team. BF guidance states that regional teams should refer any information they receive directly to BFNIH so that a URN can be issued. File sampling indicated that this was happening where the regional team decided the information should be developed, but not where it decided 'no further action' was required.

ATHENA

4.42 At the time of inspection, IE and BF intended that ATHENA should be used by staff to record Intelligence Reports (IRs) created for internal and external dissemination, thereby providing a corporate record of information assessed as having some intelligence value. ATHENA was accessible only to intelligence staff in IE and BF.

4.43 The IIM states that '*All Home Office Intelligence Officers are required to record information on the ATHENA Intelligence system, in accordance with the system operating procedures and Departmental Security Unit instructions on the use of computers and IT.'* It goes on to state that *'IRs must also meet at least one of the DPA standard grounds:*

- The interests of national security
- The prevention or detection of crime or disorder
- The apprehension or prosecution of offenders
- The assessment or collection of any tax or duty
- A significant public interest.'

4.44 ATHENA operated under a contract from a third party provider, Serco. In October 2015, the senior responsible officer for the system, who at the time of the inspection was the director of intelligence for IE, had identified in a document setting out the user requirement for the new

single intelligence platform that ATHENA was not compliant with either Data Protection or Freedom of Information legislation. This was because there was no mechanism for the review, retention or deletion of information.

4.45 The SRO wrote that the Information Commissioner (ICO) had described ATHENA's lack of compliance as 'unacceptable', and the Home Office risked being fined up to £2m per offence should the ICO take further action. Non compliance presented a barrier to wider data sharing, which SIP would overcome.

4.46 File sampling revealed an inconsistent approach to the recording of intelligence on ATHENA. For example, staff in one OIU said they were routinely recording the outcome of employer compliance visits on ATHENA as intelligence reports. Staff were aware that ATHENA was due to be switched off at the end of May 2016 (to be replaced by a new system), but explained that they were creating IRs so that the intelligence would be *'available to all colleagues within intelligence'*. Meanwhile, staff in other intelligence units were creating IRs only to disseminate intelligence to external partners, and were using IMS for internal referrals.

Other systems

4.47 In IE, the National Operations Database (NOD) must be updated with all information relevant to ICE team activity, including outcomes, for example details of persons arrested and a debrief of the operation. BF officers who made seizures at the border were required to update Centaur (an HMRC owned database of individuals concerned with or suspected of involvement in the importation of illicit or duty evaded goods). In addition, both IE and BF had to update the Casework Information Database (CID) when they encountered immigration offenders or suspected offenders.

4.48 IE and BF staff were often required to update multiple screens on different systems with the same information as these systems were not integrated. For example, when an IE enforcement operation resulted in an arrest, the information had to be recorded on NOD, ATHENA and on CID. When BF made a seizure the information was recorded on Centaur, detailing the offender, the commodity and amount seized etc. An information report was also placed on Centaur so that other systems, for example Semaphore (advanced passenger information), would identify offenders when their data was 'washed' against Centaur.

4.49 During interviews and focus groups, operational staff reported that updating IT systems was a significant call on their time. Inspectors confirmed this during file sampling, when they were required to consult several databases to gain an accurate picture of how an allegation or intelligence record had been handled.

4.50 BF Intelligence staff reported that they did not have access to all of the IT systems required to undertake thorough research, in particular to Centaur and Semaphore. Access was available in some regional offices but not in others.

4.51 Centaur could be accessed only through HMRC's Stride network, which IE and BF staff could access through the Home Office POISE network. The Home Office paid for a certain number of licenses for Stride. Semaphore was not accessible via POISE, but used its own more secure network. As with Centaur, the number of licences was limited, and any extension of Semaphore would also require special cabling etc., which would be expensive.

4.52 Senior managers were aware of staff concerns and pointed to the difficulties of providing routine access to these systems, not least the cost. However, they acknowledged that intelligence staff would benefit from greater access as it would facilitate their research. At the time of the inspection, a review of licence holders for Centaur and Semaphore was being conducted in order to identify opportunities to reallocate access where it was currently limited or not available.

Transformation: single intelligence platform

4.53 IE, BF and HM Passport Office had been collaborating to create a new IT platform to meet their intelligence needs, with IE taking the lead. The Single Intelligence Platform (SIP) was due to 'go live' on 1 May 2016, when it would replace ATHENA. SIP was being developed using an 'agile development model', which meant that the functionality of the system would be developed and implemented in stages. No strict timelines had been set for the project, so that new functionality could be thoroughly tested and made stable before it was released.

4.54 The user requirement document outlined 14 benefits that the new system would provide. Figure 5 refers.

Figure 5: Proposed benefits of SIP, as outlined in user requirement	
Relational POLE (People, Objects, Locations, Events) database.	Superior management information functionality
Enhanced search functionality	Superior reporting functionality
Integrated workflow management functionality	Accessibility to intelligence and non intelligence staff
Repository for Border Force seizure and excise data	Improved allegation management
Broader range of document production	Interface with internal Border Force intelligence systems
Review, retain, delete functionality	interface with external systems
Assurance functionality	Immediate event notification mechanism

4.55 The user requirement document outlined the benefits against each requirement and gave an overview of other benefits, including efficiency savings, financial savings and legal compliance, and the removal of a lot of duplication for IE and BF. The first release would enable intelligence reports to be created and disseminated.

4.56 Senior managers stated that the creation of intelligence reports in a relational database would provide immediate benefits in terms of automatically identifying duplicate records or records where an 'entity'[18] existed more than once, which ATHENA did not do. For example, if a mobile phone number was linked to two IRs the system would highlight this and provide immediate access to both reports via hyperlinks.[19] Future functionality included the ability to chart connections between entities to create richer intelligence pictures.

4.57 A decision had been taken not to upload ATHENA data into SIP, as it was not technically compatible. The value of the system would increase over time as new IRs were added and the body of information increased.

18 Expanded to include, for example telephone numbers and vehicle registration number (unique and searchable data items).
19 A hyperlink is a clickable reference that links to other information on the same page or somewhere else on the system.

Home Office Data Analytics Capability (HODAC)

4.58 In addition to SIP, the Home Office had also initiated a project (HODAC) to deliver increased search capability across its IT systems. It was envisaged that HODAC would initially provide search capability of the data archived from ATHENA, and then extend to other systems, including relevant external systems.

Conclusions

4.59 Both IE and BF have developed and implemented the key components of the National Intelligence Model (NIM), adapted where necessary to suit their particular circumstances and needs. Therefore, to the extent that NIM compliance is the measure of being 'intelligence-led', both have largely achieved this.

4.60 However, at the detailed level some elements are either missing or not working effectively. This is particularly true of 'systems products' (relevant IT systems and data enabling information/ intelligence to be stored, retrieved, researched, developed etc.). For example, while the Intelligence Management System (IMS) provides the functionality to record information received and to track what is done with it, BF is not using this system except for allegations submitted via the online reporting form, and is instead using local spreadsheets which are not accessible to BF staff in other offices and regions, or to IE.

4.61 Access to certain IT systems, required to check whether new information connects to what is already known, is limited and uneven. It is dictated more by history (they are mostly legacy systems), geography (terminals are where they were needed under old organisational structures) and the cost of making changes (additional licences and new installations) than by any sense of current business needs, although a review of licence holders for Centaur and Semaphore was underway at the time of the inspection. For operational (frontline) staff the duplication of effort required to update two or three non-integrated systems with the same information acts as a powerful disincentive to feeding the intelligence function.

4.62 IE, BF and HM Passport Office had been collaborating on a new Single Intelligence (IT) Platform that will better meet their intelligence related business needs. The incremental approach to development and roll out of new SIP functionality was prudent, and over time SIP will provide significant improvements in the Home Office's search and data matching capabilities. In the short term, the planned switching off of ATHENA (at the end of May 2016) had caused inconsistencies in how Intelligence Reports were being created and stored.

