Independent Chief Inspector of Borders and Immigration

An inspection of Border Force insider threat

January – March 2023

David Neal

Independent Chief Inspector of
Borders and Immigration

An inspection of Border Force insider threat

January – March 2023

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

September 2023

This publication is available at www.gov.uk/official-documents

This publication is also available at www.gov.uk/ICIBI

Any enquiries regarding this publication should be sent to us at

Independent Chief Inspector of
Borders and Immigration,
1st Floor, Clive House,
70 Petty France,
London SW1H 9EX
United Kingdom

ISBN 978-1-5286-4393-1
E02956811 09/23

Printed on paper containing 40% recycled fibre content minimum.

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His 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.gov.uk/ICIBI

Email us: chiefinspector@icibi.gov.uk

Write to us: Independent Chief Inspector of
Borders and Immigration
1st Floor, Clive House,
70 Petty France,
London, SW1H 9EX
United Kingdom

Contents

Foreword

The UK border provides the opportunity for individuals responsible for protecting it to commit criminal acts.

Border Force presents itself as a uniformed, law enforcement organisation but is governed by Civil Service rules and leadership. The nature of its unique work means that Border Force staff are distinct from many other Home Office civil servants, having privileged access to critical assets, whether these are property, data, or contraband.

The public expects that Border Force staff are held to a higher account by rules and regulations tailored to their work and commensurate with the level of trust and responsibility placed upon them. When their standard of behaviour falls below what is expected, swift action should be taken.

Border Force needs to ensure its ability to identify and respond to insider threat risks is consistent with other law enforcement organisations, where expectations are set out in legislation. Additionally, senior leaders must be given the tools to reduce the risk of insider threat to enable them to lead and govern their organisations efficiently and effectively. This inspection found that these necessities are currently not consistently and wholly available within Border Force.

Where Border Force can make decisions and execute projects to combat the risk of insider threat, the results have been somewhat positive. These include initiatives such as its enhanced employee screening process, through the introduction of additional security checks from September 2020; and the creation of the People Protection and Risk Team and 'Protecting People Policy', providing a means of early intervention where potential staff vulnerabilities can be identified, and risks alleviated. That notwithstanding, its overall ability to implement further measures is hindered by its position within the Home Office and Civil Service, where the inability to differentiate between roles in policy terms means its ambitions cannot always be realised.

Organisational structures for insider threat were found to be confused, with complex inter-relationships and unclear lines of accountability leading to those who are responsible for its leadership and governance. As it must be similarly unclear to those within the organisation, responsibility needs to be clearly aligned with accountability and authority to promote a clear, strategic direction which can then be operationalised.

Fundamental to reducing the risk of insider threat is the need for a strong culture and clear identity. Anecdotally this is inconsistent; I frequently meet Border Force staff who still identify themselves as either Customs Officers or Immigration Officers. In his comprehensive report from summer 2022, Alexander Downer reported similar issues.

Additionally, the most recent Border Force People Survey signposts a dissatisfied workforce which is a breeding ground for insider risk to grow and become insider acts, enabled by privileged access. The provision of important data, such as on Human Resources related misconduct matters, and other potential indicators of insider threat, would allow Border Force to understand the behaviour of its staff and, therefore, identify and reduce risks through early interventions or supportive measures. At present, no one is able to see the full picture of insider threat across Border Force.

[Redacted.] Educating new staff about insider threat as early as possible after joining the organisation would also assist in addressing risks.

Importantly, role-based risk assessments must be introduced in key areas and specialist roles that are at the forefront of our border security response. [Redacted].

I engage regularly with Border Force staff, and it appears to me that few would disagree that they should be held to a significantly higher level of accountability. Higher standards, when applied to wider cohorts of recruits into Border Force, will not speed up recruitment and likely will cause an immediate challenge in areas where there are acute shortages of personnel. However, this is not a reason to delay action.

Policing is facing the damaging fallout of an organisational structure that is failing to properly account for its insider threat. As Border Force plays a leading role in securing our border, it needs to be equipped for success. On the evidence of this inspection, it does not appear to be the case that it is as equipped as it could, or ought to be, and the risk of wider reputational consequence remains.

This report makes eight recommendations and was sent to the Home Secretary on 26 May 2023.

David Neal
Independent Chief Inspector of Borders and Immigration

1. Key findings

1.1 Inspectors considered the effectiveness of Border Force's current approach to identifying, responding to, and mitigating insider threat in Border Force. The following thematic areas, based on the National Protective Security Authority's (NPSA) guidance (which is explained more fully at paragraph 3.1) was used as a benchmark against which to consider this effectiveness.

Leadership and governance

1.2 Border Force's response to the risk from insider threat is administered by the Border Force Insider Threat and Integrity Team (BF ITIT). BF ITIT is a dedicated resource responsible for a programme of projects to mitigate risks from insider threat, referred to broadly as the Border Force Insider Threat Programme. The project arm of the team develops and tests projects to mitigate risks from insider threat. The operational arm of the team undertakes the day-to-day running of some elements of the programme which have become 'business as usual' work.

1.3 BF ITIT reports to the Border Force Insider Threat and Integrity Committee (BFITIC), which is chaired jointly by the Director General of Border Force who has oversight and governance of the Border Force Insider Threat Programme.

1.4 Inspectors concluded that while measures existed in Border Force to identify insider threat, there was a lack of resource within the People Protection and Risk Team (PPRT) which may also impact on Border Force's ability to deliver the expansion of some projects, such as additional security checks (ASCs) and mandatory declarations. Additionally, some processes introduced to mitigate the risks from insider threat rely on resource from the National Crime Agency (NCA) and the police, either to undertake checks or provide information. Should NCA and/or police organisational priorities diverge from those of Border Force, resource may be withdrawn, and the effectiveness of these mitigations will be limited. However, this is mitigated by the funding and agreements in place with partner agencies as well as Border Force direct access to systems.

1.5 The BFITIC and BF ITIT sit within a wider organisational structure linking other Home Office, Civil Service and government stakeholders. Inspectors found the overall governance picture to be confused, and the functions and specific responsibilities of the various governance boards the BFITIC feeds into blurred. Although Border Force viewed the Director General of Border Force as the single responsible officer for insider threat, sitting in a wider organisational structure meant there was a lack of clear governance from a single, accountable owner who could make independent decisions for their organisation.

1.6 Border Force told inspectors about the actions the committee wanted to take, such as the implementation of drug and alcohol testing and accessing Human Resources (HR) data, which had so far been unsuccessful. Decisions made by the Director General, with agreement of the committee, could not be autonomous and needed to consider the impact on the wider Home Office and its employees, and vice versa. Inspectors did not see evidence of a clear escalation route to a higher authority outside of Border Force, which may have contributed to these difficulties.[1]

1.7 Inspectors were provided with the Border Force Insider Threat Control Strategy, an internal document derived from Border Force's Operational Assurance Directorate. It is not up to date and, when considered against the requirements set out by the NPSA, lacks the overarching vision or strategy governing the overall Border Force insider threat programme. Inspectors considered it to be a plan on how the insider threat programme might be operationalised, rather than a wholesale organisation strategy set at the top of the organisation.

Organisational culture and trust

1.8 Border Force has demonstrated willingness to build organisational trust and develop a supportive culture by creating PPRT and introducing a dedicated 'Protecting People Policy' alongside its network of integrity leads. There is also a wide range of welfare support available to Border Force staff. Inspectors considered that this emphasis on supporting staff went some way to demonstrating the value Border Force places on its employees.

1.9 However, inspectors found that despite Border Force making significant efforts to include staff in decision making, communicate information, and ensure fair processes were in place to deal with discipline and grievances, there was evidence of a lack of engagement, and wide-level disaffection within the organisation. This was particularly evident in relation to pay and had resulted in industrial action. During a visit to Dover, inspectors noted the potential delineation between Border Force officers at Executive Officer and Assistant Officer grades, was unclear, potentially leading to staff being paid different salaries for the same work.

1.10 People survey results evidenced low levels of staff engagement, and loyalty to Border Force was consistently lower than those across the Civil Service as a whole, indicating a lack of shared identity and cohesion within the organisation.

1.11 Disaffection and financial motivations can both contribute to employees undertaking unauthorised insider acts for their own benefit or to exact revenge against management. As a result, inspectors concluded the risk to Border Force from insider threat is likely heightened, and it is currently challenging to attain support across the organisation for the risk mitigation measures they would like to introduce.

Employee screening

1.12 Through baseline protective security standards, National Security Vetting and additional security checks (ASC), Border Force has developed an employee screening process over and above standard screening for Home Office employees. The ASC process was introduced on 16 September 2020 to determine a candidate's suitability for employment in a law enforcement agency. As of 19 January 2023, 581 applicants have failed the checks and been denied Border Force roles. Those individuals could otherwise have posed a significant risk to Border Force.

1.13 [Redacted].[2]

[1] In its factual accuracy return, the Home Office stated for HR issues there is a clear escalation route – to the Chief People Officer.

[2] [Redacted].

1.14 [Redacted]. However, the ability to do this is hampered by wider HR processes and the potential impact on existing employment, as well as a lack of the appropriate resources to cope with the additional workload.

1.15 [Redacted].

Employee monitoring

1.16 A ‘mandatory declaration’ policy is used by Border Force to monitor for insider threat risks. It is well established and has been upgraded from a paper-based process to an online declaration. Border Force told inspectors that the relaunch of the programme will focus on line management discussions, while also providing better management information for analysis on the risks that are declared.

1.17 Border Force rightly recognises the important role the line manager plays in both identifying issues and supporting employees, and inspectors considered this role in employee monitoring. Senior leaders in Border Force at Dover showed a strong understanding of the financial drivers of insider threat, and how managers were instrumental in mitigating such risks. However, while Dover held locally-organised training sessions for Higher Officers (the majority grade of line managers in Border Force), inspectors found a lack of specific training nationally for line managers on insider threat.

1.18 Changes to the mandatory declaration policy implementation have been slower than Border Force anticipated. Inspectors found that the project has encountered delays due to reprioritisation to support the wider COVID-19 response, Data Protection Act issues, and workforce resourcing in Home Office teams external to Border Force. Border Force is working to address the Data Protection GDPR issues and had appointed a specialist data protection lead to address these issues.

1.19 [Redacted].

1.20 Inspectors found that Border Force had struggled to introduce drug and alcohol testing (DAT) for staff despite it being an initial objective of the Border Force Insider Threat Programme in 2018. The options paper to support DAT included little evidence as to why it was required and relied on the rationale that it was a reasonable expectation of Border Force as a law enforcement agency. As a result, random DAT testing of all staff lacked the support of trade unions and was at risk of legal challenge due to it being a policy, rather than a contractual or legal requirement. Despite this, inspectors noted the DAT proposal was generally well received by Border Force officers in Dover. These officers felt DAT was appropriate due to the nature of the work they undertake, which involves the searching and seizing of drugs and alcohol.

1.21 The DAT project has also experienced delays due to ongoing discussions about how it may impact wider Home Office policy in regard to consuming alcohol on duty. Additionally, delays have also been experienced as a result of the Home Office contract with the testing supplier being reviewed, and the requirement to ensure that the successful supplier is able to comply with data protection requirements.

1.22 Border Force officers have unique access to vulnerable people, high-value property, goods, data, and contraband. [Redacted].

Insider risk assessment

1.23 Border Force has assessed the risk of insider threat to its organisation, resulting in the creation of a control strategy. However, this does not appear to have been updated since its creation in 2021.

1.24 Border Force does not conduct role-based risk assessments and senior leaders felt they had no value. Additionally, Border Force was keen to avoid singling out particular grades for insider threat activities, which role-based risk assessments could potentially do. [Redacted].[3] Inspectors considered that role-based risk assessments could help support why Border Force sometimes chose to address insider threat in a particular job role, and not others.

1.25 Inspectors found that data in relation to insider threat within Border Force is limited. BF ITIT is unable to access information held by HR teams which severely limits its ability to assess the risk from within Border Force and drive through desired projects.

1.26 There was effective local practice at Dover port to mitigate the risk of a staff member exploiting their position to act unlawfully. However, despite awareness among Border Force staff of integrity leads and the PPRT, staff reported being more likely to raise issues and concerns through their line managers and HR routes. [Redacted].

1.27 Data held by BF ITIT is not routinely analysed to support recommended projects or identify trends. While Border Force had attempted to address this by commissioning external analysis, its value was restricted due to difficulties sharing information with the analyst, and concerns around protecting data. Management information and data to identify potential risks and assess outcomes could not be provided by BF ITIT for the Joint Anti-Corruption Intelligence Team (JACIT).

1.28 [Redacted].

Investigation and disciplinary practices

1.29 The efficiency and effectiveness of JACIT was difficult to discern due to their limited ability to share data. Home Office staff expressed concerns about a lack of intelligence packages to investigate from JACIT, and Border Force was unable to provide inspectors with details of to whom JACIT cases had been tasked.

1.30 JACIT appears to be ‘joint’ in name only. Although housed in an NCA building, there are no NCA-embedded officers. The unit is entirely resourced by Border Force, and Home Office Security is not supplying resource. Additionally, there is difficulty sharing information (particularly NCA-owned intelligence) outside Border Force and the NCA, including with Home Office Security.

1.31 JACIT was unable to easily access employment information about Border Force officers from Home Office HR systems. This lack of basic information hindered its ability to quickly identify and locate staff members to corroborate or disprove intelligence and route cases for investigation or close as appropriate.

1.32 Further challenges were identified with information sharing between the Protective Security aftercare team and HR. Data held by these teams could not be shared with BF ITIT, except

[3] [Redacted].

in specific circumstances. Inspectors concluded that information about how behaviours, lifestyle, and personality could influence the risk of insider threat to Border Force could not be fully assessed.

1.33 Additionally, analysis of data regarding the reporting and investigation of insider threat issues is limited, in large part due to issues of sharing data across teams. Data provided to inspectors was not detailed and did not allow inspectors to objectively analyse trends in intelligence and investigations. It was unclear what types of cases were being received and whether data supported the introduction of the proposed projects.

1.34 There were numerous avenues by which allegations, behaviours, or concerns could be investigated or dealt with, but limited ability to share data between teams. This raised concerns over the consistency of handling cases and how data would be shared with BF ITIT. Inspectors concluded that BF ITIT may be unaware of insider risks arising from HR issues within the workforce, unless directly notified, as this would depend heavily on line manager input. It was of great concern to inspectors that staff in both Border Force and the Home Office agreed that no one was able to see the full picture in relation to insider threat. Inspectors judged this could skew the picture of the broader organisational risk, and consequently how risk could be effectively mitigated.

1.35 The lack of clear and consistent processes and reporting requirements increases the risk of inconsistent outcomes, and lack of action. Lessons should be learned from recent Metropolitan Police cases where opportunities for early intervention were missed, leading to officers being in post while carrying out serious crimes, as there is potential for the same to be true in Border Force.

Online personnel security

1.36 Inspectors found that mitigations have been put in place to reduce the risk of intentional and unintentional insider threat relating to online security. Security measures have been introduced to prevent unauthorised sharing of information and the introduction of malware to Home Office systems. There are plans to further improve staff awareness of online security risks and proactive measures have been introduced such as email scam tests.

1.37 Border Force and Home Office senior leaders recognised the increased risks posed by the inappropriate use of technology and social media. The use of WhatsApp (or similar messaging groups) was identified as an emerging issue. Inspectors found that Border Force officers were bound by the Home Office Social Media and Online Behaviour Policy which was not designed specifically for a law enforcement organisation with front-line operational staff. It was not sufficiently clear or consistent, and Border Force staff were confused about what was permitted. This is a risk that needs addressing, and inspectors were pleased to learn the Home Office policy is being updated, with Border Force providing input which they hope will make it more robust.

Ongoing personnel security

1.38 Border Force insider threat awareness training is optional for staff and is not part of the induction process for new recruits. At the time of the inspection, around 78% of staff had undertaken the training, which was well received. Inspectors found it concerning that the training was not mandatory, given its importance in setting the tone of a security culture, communicating risks, and signposting available support, as well as highlighting the overall standards of behaviour expected.

1.39 Inspectors found exit procedures were mainly administrative, not operationally assured, and relied heavily on a line manager's knowledge as to what access and equipment an employee held. Consequently, inspectors were not confident that the risk of insider threat once a staff member left a post or role was being robustly mitigated.

2. Recommendations

Recommendation 1

Conduct a review of insider threat in Border Force within six months, utilising NPSA advice and guidance, and considering ongoing contemporary changes in UK law enforcement, to facilitate the development of an insider threat strategic vision and a plan that is reviewed annually.

Recommendation 2

Ensure that there is a clear escalation route to a single, senior Home Office leader for the Border and Enforcement Insider Threat and Integrity Committee to resolve issues that cut across both Border Force and the wider Home Office.

Recommendation 3

Make insider threat awareness training part of formal induction training for new recruits and mandatory training for existing staff.

Recommendation 4

Publish an updated social media policy, tailored to Border Force operational staff and ensure that this is widely disseminated and communicated.

Recommendation 5

[Redacted].

Recommendation 6

Conduct role-based risk assessments in key areas and specialist roles.

Recommendation 7

Ensure relevant data from vetting, Home Office Security, and Human Resources is available to Border Force, in order to allow Border Force to create a comprehensive insider threat picture to drive early intervention.

Recommendation 8

Conduct a review of the effectiveness of the Joint Anti-Corruption Intelligence Team and map its outcomes, using data to support decisions and recommendations, to ensure the team is adding value for all partners.

3. Background

National Protective Security Authority

3.1 The National Protective Security Authority (NPSA) is the government's national technical authority for physical and personnel protective security. It was known as the Centre for the Protection of National Infrastructure (CPNI) until 13 March 2023.[4] The NPSA works with partners in government, police, industry, and academia to reduce the vulnerability of the national infrastructure.[5] It has published two data collection studies on insider threat, the first in 2009, and an updated study published in 2013. The later study included updated analysis and new insider case studies.[6]

3.2 The NPSA defines an 'insider' as: "A person who exploits or has the intention to exploit their legitimate access to an organisation's assets for unauthorised purposes."[7, 8]

3.3 The NPSA categorises three types of insider threat:

- **deliberate insider** – someone who obtains employment intent on abusing their access to the organisation
- **volunteer or self-initiated insider** – someone who obtains employment without deliberate intent to abuse their access to the organisation, but at some point, decides to do so
- **recruited or exploited insider** – someone who obtains employment without deliberate intent to abuse their access to the organisation, but at some point, is recruited or exploited by a third party to do so

3.4 The data collection study of 2013 identified the primary motivations in insider cases where damage was significant to the organisation (both private and government):

- Financial gain (47% of cases)
- Ideology (20% of cases)
- Desire for recognition (14% of cases)
- Loyalty to friends/family/country (14% of cases)
- Revenge (6% of cases)[9]

[4] https://homeofficemedia.blog.gov.uk/2023/03/13/national-protective-security-authority/

[5] National Protective Security Authority (NPSA) website: https://www.npsa.gov.uk/

[6] NPSA website, Learning and Resources, NPSA Insider Risk Mitigation digital learning, Module 1 – Introduction to NPSA Insider Research, Resources, CPNI Insider Data Collection Study (published April 2013), https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

[7] NPSA website, Learning and Resources, Insider Risk Mitigation digital learning, Module 1 – Introduction to NPSA Insider Research, Resources, NPSA Insider Data Collection Study (published April 2013), p6, https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

[8] On 25 May 2023, and after the drafting of this report, the NPSA announced it had updated its definition of an 'insider' to: "Any person who has, or previously had, authorised access to or knowledge of the organisation's resources, including people, processes, information, technology, and facilities." It also re-defined 'insider threat' as: "An insider, or group of insiders, that either intends to or is likely to cause harm or loss to the organisation."

[9] NPSA website: Centre for the Protection of National Infrastructure (CPNI), 'Insider data collection study', (published April 2013), https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

3.5 Motivations for undertaking insider acts are complex and it is seldom the case that there is a single motivation, with many acts being driven by a "cluster and combination of these behaviours, not just one".[10] Workplace disaffection plays an important role, but other impetuses behind insider acts exist, such as: personality, lifestyle, circumstances, and behaviours of concern.[11]

3.6 While organisations are not required to adhere to NPSA advice, as they are the nationally recognised authority, their guidance provides a robust model against which to compare the Border Force approach. This report is framed around advice provided by the NPSA.[12]

Home Office Anti-Fraud and Corruption Strategy

3.7 The 'Home Office Anti-Fraud and Corruption Strategy', and accompanying policy and plan, were published internally in March 2017. Border Force, as a directorate of the Home Office, is subject to this strategy, policy, and plan. The strategy "outlines [the Home Office's] commitment to creating a culture that will not tolerate fraud, corruption and bribery by maintaining high ethical standards and sound controls, based on the '4P's' model" of prevent, pursue, protect, and prepare. The policy sets out the Home Office definitions of fraud, bribery, and corruption, and the plan covers the immediate action to be taken when fraud and/or corruption is suspected. No updates or review of these documents have been undertaken since publication.

UK Anti-Corruption Strategy 2017-2022

3.8 The 'UK Anti-Corruption Strategy 2017-2022', published in December 2017, defined insider threat as: "A person who exploits their position, or access to an organisation's assets, for unauthorised purposes."[13]

3.9 The strategy set out "an ambitious and long-term framework for tackling corruption" and identified six priorities which would be the focus of the Home Office's efforts up to 2022.[14] The first was to reduce the insider threat risk in four critical domestic sectors – borders, prisons, policing, and defence, so that "the opportunities for corrupt insiders to operate and exploit weaknesses were reduced" and there would be "greater confidence in the integrity of key institutions and sectors".[15]

3.10 In relation to borders, the UK Anti-Corruption Strategy 2017-2022 committed to: "Implementing a comprehensive programme of work to understand, manage and mitigate the vulnerabilities that could be exploited by corrupt insiders at UK airports, maritime ports, and international rail terminals (UK Ports)."[16]

[10] NPSA website, Learning and Resources, Insider Risk Mitigation digital learning, Module 1 – Introduction to NPSA Insider Research, video transcript, https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

[11] NPSA website, Learning and Resources, Insider Risk Mitigation digital learning, Module 1 – Introduction to NPSA Insider Research, video transcript, https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

[12] NPSA is used throughout the report, although some areas of the NPSA website, and the resources they have produced, may still refer to CPNI.

[13] GOV.UK, UK anti-corruption strategy 2017 to 2022 (published 11 December 2017), p31, https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022

[14] GOV.UK, UK anti-corruption strategy 2017 to 2022 (published 11 December 2017), p7, https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022

[15] GOV.UK, UK anti-corruption strategy 2017 to 2022 (published 11 December 2017), p8, https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022

[16] GOV.UK, UK anti-corruption strategy 2017 to 2022 (published 11 December 2017), p32, https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022

3.11 Prior to the publication of the UK Anti-Corruption Strategy 2017-2022, Border Force had a small integrity function. As a result of the border being identified as a high-risk area for corruption and insider threat under the UK Anti-Corruption Strategy 2017-2022, as well as some high-profile cases of insider threat involving Border Force staff, this work expanded, and the Border Force Insider Threat Programme was formally launched in 2018.

3.12 These high-profile cases included that of Simon Pellett, who was found guilty in 2018 of offences relating to firearms and drugs while serving as a Border Force officer and was sentenced to 23 years in prison. Pellet used an official vehicle in the commission of his crimes, and his role, access, and knowledge could likely have contributed to his ability to commit the offences.[17]

Regulations

3.13 The requirement for a Civil Service code of conduct to be published is set out in legislation.[18] The Civil Service Code details the expectations placed on civil servants when carrying out their role, based on core values. Civil servants are expected to carry out their roles with "dedication and a commitment to the Civil Service and its core values: integrity, honesty, objectivity and impartiality".[19]

3.14 The Civil Service Code also details how civil servants can raise concerns if they believe they are being required to act in a way that conflicts with the code, or the actions of others conflict with the code. Additionally, Border Force officers must comply with the Border Force Code of Ethics, a mandatory declarations scheme, and Home Office policies on personal conduct, discipline, arrest, or conviction on criminal charges, and social media. Combined, these reflect the position of Border Force as a law enforcement organisation, sitting as a directorate, within the Home Office.

3.15 First introduced in 2016, the Border Force Code of Ethics is published internally, and "extends beyond the workplace and core working hours to any situation where there is a clear and sufficient connection between the employees' conduct and their employment". It is based around four Border Force values which complement those in the Civil Service Code. The Border Force values are: 'commitment, discipline, respect, and moral courage'. The Code of Ethics details that it is "especially relevant when [an officer] is facing a new or unusual situation, or [they] need to use [their] judgement or discretion". Civil Service values overarch Border Force values, and any breach of the Civil Service code is considered under disciplinary procedures.

3.16 The Border Force mandatory declarations scheme has been in place since Border Force came into existence in 2016. The scheme helps ensure that any risks posed by employees' sponsorship of immigration or migration applications, outside employment, criminality, personal finance, or business interests can be mitigated with relevant actions agreed with line managers. The mandatory declarations scheme applies to all Border Force employees.

3.17 UK Border Agency (Complaints and Misconduct) Regulations 2010 (section 23) included provisions for the Independent Office for Police Conduct (IOPC) to carry out investigations into

[17] The Independent, "UK border officer jailed for 23 years over multi-million pound guns and drugs smuggling plot,"(published 16 November 2018), https://www.independent.co.uk/news/uk/crime/uk-order-officer-jailed-guns-drugs-smuggling-simon-pellett-a8637761.html

[18] Legislation.gov.uk, Constitutional Reform and Governance Act 2010, Part 1, Chapter 1, section 5, https://www.legislation.gov.uk/ukpga/2010/25/section/5

[19] GOV.UK, Civil Service reform, Civil Service: values and standards of behaviour, The Civil Service Code, (published 30 November 2010), https://www.gov.uk/government/publications/civil-service-code

the conduct of warranted Border Force officers (as well as other warranted Home Office staff, officials or contractors), who undertake either customs or immigration functions.[20]

3.18 The Professional Standards Unit (PSU), part of Home Office Security, is the single point of contact within the Home Office for the IOPC. An internal Home Office document details that PSU is obliged to engage the IOPC where the matter has resulted in one of the following circumstances:

- "death or serious injury
- serious assault
- a serious sexual offence
- serious corruption
- a criminal offence aggravated by serious discriminatory behaviour on the grounds of a person's race, sex, religion, age, sexual orientation or disability
- an infringement of Articles 2 or 3 of the European Convention on Human Rights
- conduct whose gravity or other exceptional circumstances make it appropriate for the Home Office to refer the matter to the IOPC"

[20] Legislation.gov.uk website, The UK Border Agency (Complaints and Misconduct) Regulations 2010, https://www.legislation.gov.uk/uksi/2010/782/contents/made

4. Scope and methodology

4.1 This inspection focused on:

- the measures that exist to identify insider threat in Border Force
- how the risk of insider threat to Border Force is mitigated and responded to

4.2 This inspection considered the insider threat posed by Border Force staff. It did not include threats posed by staff employed by private contractors. It did not look at physical security or insider risk to physical critical assets.

4.3 During the course of this inspection, inspectors:

- conducted research using open-source material and Home Office guidance available to staff
- held a familiarisation meeting with the Border Force Insider Threat and Integrity Team (BF ITIT) on 11 January 2023
- received and analysed documentary evidence and data provided by the Home Office
- analysed the results of the 2022 Civil Service 'People Survey' for Border Force
- interviewed and held focus groups (via Microsoft Teams and in person) with Border Force and Home Office staff from grades Assistant Officer to Senior Civil Servant, between 6 February 2023 and 2 March 2023
- observed Border Force operational areas in Dover Eastern Docks
- interviewed (via Microsoft Teams and in person) representatives from law enforcement agencies, other government departments and agencies, and a trade union, between 6 February 2023 and 2 March 2023
- attended a Border Force Insider Threat Awareness session presented over Microsoft Teams by BF ITIT
- completed National Protective Security Authority Risk Mitigation digital learning
- presented a debrief of findings from the onsite phase of the inspection to Home Office senior leaders on 27 February 2023

5. Inspection findings: Leadership and governance

Figure 1: National Protective Security Authority (NPSA) guidance used by inspectors to consider Border Force's effectiveness in this area

Leadership and governance[21]

Strong security leadership can ensure you have effective security strategies

Positive and visible, board-level support for protective security is vital to demonstrate to staff the value placed on personnel and people security policies and procedures. As part of an overarching protective security strategy, strong security governance will:

- deter employees who may wish to harm your organisation by creating an open and transparent organisational framework where security is actively promoted as the responsibility of all staff while providing appropriate resource and support in implementing a proportionate, multi-disciplinary approach to countering insider threats

NPSA research has identified that a single accountable board-level owner of security risk and a top-down implementation of security policies and expected behaviours is likely to promote a more compliant and consistent approach across your organisation.

Inadequate corporate governance structures and a lack of awareness of insider threat at a senior level can undermine effective security strategies and make it harder to detect, investigate, and prevent insider activity.