4.63 IE and BF both have NIM compliant Tasking & Coordination processes in place to identify operational priories and determine resource allocations at strategic and tactical levels, and both produce a range of intelligence products to feed these processes, with intelligence analysts in attendance at Tasking & Coordination Group meetings. Both IE and BF allow for regional and local differences (threats and opportunities) in terms of how national priorities are interpreted and implemented on the ground. However, the inspection revealed that local TCGs were rejecting 'packages' that met national and regional priorities on the basis that they did not meet local priorities, and some intelligence staff complained that operational staff were more opportunity-driven than intelligence-led.

4.64 Ostensibly, the primary knowledge product used for guidance by both IE and BF intelligence staff is the Immigration Intelligence Manual. This was produced by IE in 2013 and last updated in 2014, since when both IE and BF have undergone significant structural changes and changes to processes. In practice, IIM is a high level statement of principles rather than a 'how to'

manual, and both IE and BF Intelligence issue separate detailed operational instructions relating to specific processes and changes. The IIM and operational instructions are available to staff via the Home Office intranet. Searching for specific guidance sometimes requires several attempts, and it is not easy to know whether the results are the latest version or whether there is other relevant guidance. However, the IIM is to be replaced in 2016 by a Professional Practice Manual (PPM) and a BF Intelligence Manual (BFIM).

Recommendations

The Home Office should:

- Ensure that the Intelligence Management System (IMS) is being used to its full potential, specifically that BF uses IMS to record all allegations it receives not just those received via the online reporting form, and desists from using local spreadsheets.
- Pending the development and implementation of full Single Intelligence Platform (SIP) functionality, review IE and BF user access to IT systems that support key intelligence functions, in particular the receipt, evaluation and checking of information for links to what is already known, and where necessary reallocate or extend licences and system availability.
- Ensure that the Professional Practice Manual when produced is readily accessible and searchable via the Home Office intranet, and that future amendments to it identify what has changed (and why) and are clearly marked with the operative date. In the meantime, cleanse the Home Office intranet of intelligence related material that is no longer valid, and collect extant operational instructions in one place for ease of reference.

5. Learning from previous inspections and reviews

Independent Chief Inspector inspections

5.1 In 2011, the Independent Chief Inspector (ICI) published '*Preventing and detecting immigration and customs offences: A thematic inspection of how the UK Border Agency receives and uses intelligence*'.[20] In 2014, the ICI published '*An Inspection of the Intelligence Management System*'.[21]

5.2 The key areas requiring improvement identified in these two inspections were:

- the management of allegations (received from members of the public);
- the defining of intelligence requirements;
- the effectiveness of intelligence, analysis and management information;
- the tasking process; and
- Training.

5.3 According to the Home Office, it has already made the recommended improvements or is in the process of making the necessary changes in response to the two inspection reports. These are summarised below.

Allegations

5.4 With regard to the management of allegations, the Home Office introduced the Intelligence Management System (IMS) in September 2012. IMS is now used by IE to record all allegations, however these are received. BF also uses IMS to record allegations received centrally via the online reporting form. But, BF records allegations received locally at ports on locally maintained spreadsheets and databases that are not linked or uploaded to IMS, and are therefore not centrally retrievable.

Intelligence requirements

5.5 Both IE and BF produce documents in which their intelligence requirements are defined. The IE Annual Threat Assessment and the BF control strategy and set out what intelligence is required alongside the threats that need to be addressed. However, based on focus groups and interviews, and key documents such as minutes of TCG meetings, they have yet to prove effective in encouraging operational staff to report the intelligence they acquire during the course of their work.

20 http://icinspector.independent.gov.uk/wp-content/uploads/2011/02/Preventing-and-detecting-immigration-and-customs-offences.pdf.
21 http://icinspector.independent.gov.uk/wp-content/uploads/2014/10/An-inspection-of-the-Intelligence-Management-System-FINAL-WEB.pdf.

Intelligence, analysis and management information

5.6 Both IE and BF produce reports analysing all activity and threats so that trends can be identified. Since 2013, IE has produced a comprehensive monthly performance pack for IE and UKVI, which provides statistics across a range of data, including the volume of information received, sources of intelligence, the number of operations and the outcomes. BF also produces statistics on the volume of information received and the number of alerts issued or targets produced. However, BF does not produce any statistics on outcomes linked to the intelligence.

Tasking

5.7 Both IE and BF have tasking processes and structures (Tasking & Coordination Groups) at national, regional and local levels that set strategic and operational priorities and look to ensure that the necessary resources are allocated to deliver them.

Training

5.8 The recommended improvements in training focused on the requirement to ensure that all staff using IMS received adequate training, supported by up to date guidance. IMS users receive 'on the job' training and the Home Office has produced an 'IMS User Guide and Tutorials' document which is available to all staff on the HO intranet.[22] At the time of the inspection, classroom based IMS training was also available; all new staff received this as part of their induction, and the IMS training module was available to existing staff who required refresher training.

Deloitte Review of intelligence processes

5.9 In 2014, IE and BF appointed the consultancy firm Deloitte to review their existing intelligence processes. Each had its own objectives for this review.

Figure 6: objectives for the Deloitte review

Immigration Enforcement	Border Force
Review intelligence in relation to four specific areas: • The value and impact of different intelligence products; • The flow of data (i.e. information and intelligence) into Immigration Intelligence (II); • The tasking process; • The feedback loop (how customers respond to products).	To achieve financial savings of 4% (all cashable) in FY14/15; To provide a platform for further efficiency savings in FY15/16; final numbers have not been specified yet, but they are likely to be similar to those affecting FY15/16; To identify efficiencies beyond those identified above, to close gaps in provision or enable re-investment into high value Intelligence and targeting services; and To identify opportunities to improve intelligence services, such that they improve the efficiency and effectiveness of operational customers (internal and external).

22 Last updated 25 September 2013.

BF response to Deloitte: Target Operating Model

5.10 In March 2014, BF responded to the Deloitte report, referring to the planned publication of a new Target Operating Model in April 2014. The key elements of the new Target Operating Model are set out below:

- Enable improved frontline delivery by strengthening our focus on our objectives;
- Build stronger, two way relationships with our customers and partners, through clearer ways of working, well defined feedback approaches and simplified lines of communication;
- Consolidate the number of different products we provide, and increase quality;
- Remove duplication by standardising and improving critical processes, including debriefing, to allow a better prioritisation of our effort;
- Simplify our organisation structures so we can operate as one, and so that it is easier to understand how we work;
- Improve the distribution of our officers, improving our alignment to risk and demand;
- Improve our supervision ratios, applying consistent reporting relationships;
- Improve our officers' access to critical systems, customers and partners;
- Simplify and strengthen our governance, fully adhering to NIM principles; and
- Enable smarter decisions by improving the information available to our managers.

Continuous Improvement

5.11 As part of the implementation of its Target Operating Model, BF created Analysis and Development Teams (ADT), and an ADT Operating Model was published in March 2015. During the transition to ADTs, BF asked the Home Office's Continuous Improvement Unit (CIU) to help develop ADTs in a way that ensured processes were consistent and staff capability was sufficient to meet the aspirations set out in the ADT Operating Model. In September 2015, the ADT Project Board agreed that the initial focus of the ADT teams would be the receipt of intelligence and its allocation for analysis and development.

5.12 The CIU reported in October 2015[23] and its key findings were that *'The process for receipt and allocation of Intel is inefficient and inconsistent, encourages duplication and the completion of nugatory work. This unnecessarily large administrative burden reduces the time that is spent on value added intelligence gathering and analysis."*[24] The central recommendation from that report was the development of a standard process for receipt and allocation by the BFNIH and ADTs, which would involve:

- establishing principles for a universal system, underpinned by single ownership of Intel;
- conducting a series of workshops to identify and develop best practice; and
- developing a single set of standard operating procedures and creating optimal workspaces with visual management.

5.13 The BF Continuous Improvement Team carried out a number of workshops, and on 20 November 2015 the ADT name was dropped and the ADT units were renamed 'BF Intelligence [Region]' e.g. BF Intelligence North. However, as at mid May 2016 the ADT Operating Model had not been revised.