An overarching protective security strategy

5.1 The risk of insider threat at the border not only comes from Border Force staff, but also from staff working at ports for private companies and organisations. As a result, two distinct insider threat programmes were created following the publication of the UK Anti-Corruption Strategy 2017-2022. One, led by Border Force, related to the internal threat posed by Border Force staff, and is the focus of this inspection. The other is led by the Homeland Security Group, focusing on the threat posed by external staff employed at ports. In addition, the National Crime Agency (NCA) has responsibility for all crime at the border.[22]

Leadership: Border Force's response to insider threat

5.2 Border Force's response to insider threat is led by the Border Force Operational Assurance Directorate (BF OAD).

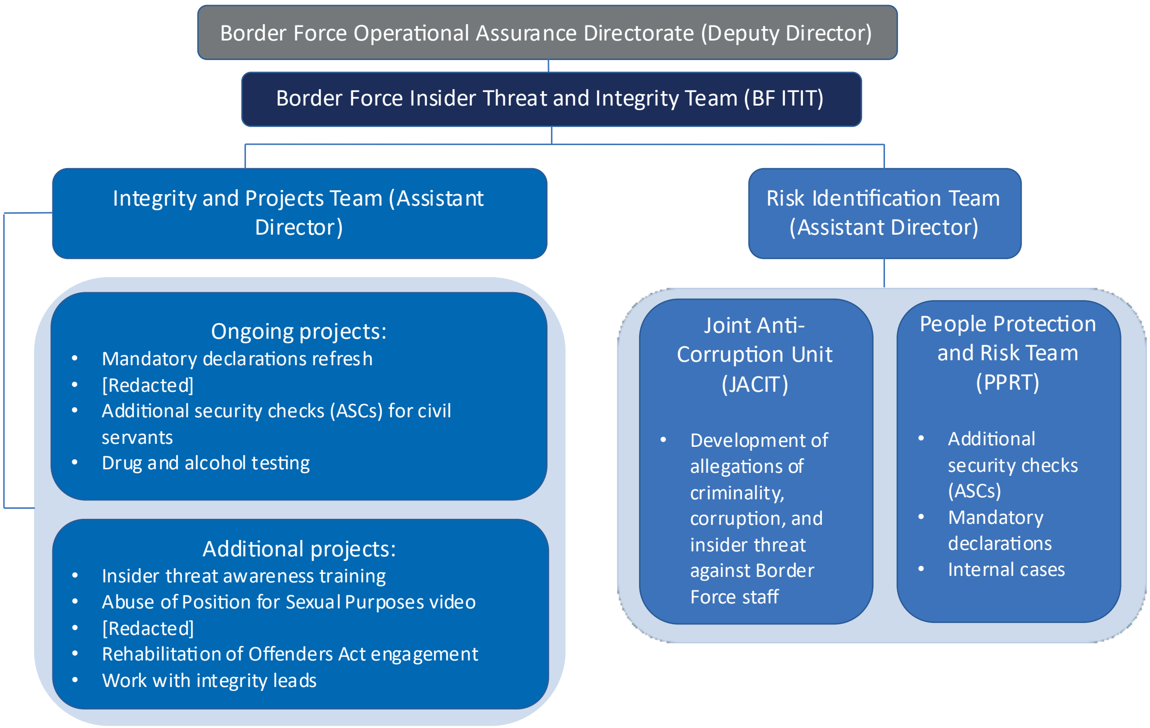
[21] NPSA website, Advice and Guidance, Personnel and People Security, Insider Risk, Leadership and Governance, https://www.npsa.gov.uk/leadership-and-governance accessed 9 March 2023.

[22] Homeland Security Group is responsible for the work in the Home Office to counter terrorism and to cut serious and organised crime. It co-ordinates domestic and some overseas work on these issues across government.

Border Force Insider Threat and Integrity Team

5.3 The Border Force Insider Threat and Integrity Team (BF ITIT) within BF OAD is responsible for delivery of the Border Force Insider Threat Programme. BF ITIT is made up of a project capability and operational arm. The project capability arm is known as the Integrity and Projects Team. The operational arm is known as the Risk Identification Team and is composed of two sub-teams. Firstly, an intelligence function known as the Joint Anti-Corruption and Intelligence Team (JACIT). Secondly, a personnel support and risk management function known as the People Protection and Risk Team (PPRT). This is illustrated in Figure 2.

Figure 2: Organogram of the Border Force Insider Threat and Integrity Team



Border Force Operational Assurance Directorate (Deputy Director)

Border Force Insider Threat and Integrity Team (BF ITIT)

Integrity and Projects Team (Assistant Director)

Ongoing projects:
- Mandatory declarations refresh
- [Redacted]
- Additional security checks (ASCs) for civil servants
- Drug and alcohol testing

Additional projects:
- Insider threat awareness training
- Abuse of Position for Sexual Purposes video
- [Redacted]
- Rehabilitation of Offenders Act engagement
- Work with integrity leads

Risk Identification Team (Assistant Director)

Joint Anti-Corruption Unit (JACIT)
- Development of allegations of criminality, corruption, and insider threat against Border Force staff

People Protection and Risk Team (PPRT)
- Additional security checks (ASCs)
- Mandatory declarations
- Internal cases

5.4 BF ITIT has also recently added a data specialist to consider the data requirements and issues across both the projects team and the Risk Identification Team.

Integrity and Projects Team

5.5 The Integrity and Projects Team works to develop and deliver the objectives of the Border Force Insider Threat Programme.

5.6 Internal documents relating to the Border Force Insider Threat Programme showed that from its inception in 2018, the programme had five objectives as outlined in Figure 3.

Figure 3: Border Force Insider Threat Programme objectives

2018 – Objective	2023 – Current status
“Initiate a ‘Proof of Concept’ Joint Anti-Corruption Intelligence Team with Home Office Security and the National Crime Agency (NCA), focused on Border Force corruption.	Met – now business as usual
Develop a detailed proposal to carry out additional security checks on Border Force staff.	[Redacted]
[Redacted]	[Redacted]
[Redacted]	
Develop a detailed proposal for drugs and alcohol testing of Border Force staff.”	

5.7 The Integrity and Projects Team also has responsibility for several other projects, some of which are ongoing and some completed, as illustrated in Figure 4:

Figure 4: Integrity and Projects Team’s additional projects

Completed projects	Ongoing projects
Migration of mandatory declarations from email-based forms to the Central Operations Platform – delivered March 2020[23]	[Redacted]
Refreshed the Border Force Code of Ethics – delivered 2021	[Redacted]
Created the Joint Anti-Corruption Team (JACIT) – delivered as a proof of concept in 2018, and became ‘business as usual’ in 2019	[Redacted]
Created the People Protection Risk Team (PPRT) – delivered in 2019, with a review planned at the three-year life-time point	[Redacted][24]
Protecting People Policy – delivered 2021	[Redacted]
Insider threat awareness sessions – delivered 2020, with an ongoing rolling programme of sessions	[Redacted]
Researching the possible prevalence of ‘abuse of position for sexual purposes,’ as a result of high-profile cases in the police with awareness video already produced for staff	

[23] The Central Operating Platform (COP) is a bespoke Border Force IT system that digitises Border Force forms.
[24] [Redacted].

Risk Identification Team

5.8 The Risk Identification Team has responsibility for projects that have become 'business as usual' via its two sub-teams.

5.9 JACIT is responsible for receiving, recording, and developing intelligence and information with partners. Where possible intelligence is tasked to investigating teams or line managers, via PPRT.

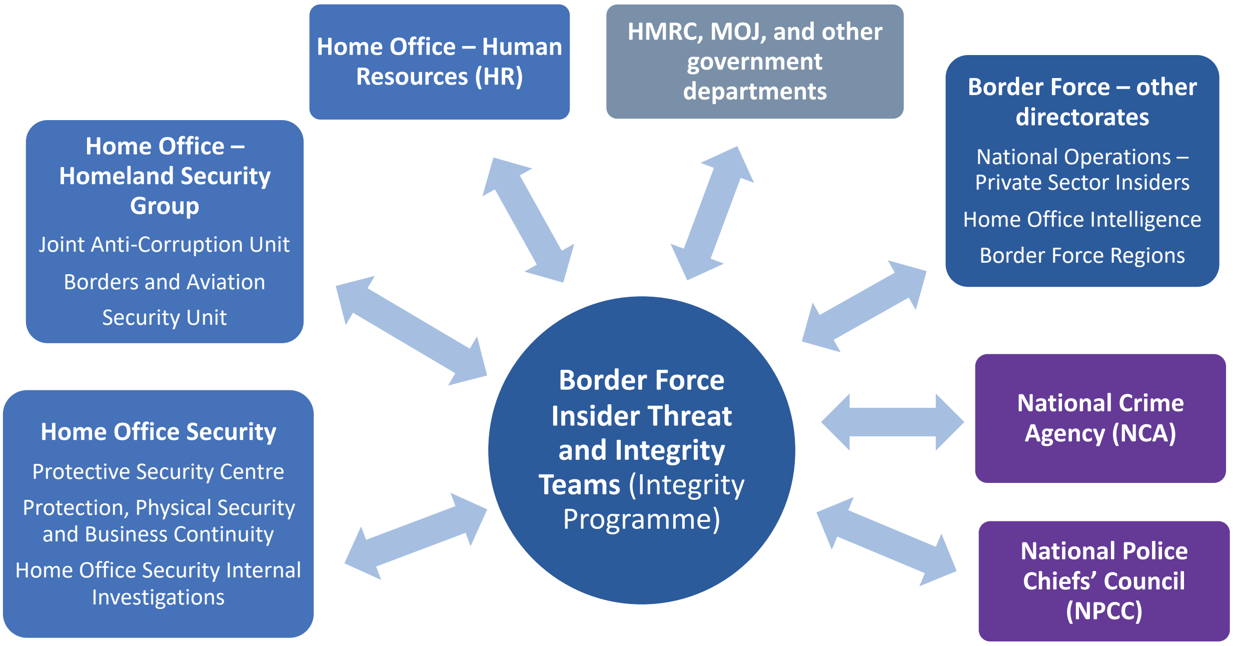
5.10 PPRT is responsible for undertaking:

- the delivery of ASCs for new recruits external to the Civil Service
- reviews of positive mandatory declarations in conjunction with line managers and integrity leads where advice and guidance is requested
- reviews of internal cases of identified risk brought to the attention of PPRT by JACIT, line managers, or integrity leads, or self-referrals from staff members

Stakeholders

5.11 BF ITIT works with a wide range of stakeholders internally to Border Force, within the wider Home Office and externally, as illustrated in Figure 5.

Figure 5: Border Force Insider Threat and Integrity Team key partners


Home Office – Human Resources (HR)
HMRC, MOJ, and other government departments
Border Force – other directorates
National Operations – Private Sector Insiders
Home Office Intelligence
Border Force Regions
Home Office – Homeland Security Group
Joint Anti-Corruption Unit
Borders and Aviation Security Unit
Border Force Insider Threat and Integrity Teams (Integrity Programme)
National Crime Agency (NCA)
Home Office Security
Protective Security Centre
Protection, Physical Security and Business Continuity
Home Office Security Internal Investigations
National Police Chiefs' Council (NPCC)

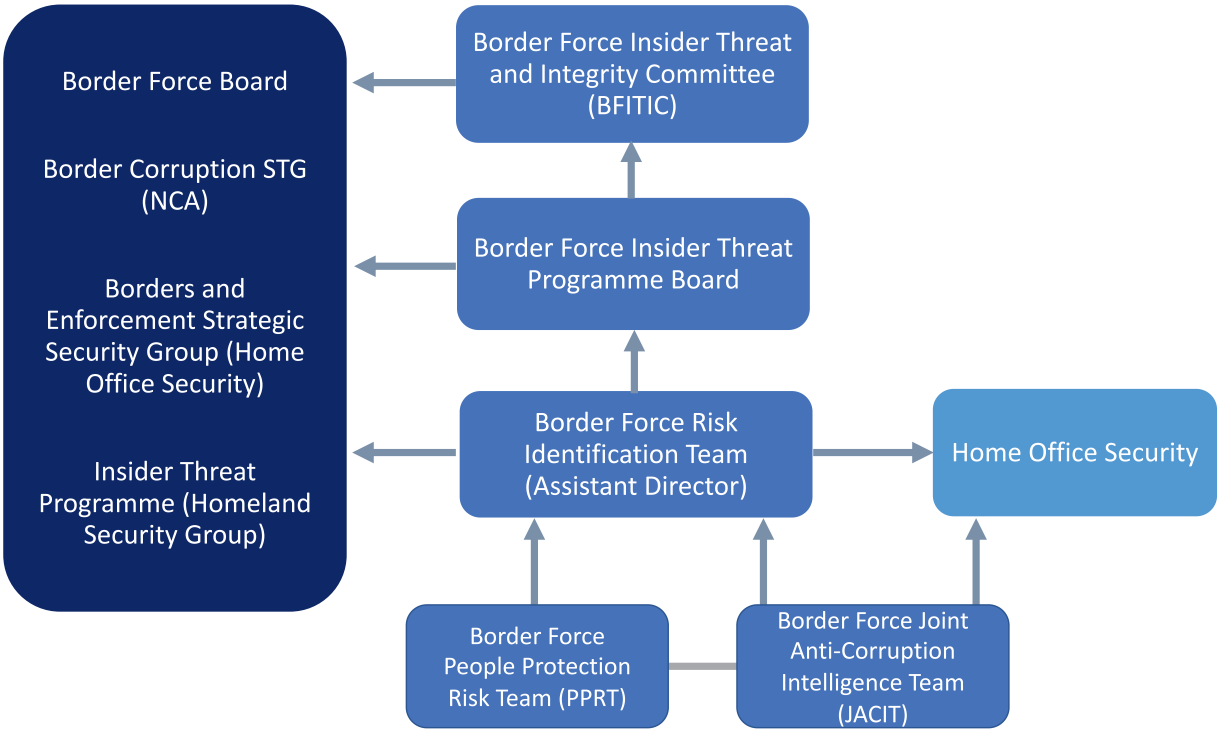
5.12 An external stakeholder described Border Force as a 'key stakeholder' at the quarterly National Police Counter-Corruption Advisory Group (NPCCAG) chaired by the National Police Chiefs' Council. This is attended by various policing bodies and government departments including the Crown Prosecution Service and HM Prison Service. Border Force had actively engaged with the group, taking away best practice from partners, such as advice on abuse of position for sexual purposes. Border Force had also recently delivered a presentation on ASCs to share effective practice with others.

Governance

Updated governance structure

5.13 Border Force provided details of the various bodies within both its own organisation and across the wider Home Office and government that played a role in its response to insider threat, as shown in Figure 6:

Figure 6: Governance structure as depicted in the Border Force Insider Threat and Integrity Committee terms of reference[25]



Border Force Board
Border Corruption STG (NCA)
Borders and Enforcement Strategic Security Group (Home Office Security)
Insider Threat Programme (Homeland Security Group)
Border Force Insider Threat and Integrity Committee (BFITIC)
Border Force Insider Threat Programme Board
Border Force Risk Identification Team (Assistant Director)
Home Office Security
Border Force People Protection Risk Team (PPRT)
Border Force Joint Anti-Corruption Intelligence Team (JACIT)

Border Force Insider Threat and Integrity Committee

5.14 The Border Force Insider Threat and Integrity Committee (BFITIC) provides 'top-level governance' to the Border Force Insider Threat Programme. It has oversight of identified insider and integrity risks and feeds into the Borders and Enforcement Strategic Security Group.

5.15 In April 2022, the 'One Home Office' initiative planned to merge the Directors General of Border Force and Immigration Enforcement into a single post, combining the two organisations into one 'Borders and Enforcement' body.[26] The One Home Office plan for one Director General was never realised; however, legacy elements of the initiative remain where the two organisations have looked for opportunities for closer alignment, and as a result for a short period the BFITIC, then known as the Borders and Enforcement Insider Threat and Integrity Committee (BEITIC) was jointly chaired by the Directors General of Border Force and Immigration Enforcement. This has now reverted to being chaired solely by the Director General of Border Force.

[25] Border Force Insider Threat and Integrity Committee (BFITIC) was previously known as the Borders and Enforcement Senior Steering Group (SSG).
[26] 'One Home Office' is a transformation programme that aims to build an organisation which is flexible, resilient, outward-facing, and better able to respond to changing circumstances.

5.16 Alongside the Director General, membership of BFITIC consists of senior leaders from Border Force, UKVI integrity teams, Home Office Security, Protective Security Centre (Operations), Home Office Human Resources, Joint Anti-Corruption Unit, and the Border Force Intelligence Team. Such a multi-disciplinary approach allows the committee to be alive to emerging issues in other areas of the Home Office, which can be considered to ensure that risk and any measures Border Force may wish to take are consistent and proportionate.