23 ADT D2 Describe Report by the BF Continuous Improvement Unit dated 26/10/2015.
24 This was contained within the Executive Summary on slide 2 of the report.

5.14 The continuous improvement work resulted *inter alia* in the BFNIH being authorised to mark as 'No Further Action' (NFA) information it assessed as having little or no value, rather than being required as under the ADT Operating Model to pass the information to an ADT. This meant that ADTs/BF Intelligence Regions were no longer having to record and process information that had already been assessed.

5.15 BFNIH also sent copies of every Immediate Event Notification (IEN)[25] to every region. Each BF regional Intelligence Team (BFIT) then had to record and log all information that was received. As a result of the continuous improvement work, regional offices were empowered to decide on the relevance of IENs, and could delete those deemed not relevant rather than record and process them. Staff reported that this made them more efficient.

IE response to Deloitte

5.16 IE published its response to the Deloitte report in November 2014[26], proposing a '*new future state design for intelligence*.' The response contained detailed solutions to the issues identified, and IE stated that by implementing these solutions they would;

- Categorise threats using a person centred approach focused on immigration status and risk of harm/cost to the system, to reduce overlap and duplication;
- Cascade these threats throughout the organisation and help develop priorities based on these which are aligned for all teams and lead to more targeted activity;
- Align business planning and tasking cycles to ensure resourcing is focused on delivering the wider organisation's priorities, and to reduce the disconnection between the strategic and operational tiers of tasking and coordination;
- Create a more collaborative approach to all tasking, with clearer expectation setting and greater tracking of tasks, actions and outcomes to increase accountability;
- Develop an enhanced culture within the IE where the value of intelligence is recognised by all teams and at all levels, leading to increases in the volume and quality of information and intelligence;
- Facilitate the development of more robust recommendations through greater interaction between Intelligence and frontline teams;
- Ensure that the management information collected is fit for purpose for IE, telling the organisation what it needs to know, rather than focusing on what is easy to collect, and showing the value that intelligence adds and evidencing 'what works'.

5.17 This work led to the restructuring of the whole intelligence process, which saw the creation of the RED team functions and the extension of the IIC's working hours. IE also employed continuous improvement techniques, gathering evidence of how new processes were working after the re-structure. This included options for how the marriage referral and assessment unit would operate.

Work in progress

5.18 IE and BF have each embarked on major transformation programmes with a view to improving how intelligence is managed.

25 Where an event at the border meets agreed notification requirements, e.g. the volume of a commodity seizure, BF must submit a notification of the event in order that all BF become aware of the event. It is used to disseminate intelligence across BF.
26 Immigration Intelligence – Driving an Intelligence Led Organisation. Final Deliverable (18/11/2014).

5.19 BF began in 2014 looking at three themes: people, processes, and technology. These were covered by two key transformation projects: professional skill sets for staff (full integration of NBTC/passenger targeting); and A truly intel-led organisation (effective intelligence flows; delivery of a single intelligence platform; advanced freight targeting capability; operational decision manager in NBTC; and delivery of a data analytics capability for BF).

5.20 The transformation programmes were ongoing at the time of the inspection. Continuous Improvement reviews ensured that changes were evaluated and new processes amended where necessary.

Intelligence professionalisation programme

5.21 IE and BF had worked with the National College of Policing, the National Crime Agency (NCA), Her Majesty's Revenue & Customs (HMRC) National Offender Management Service (NOMS), the Cabinet Office, and National Counter Terrorism Policing on a programme to establish professional standards for its intelligence roles. The use of the National Occupational Standards developed by Skills for Justice[27] for law enforcement intelligence and analysis roles meant that accreditation gained by IE and BF staff would be recognised by other agencies, such as the police and NCA. Under the IE and BF Intelligence Professionalisation Programme (IPP), which was due to go live in March 2016, staff would be able to gain accreditation by collecting workplace evidence over an 18 month period. The accreditation would remain valid for three years, and the National College of Policing would maintain a register of accredited staff.

5.22 The following roles were covered by National Occupational Standards:

- IPP assessor;
- Intelligence analyst;
- Intelligence analyst researcher;
- Operational intelligence researcher;
- Intelligence unit supervisor;
- Intelligence manager;
- Director of intelligence;
- Intelligence analyst;
- Senior intelligence analyst; and
- Head of intelligence analysis.

Analyst training

5.23 In addition to the IPP, IE analysts received training through Business Embedded Trainers (BETs), as well as attending formal training courses. In 2015, the following formal courses had been delivered:

- Analysis foundation (2 courses, 5 days each);
- Communications data analysis (2 courses, 5 days each); and
- Briefing, peer review and crafting the intelligence product (pilot courses).

27 https://www.skillsforjustice-ppf.com/.

The following courses were planned for 2016:

- Analysis foundation (2 courses, 4 days each);
- Facilitation of analysis (3 courses,half a day each);
- Analytical briefing (3 courses, 1 day each); and
- Crafting the intelligence product (4 courses – 3 days each).

5.23 During the inspection, staff in focus groups and interviews said that training courses were not always available for analysts due to budgetary constraints, although they had received training from the BETs within the analysis teams.

5.24 Border Force analysis had also developed bespoke training in conjunction with HMRC and the NCA, delivery of which was a collaborative effort involving all three agencies.

5.25 For roles not covered by the National Occupational Standards, for example Targeting Staff, BF was mirroring the IPP process to ensure that staff in those roles could also develop against an agreed set of standards. These were being developed at the time of the inspection.

Conclusions

5.26 IE and BF have both demonstrated their commitment to learning and improvement in relation to their management and use of intelligence. Two previous inspections, including one of the then UK Border Agency in 2011, identified a number of key areas where improvements were required, and IE and BF have either implemented or were making progress with all of these.

5.27 In 2014, Deloitte was commissioned by both IE and BF to conduct a review of intelligence. While their specific objectives differed, IE and BF were both looking to Deloitte to identify potential improvements in their structures, processes and impact. Each produced a detailed response to the review, setting out their respective visions for the intelligence function. These involved major transformation programmes, which both IE and BF have been pursuing, applying continuous improvement principles and on occasion seeking input from the Home Office Continuous Improvement Unit.

5.28 A significant element of transformation is the Intelligence Professionalisation Programme (IPP), which was due to go live in March 2016, and through which intelligence staff would be able to gain accreditation from a national organisation (the IPP Board) and which will be recognised by other law enforcement agencies

Recommendation

The Home Office should:

- Conduct a stock take in relation to the implementation by IE and BF of their 'visions' for intelligence set out in response to the 2014 Deloitte review, and identify and prioritise those elements that require further work.

6. The Intelligence 'cycle'

Introduction

6.1 The process by which information is collected, assessed for its intelligence value, shared, and used to inform and drive decisions and actions is routinely described as the 'intelligence cycle'. While the notion of a 'cycle' works at the highest level, it does not capture fully the flows and dependencies that make up any organisation's intelligence processes. Moreover, to be fully effective these processes must be tailored to the specific business needs and opportunities of the organisation, so while there are certain common elements there is no 'one size fits all' model.

6.2 The inspection did not examine in detail every aspect of each stage of the IE's and BF's intelligence processes, but focused on key elements, looking at how they were designed to work and examining the evidence for whether they were working efficiently and effectively. Where the inspection found differences of approach between IE and BF, it looked at the rationale for these differences.

6.3 Intelligence practitioners give different labels to the various stages of the 'cycle'. The inspection used the following:

Requirement setting

Collection

Evaluation

Analysis and assessment

Dissemination and feedback

Requirement setting

Strategic

6.4 Both IE and BF produce annual strategic assessments that set out the range of threats they are required to combat, what is known about each of them and where there are gaps in knowledge. The latter inform the 'intelligence requirement', that is the particular information that IE(UKVI) and BF and their operational partners want to acquire, This is broken down by theme. For IE, for example, the themes include human trafficking and illegal working, and for BF they include clandestine entry and immigration rules abuse.[28]

28 The 2015 BF Annual Threat Assessment (ATA) and Control Strategy (CS) graded BF's level of knowledge of 27 thematic areas, such as Alcohol; Medicines; and Products of Animal Origin, broken down by modes of entry to the UK, for example Roll On/Roll Off ferries The 2016 inspection of General Aviation and General Maritime noted that BF's knowledge was rated as 'poor' in 20 of the 27 thematic areas for GA, and for 26 of the 27 areas for GM. BF staff interviewed referred to the many 'unknown unknowns' in relation to the threats and risks surrounding GA and GM. http://icinspector.independent.gov.uk/wp-content/uploads/2016/01/ICIBI-report-on-GAGM-14.01.2016.pdf.

Tactical/operational

6.5 At the tactical or operational level, intelligence requirements typically focus on known or suspected offenders, associates or those fitting a threat profile, locations or addresses, or particular (criminal) activities or events, often referred to as 'entities'. However, based on the minutes of IE regional tasking boards, intelligence requirements do not feature explicitly in TCG discussions.

Collection

'Routine', 'Tasked' and 'Volunteered' Information/intelligence

6.6 Intelligence-led organisations have different capabilities and opportunities for collecting information to fulfil their intelligence requirements. However, all information/intelligence collection falls into one of three broad categories: the trawling of relevant information and data sources, some parts of which may be automated, machine to machine; the tasking of staff and others to collect required information/intelligence using a variety of authorised means; and the collection of information/intelligence that is volunteered.

6.7 The IIM describes these as follows:

> *Routine information/intelligence collection*
>
> *On a daily basis a set collection of Home Office and external systems, both open and closed sources, should be scanned.*
>
> *Tasked information/intelligence collection*
>
> *This information is deliberately sought and collected to support research, development or analysis as sanctioned through the tasking and coordination process or local requirements. This could be in response to the Agency intelligence requirement or intelligence collection plans.*
>
> *Volunteered information/intelligence collection*
>
> *Information/intelligence may come directly into the intelligence unit from members of the public or internal/external stakeholders.*
>
> *IE and BF sources of Information/Intelligence*

6.8 In August 2013, the Home Office introduced an online reporting form[29] to enable suspicious activity reported by members of the public to be routed automatically onto IMS.

6.9 Up until July 2015, IE monthly performance data included a breakdown of the sources of allegations recorded on IMS. From August 2015, following a management review of the performance packs, this data was no longer collected in this format.

6.10 Figure 7 shows the sources of allegations recorded on IMS (IE and BF) between August 2014 and July 2015.

29 https://www.amsallegations.homeoffice.gov.uk/default.aspx/RenderForm/?ID=bMocLLD1aE8&F.Name=Lf62UB7cz4C&HideToolbar=2&fs2s=Xb9oKWcFuYZ&fs2c=GjAbepE5obj&fs2svr=LPA.

Figure 7: sources of allegations recorded on IMS between August 2014 and July 2015	
Source	Number of allegations
Public	49109
Other government departments	17818
Crimestoppers	7540
MP	150
Total	**74617**

6.11 In interviews and focus groups, staff commented that IE was overly reliant on allegations received from members of the public, and did not gather enough intelligence through enforcement teams and Field Intelligence Officers (FIOs). As a result, it was reactive rather than proactive. Their views echoed the 2014 Deloitte report, which found '*some reliance on public allegations which are not the most efficient way for IE to direct its activity*'.

Internal referrals

6.12 An 'internal referral form', which mirrors the public reporting form, is available to staff on the Home Office intranet. The internal referral form also routes information directly onto IMS. IE performance data did not breakdown how many of the IMS allegations recorded were made by staff using the online referral form, so the extent of internal reporting was unclear.

6.13 However, the IE risk register for December 2015 noted *'there is a risk that Crime and Enforcement teams are not using IMS'* which could lead *'immigration intelligence [to] take inappropriate action because they are not aware of all the facts'* resulting in *'possible harm to staff, reputational damage or loss of confidence in the department'* As mitigation, a 'deep dive' review of intelligence support had commenced, which by March 2016 had led to changes to the training of ICE team staff, improved communications regarding the referral form, and an immigration intelligence website incorporating up to date guidance for intelligence staff. However, the 'Enforcement Guidance & Instructions', used by ICE team staff, which describes the legal frameworks for recording and disseminating intelligence externally, but not how to share it internally, had not been updated.

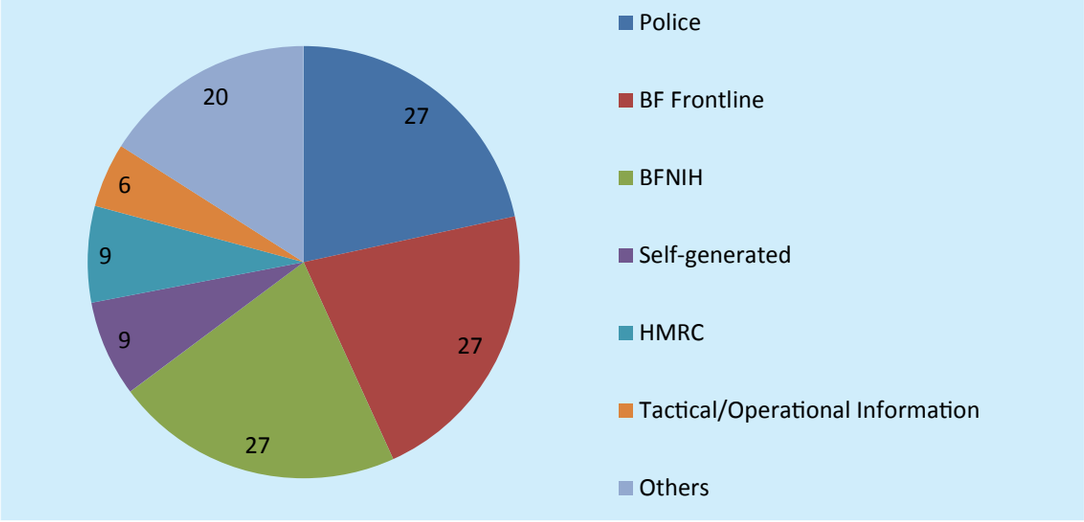
6.14 In UKVI, Temporary Migration staff said before new structures were introduced in 2015 there had been an Intelligence team that had acted as a thematic hub for temporary migration intelligence, and another for permanent migration intelligence, to which staff could refer information, for example if they found something relevant in an application they were handling. These teams had been disbanded, and staff were now expected to make all temporary and permanent migration referrals using the 'internal referral form'. Meanwhile, sham marriage referrals were to be made to a new Marriage Referral Assessment Unit (MRAU), which was also introduced in March 2015.

6.15 Guidance for UKVI caseworkers, 'Casework instruction – referrals to intelligence', which was available on the HO intranet, had not been updated since November 2014, and still referred to old structures and reporting arrangements. It made no reference to the online referral form. Staff who despite this had used the online referral form said that it was 'not user friendly', it took time to access via the intranet, and was time consuming to complete.

6.16 BF guidance[30] requires frontline staff to use IMS to refer allegations of immigration and customs abuse, so that a corporate record is created, enabling the information to be correctly processed (assessed, researched, developed or disseminated internally and/or externally). During interviews and focus groups, BF staff reported that they did not use IMS, but instead referred information either to BFNIH or to their own BFRIT via email or telephone calls.

6.17 BF data showed that in September 2015 frontline officers were the source of over 1,500 pieces of information/intelligence. In January 2016, the figure was less than 500. Of 125 records sampled (25 from each regional intelligence unit then in existence; BF has since reduced to four regional units), the most common sources of information/intelligence were the Police, BF frontline staff, and BFNIH. None of the 27 pieces of information/intelligence received from BF frontline staff had been submitted using the 'internal referral form'. Figure 8 refers.

Figure 8: sources of Border Force information for intelligence purposes



Note: 'Others' refers to submissions from NCA, Regional Intelligence Units, Public allegations made via IMS, CFI Teams and International Liaison Officers, who submitted 5 or fewer pieces of information/intelligence.