5.17 The BFITIC also follows developments in the Home Office and partner organisations to ensure that Borders and Enforcement related strategy is aligned to and influences strategies in these areas. Where there are challenges aligning with wider Home Office strategies, projects may be unable to progress until agreement is reached or an alternative way forward is found.

5.18 The initial iteration of the BFITIC oversaw the delivery of the Home Office Second Permanent Under-Secretary's programme on insider threat and named the Director General of Border Force as the single responsible owner.[27]

5.19 In the evolution of the group to the BFITIC, the Home Office Second Permanent Under-Secretary no longer appeared in the terms of reference. Inspectors concluded the BFITIC appeared to have lost this link to higher authority in the Home Office, and that this may have contributed to difficulties resolving issues. Access to a more senior authority might enable Border Force to escalate matters where wider Home Office or Civil Service policies impact on the ability of Border Force to implement mitigation measures.

5.20 Staff within Border Force and the Home Office named the Director General of Border Force as the single accountable board-level owner of insider threat coming from Border Force.

Border Force Insider Threat Programme Board

5.21 Membership of the Border Force Insider Threat Programme Board largely mirrors that of the BFITIC, although representation is at a more junior level and is chaired by the Director of Border Force Operational Assurance Directorate (BF OAD). BF OAD provides a second-line assurance and risk function across Border Force, with line managers being the first line of assurance.

5.22 The board communicates information about the Border Force insider threat programme to key stakeholders and resolves any deviations from plans and any conflicts within the programme. Broadly, its role is to:

> "Scrutinise and agree positions to be taken at the Borders Force Insider Threat and Integrity Committee (the BFITIC), which is the top level of programme governance, chaired by the Border Force DG. [It] also provides an opportunity for attendees to brief their seniors attending the BFITIC, which is usually scheduled for around a week later."

Further insider threat boards and groups

5.23 Border Force provided a list of six further boards and groups to which it contributes but said that these were not oversight bodies, despite some being included in the governance diagram from the BFITIC terms of reference. These were:

- Security Strategy Board (led by Home Office Security)

[27] The initial iteration of the BEITIC was known as the Senior Steering Group (SSG). It was renamed to avoid confusion with the Strategic Security Group, whose acronym was also SSG.

- Borders and Enforcement Strategic Security Group (led by Home Office Security)
- National Crime Agency Boards (including the borders corruption sub-threat group)
- the cross-government Deputy Directors Board on Anti-corruption (led by the Home Office Joint Anti-Corruption Unit)
- the National Police Chiefs' Council Anti-Corruption Advisory Group (led by South Yorkshire Police)
- Homeland Security Group – Ports and Borders Insider Threat Programme Board (now defunct)

5.24 Each directorate of the Home Office has a Strategic Security Group, looking at cross-cutting security issues, with executive leadership and oversight coming from the Senior Security Board (SSB). The SSB is held quarterly and is chaired by the Chief Security Officer or a nominated deputy. It is responsible for making decisions and if necessary, escalating matters to other strategic boards, including the Government Security Board at Cabinet Office, the Home Office Executive Committee, and other Home Office Boards, depending on the nature of the issue raised. A Home Office senior leader explained that the SSB often discusses insider threat, and reports quarterly to the Home Office Second Permanent Under-Secretary.

5.25 Overall, this suggested there was some external oversight of Border Force relating to insider threat. However, there was some confusion between Border Force and the Home Office as to the functions, relationships and oversight that existed between the boards.

Border Force insider threat risk register

5.26 Border Force risk registers state that the risks from insider threat are owned by BF ITIT, except for 'unbudgeted financial pressures', which is owned by the Border Force Deputy Director. Inspectors noted that risks were not owned by the Director General of Border Force or the BFITIC, who have the responsibility for strategic decisions, undermining the governance structure that Border Force has in place for its Insider Threat Programme. It was unclear to inspectors why risks where not owned by a single, accountable board-level owner in line with NPSA advice.

5.27 The open risks to the programme are listed as:

- General Data Protection Regulation (GDPR) and data processing
- unbudgeted financial pressures
- insider threat HR data
- insider threat data from law enforcement and other third-party information
- trade union buy-in

5.28 Examination of the risk register by inspectors indicated that the risks are regularly reviewed and BF ITIT is taking what steps it can to resolve issues as promptly as possible. For example, a Grade 7 Data Protection specialist was recruited in October 2022 to work through data sharing issues and liaise with the Government Legal Department and the Office of the Data Protection Officer. However, the risks are often complex and ownership of them at a more strategic level might enable them to be mitigated more effectively.

Provision of staff resource

5.29 Border Force officers told inspectors that the volume of work in relation to additional security checks (ASCs) was extensive and had to be completed within tight timeframes. Moreover, a Border Force senior leader confirmed there would be resource implications for the Border Force Insider Threat Programme if the additional security checks or the mandatory declarations workstreams were to be expanded. A Border Force senior leader explained it was difficult to estimate how big the impact would be until the work started and more data was available, but narrative evidence provided to inspectors highlighted that "[redacted]".

5.30 Additionally, delivery of the Joint Anti-Corruption Intelligence Team (JACIT) and the ASCs for external recruits to the Civil Service are heavily reliant on NCA and police resource. This could become a concern should organisational priorities diverge and the NCA and police choose not to provide this resource.

5.31 Inspectors found that resource was also an issue when it came to analysing data. Border Force senior leaders told inspectors that in order to analyse data held by the Risk Identification Team, an analyst resource would be required.

5.32 Inspectors accepted that future resource was largely dependent on decisions made about the direction of projects; however, it appeared that staff resource was a risk to the effectiveness of those projects already delivered and operating as 'business as usual'.

5.33 Inspectors found that more work needed to be done to be able to implement the full range of proposed measures that Border Force wishes to pursue. A lack of adequate resourcing would impact on the ability of Border Force to implement expansion of existing measures, [redacted]. Senior managers should review the resources available to the teams who lead on delivering insider threat mitigation.

Reviews and strategy

5.34 Border Force told inspectors that the Border Force Insider Threat programme was under constant review by the Director General of Border Force as senior responsible officer. As such, the programme did not require an annual review.

5.35 While inspectors accepted the progress of projects was discussed at each meeting of the BFITIC and Insider Threat Programme Board, there was no holistic review of the overall programme, its effectiveness, and the data on which decisions were based. Inspectors considered this contributed to issues and risks, such as the risks around [redacted], remaining unresolved for several years.

5.36 In response to the evidence request for copies of any Home Office or Border Force insider threat reviews or assessments, Border Force provided the Home Office Anti-Fraud and Corruption Policy, Strategy and Plan, from March 2017, and a copy of the analysis and assessment it had commissioned from Border Force Intelligence. Inspectors found no indication that the Home Office Anti-Fraud and Corruption Strategy and accompanying policy and plan, had been reviewed or updated since 2017.

5.37 Evidence provided to inspectors also included the Border Force Insider Threat Control Strategy, dated 31 August 2021. The document "aims to set out clear objectives in the identification, management and mitigation of insider threat within Border Force". However, this too had not been updated since its creation, despite detailing it would be reviewed every six months.

5.38 Furthermore, the UK Anti-Corruption Strategy 2017-2022 has concluded. Yearly updates tracking the progress of the commitments made by the strategy were published in 2020 and 2021, relating to work undertaken in the first three years of the strategy. At the time of writing, updates for years four and five of the strategy have not been published.

5.39 Inspectors considered that the lack of holistic reviews of the Border Force Insider Threat Programme and up-to-date supporting strategy documents meant the strategic vision for the programme had been lost.

Summary

5.40 Inspectors considered that positive steps and progress had been made in Border Force's implementation of measures to tackle insider threat following the introduction of wider government strategy and the Border Force Insider Threat Programme. However, there is no single, accountable board-level owner and a lack of reviews, which NPSA advice considered to be fundamental.

5.41 Inspectors recognised that it was difficult to establish a simple organisational framework relating to Border Force's response to insider threat. There were many stakeholders involved in this work, sitting both within Border Force, within the Home Office, and the wider Civil Service which resulted in a confused governance picture. While staff were able to identify the Director General of Border Force as the owner of the risk of insider threat, in practice, the situation is more complex, with wider engagement across the Home Office required to agree and implement mitigation measures.

5.42 The lack of clear governance from a single, accountable board-level owner appears to be affecting the ability of Border Force to introduce some of the mitigation measures desired. Lack of access to the full range of pertinent data is a particularly limiting factor, alongside wider HR policies and procedures being set outside of Border Force.

5.43 Figure 7 summarises what inspectors consider to be working well and what requires further attention.

Figure 7: Leadership and governance summary table

Working well	Further attention required
Dedicated resource within Border Force to address insider threat issues and progress the Border Force Insider Threat Programme	Confused governance picture
Ongoing programme of work to mitigate the potential risks posed by insider threat	No single responsible owner who can make decisions taking account of the impact on both Border Force **and** the wider Home Office
	Key elements of the Border Force Insider Threat Programme are reliant on NCA and police resource
	No annual review to consider the effectiveness of the Border Force Insider Threat Programme, or up-to-date strategic vision

6. Inspection findings: Organisational culture and trust

Figure 8: National Protective Security Authority (NPSA) guidance used by inspectors to consider Border Force's effectiveness in this area

Organisational culture and trust[28]
Strong protective security relies on the trust built between employer and employees
• Importance of good relationships between management and employees to preserve organisational trust • Poor management and grievance procedures could add to dissatisfaction • Disaffection could lead to increased risk of insider acts • Importance of open, honest, consistent, and respectful communication • Organisations should demonstrate that they value employees

People Protection Risk Team and People Protection Policy

6.1 Border Force Operational Assurance Directorate (BF OAD) has responsibility for insider threat within Border Force and has introduced measures to improve organisational trust.

6.2 [Redacted].

6.3 An accompanying 'Protecting People Policy' was published internally in March 2021 to provide a set of principles to help mitigate risks surrounding personnel security and potential insider threat. It was intended to set the 'cultural tone' that Border Force wishes to support staff who are vulnerable to corrupting pressures. It also provides advice for line managers in handling these cases.

6.4 Despite the attempt to improve organisational trust and promote a more supportive culture through the Protecting People Policy, a Border Force senior leader explained that the policy may not have landed as well as hoped with staff as it was the first thing to be published on SharePoint.[29] Insufficient communication and staff unfamiliarity with SharePoint may have resulted in a lack of awareness of the policy.

Communication regarding insider threat

6.5 A Border Force officer told inspectors that, prior to the introduction of the Border Force Insider Threat Programme, there had been a "culture of fear" where people were scared to report issues relating to vulnerability or insider threat. They said that Border Force was conscious

[28] NPSA website, Learning and Resources, Insider Risk Mitigation digital learning, Module 3 – Leadership Role in Preserving Organisational Trust, https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

[29] SharePoint is a Microsoft Office internet based collaborative application that enables organisations to store, share, edit, and manage documents.

about helping staff feel "secure in coming forward" and providing lots of different channels to seek help or advice.

6.6 In addition to the People Protection Risk Team (PPRT), Border Force had also created a network of 'integrity leads' as a conduit to staff to circulate information and newsletters and update their SharePoint communications platform.

6.7 There was also an Integrity Lead Forum comprising representatives from each Border Force region and supporting commands, led by the Border Force Insider Threat and Integrity Team (BF ITIT). The forum played a key role in leading the Border Force approach to insider risk, aiming to create a culture where staff are aware of insider threat and integrity related risks and vulnerabilities. The forum promoted insider threat training, encouraged staff to report concerns, and signposted staff to available support. In addition to providing written communication around integrity and insider threat, integrity leads act as the conduit for two-way communication between operational teams and the Border Force Insider Threat Programme. Home Office Security staff and Border Force officers also described sharing lessons learned from different parts of the business and previous investigations.

6.8 While some Border Force officers in Dover were not fully aware of the PPRT, they were aware of who the local integrity leads were. However, some said that they would be more likely to approach line managers or Human Resources colleagues if they were concerned about someone's conduct, behaviours, or wellbeing. There was no formal process to notify their integrity lead. This suggested that while the Integrity Lead Forum was a useful way of disseminating information, raising awareness of insider threat and integrity issues with staff, and promoting a security culture, it mainly broadcast, rather than received information. Details of emerging trends and issues may not be visible to integrity leads, unless they were specifically notified, resulting in limited value as a feedback loop.

People Survey

6.9 Border Force employees were encouraged to complete the 2022 'People Survey' which measured staff engagement, how they felt about their work, and their understanding of the Civil Service Code. It was conducted across Civil Service organisations and closed on 31 October 2022. There were 4,577 Border Force responses, representing 49% of the workforce. In order to provide an assessment of the culture that exists within Border Force, inspectors analysed the Border Force responses to the People Survey, as well as speaking to staff and senior leaders. A key measure of the survey is 'employee engagement', which is a "workplace approach designed to ensure that employees are committed to their organisation's goals and values, motivated to contribute to organisational success".

Border Force employee engagement

6.10 Employee engagement scores were significantly lower for Border Force staff than in other parts of the Civil Service. Forty-two percent of Border Force staff who completed the survey agreed with the statement: "I am proud when I tell others I am part of my organisation" (compared with 67% across the Civil Service), with 28% disagreeing or strongly disagreeing with the statement.

6.11 Thirty-two percent of Border Force staff felt a strong personal attachment to the organisation, (compared with 51% across the Civil Service). Some Border Force officers in Dover told inspectors they felt loyalty towards their immediate colleagues and team but less so towards

Border Force: "I think there is loyalty to people, to your colleagues, but not to the organisation. Teams are very close, but people don't feel looked after by the organisation."

6.12 While 58% of Border Force staff who responded indicated that they felt valued for the work they did, (compared with 71% across the Civil Service), 23% did not feel valued.

6.13 The lower engagement scores for Border Force, in comparison with the rest of the Civil Service, indicate that many staff did not fully identify with the organisation. A sense of loyalty and engagement is important for a positive organisational security culture, whereas low morale and disengagement increase the risk of insider threat. Border Force is an area already categorised as a high-risk organisation for insider threat. Employees with motive could use their considerable knowledge and opportunities to act unlawfully.

Border Force and the Home Office

6.14 As civil servants, Border Force officers are bound by the Civil Service Code. The Civil Service Code sets out the expectation that civil servants will carry out their role with dedication and a commitment to the Civil Service and its core values of integrity, honesty, objectivity, and impartiality.[30] Nationally, 84% of Border Force staff who completed the 2022 People Survey agreed with the statement: "I understand the Civil Service Code and what it means for my conduct." Inspectors determined this high proportion indicated a good understanding of the standard of behaviour required by the Border Force from its employees.

6.15 Border Force officers are subject to Home Office and wider Civil Service policies, but, as operational law enforcement officers, their role is very different to that of many Home Office staff. As part of the Home Office, Border Force is restricted in terms of setting or amending policy, making it more difficult to mitigate against insider threat.

6.16 Border Force senior leaders reported that there was a tension between the decisions Border Force wanted to take as a law enforcement command, and the decisions they were able to take as a directorate of the Home Office. The Border Force senior leader went on to explain that other law enforcement agencies have specific regulations, set out in statute law, around officer conduct. These provide a lawful basis to take action, make decisions and share information in relation to staff conduct internally within their organisations. They stated: "That is what is odd about [Border Force] being civil servants doing a law enforcement role. We do not have a bit of legislation saying what we can and cannot do." Inspectors considered this offered some explanation as to why mitigations were difficult to implement.