Evaluation

IE

6.18 Under 'receipt of intelligence' the IIM contains the following statement:

> *'All incoming information and intelligence is assessed against set criteria to identify risk, and or threat, or information and intelligence that meet local or national priorities.'*

6.19 Since November 2015, RED teams and IIC have acted as a filter for all information received through IMS, triaging it so that only useful information linked to IE priorities is passed on for further action. Intelligence and enforcement managers sit on both national and regional tasking and coordination boards and feed priorities back to the RED teams and IIC so that they make the correct decisions about the incoming information.

30 Guidance on Receiving & Disseminating Intelligence, dated 8 May 2015.

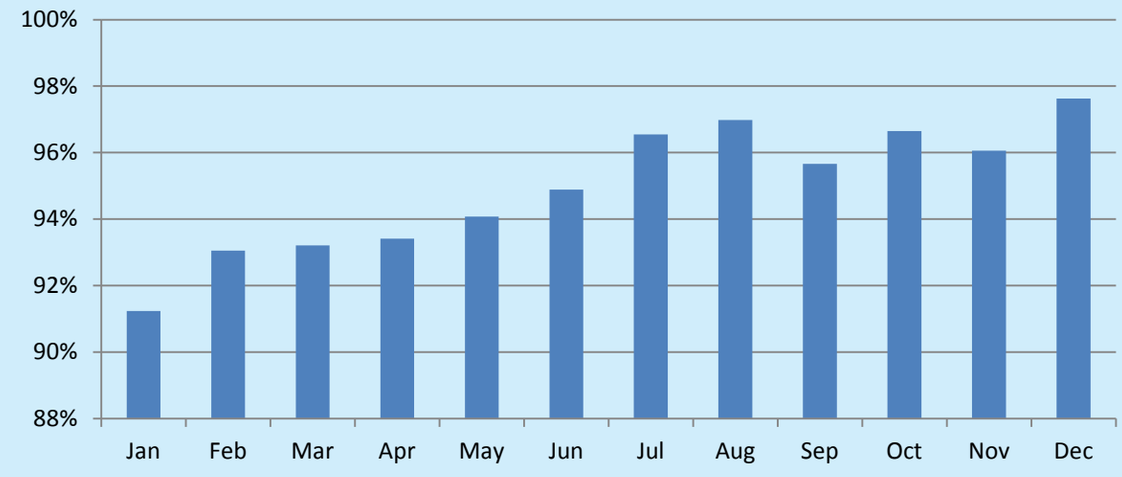
6.20 IIM states that as part of a 'receipt profile'[31] intelligence staff should 'apply the IHM grading'. The Intelligence Handling Model (IHM) is immigration centric and therefore not used by BF. It categorises information against three criteria, 'threat or risk', credibility' and 'priority', in order to support IE in '*providing the right information to the right people, on time.*' The criteria as set out by IE are shown in figure 9.

Figure 9: intelligence handling model criteria

Level of threat or risk (denoted by a single letter associated with the traffic light grading system)	**Level of credibility** (denoted by a number in the range 1-3)	**Level of priority** (denoted by a numerical value in the range 1-3)
RED The risk and or threat exists	**1** The intelligence has some credibility	**1** Relevance to priorities (set nationally and locally)
AMBER Immediacy of action required	**2** The credibility cannot be determined	**2** The information needs of enforcement and crime teams (as outlined by them)
GREEN Relevance to immigration law	**3** The intelligence is lacking in credibility	**3** The scale of the immigration breaches in terms of volume or complexity
WHITE Non relevance to immigration law		

6.21 From June 2012, the then UKBA adopted a performance target requiring information to have been assessed within 48 hours of receipt. IE has continued to use this target, which it refers to as 'the compliance rate'. Figure 10 shows IE's reported compliance rate throughout 2015. The RED teams were created in November 2015.

Figure 10: IE Intelligence compliance rates for 2015



31 A term used within the IIM that describes a set of steps or actions that should be taken upon receipt of information or intelligence.

6.22 Information received between 1 July and 30 September 2015 was inspected. Of the 39 pieces of information examined that were assessed as 'no further action', 27 (69%) had been assessed within 48 hours of receipt, and four did not have an IHM grading recorded on IMS. Of the 99 cases sampled that were referred to a Tasking & Coordination Group for action, 86 cases (87%) either met the 48 hour timeframe or this did not apply (as the allegations were not received from members of the public).

BF

6.23 Much of the information BF receives from internal and external sources (e.g. NCU, Police, Overseas law enforcement agencies etc.) goes directly into the BF National Intelligence Hub (BFNIH). Where information is received first by a BF regional Intelligence Team (BFIT), the BFIT will assess it. Information assessed as actionable must be referred to the BFNIH to attach a Unique Reference Number (URN) and to allocate it to a regional unit to deal with. The BFNIH will run URN and 'deconfliction' checks to ensure that no other Home Office or other agency is working on any of the 'entities' mentioned to ensure that operations are not compromised or actions duplicated. In practice, most new intelligence is passed to a BFIT, who can reallocate it but must inform the BFNIH.

6.24 The BF guidance for receiving and disseminating intelligence states that the *'Border Force Intelligence receiving Officer, as first recipient of operational intelligence, is responsible for inputting that intelligence onto a system (Mycroft Athena or Centaur – a system used to log commodity seizures) if not already recorded.'* BFNIH uses a bespoke database to record the information it receives. For the 12 months from 1 April 2015 to 31 March 2016, 28,000 entries were recorded on this database. However, file sampling identified that BFITs recorded information on locally-maintained, non standardised spreadsheets. This information was not searchable centrally, and could not easily be linked to any further information that was received.

6.25 In interviews and focus groups, BF staff said that there was no 'go to system' for intelligence in BF. Most information about customs seizures was recorded on Centaur, the legacy Customs system, which was not linked to IMS or other systems, and therefore the intelligence recorded by BF was not available to IE and UKVI.

6.26 Information received by BF between 1 July and 30 September 2015 was examined to check whether the initial assessment was completed within 48 hours; whether there was an audit trail for the action taken; and whether the action taken was appropriate.

6.27 Of 50 pieces of information received and dealt with by the BFNIH, all 50 had been assessed within the 48 hour target time (the longest time taken 5 hours and 27 minutes). Of 125 pieces of information received and assessed by the then five regional offices (25 from each), there were none where a record had been made of the time and date of receipt and assessment. The date only was recorded in 64 cases, from which it was possible to deduce that 38 had been assessed within one or two days. In the 60 instances where the date of receipt had not been recorded, the information had not been relevant to the regional office where it had been originally received. This included immediate event notifications[32] that were not relevant to that particular region.

32 Immediate Event Notifications (IEN) are used to disseminate intelligence quickly across BF. Where an event at the border meets agreed notification requirements, e.g. the size of a commodity seizure, the officers concerned must issue an IEN that all BF officers are made aware of it.

Identifying 'duplicate' allegations

6.28 It is important in terms of the efficient use of staff time to identify at the initial receipt stage if an allegation duplicates information that has already been received or is known. Because information relevant to IE/UKVI and BF interests is recorded on different Home Office IT systems for which there is no single search facility, and because access to these systems is uneven, the process of checking can be laborious. Nor is it uniform, since it is a matter of judgement whether a search is necessary or likely to be of value. The same is true for systems not owned by the Home Office, a search of which might help to confirm or match new information with existing records.

6.29 Figure 11 shows the further checks recorded by IE for the sample of 39 allegations that resulted in 'no further action'.

Figure 11: Record of checks against other systems for 39 NFA allegations from the period 1 July to 30 September 2015	
CID	21
CRS[33]	13
Other[34]	10
ATHENA	2
Experian[35]	4
WI[36]	None
PNC[37]	None

6.30 The ability to search a particular system will depend on what data is held and how it is structured. In terms of the systems available to IE and BF, searching by name (of individual) is most common and most useful. Of the 39 NFA allegations sampled, 33 referred to one or more named individuals, although not always by the full name.

6.31 Based on the sufficiency of the information received initially by IE, the NFA decision was reasonable in 37 out of 39 cases. In one of the two remaining cases a 'duplicate' record was identified on IMS, but both were closed so that no action was taken on either. In all, seven of the 39 NFA allegations were assessed as NFA because a 'duplicate' existed on IMS. In two of these seven cases, including the one closed in error, there was evidence that other systems had also been checked.

6.32 The second case is detailed at figure 12.

33 Case Reference System – a HO database containing details of all visa applications.
34 'Other' could include open source internet searches, voters' lists and the Home Office National Operations Database.
35 Experian – commercial database holding credit reference information and personal information held by financial institutions.
36 Warnings Index – a HO System used to ascertain whether individuals are of interest to the Home Office.
37 Police National Computer – https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/488515/PNC_v5.0_EXT_clean.pdf.

Figure 12 – Case Study: Allegation of sham marriage assessed as 'no further action'

- IE received an allegation of a sham marriage, which at the time was a priority threat category;
- The allegation included a partial name;
- The details provided were insufficient to search Home Office systems, and the allegation was assessed as 'no further action';
- However, although the allegation contained details for the person named, which could have been researched using other sources, no further research had been done to identify the individual, verify the allegation and assess whether the information was actionable.

IE response

IE responded that staff dealing with the initial receipt of allegations were not trained to research some specific sources, and that this type of research is not always appropriate or possible. Given that the alleged offence met priorities, the case could have been referred [to an OIU] to consider whether additional research was appropriate in this case.

Recording 'Outcomes'

6.33 BFNIH refers to the action it takes after receiving information as the 'outcome'. The possible 'outcomes' for information received by the BFNIH are:

- Forwarded;
- Returned;
- Product issued[38]; or
- No further action.

6.34 For BFITs possible 'outcomes' include the result of any operational tasking or use of the information (which is how IE uses the term). The 'outcomes' used by BF are shown in figure 13 along with the outcomes recorded for the 125 sampled regional allegations.

Figure 13: Outcomes recorded by BF

Duplicate	1
Intelligence disseminated	9
Intelligence report created and nominal flagged where necessary	19
Intervention: allowed to proceed	5
Intervention: arrest	1
Intervention: Seizure	1
Intervention: refused entry	3
NFA	28
Nominal flagged on relevant systems	5

38 A product could be an Intelligence Report, a targeting Alert, border suspect message, or entry on warning systems.

Ongoing operation	2
Recipient did not action	1
Referred to internal team for further action	4
Research undertaken	8
Upstream disruption	3
Total	**90**

6.35 The outcome was not recorded in 35 of the 125 cases, and therefore it was not possible to assess whether these allegations had been dealt with appropriately. In a further 13 cases where the outcome was clear, the record was not sufficiently detailed to determine whether they had been dealt with appropriately. The outcome in the remaining 77 cases appeared to be correct.

Analysis and assessment

Intelligence development

6.36 While some information/intelligence is complete and actionable at the point of receipt, in many instances it will require further work by intelligence staff to 'develop' or 'enrich' it for it to be of use operationally. This might involve researching other information/intelligence and analysing it to look for links or patterns. Intelligence development is a routine part of any 'cycle', resulting in various strategic and tactical intelligence products, but it may also be in response to an urgent operational demand, as recognised in the IIM, '*Fast track (between hours agreed) research and intelligence assessments are provided in response to major / high profile incidents, time critical incidents and live operations.*'

OIUs

6.37 Senior managers in IE believed that as OIUs were no longer responsible for the initial evaluation of information received into IMS, they would have time to research and develop more and better quality intelligence 'packages' to present to TCGs for action. At the time of the inspection this had not been in place for long enough to be properly tested. However, MI data[39] for the period February 2015 to January 2016 showed that OIUs had produced 13,745 'packages' for TCG consideration. Figure 14 shows the outcome of the TCG decision.

Figure 14: outcome of TCG decisions for OIU 'packages' in workflow between February 2015 and January 2016	
Accepted	10,999
Rejected at TCG	1,522
Rejected pre TCG	478
Ready for TCG	326
Hot tasked	193
In development	138
No decision	89
Total	**13,745**

39 Immigration Intelligence Performance Pack September, 2015. Slide 3: figures contained in table entitled 'TCG Decision – Immigration Intelligence packages'

Creation of Intelligence Reports

6.38 File sampling of 99 'packages' revealed that research and intelligence was routinely attached in the form of a tasking sheet. However, intelligence reports had been created on ATHENA in only three of the 17 cases where individuals were encountered and arrested. One of these cases was an example of dissemination to an external agency reporting an operational success based on information the other agency had provided. See figure 15.

Figure 15: Example of external dissemination

- On 19 July 2015, information was received from DWP[40] to the effect that a person known to have been previously deported was using an address in the UK;
- Research by the OIU using internal systems as well as data on other government systems confirmed this to be the case;
- On 14 August 2015, the OIU created an Intelligence 'package';
- On 18 August 2015, the 'package' was accepted as a 'hot tasking' for deployment of ICE team resources;
- On 9 September 2015, the ICE Team made an enforcement visit to the address and arrested the subject of the allegation, who was placed in detention;
- On 25 September 2015, the subject Voluntarily Departed the UK; and
- An Intelligence Report was created on ATHENA and disseminated by IE to DWP.

Crime development teams

6.39 Crime Development Teams (CDT) formed part of OIUs. Their primary role is to support Criminal and Financial Investigation (CFI) Teams by developing intelligence 'packages' and providing ongoing support once the initial 'package' had been developed. CFI teams investigate what is referred to in the NIM model as level 2 and level 3 crime:

- Level 2: regional crime, crime which covers more than one IE or BF region
- Level 3: serious and organised crime that is usually national or international.

6.40 Investigations conducted by CDT can be lengthy and involve various phases of intelligence research and development. Where OIU 'packages' are developed and passed to a Tasking & Coordination Group meeting to action, CDT staff maintain a regular dialogue with CFI teams to ensure that research is provided when required, for example when new evidence is found.

6.41 Staff in CDTs reported that they had not received any additional training when starting their new roles. While they were all experienced Intelligence Officers, having worked in OIUs previously, they did not consider they had the necessary skills, knowledge or experience to deal confidently with complex investigations. Senior managers within IE acknowledged this shortfall, indicating that it would be addressed as part of the ongoing change process.

40 Department for Work and Pensions.

Dissemination and feedback

Dissemination

6.42 According to the IIM, having received, assessed and initiated any further research, the next step is:

> *'dissemination to the appropriate party' which 'could include other national or international agencies or Government intelligence services'.* The IIM states that *'it is essential that intelligence is disseminated to the appropriate unit, department or agency requiring the material in a timely fashion.'*

It continues:

> *'Information may be disseminated through soft copy, verbal or hard copy means. Where material is passed via hard copy or verbal means it is essential that a record is kept of the recipient(s). Any verbal or hard copy dissemination should be followed up by a soft copy as soon as practicable to ensure a full audit of information and intelligence disseminated. The main responsibilities of this process are to:*
>
> - *Sanitise information/intelligence appropriately for the recipient and consider confidential briefing to fully inform the recipient.*
> - *Maintain an auditable trail of decision making and dissemination.'*

6.43 In addition to the IIM, IE and BF separate guidance relating to the dissemination of intelligence. IE's operational instructions included 'Dissemination of information regarding alleged visa abuse'[41] and 'Intelligence sharing with the NCA.'[42] These contained specific guidance regarding the role of the Immigration Intelligence Centre (IIC).