6.17 In 'An Independent Review of Border Force' (published in July 2022), Alexander Downer discussed the importance of the Border Force brand in creating a sense of cohesion, which is important for staff morale and commented that:

> "Border Force should have a distinct identity and voice within the Home Office, based around their unique characteristics as a uniformed force."[31]

6.18 A lack of corporate identity and cohesion could increase the risk of insider threat. This risk remains unmitigated while Border Force is unable to own and implement all of its own policies and act independently as a law enforcement agency.

[30] GOV.UK, Civil Service Reform, Civil Service values and standards of behaviour, The Civil Service Code, (published 30 November 2010), https://www.gov.uk/government/publications/civil-service-code

[31] GOV.UK, An Independent Review of Border Force, (published 20 July 2022), page 11, https://www.gov.uk/government/publications/independent-review-of-border-force

Pay

6.19 The 2022 People Survey results showed pay was the top theme for the "one change" that staff would most like their organisation to make in the next 12 months (mentioned by 1,154 members of staff). Border Force officers in a focus group in Dover told inspectors that some staff relied on shift-working allowances and six-day working, without which they may struggle financially. During the inspection, some Border Force staff took industrial action related to pay.

6.20 Inspectors considered that pay is one of the ways an organisation can demonstrate the value they place on employees. Border Force employee pay is determined by Home Office pay ranges for each grade. In addition, there are potential additional allowances that Border Force receive for shift working, on-call hours, weekend and public holiday working, and flexibility. Many Border Force staff have seen their salaries depreciate in real terms as pay has failed to keep up with inflation, and it is an issue which has led to industrial action.

6.21 The NPSA 2013 Insider Data Collection Study found that financial gain was the most common motivation for insider threat, accounting for 47% of cases in the study.[32] Therefore, the risk of insider threat due to financial gain is likely to increase where staff face increasing financial pressures.

6.22 Border Force officers in Dover highlighted that the work of an Executive Officer (EO) and an Assistant Officer (AO) was very similar in Dover. An officer who line managed both grades told inspectors that the ability to undertake immigration arrests used to be the defining line between the two grades but that AOs could now undertake arrest training: "The AOs and EOs do exactly the same job, there is no difference in their defined job roles and responsibilities, just the pay." This is a situation that has the potential to lead to resentment and disaffection of staff at the lower pay grade.

Communication with staff

6.23 Good communication is important in fostering trust in an organisation. The 2022 People Survey indicated that 46% of Border Force staff who completed the survey (compared with 66% across the Civil Service), agreed with the statement: "My organisation keeps me informed about matters that affect me." The results showed 26% disagreed and 28% gave a neutral response in answer to the same statement.

6.24 A Border Force officer told inspectors that the level of communication "completely depends on where you are, who your managers are and varies widely from tiny ports to huge ports …". Some Border Force officers said that it was easy to miss information due to the large number of emails they received and lack of time to read them. Other officers described "email fatigue" from receiving too many emails.

6.25 A Border Force senior leader in Dover described efforts they had made to improve communication through "a number of staff engagement groups" and a local bi-monthly magazine highlighting success and providing updates on staffing and processes, and speaking to staff face-to-face. However, survey results for Dover regarding communication were similar to national results.

6.26 Inspectors established that there was a clear desire to develop the open, honest, consistent, and respectful communication through a variety of communication methods and channels.

[32] NPSA website: Centre for the Protection of National Infrastructure (CPNI), 'Insider data collection study', April 2013, https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

However, the practicalities of communicating across a large organisation where many employees work shifts meant key messages may be missed by some staff, and others felt overwhelmed, resulting in gaps still being evident.

Decision making and change

6.27 Of the Border Force staff who completed the 2022 People Survey, under half agreed with the statement: "I feel involved in the decisions that affect my work" and only 21% agreed that change was managed well.

6.28 Home Office senior leaders told inspectors that it was acceptable for staff to disagree with policy, but it had to be done in a "professional" way. However, only a third of Border Force staff who completed the survey agreed that it was safe to challenge the way things were done. Fifty-six percent agreed that: "In my organisation people are encouraged to speak up when they identify a serious policy or delivery risk", which was 18% less than the overall score for the Civil Service.

6.29 A Border Force officer told inspectors that there was a "change lead" and "change SPOCS" (single points of contact) within Border Force who communicated changes to staff. Staff were able to contribute to decision making through an initiative called 'All Ideas Matter' whereby they could submit ideas for consideration by a panel of relevant business experts.

6.30 While Border Force was attempting to involve staff in decision making and change management, the results of the 2022 People Survey indicated that these initiatives were not sufficient to address dissatisfaction among staff or to mitigate against the associated risk of insider threat.

Discipline and grievances

6.31 While 73% of Border Force staff who completed the 2022 People Survey agreed with the statement: "I am treated fairly at work", 14% disagreed. Survey results across the Civil Service were better, with 85% agreeing with the statement.

6.32 Discipline and grievances are dealt with under Home Office policies. The Home Office has a 'Conflict Resolution Service' which provides coaching and training for line managers and an 'Early Resolution Service' supported by Human Resources (HR) case working which provides confidential advice to all staff.

6.33 Additionally, a Home Office senior leader informed inspectors of a joint initiative between Professional Standards Unit (PSU) and Borders & Enforcement to train Border Force officers to investigate discipline and grievance cases. Due to a lack of internal capability, the current model of identifying and commissioning a manager to investigate allegations does not work, leading to excessive delays and lack of consistency in the approach and handling of disciplinary and grievance processes. The pilot is aimed at improving the investigation process, which is undertaken by an investigation manager. Inspectors considered this reflected a recognition of staff concerns, although the initiatives may need more time to mature before results are realised.

Staff welfare

6.34 Nationally, 80% of Border Force staff who completed the 2022 People Survey agreed that their manager was considerate of their life outside work. Border Force officers in a focus group in Dover told inspectors that they had "very supportive" line managers.

6.35 The Home Office has a range of welfare support available to Border Force staff, including HR, Occupational Health, Employee Assistance Programme, Trauma Risk Management, Mental Health First Aiders, and the Home Office intranet Health, Safety, and Wellbeing Home Office SharePoint page. In addition to the dedicated 'Protecting People Policy' and creation of the PPRT, these demonstrate a wide range of staff support measures to assist those who may pose a potential risk of insider activity.

6.36 A Border Force senior leader provided inspectors with a 'Border Force Cost of Living Managers' Guide' pamphlet which had been distributed to staff in their region. It outlined the effects of stress on physical and mental wellbeing, the potential for conflict of interest outside official duties, how to spot signs that a staff member is struggling, and sources of support and guidance. They also said that staff had the opportunity to join in "all sorts of 'dial-ins' on the cost of living" and managers had been proactive in identifying individuals who may present a bigger risk than others.

6.37 Inspectors considered this emphasis on supporting staff went some way to demonstrating the value placed on employees.

Summary

6.38 Overall, inspectors found that Border Force is seeking to support its staff to create a positive organisational culture of trust and support, in line with NPSA advice. However, the stark scores of its People Survey indicate high levels of dissatisfaction. This was especially evident in areas such as feeling a personal attachment, loyalty to, and feeling valued by Border Force. Coupled with greater dissatisfaction with pay, inspectors considered that Border Force needed to remain alert to the resultant increased risk of insider threat.

6.39 Figure 9 summarises what inspectors consider to be working well and what requires further attention.

Figure 9: Organisational culture and trust summary table

Working well	Further attention required
Good support for vulnerable staff through wellbeing initiatives and creation of PPRT	People Survey 2022 results indicate that Border Force staff engagement levels are concerning (and lower than the Civil Service averages), increasing the risk of insider threat
Initiatives to include staff in decision making and improve communication	Border Force identity and cohesion, and limits on Border Force's ability to act independently of the Home Office
Positive evidence of communication and trust among staff and managers in Dover	Pay
	Role delineation of Border Force officers at Executive Officer and Assistant Officer grades at Dover

7. Inspection findings: Employee screening

Figure 10: National Protective Security Authority (NPSA) guidance used by inspectors to consider Border Force's effectiveness in this area

Employee screening[33]

Robust employment screening policies and procedures are essential in organisations meeting their legal obligations and setting a foundation for a safe and secure workplace

Appropriate screening measures help to provide cost effective and legally compliant assurance that only the right people, in the right job roles, are working within your organisation.

As part of an overarching protective security strategy the appropriate application of pre-employment screening will:

- deter applicants who may wish to harm your organisation from applying for employment
- detect individuals with an intent to harm your organisation at the recruitment/application phase
- deny employment to individuals intending to harm your organisation and deny employment in roles for which the applicant is unsuitable

Home Office recruitment

7.1 Inspectors learned that decisions on insider threat were not made in isolation and involved partnership and cross-cutting work across government. Recruitment of Border Force officers is managed centrally through the Home Office Resourcing Centre (HORC) and the Government Recruitment Service (GRS). A Home Office senior leader explained: "Border Force don't own National Security Vetting or HR data and that does limit some of the things they are able to do."

7.2 The Baseline Personnel Security Standard (BPSS) is mandatory in the public sector and is required for the recruitment of all civil servants.[34] This involves checks on an employee's identity, right to work in the UK, and recent work history. These checks are carried out on all potential employees, even those transferring from other government departments.

National Security Vetting

7.3 The BPSS is one of four levels of personnel security controls available to the Home Office depending on the level of assurance required for the role. The others are the Counter-Terrorist Check (CTC), Security Check (SC) and Developed Vetting (DV). The BPSS is not a security

[33] NPSA website, Advice and Guidance, Personnel and People Security, Insider Risk, Employee Screening, https://www.npsa.gov.uk/employment-screening accessed 24 April 2023

[34] GOV.UK, HMG Baseline Personnel Security Standard (BPSS), (published May 2018), https://www.gov.uk/government/publications/government-baseline-personnel-security-standard

clearance whereas the CTC, SC, and DV are all formal security clearances obtained through the National Security Vetting process.[35]

7.4 National Security Vetting is conducted for national security purposes. All Border Force staff require a minimum of SC clearance. Border Force officers in more sensitive roles may require DV clearance, which is an 'intrusive', higher level of clearance.

7.5 A Home Office senior leader told inspectors that National Security Vetting levels will be changing over the next two years. Level 2 (the SC clearance equivalent) will include broader checks such as social media profiles and barring lists (for example, the police barring list which contains details of those who have been dismissed from the police). These checks will be repeated every six to 12 months.

7.6 UK Security Vetting, which is part of the Cabinet Office, carries out most of the checks on new entrants. The Home Office Protective Security Centre (previously known as Cluster 2 Security Unit) conducts any follow up enquiries or issues that arise after security clearance is granted.

Additional security checks

7.7 As a result of reports from the National Crime Agency (NCA) of potentially corrupt Border Force officers performing front-line roles, one of the initial five objectives of the Border Force Insider Threat Programme was to introduce additional security checks for Border Force staff. On 16 September 2020, Border Force introduced additional security checks (ASCs) for all recruits into Border Force, who were external to the Civil Service. A Home Office senior leader said that the ASC process considered a candidate's suitability for employment in a law enforcement role and was similar to police vetting.

7.8 ASCs are conducted by the People Protection Risk Team (PPRT) and include checks on [redacted]. ASCs are processed in parallel with National Security Vetting to ensure a timely delivery.

7.9 [Redacted].

7.10 The Home Office told inspectors that complex cases would be discussed by a panel comprising senior managers and the director of the Insider Threat Integrity Team. Where ASCs results were ambiguous, officers made further enquiries. PPRT guarded against the risk of unconscious bias by removing candidate details and by having a team that was very diverse in terms of "gender, age, and ethnicities".

7.11 A union representative said that Border Force Insider Threat and Integrity Team (BF ITIT) had involved them in discussions about ASCs from the start and that the union was supportive of this initiative.

7.12 [Redacted].

7.13 [Redacted].[36]

7.14 [Redacted]. In December 2022, four Border Force officers were arrested on suspicion of misconduct in public office and conspiracy to steal (one of whom was also arrested on

[35] GOV.UK, HMG Baseline Personnel Security Standard (BPSS), (published May 2018), https://www.gov.uk/government/publications/government-baseline-personnel-security-standard

[36] GOV.UK, UK anti-corruption strategy 2017 to 2022, (published 11 December 2017), p8, https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022)

suspicion of immigration offences).[37] They had been Immigration Enforcement officers at the time of the suspected offence but responsibility for their work moved to Border Force on the day of their arrest. This was due to the transfer of responsibility for small boat migrant arrivals from the Clandestine Channel Threat Command in Immigration Enforcement to the Small Boats Operational Command. [Redacted].

7.15 [Redacted].[38] [Redacted]. Inspectors were surprised to learn that the baseline personnel security standard would not highlight that employment history information may be incorrect.

7.16 [Redacted].[39] [Redacted].

Summary

7.17 In line with NPSA advice, Border Force has implemented a good screening process in addition to existing Home Office recruitment screening and National Security Vetting. This has been effective in detecting many external candidates who were unsuitable for employment within a law enforcement agency and denying them entry to the organisation. The introduction of the additional screening checks is also likely to have acted as a deterrent for others. However, the lack of ASCs for existing Civil Service employees (including some high-risk staff) increases the risk of insider harm.

7.18 [Redacted].

7.19 Figure 11 summarises what inspectors consider to be working well and what requires further attention.

Figure 11: Employee screening summary table

Working well	Further attention required
BPSS, National Security Vetting, and ASCs form a good screening process	[Redacted]
ASCs identifying unsuitable candidates	[Redacted]

[37] www.lbc.co.uk 29 December 2022 https://www.lbc.co.uk/news/border-force-official-arrested-illegal-immigrant
[38] [Redacted].
[39] [Redacted].

8. Inspection findings: Employee monitoring

Figure 12: National Protective Security Authority (NPSA) guidance used by inspectors to consider Border Force's effectiveness in this area

Employee monitoring[40]

Monitoring and assessment is an essential element of good personnel security

It is important that the risks an employee may pose are not only reviewed at the pre-employment stage. A programme of monitoring and review should be in place to enable potential security issues, or personal issues that may impact on an employee's work, to be recognised and dealt with effectively throughout their career.

There are different mechanisms to enable this, for example:

- Line management – ensuring line managers are well-equipped to endorse best practice security and engage with their staff to help them understand security behaviours; they play a key role in helping the organisation develop a good security culture
- Staff vetting reviews – ensuring employees are regularly reviewed for security clearances helps to keep sight of any significant changes individuals may go through and how this may impact on their organisational engagement

8.1 [Redacted].

Mandatory declarations

8.2 Mandatory declarations involve all Border Force staff making a declaration against whether:

- [redacted][41]

8.3 [Redacted].

8.4 Officers are required to make mandatory [redacted] or when there is a change in the individual's circumstances in relation to the declarations, such as being arrested, or entering into an IVA. Introduced as a manual process in 2016, the declaration was migrated to the Central Operating Platform (COP) in 2020.[42]

8.5 Changes to the mandatory declarations project have been slower than the Integrity and Projects Team expected. Border Force senior leaders told inspectors that the Integrity and Projects Team had been trying to implement a 'version 2' of mandatory declarations for over two years. This would provide better data and make the declaration process for staff "smoother and easier to navigate" while also improving the quality of management

[40] NPSA website, Advice and Guidance, Personnel and People Security, Insider Risk, Monitoring and Review, https://www.npsa.gov.uk/insider-risks/monitoring-review accessed 24 April 2023.