6.44 In May 2015, BF Intelligence Directorate (BFID) Transformation Program issued 'Guidance on receiving and disseminating intelligence (for inclusion in Professional Practice Manual)'. This outlined the BF intelligence Target Operating Model for receiving and disseminating intelligence, and clarified the central role the BFNIH played in the new model. The transformation program also issued detailed 'Guidance on Debriefing'[43] which reminded staff that '*Every member of the organisation should have the knowledge and confidence to receive, evaluate and share information….'*[44]

6.45 The BFNIH played a central role in the receipt and dissemination of intelligence. Where an immediate threat to the border was identified, for example where a known drug smuggler was returning to the UK and was suspected of being in possession of contraband, BFNIH would request a WICU entry if one was not already in place, and disseminate a Border Suspect Message (BSM)[45] to the relevant targeting team, who in turn would issue a target sheet to frontline staff if appropriate. This occurred on a daily basis.

6.46 BF Management Information (MI) in relation to intelligence received and disseminated was collected locally on non networked databases by the BFRITs and by BFNIH. It was not uniform and there were gaps. Figures 16 and 17 refer.

---

41 Reference 150501 published 05/09/2014.
42 Reference 141001 published 08/10/2014.
43 Published in December, 2014.
44 Para 2.1 of the document.
45 A message used to alert targeting teams of suspicious arrivals (passengers, goods) who then assess the message and issue formal. targeting sheets to frontline staff if appropriate.

Figure 16: BF regional MI for intelligence received and disseminated between 1 April 2014 and 31 March 2015

	North	Central	Heathrow and South	South East & Europe
IMS notifications received	304	N/R	679*	233
IENs received	916	1563	2939**	944
Entries onto local ADT database	4147	286	12329	8127
Target sheet created	258	N/R	N/R	4115
Intel alert/brief/report created	926	N/R	4393	2885
IR created and disseminated to other law enforcement agency	283	N/R	831	1855

N/R = Not recorded
* = LGW unable to access this data
** = LGW did not record IENs if not relevant to the region[4647]

Figure 17: BFNIH MI for intelligence received and products disseminated between 1 April 2014 and 31 March 2015, and between 1 April 2015 and 31 November 2015

	01.04.14 to 31.03.15	01.04.15 - 30.11.15
IMS notifications received	1931*	2433
IENs received	12762	7703
Entries onto BFNIH database	28496	19937
NFA	772	433
Border suspect message	588	365
Deployment[46]	54	28
Urgent request for entry onto warnings index (IS200)	1779	1245
NBTC Alert[47]	27	21
Creation of an intel alert/brief/report	431	365
Number resulting in the creation of an IR disseminated to another LEA	175	141

*= Partial dataset; full data capture only from 1 June 2014

RALON

6.47 Part of IIC's role was to receive time critical intelligence from overseas, for example relating to an individual due to arrive in the UK, and ensure that BF or other law enforcement agencies were notified immediately. The inspection identified that IIC was receiving unsanitised intelligence from those overseas RALON posts with no access to

46 Where information received is time critical and requires immediate deployment of resources.
47 Where passenger data which is washed against HO systems by the National Border Targeting Centre and identifies suspect travellers or passengers of interest, alerts are sent by NBTC to the port where the passenger is due to arrive.

IMS. This was contrary to IIM guidance[48], which states that the dissemination process should '*Sanitise information/intelligence appropriately for the recipient and consider confidential briefing to fully inform the recipient.*'

6.48 IMS was the most efficient way of providing sanitised information[49], as it has a separate page for the source details which is accessible only to staff with the appropriate clearance. At the time of the inspection it was being rolled out to overseas posts. Managers stated they were prepared in the interim to accept the risk of receiving unsanitised information from those yet to be connected.

6.49 Where intelligence was received that was relevant to the RALON network, IIC would disseminate it.

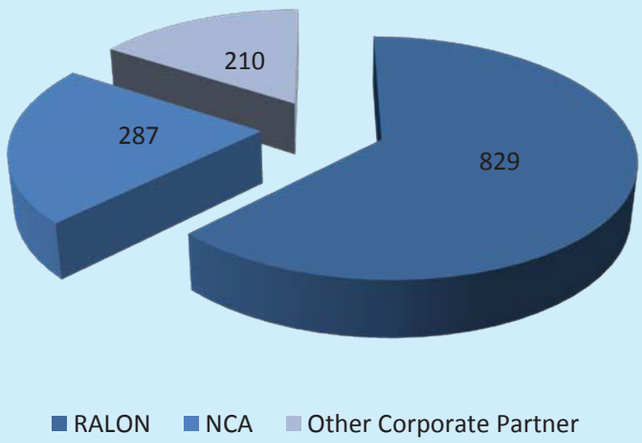
Dissemination and intelligence sharing with other agencies

6.50 RALON guidance for overseas and UK staff sets out how to share information with other agencies in a way that is Data Protection Act compliant. The guidance makes clear the need to have formal agreements in place for large or regular data exchanges. IE had signed a number of Memoranda of Understanding (MOUs). These included agreements regarding joint investigative work with, for example, the Serious Fraud Office, Her Majesty's Revenue and Customs, and with foreign services, such as US Homeland Security and Canadian Immigration. This enabled II to share information in an effective and legally compliant way.

6.51 Where intelligence needed to be disseminated by IE to external partners, the guidance required IRs to be created using ATHENA. File sampling showed that where IE received high harm intelligence, this was being correctly identified, prioritised and disseminated to the police or other affected law enforcement agencies through using the IHM.

6.52 IE produce monthly performance packs covering Immigration Intelligence and RALON. These summarise what intelligence products have been produced, and report some of the outcomes. IE provided[50] a high level breakdown of the recipients of the 1,326 Intelligence Reports disseminated by the IIC between October 2014 and September 2015; see Figure 18. During the same period, IIC processed 3,017 allegations on IMS.

Figure 18: intelligence reports disseminated by IIC October 2014 to September 2015



48 Section 8.5.
49 Sanitised information ensures that the source of the information is protected, and details of the source are not disclosed.
50 Taken from the September, 2015 Performance Pack

Feedback and debriefing of operations

6.53 The inspection found that intelligence from operational activity was not routinely fed back to intelligence teams. In IE, the relevant guidance is found in two places. Firstly, the 'enforcement instructions & guidance', which is used by ICE team enforcement staff, refers[51] to the need for intelligence to be fed back in relation to crime reduction operations and street operations. It states that for both types of operations, the officer in charge must '*hold a debrief and report the results back to the intel unit*', although it did not specify how this should be done. Other types of enforcement visits were not mentioned.

6.54 Secondly, the IIM includes an entry on 'Intelligence Capability and Coordination Unit ICE Tasking Sheet.' This should be completed by an OIU when they develop an intelligence 'package' and further information should be added to the form by an enforcement team once it has completed the enforcement visit. The 'Enforcement Team Use Only' section of the form states that the information noted on the National Operations Database (NOD)[52] should be copied onto the form before returning it to the OIU. However, ICE team managers and the staff saw this as a duplication of effort and did not complete the tasking sheet. Enforcement staff also said that they did not have access to IMS, but repeated that entering the debrief information onto IMS would be a duplication of effort and was inefficient.

6.55 File sampling looked at how information gained from enforcement visits was fed back into the intelligence 'cycle'. In 53 cases of the 99 sampled an enforcement team had made an arrest based on the intelligence provided to them by an OIU. In 44 of the 53 cases a debrief had been saved on NOD. None of the 44 debriefs had been referred back to an OIU.

6.56 When BFNIH disseminates an Intelligence Report it asks for feedback. BFNIH rated its products 'low', 'medium', 'high' or 'top' with regard to chasing feedback if it was not forthcoming. Frontline BF staff commented that they were not clear about how to report into the intelligence unit, and those that did mostly used emails. The inspection was not shown any BF guidance about debriefing and the handling of any intelligence that it produced, nor any performance data relating specifically to feedback on disseminated intelligence reports.

Field Intelligence Officers

6.57 Both IE and BF have appointed Field Intelligence Officers (FIOs), within OIUs and BFITs respectively, to develop intelligence. Meanwhile, operational staff are responsible for feeding in any intelligence they acquire.

6.58 Within IE, managers and staff commented that FIOs were not able to go out into the field either on their own or as part of an enforcement team to gather intelligence because of their administrative duties in the office. Staff said this created an intelligence gap as they were unable to build relationships with stakeholders and the community, or work alongside enforcement teams with a view to conducting further research and developing any intelligence they may have gathered.

6.59 Senior managers acknowledged the lack of field intelligence activity. They expected that the introduction of the RED teams would mean that FIOs should have more capacity to gather intelligence in the field, and in some areas FIOs were starting to be seconded to enforcement teams.

51 Chapter 31, updated 25 August 2015.
52 NOD is used by enforcement teams to record the debriefings of their visits.

6.60 In response to the inspection of general aviation and general maritime[53], published in January 2016, the Home Office stated[54]:

> *'There is now a network of around 100 Field Intelligence Officers working for Border Force based around the country, able to work with airfield operators, harbourmasters and voluntary groups to ensure that suspicious activity is reported and acted upon.'*

6.61 BF managers described the FIO role as providing the link between frontline staff in ports and BFRITs, exchanging intelligence, and receiving and giving feedback on its quality and validity. However, in interviews and focus groups, BF FIOs said that in practice they were unable to engage with frontline staff because of time constraints caused by their office based administrative duties, which included monitoring inboxes and sending out internal communications. Frontline staff commented that they were not aware of the existence of FIOs and their role.

National joint debriefing team

6.62 A National Joint Debriefing Team (JDT), funded by the NCA and staffed by IE, BF and NCA was created in Autumn 2015. A team fulfilling a similar function had been disbanded four years ago.

6.63 The JDT was set up to gather intelligence on Organised Immigration Crime linked to clandestine entry into the UK. It is a ring fenced resource tasked by the NCA. The team had produced an analysis that had been circulated to various areas of IE and BF. The team said it believed it was *'an untapped resource',* but it was not funded to travel to conduct debriefs and commented *'if the interview is too far away, we decline'*.[55]

Providing feedback to the source of an allegation

6.64 In its report on *'The Work of the UK Border Agency'* (January-March 2013)[56], the Home Affairs Select Committee discussed the use of IMS, noting that:

> *'Numerous Government Ministers, including the Prime Minister who in a speech in October 2011 to 'report suspected illegal immigrants to our Border Agency', have reiterated the need to report immigration abuse to officials. We continue to be concerned that despite making formal allegations about immigration abuse, those who do so are not informed of the outcome of their complaint. This risks undermining confidence in the system and could lead to reluctance to report such allegations if the public perceive that no action is being taken. We recommend that the directorate respond to those who make allegations to inform them of the outcome of their investigations.'*

6.65 The 2014 inspection of IMS highlighted a lack of training and awareness regarding when the source of an allegation could be contacted. File sampling therefore looked at whether the source of an allegation had specifically requested to receive feedback, and whether there was any evidence that feedback had been provided. Of the 39 IE 'no further action' cases sampled, nine sources had requested feedback (all had provided contact details). Feedback had been provided in five cases.

---

53 http://icinspector.independent.gov.uk/wp-content/uploads/2016/01/ICIBI-report-on-GAGM-14.01.2016.pdf.
54 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/491879/Formal_response_to_ICI_report_on_GA_GM_-_14_January_2016.pdf.
55 At the Factual Accuracy stage, the Home Office stated' The JDT has a national remit in that it deploys all over the UK to debrief clandestine entrants and also overseas (within the EU) where there are opportunities to gather intelligence alongside overseas law enforcement partners.'
56 http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/616/61602.htm.

6.66 BF did not record whether feedback had been provided to sources.

Conclusions

6.67 The intelligence 'cycles' in IE and BF involve a number of detailed processes and 'handoffs'. Two are particularly important to overall efficiency and effectiveness of the intelligence function. The first concerns the receipt, initial evaluation and distribution of new information. The second concerns how well frontline staff engage with and support the intelligence function. This has often been a challenge for law enforcement agencies.

6.68 Based on the evidence provided to this inspection, both IE and the BFNIH make a correct and timely (within the target time of 48 hours for II and a maximum of 24 hours for BFNIH) initial evaluation of the vast majority of the information they receive. IE relies on its Intelligence Handling Model (IHM) to achieve its aim of '*providing the right information to the right people, on time.'* However, IHM is regarded as immigration centric and therefore not used by BF. BFNIH's task is essentially to move any credible and actionable information on to a BF region to action, which it does efficiently. However, based on file sampling, it is less clear to what extent BF regional intelligence teams are efficient in terms of the 48 hour target or effective in the action they take, since there is no consistency to regional record keeping and the records sampled contained many gaps.

6.69 Between August 2014 and July 2015, two thirds (c.50,000) of all allegations recorded on IMS were from members of the public, which as the 2014 Deloitte review recognised were 'not the most efficient way for IE to direct its activity'. Referrals from IE, UKVI or BF frontline staff were potentially more valuable, as these staff should be more aware of what is of organisational interest or concern. However, numbers of internal referrals were low, either because frontline staff failed to understand the importance of making referrals, were misdirected regarding how to make them, or did so in ways that were non compliant and therefore difficult to audit.

6.70 Within IE the risk that ICE teams were not making use of IMS to make referrals had been recognised and changes had been made to the training and guidance provided to ICE team staff. In the case of UKVI, IE structures and processes dealing with UKVI related intelligence (e.g. regarding temporary and permanent migration) changed in 2015, but guidance for UKVI caseworkers, available on the Home Office intranet, had not been updated since November 2014. Meanwhile, despite up to date guidance requiring them to use IMS, BF front line staff were using emails and telephone calls to refer allegations of immigration and customs abuse.

6.71 There was a similar picture with feedback, including any new intelligence, from operational teams acting on the intelligence 'packages' they received, despite the teams completing operational debriefs. This was largely due to the fact that reporting arrangements were unclear (BF) or involved the duplication of effort (IE). While the IE and BF Field Intelligence Officers (FIOs) were a potential solution, they were weighed down with administrative office based duties and did not have the capacity to get 'into the field' and collect feedback and newly acquired intelligence from frontline staff to pass back to intelligence colleagues,

Recommendations

The Home Office should:

- Set and enforce (through clear guidance and quality assurance) appropriate standards for the receipt, initial evaluation and distribution, including for record keeping, giving consideration to whether the Intelligence Handling Model (IHM) used by IE could be adapted for BF use.
- Ensure that all frontline staff in IE, UKVI and BF are fully aware of their obligations with regard to referring and reporting information, intelligence and feedback to intelligence colleagues, and that the processes and mechanism for doing this are clearly set out.
- Review the responsibilities and workloads of field intelligence officers with a view to reducing their time spent on office based administrative duties and enabling them to get 'into the field' to collect feedback and new intelligence from frontline staff.

Annex A

The onsite phase of the inspection took place between 1 February and 3 March 2016.

Figure 19 records the locations where the inspection team conducted interviews and focus groups.

Figure 19: Locations visited

Immigration Enforcement	Border Force
• Vulcan House, Sheffield • Apollo House, Croydon • Amadeus House, Heathrow • Eaton House, Hounslow • Capital Buildings, Liverpool	• Border Force National Intelligence Hub, Dover • Dover Eastern Docks • Martello House, Folkestone • Ashdown House, Gatwick Airport • Manchester Airport • NBTC

Figure 20 details the grades and numbers of staff that were involved in the interviews and focus groups.

Figure 20: Number and grades of staff seen

Immigration Enforcement		Border Force		UKVI	
Grade	**No of Staff**	**Grade**	**No of Staff**	**Grade**	**No of Staff**
Director of intelligence	1	Director of intelligence	1		
Deputy director (G6)	3	BF deputy director (G6)	2		
Assistant director (G7)	11	BF assistant director (G7)	7	Grade 7	1
Senior executive officer	11	BF senior officer	11		
Higher executive officer	12	BF higher officer	9	Higher executive officer	1
Executive officer and administrative officer	68	BF officer and BF assistant officer	57	Executive Officer and Administrative Officer	7
Total	**106**	**Total**	**87**	**Total**	**9**
Combined total	**202**				

The inspection team also attended a presentation on the Single Intelligence Platform.

ISBN 978-1-4741-3669-3