[41] [Redacted].

[42] Central Operating Platform (COP) is a bespoke Border Force IT platform that digitises existing Border Force forms.

information (MI) that can be [redacted]. A shortage of system developers within Digital, Data, and Technology (DDaT), along with GDPR complexities, meant that the upgrade had not taken place, although Border Force senior leaders told inspectors they were hopeful it would be implemented in March 2023.

8.6 The number of total declarations received since December 2019, broken down by positive and negative results, is illustrated in Figure 13.

Figure 13: Mandatory declaration outcomes from December 2019 to January 2023

Mandatory declarations	Total submissions received
Negative	15,502 (80.1%)
Positive	3,851 (19.9%)
Total	19,353

8.7 Figure 14 breaks down the positive results over the same timeframe by category. Staff taking secondary employment is the overwhelming reason for a positive declaration.

Figure 14: Breakdown of mandatory declaration positive results from December 2019 to January 2023

Types	Percentage of positive submissions
Other employment	76%
Criminality	11%
Sponsorship	10%
Financial	2%
Business interests	1%

8.8 People Protection Risk Team (PPRT) Border Force officers explained the laborious process of checking COP for any declarations that may require further investigation. [Redacted]. As a result, PPRT would contact the member of staff or their line manager to gain further information to progress the case and ascertain what support or action was appropriate.

[Redacted]

8.9 [Redacted].

8.10 [Redacted].

8.11 [Redacted].

8.12 [Redacted].

Drug and alcohol testing

8.13 In 2018, drug and alcohol testing (DAT) of Border Force staff was cited as a potential mitigation to insider threat in a project initiation document (PID) produced by Border Force Operational Assurance Directorate. An options paper recommending 'with-cause' DAT was submitted in May 2018 to the Border Force Senior Steering Group (now known as the Border Force Insider Threat and Integrity Committee, or BFITIC). [Redacted].

8.14 Border Force recognised implementing 'random' testing of staff as "high risk", with the potential for litigation and trade union opposition appearing significant factors.

8.15 Additionally, the minutes of the BFITIC from September 2022 reference that the policy on drugs and alcohol was largely written, but that the zero-tolerance approach in relation to alcohol was at odds with the Home Office policy, where the consumption of alcohol while on duty is only strongly discouraged, but not prohibited. The BFITIC was clear that it wanted a zero-tolerance approach, and also that "both tests [alcohol and drugs] should be carried out at all times, regardless of behaviours, symptoms, manager's concerns or staff's admissions, to ensure a consistent approach was held across the business."

8.16 While police regulations have been amended to change provisions on drug and alcohol testing of police officers, the Border Force project highlights the tension between Border Force as a 'law-enforcement agency' but also a directorate of the Home Office.[43] Trying to implement DAT as a policy would have implications on wider Home Office employment conditions.

8.17 The Border Force Insider Threat Programme states that trade unions, while not championing the testing, "have expressed an understanding of the motivation for its introduction" and that one union resented "the proposal to ban any drinking while on duty, as this restriction does not apply anywhere else within the Home Office".

8.18 [Redacted]. The Director General of Border Force is "happy that Border Force remains aligned with the rest of the Home Office, where drinking is strongly discouraged, rather than totally prohibited". It is noted that Border Force staff will still need to keep under the identified alcohol limit, which is in line with the drink drive limit for England, Wales, and Northern Ireland.

8.19 At the time of this inspection, Border Force had yet to implement drug and alcohol testing, despite the project initiation document suggesting the project has been in development for five years, since 2018. Most of the logistics and background work are complete, but it can only be implemented once a "final decision has been taken on the zero-tolerance approach, and once the General Data Protection Regulation (GDPR) considerations are confirmed as fully addressed". Additionally, the project relies on a testing 'supplier' being used through an existing Home Office Occupational Health contract to avoid entering a new tendering process. However, the Home Office is currently reviewing the Occupational Health Service contract through a tender process, which leaves a degree of uncertainty for the project.

8.20 During interviews Border Force senior leaders challenged the idea that progress had been slow. However, an external stakeholder told inspectors that it was "really surprising it's taken so long to get through" adding that: "Drug testing really is easy to push through in a law-enforcement agency – it's expected."

[43] GOV.UK, Circular: testing police officers for substance misuse, (published 30 April 2012), https://www.gov.uk/government/publications/testing-police-officers-for-substance-misuse

8.21 In its position statement, Border Force outlined the benefits of DAT:

> "Staff make decisions affecting people's lives and the nation's security; they represent the department in public; they search for the drugs we are testing them against; and they are trained in physical force. The public must trust the department, and its staff, to keep the border secure."

8.22 This view was echoed in onsite interviews, with a Border Force senior leader stating: "We enforce the law around drugs and alcohol, it's a farce we're not doing testing." Another Border Force senior leader commented: "It's not as if we're getting referrals about being drunk on the job but it feels like something we should do."

8.23 Border Force provided inspectors with an undated staff survey on the use of drugs and alcohol. The survey, which was completed by 60 members of staff, featured ten questions, and allowed staff to answer multiple choice questions. Space was also provided for staff to add their own comments, if required. As reflected in the Dover onsite interviews, the survey findings supported DAT.

8.24 However, trade unions expressed misgivings over the survey, in terms of who was approached to complete it and what was perceived as the leading nature of the questions.

8.25 [Redacted].

8.26 [Redacted].

Line management and employee monitoring

8.27 The role of line managers was described by an external stakeholder as being that of "the first responders". [Redacted]. However, Border Force senior leaders told inspectors of locally organised Higher Officer events at Dover which had received input from the Border Force Insider Threat and Integrity Team and integrity leads.

8.28 [Redacted]. The lack of consistency was mentioned by several staff, including a Border Force senior leader.

8.29 A Border Force senior leader told inspectors the relaunch of mandatory declarations would feature an increased emphasis on employee and manager discussions, adding that the project was "about people speaking to managers, we need to make that really clear when relaunching".

8.30 A senior leader told inspectors that upon finding out that an officer was working extra shifts when they hadn't previously, they spoke to the officer to find out if there had been a change in their financial circumstances. There was a good understanding of the financial drivers of insider threat, and the role that line managers played to mitigate it.

8.31 While inspectors only visited Border Force operations at the Port of Dover, where inspectors found strong evidence of a proactive approach to employee monitoring by Border Force senior leaders, it is hoped that such practices are replicated more widely across Border Force.

Searching of staff

8.32 [Redacted].

8.33 Inspectors reviewed a narrative description of the Border Force Insider Threat Programme, which detailed the following as ongoing projects:

- [redacted]
- [redacted]

8.34 [Redacted].

8.35 [Redacted].[44]

8.36 [Redacted].[45]

8.37 Other legislation that gives powers to other law enforcement officers permitted to use it for the stopping and searching of individuals includes:

- UK Borders Act 2007 (section 2 (a) and (b))
- Police and Criminal Evidence Act 1984 (sections 1 and 24)
- Aviation Security Act 1982 (sections 24B and 27)
- Aviation and Maritime Security Act
- Port Security Regulations 2009 (regulation 25(3))
- Terrorism Act 2000 (Part VIII General, section 116)
- Firearms Act 1968
- Misuse of Drugs Act 1971

8.38 [Redacted]. Border Force would be required to call on external investigation teams such as the Anti-Corruption Criminal Investigation Unit, or other law enforcement agencies if there were evidence of a criminal offence not covered by CEMA. [Redacted].

Summary

8.39 In line with NPSA advice, Border Force has an established programme of monitoring and review through its mandatory declaration programme, introduced in 2016. This programme ensures issues such as financial difficulties or secondary employment can be recognised and managed. The programme was migrated to a digital platform in 2020; however, updates to make the process more streamlined and produce better management information have been delayed due to internal pressures in DDaT.

8.40 [Redacted].

8.41 Additionally, a lack of specific training and prescriptive guidance as to how Border Force line managers address concerns or issues that may impact insider threat, may lead to an inconsistent approach and mean data held by Border Force does not reflect the true insider threat picture of their organisation.

8.42 Figure 15 summarises what inspectors consider to be working well and what requires further attention.

[44] [Redacted].

[45] [Redacted].

Figure 15: Employee monitoring summary table

Working well	Further attention required
Mandatory declaration programme well established and improved from previous paper-based iteration	[Redacted]
Border Force Senior Leaders in Dover demonstrated understanding of employee monitoring through line management	[Redacted]
	[Redacted]
	[Redacted]

9. Inspection findings: Insider risk assessment

Figure 16: National Protective Security Authority (NPSA) guidance used by inspectors to consider Border Force's effectiveness in this area

Insider risk assessment[46]

Understanding what security risks your organisation faces is essential for developing the appropriate and proportionate security mitigation measures

There are a range of risk assessment models available which all follow the same principles:

- Identify the critical assets in your organisation
- Identity the threat (based on the intent and capability of those who could carry out the threat)
- Assess the likelihood of that threat happening in your organisation
- Assess the impact to your business if the threat occurred
- Review the adequacy of existing countermeasures
- Proposal of new proportionate measures to reduce security risks

The risks that have been identified are then used to inform the security mitigations that you implement. Carrying out a security risk assessment is crucial in helping security managers audit, and communicate to the executive Board, the security risks to which the organisation is exposed.

A 'role-based risk assessment' is described by NPSA as the "foundation of good personnel security management", helping an organisation to understand whether an insider could carry out activity based on their legitimate access to critical assets. NPSA advises that by conducting the assessment, the organisation can deploy counter measures and resources, specifically to the areas or teams identified as high risk.

NPSA guidance states the assessment focuses on the role in question and whether it requires more attention than other roles, rather than on an individual.

The Border Force Insider Threat Control Strategy

9.1 The role of the Border Force Insider Threat Control Strategy is to "prioritise activity to mitigate the threats and risks associated with corruption". Published in June 2021, the strategy document detailed that "continual updating of [the] control strategy will establish a database to evaluate the causes of risks". Annexes to the control strategy document did suggest an assessment of risk broadly in line with NPSA advice. However, much of the information considered was from the 2019 Home Office Insider Threat Assessment. Inspectors found no

[46] NPSA website, Advice and Guidance, Personnel and People Security, Insider Risk, Insider Risk Assessment, https://www.npsa.gov.uk/insider-risk-assessment accessed 24 April 2023.

evidence that the strategy itself, or the risk to Border Force from insider threat, had been reviewed since the creation of the document.

9.2 Inspectors also reviewed the 2022 Border Force Strategic Threat Assessment and copies of the last four monthly threat assessments, produced by Border Force Intelligence Analysis. Inspectors found little mention of insider threat relating to Border Force officers.

The lack of role-based risk assessments

9.3 Border Force does not conduct role-based risk assessments. A Border Force senior leader commented that they did not believe they "added any value". Another Border Force senior leader said that the possibility of introducing role-based risk assessments had been discussed but that as staff moved around between roles so often, the person was more relevant than the role: "If I have an officer that is a risk, what difference would the role be?"

9.4 Border Force's consideration of the risks of certain roles appears to happen after the event, rather than before. A project options paper produced by Border Force in 2018 included some Border Force insider threat case studies, where the individual's role was a factor. One case study related to an officer who frequently worked alone within a freight shed at an airport, another worked in a role that involved frequent, lone travel to France. While the case studies highlighted the mitigations and measures put in place after the insider act was committed, they have not led to a wider piece of work to assess which roles in Border Force are most likely to be exploited in the future.

9.5 One reason provided by Border Force as to why role-based risk assessments were not carried out was the need to avoid singling out a particular grade. One Border Force officer commented: "We shouldn't focus on certain roles from my perspective" and a senior leader stated that, in relation to proposed drug and alcohol testing, Border Force would "end up testing all front-line officers and not managers and that was a cultural risk".

9.6 Inspectors concluded that Border Force not conducting role-based risk assessments was a missed opportunity. The reasons put forward for role-based risk assessment not being implemented appeared to be a conscious management decision and ignored the fact that front-line officers of a particular grade, mainly Assistant Officer (AO) or Executive Officer (EO) grade, performed most of the operational customs and immigration functions. In not focusing on specific roles, some which permit access to controlled and secure areas, valuable and dangerous goods and commodities, expensive publicly and privately owned infrastructure and other critical assets, it was potentially not taking a full account of the risks involved in these roles.

High-risk roles

9.7 Despite reluctance by Border Force to focus attention on particular roles or grades, a Border Force [redacted].

9.8 [Redacted].

9.9 Without the risk assessment and no clear steer within Border Force, there was a lack of consensus during interviews with staff on which roles were more likely to be exploited by an insider. One senior leader told inspectors that "with our multi-skilled officers, it's hard to separate out risk" while another said the risk "is across the board. Cash teams, Class A drugs teams, immigration controls – they all carry risk."

9.10 Recognising the potential risks faced by front-line staff, Border Force officers in Dover were conscious that they were working in a high-risk area where "organised crime groups spend a lot of money to get drugs through". A Border Force senior leader said that vehicle selection for searches was a multi-layered process, and a single officer did not control selection and searches. Border Force officers told inspectors that it would be "impossible" for a single member of staff to guarantee a consignment of drugs could get through the border undetected, as another officer could still select the vehicle to be searched. Officers in a different focus group said that it would be difficult to act alone, and staff would have to be "brazen" as there were CCTV cameras everywhere.

9.11 [Redacted].

9.12 [Redacted].

Data

9.13 Data to support Border Force Insider Threat programme projects is dated, reflecting the position either prior to, or in the early stages of, the programme's existence in 2018. Data largely comes from:

- insider threat acts Border Force has experienced
- examples of insider threat acts from other law enforcement agencies
- insider threat assessments produced by the NCA, the Home Office, and Border Force itself

9.14 Border Force told inspectors that data and intelligence is used to measure insider threat risks. All intelligence received by Border Force Insider Threat and Integrity Team (BF ITIT) is recorded on a bespoke secure case management system called [redacted]. Additionally, high-level threat assessments from the National Crime Agency (NCA) and the Home Office are used to help assess risk for Border Force.

9.15 [Redacted].

9.16 BF ITIT provided data to inspectors in relation to numbers and case types across additional security checks, mandatory declarations, operational security and JACIT between January 2022 and December 2022. Similar data was also provided in respect of security breaches and Human Resources (HR) misconduct cases across the same period.

9.17 This showed JACIT had received 127 referrals over the period, and of those 90 had been closed. A total of 30 cases from the period requested were in live development. An additional 37 cases opened prior to January 2022 also remained in live development. However, it was unclear how the case data linked across the time period, what the case types referred to, and what outcomes or actions had resulted.

9.18 [Redacted].

9.19 This analysis reviewed cases from June 2018 to March 2020 and findings were published internally in early 2022. Completion and publication of the report were delayed for various reasons, including during the COVID-19 pandemic when higher priority work took precedence and difficulties obtaining access to and sharing information held by JACIT, suggesting that even when BF ITIT commission work themselves, they experience issues sharing data.

9.20 Key judgements from this analysis included:

> "Corruption specific reports represent less than 1% of Border Force approximate 9,000 personnel headcount, with approximately 87% of these reports unverified as of January 2021. Furthermore, 49% of JACIT cases relate to local management issues such as poor training, attendance, and time management rather than corruption.
>
> Whilst improving, initial and continuous vetting procedures are insufficient. Vetting primarily focuses on the threat from national security as opposed to criminality and omits key vulnerability indicators such as high-risk associations. [Redacted]."

HR data

9.21 [Redacted].

9.22 [Redacted].

Summary

9.23 Border Force did undertake an assessment of risk from insider threat, broadly in line with the advice from NPSA, leading to the creation of the Border Force Insider Threat Control Strategy document. However, it has not been reviewed, and the ambition to continually update the strategy and create a database of risks and causes has not been realised.

9.24 Border Force does not conduct role-based risk assessments as advised by NPSA, and does not appear to see the value in doing so. Projects have been initiated based on putting an idea to the test, rather than clear analysis or evidence of an issue. This is not only inefficient and ineffective, but greatly reduces the chance of success as a robust evidential basis to compel their introduction is missing.

9.25 The inability to access and analyse data limits Border Force's ability to determine risk and respond to insider threat, and monitor trends against characteristics such as location, grade and role. Data is not informing the programme in a meaningful way, either in determining the mitigations taken or assessing their effectiveness.

9.26 Figure 17 summarises what inspectors consider to be working well and what requires further attention.

Figure 17: Insider risk assessment summary table

Working well	Further attention required
Evidence of initial assessment of insider threat to form a control strategy	No recent review of insider threats and causes, or control strategy
Evidence of effective practice in risk mitigation at Dover for front-line officers	Lack of role-based risk assessments
	High-risk roles have not been identified and mitigated against
	[Redacted]
	Data held by JACIT and PPRT is not routinely analysed and used to identify trends or used in support of projects

10. Inspection findings: Investigation and disciplinary practices

Figure 18: National Protective Security Authority (NPSA) guidance used by inspectors to consider Border Force's effectiveness in this area

Investigation and disciplinary practices[47]
The primary duty for an investigator is to establish the true facts, while adhering to appropriate Human Resources policy and employment laws
Organisations can react disproportionately to accusations, which can lead to costly employment tribunals or an unhappy and disaffected workforce. Conversely, organisations which fail to take any appropriate investigative and subsequent disciplinary action can create a culture where staff actively disregard security policies and processes. With correct procedures in place, employees who understand policies and regulations, and competent trained investigative staff, your organisation is better equipped to avoid these pitfalls and maintain trust.

Reporting mechanisms

10.1 Border Force Insider Threat awareness training identified the following reporting options for staff to raise insider threat concerns or seek advice or support:

- their line manager
- their local integrity lead
- a dedicated email address for the People Protection Risk Team (PPRT)
- a dedicated email address for the Internal Investigations Unit (IIU)
- a dedicated telephone number for the IIU
- a dedicated email address to report whistleblowing concerns
- a dedicated email address for the Protective Security aftercare team

10.2 Additionally, staff can report concerns under the Civil Service Code through their line management chain or through a nominated officer.[48]

10.3 Members of the public can make reports via 'Crimestoppers' if they suspect a Border Force officer of criminal activity.[49] Intelligence and allegations from the public may also be received via the departmental complaints system.[50, 51]

[47] NPSA guidance, Advice and Guidance, Personnel and People Security, Insider Risk, Investigation and Disciplinary, https://www.npsa.gov.uk/investigation-and-disciplinary accessed 24 April 2023.

[48] GOV.UK, Civil Service reform, Civil Service: values and standards of behaviour, The Civil Service Code, (published 30 November 2010), https://www.gov.uk/government/publications/civil-service-code

[49] Crimestoppers is an independent crime-fighting charitable organisation that allows people to call anonymously to pass on information about crime.

[50] UK Parliament, Written questions, answers and statements, Civil Servants: Complaints, Question for Cabinet Office, UIN 202292 tabled on 14 December 2018, https://questions-statements.parliament.uk/written-questions/detail/2018-12-14/202292

[51] GOV.UK, Home Office, Complaints procedure, https://www.gov.uk/government/organisations/home-office/about/complaints-procedure

10.4 Information may also be submitted to the Home Office by external partners.

Internal Investigations Unit

10.5 All referrals regarding corruption, fraud or insider threat are notified to the Internal Investigations Unit (IIU) which is part of Home Office Security and sits outside Border Force. The information is then triaged, centrally recorded, and sent to the relevant teams, outlined below, to develop or investigate.

Anti-Corruption Criminal Investigation Unit

10.6 Allegations relating to Home Office staff and contractors are sent to the Anti-Corruption Criminal Investigation Unit (ACCIU), which sits within Home Office Security. ACCIU can investigate anything to do with a person's position at work, such as abuse of position, breaches of policy or criminal offences, and can refer cases for prosecution. A Home Office senior leader said that where intelligence relates to staff, and involves drug importation or organised crime, ACCIU would expect the National Crime Agency (NCA) to take primacy, or they may investigate in partnership. Low-level drugs cases may be passed to the police or NCA.

Joint Anti-Corruption Intelligence Team

10.7 [Redacted].[52]

10.8 JACIT was established as a joint team across Border Force, NCA, and Home Office Security, and originally included dedicated resource from each agency. The team is now only resourced by Border Force staff, although inspectors were unable to clarify when and why this happened. JACIT researches and develops intelligence and works collaboratively with the NCA and Home Office Security to deconflict intelligence, make use of information they hold, and of their expertise.

10.9 Once intelligence has been developed, JACIT assigns or 'tasks' cases to the relevant agency or team for action. These 'operational responders' are Home Office Security, NCA Anti-corruption, or other law enforcement agencies.

10.10 Cases that do not meet the criminality threshold, but identify unacceptable or improper behaviour, indirect links to criminality (individual or organised) or vulnerabilities around integrity and behaviour, should be transferred to the People Protection Risk Team (PPRT).

10.11 As detailed in the analysis of the corruption threat within Border Force, commissioned and published internally by Border Force in early 2022, 87% of corruption allegations analysed were unverified. This appeared to be a high proportion of cases. However, a Border Force officer told inspectors that some allegations received by JACIT do not contain enough information to identify a specific staff member or corroborate the allegation. [Redacted]. This inability to easily access staff data could impair JACIT's ability to corroborate intelligence or identify potential insider threat.

[52] [Redacted].

Communication between Joint Anti-Corruption Intelligence Team and Anti-Corruption and Criminal Investigation Unit

10.12 A Home Office staff member described a positive relationship with a JACIT member of staff, who they could go to if they “needed anything”. However, other Home Office staff commented that they had little engagement with JACIT in recent years and that lately there had been “lots of cancelled meetings”. Border Force reported that it may refer insider threat cases, particularly on the “immigration side” into other parts of Home Office Security, where appropriate, for example the Protective Security aftercare team, but that there were two ‘case conferences’ due with ACCIU.

10.13 Issues regarding the tasking process out of JACIT were raised by the Home Office. Home Office staff and senior leaders told inspectors that they had expected JACIT to enrich intelligence and pass actionable intelligence packages to ACCIU, where ACCIU could take primacy. However, some Home Office staff and senior leaders said that ACCIU had “never” received a package from JACIT.

10.14 Border Force senior leaders were asked to comment on the claimed lack of referrals and intel packages back into ACCIU. They expressed surprise but conceded that JACIT had not received “a lot of immigration [cases relating to insider threat]” and that this was where ACCIU “arrest capability lies”, and that ACCIU did not have any “covert capability.” In evidence provided to inspectors, Border Force had reported that “there is currently no capability within ACCIU for the investigation of criminality relating to the detection [customs] side of Border Force business”.

10.15 Home Office Security staff told inspectors that they were not sure what Border Force meant by that statement, explaining that while drug importations involving organised crime groups would be passed to the NCA, they would be able to deal with smaller-scale drug offences relating to a Border Force officer. They also described a “terrible misconception” of what ACCIU could and could not do. ACCIU had “very experienced investigators” including full financial capability and a media investigator. ACCIU also had the potential to task Immigration Enforcement covert capabilities or those of other law enforcement agencies. While they acknowledged that ACCIU was a small team and was limited in what it could take on, they said: “We can do everything in-house. It’s just about the size of the operation.”

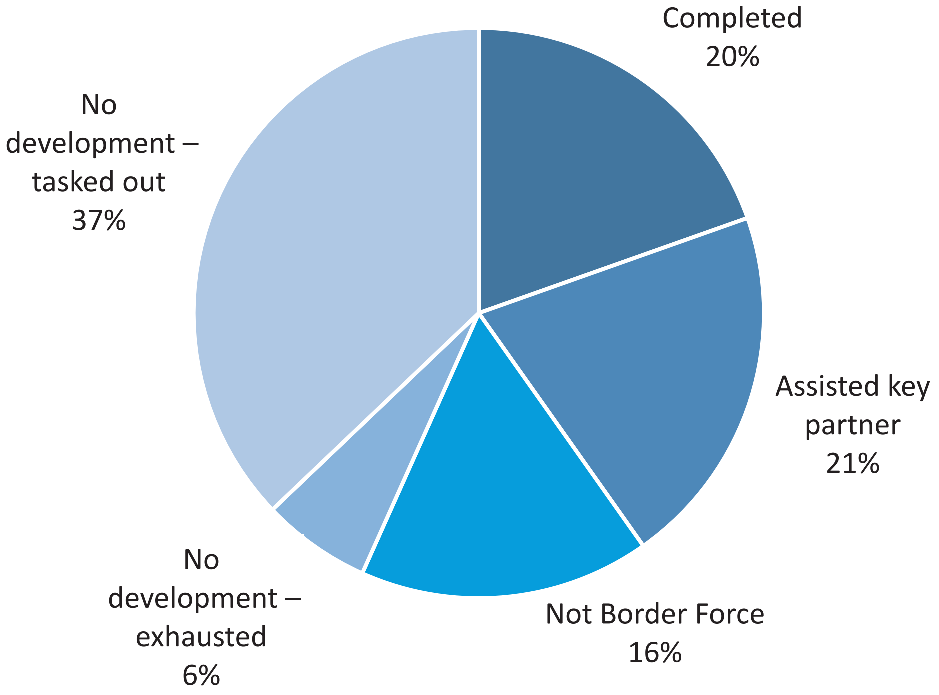
10.16 Border Force and Home Office staff told inspectors that JACIT sent closure reports to IIU if they could not develop the intelligence further, so that the case could be closed on the central record. However, [redacted].

10.17 [Redacted].

Joint Anti-Corruption Intelligence Team management information

10.18 Inspectors requested data from Border Force regarding allegations of insider threat or corruption, misconduct, or security breaches involving Border Force staff from 1 January 2022 to 31 December 2022, including outcomes. Border Force provided some data specifically relating to cases dealt with by JACIT, but this did not include the amount of detail requested. The data provided on outcomes is displayed in Figure 19.

Figure 19: Outcomes of cases closed by the Joint Anti-Corruption Team, 1 January 2022 to 31 December 2022



10.19 The data revealed that 127 referrals had been received, of which 30 remained in live development. Of the 97 cases closed by JACIT in 2022, it was not possible to identify to whom cases had been assigned or 'tasked', although 20 were recorded as assisting a key partner.

10.20 Inspectors noted from evidence provided by Border Force, that JACIT deploys MoRiLE scoring, commonly used across law enforcement agencies, and cases suitable to be tasked to external partners such as the NCA and police would likely be prioritised as a result.[53]

10.21 When asked if there had been any analysis of how successful JACIT had been in terms of being able to forward on intelligence packages, a Border Force senior leader explained:

> "On the risk side of things, we would like to see more of that work in JACIT … JACIT has a lot of data owned by the NCA, and we can't share that with anyone."

Human Resources investigations and insider threat

10.22 Cases relating to Border Force staff that do not meet the threshold for criminal investigation still come through IIU and JACIT but are then assigned to PPRT. Despite undertaking some investigatory checks as part of the separate additional security checks (ASCs) process, PPRT is not an investigatory function, and cannot undertake investigation of cases received from JACIT. Where the information relates to an identifiable member of staff, PPRT will hand off to the line manager, giving advice and support to line managers to manage risks.

10.23 As detailed in the analysis of the corruption threat within Border Force, commissioned and published internally by Border Force in early 2022, 49% of cases analysed related to local management issues rather than corruption.

[53] MoRiLE means 'Management of Risk in Law Enforcement' and is a commonly used methodology across UK law enforcement agencies to support prioritisation of their work, and assesses the potential impact of crime and harm, to individuals, the community, public expectation, and the environment.

10.24 Personal behaviours are a risk factor in insider threat, but Border Force Insider Threat and Integrity Team may not always be aware of behaviours or issues that impact insider threat. Information, concerns, and allegations may also be reported directly to line managers or to integrity leads. If the issue does not relate to corruption, there is no requirement for these cases to be notified to the Border Force Insider Threat and Integrity Team. However, line managers and integrity leads may choose to contact PPRT for advice. For issues that do not relate to corruption, line managers may choose to consult Human Resources (HR) casework, and decide themselves on any supportive or disciplinary action, including whether a referral to the Professional Standards Unit (PSU) is required.

10.25 Inspectors considered that the lack of clear and consistent processes, reporting requirements, and training could lead to inconsistent courses of action, depending on the line manager involved. This could in turn lead to the failure to identify an insider threat. Lessons should be learned from recent Metropolitan Police cases where opportunities for early intervention were missed, leading to officers being in post while carrying out serious crimes.[54, 55]

10.26 However, this is being partially mitigated by the introduction of a Professional Standards Unit (PSU) pilot to train Border Force officers to investigate discipline and grievance cases, with the intention of improving consistency of decision making.

10.27 As part of the request for data on allegations of insider threat or corruption, misconduct, or security breaches involving Border Force staff from 1 January 2022 to 31 December 2022, Border Force approached HR and was able to provide a spreadsheet with some limited data on misconduct for the period, explaining:

> "The spreadsheet detailing misconduct cases from HR shows the dates that the misconduct was raised with HR. The method of referral is solely internal via email, telephone or verbal. A synopsis of each case cannot be provided without cross checking with several other [HR] data sources which is not feasible within the time constraints."

10.28 The spreadsheet showed that in the period requested, there were 287 misconduct referrals received. There was not enough information to draw any meaningful inferences about the types of cases received or methods of referral. While some cases remained ongoing, outcomes for those cases which had concluded ranged from 'not upheld' and 'no action' through to 'informal action,' written warnings, demotion, and dismissal. Of the 287 cases, in three cases the outcome was the resignation of the officer and in another three cases the outcome was withdrawal of the complaint.

Professional Standards Unit and Independent Office of Police Conduct

10.29 The PSU is part of Home Office Security. The role of the PSU is to investigate serious misconduct allegations and complaints against Home Office staff and contractors.

10.30 PSU provides reports on the outcomes of its own and Independent Office of Police Conduct (IOPC) investigations to HR. Home Office staff told inspectors that PSU made "very few, barely any" referrals to IOPC annually, as most cases did not meet their criteria (outlined in chapter 3: background). An IOPC representative said that they currently had only two live

[54] The Guardian, 13 February 2023, https://www.theguardian.com/uk-news/2023/feb/13/wayne-couzens-pleads-guilty-to-three-counts-of-indecent-exposure

[55] Sky News, 17 January 2023, David Carrick: Timeline of Met Police's missed opportunities to stop serial rapist | UK News | Sky News

Border Force cases but they had a point of contact within JACIT, with whom quarterly meetings were held.

10.31 PSU policy restricts it from sharing investigation outcome information directly with BF ITIT, although the information would be known by individual line managers. A Home Office senior leader explained: "We have a privacy information notice, which lays out how the Home Office will use and share its data. It doesn't allow HR to share certain data outside of the line management chain."[56]

Protective Security aftercare team

10.32 All members of Border Force staff have some level of National Security Vetting. Information that may impact a Border Force staff member's security clearance may be passed to the Protective Security aftercare team by IIU, JACIT, PPRT, or other investigation teams. Staff are also advised how to contact the Protective Security aftercare team when they receive their National Security Vetting clearance.

10.33 National Security Vetting is done for national security purposes and has a wide-reaching remit to gather information but cannot be easily shared. A Home Office senior leader explained: "The privacy and information notice says we can only share [NSV related] information essentially if [a person] is an immediate danger to themselves, or others, or there is an undetected serious crime."

Data sharing

10.34 Data sharing was a recurring theme throughout this inspection. Information held and collected that has a bearing on insider threat is highly personal and sensitive. Teams involved in the collection, development, and investigation of the information have a responsibility to handle information in line with the General Data Protection Regulation (GDPR), and their respective privacy and information notices.

10.35 An example provided to inspectors by a Home Office Security member of staff, illustrated the frustrations that the difficulty of sharing information could cause.

> "A product was passed to JACIT, they had information, it went from them to PPRT, to cluster 2 [Protective security aftercare team], who contacted us but wouldn't divulge information. We're stuck. What can we do with someone when they've passed vetting … vetting can't tell us the information?"

10.36 [Redacted].

Summary

10.37 It was clear to inspectors that Border Force and the wider Home Office placed great importance on ensuring allegations could be reported and passed to investigators to establish facts, while adhering to appropriate HR policy and employment laws, in accordance with

[56] In its factual accuracy response, the Home Office stated: "Home Office Security have asked to clarify that PSU and Internal Investigations do not own any HO policies. The HO privacy notice underpins the parts of GDPR and how HR dictate the use of that data. This does not mean that the information cannot be shared. Investigations, most typically public complaints, disciplinary and grievances, can reveal very personal data and so whilst sharing of information does occur it is unlikely to be ever justifiable or proportionate to share all data." It also asked for the following statement to be added: "Data can be shared post investigation, which incorporates the final hearing and any subsequent appeals lodged, to highlight risks and threats, which sits within the responsibility of the commissioning area, most commonly the decision manager or chain of command."

NPSA advice. However, inspectors found that the numerous avenues by which allegations, behaviours, or concerns could be investigated or dealt with led to siloed working. [Redacted].

10.38 [Redacted].

10.39 Figure 20 summarises what inspectors considered to be working well and what requires further attention.

Figure 20: Investigations and disciplinary practices summary table

Working well	Further attention required
Wide range of reporting mechanisms to report insider threat, funnelled through a specific team	[Redacted]
Wide range of teams available to respond to allegations	[Redacted]
	[Redacted][57]
	No one can see the full picture of insider threat across Border Force
	[Redacted]

[57] [Redacted].

11. Inspection findings: Online personnel security

Figure 21: National Protective Security Authority (NPSA) guidance used by inspectors to consider Border Force's effectiveness in this area

Online Personnel Security[58]

Organisations should have clear policies in place to protect themselves from the harm caused by online actions and/or views of members of their own workforce, particularly in their use of social media. The online activities of employees can inadvertently impact the operations and reputation of the employer leading to financial damage for the organisation.

To mitigate the risks posed by digital technology:

- Ensure staff are aware of online risks
- Staff should be educated to recognise approaches in person or online
- Social media policies should be in place
- Staff should be aware of their online footprint

11.1 Home Office internal communications to staff highlight that the organisation holds a significant amount of operational, personal, and sensitive data. This data could be useful to adversaries such as hostile states or criminals. As Home Office employees, Border Force staff are subject to Home Office policies relating to data and technology.

11.2 The Home Office Digital, Data and Technology (DDaT) Strategy sets the direction for how the Home Office delivers better services and organises the technology and data estate more efficiently. DDaT helps the Home Office adapt to the growing availability and influence of data for both the department and its customers. This involves supporting the delivery of data as a strategic asset for the department by embedding consistent policies, processes, standards, and tools for data management.[59]

Phishing/spear phishing

11.3 Civil servants are vulnerable to approaches via email from persons purporting to be reputable stakeholders to obtain government information under false pretences. This is known as 'phishing'. A more targeted attack on a specific person is known as 'spear phishing'.[60]

11.4 The Home Office has mitigated the risk of accidental divulging of information or clicking on malware links by introducing technical controls such as quarantining suspicious emails (which must be reviewed and blocked or released by the recipient). A Border Force officer told

[58] NPSA website, Learning and Resources, Insider Risk Mitigation digital learning, Module 9 – Online Personnel Security, https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

[59] GOV.UK. Home Office Digital, Data and Technology Strategy 2024, (updated 20 October 2021), https://www.gov.uk/government/publications/home-office-digital-data-and-technology-strategy-2024/home-office-digital-data-and-technology-strategy-2024

[60] NPSA website, Learning and Resources, Insider Risk Mitigation digital learning, Module 9 – Online Personnel Security, https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

inspectors that Home Office Security also sent out communications to staff "fairly frequently" about the risks of phishing and malware.

11.5 Inspectors learnt about a Border Force initiative that demonstrated effective practice. The local compliance team set up a test to see if staff would click a link on fake phishing emails that Home Office Security had created. Staff who clicked on the link were contacted immediately and provided with information about online security. Various tests were run over several months and "the number of people clicking the link diminished".

Unauthorised devices

11.6 Malware can be introduced to an organisation's IT system via seemingly harmless items such as USB sticks given as free gifts at conferences, or 'road apples' (for example a USB stick deliberately left on the ground outside a company building, with the intention that it will be picked up and inserted into a company device).[61]

11.7 A Home Office senior leader told inspectors that the Home Office mitigates against this threat through controls on malware. USB sticks were blocked for Border Force and wider Home Office staff, with access requests requiring approval from the Digital, Data and Technology Team (DDaT).

Social media risks and policy

11.8 NPSA describes social engineering as "the manipulation or exploitation of an inappropriate relationship with an unwitting employee to gain information or access either face-to-face or online."[62] Employees may be manipulated using a sense of urgency or importance, inferring risk to the employee in not actioning, or using familiarity, flattery or encouraging sympathy.

11.9 'Hostile actors' (including criminals or foreign states) can gain useful information about a staff member through their internet profile. Information about their role, who they work with, what information they have access to, how loyal they are, and personal information can be used to manipulate a level of trust.[63]

11.10 Inspectors conducted open-source research on social media sites such as Facebook and Instagram and were able to identify a small number of serving Border Force officers. While there is no suggestion that this was a disciplinary offence, this research could easily be replicated by organised crime groups and leaves the officer vulnerable to approach.

11.11 The Home Office Social Media and Online Behaviours Policy and Guidance, issued in May 2020, applies to all Home Office staff, including Border Force. It advises staff not to identify the Home Office as their employer on social media or as part of their digital identity. Staff in operational roles "must" avoid being linked to the Home Office or use personal devices or social media sites which could provide their location details or compromise their safety and/or Home Office operations.

[61] NPSA website, Learning and Resources, Insider Risk Mitigation digital learning, Module 9 – Online Personnel Security, https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

[62] NPSA website, Learning and Resources, Insider Risk Mitigation digital learning, Module 9 – Online Personnel Security, https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

[63] NPSA website, Learning and Resources, Insider Risk Mitigation digital learning, Module 9 – Online Personnel Security, https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

11.12 A Home Office Security officer told inspectors that social media was an increasing risk and that members of staff had been approached via LinkedIn by journalists pretending to want passports. Although the Home Office guidance advised against posting employment details on social media, a union representative told inspectors that senior managers had LinkedIn profiles containing details of their employment while lower grades were "penalised" and commented that: "You have to be consistent."

11.13 Inspectors heard that there were also concerns about the reputational risk to Border Force of staff using social media. The Home Office Social Media and Online Behaviours Policy states: "Staff are expected to conduct themselves online as they would in the workplace." However, a Border Force senior leader provided anecdotal evidence of an officer who had been posting inappropriate content onto a social media subscription site.

WhatsApp and other group messaging applications

11.14 There has been recent publicity over the use of instant messaging application WhatsApp by police officers and firefighters to share inappropriate material, leading to concerns over a culture of misogyny and racism in both organisations.[64, 65, 66] Home Office senior leaders told inspectors that the use of social media (including WhatsApp) was also an emerging issue in Border Force.

11.15 A Border Force senior leader told inspectors that they knew of "at least two" investigations involving staff sharing inappropriate material on WhatsApp groups but said that the groups tended to come to light as the result of something else being investigated. An ex-police officer was suspended from his role in Border Force in October 2022 due to racist messages shared in a WhatsApp group with former police colleagues.[67]

11.16 Again, staff awareness of policies was inconsistent. While one Border Force officer in a focus group told inspectors that WhatsApp groups of over three or four people had to be declared to managers, managers in another focus group were unaware of this policy.

11.17 A Home Office senior leader highlighted the need for a clear policy around the use of WhatsApp: "There is a genuine fear amongst staff. How do they draw a line between their private life and being a Border Force officer? It is fudged and they don't know where they stand."

Engagement with partners

11.18 Inspectors learned that the Home Office, including Border Force, works with NPSA and the National Cyber Security Centre (NCSC) at a strategic and operational level and they also sit on the departmental Cyber Security Committee.

11.19 A stakeholder told inspectors that NPSA had provided a lot of briefings and advice to Border Force over the previous few years. While Border Force were very receptive, NPSA had a

[64] WhatsApp is an instant messaging service that allows users to send text and voice messages, make voice and video calls, and share images, documents, user locations, and other content.

[65] The Guardian, "Met officers joked about raping women, police watchdog reveals," (published 1 February 2022), https://www.theguardian.com/uk-news/2022/feb/01/met-officers-joked-raping-women-police-watchdog-racist

[66] Manchester Evening News, "Revealed: The number of Greater Manchester firefighters under investigation for gross misconduct and sexual allegations," (published 27 February 2023), https://www.manchestereveningnews.co.uk/news/greater-manchester-news/revealed-number-greater-manchester-firefighters-26342234

[67] www.DailyMail.co.uk 6 October 2022 Home Office suspends ex-Met Police cop Rob Lewis over racist WhatsApp group chat | Daily Mail Online

sense of “Groundhog Day”, in that they were having the same conversations each time with little progress.

11.20 A Home Office senior leader thought that there was a gap in knowledge and that a working group was needed which included Border Force, Home Office Security, DDaT, and representatives from Human Resources across the Home Office directorates, “to triangulate different elements of data” to better inform the insider threat picture relating to online security.

Mitigations for online security risks

11.21 A Border Force officer said that the Home Office was updating its Social Media and Online Behaviours Policy and that Border Force staff were on the panel that would agree the updates. They commented that Border Force wanted something “stronger” than the current policy.

11.22 Home Office staff, including those employed by Border Force, are required to complete a mandatory Civil Service Security and Data Protection e-learning course, including modules on data protection and cyber security. Another senior leader described how corporate-level policies, protective monitoring, access management, and several technical controls were in place to mitigate against cyber security risks. They also highlighted awareness campaigns, information on the intranet, and some face-to-face training. However, they considered that there was not enough role-specific cyber security training. In mitigation, the Home Office was due to launch a new cyber security culture awareness and behaviour programme over the following two or three months, moving away from mandatory annual training, towards role-specific training.

11.23 In Dover, a senior leader told inspectors that training on social media was included in induction courses for new staff and was discussed on Higher Officer awareness sessions with the People Protection Risk Team (PPRT). Inspectors noted that there was a good level of awareness of the risks of social media among the Border Force officers they spoke to in Dover, despite the confusion over policy.

Summary

11.24 Inspectors concluded that mitigations have been put in place to reduce the risk of intentional and unintentional insider threat relating to online security, which goes some way to following NPSA advice around mitigating the risks posed by digital technology. Additionally, security measures have been introduced to prevent unauthorised sharing of information and the introduction of malware to Home Office systems.

11.25 However, while there was evidence of effective practice in raising awareness of online security risks, and proactive measures such as email scam tests, risks have not yet been fully mitigated. Inspectors acknowledged the plans for a new cyber security awareness and training programme, which should improve knowledge and reduce the risks of online insider harm to the security and reputation of Border Force.

11.26 Furthermore, strengthening the Social Media and Online Behaviours Policy, including providing guidance on the use of WhatsApp, should also bring more clarity and consistency for Border Force staff. However, the benefits of this will depend on the extent to which Border Force is able to secure wider Home Office agreement to its bespoke needs as a law enforcement agency.

11.27 Figure 22 summarises what inspectors consider to be working well and what requires further attention.

Figure 22: Online personnel security summary table

Working well	Further attention required
Mitigations against online threats and proactive initiative of email scam testing	Social media policy needs to be clear and consistent, with guidance relevant to operational Border Force staff
Plans for cyber security culture and awareness training due to be launched	WhatsApp policy required

12. Inspection findings: Ongoing personnel security

Figure 23: National Protective Security Authority (NPSA) guidance used by inspectors to consider Border Force's effectiveness in this area

Ongoing personnel security[68]
Develop and plan effective practices for countering the insider threat and maintaining a motivated, engaged, and productive workforce
While pre-employment screening helps ensure that an organisation recruits trustworthy individuals, people and their circumstances and attitudes change, either gradually or in response to events. The application of good ongoing personnel security principles adds huge value to physical and technical security measures in a cost-effective manner, promoting good leadership and management and maximising people as part of the security solution. The induction of new joiners is a key entry point at which their perception of security in the organisation is formed. This provides an opportunity to embed the desired security mind-set and behaviour in your employees from the outset, which is important in building and maintaining a good security culture. The point of exit is a significant stage in the employee lifecycle from a security perspective. There are a variety of reasons why an employee might be leaving an organisation and some of these reasons may give rise to a risk of confidentiality, integrity, and availability of critical assets being compromised. Therefore, it is important that effective exit and legacy controls are in place to detect and prevent any insider behaviours during the notice period and beyond.

Induction

12.1 Border Force's induction process is carried out at each local port, with a general checklist available for line managers to work through with the new employee. Several mandatory e-learning packages form part of the induction, these include:

- security and data protection
- health and safety
- counter fraud, bribery, and corruption

12.2 Insider threat awareness training is available via an internal course delivered by the Integrity and Projects Team. This course is not mandatory and does not form part of the induction process. A Border Force officer told inspectors the course will be made mandatory "this year"

[68] NPSA website, Advice and Guidance, Personnel and People Security, Insider Risk, Ongoing Personnel Security, https://www.npsa.gov.uk/ongoing-personnel-security accessed 24 April 2023.

but no specific date was provided. Integrity leads told inspectors, however, that some regions within Border Force have made the course mandatory for staff.

12.3 By February 2023, Border Force Insider Threat and Integrity Team (BF ITIT) had delivered Insider Threat awareness sessions to over 7,000 people (some of whom may have been repeat delegates) out of approximately 10,500 Border Force staff.[69] Through this training, Border Force had raised awareness of potential risks and vulnerabilities, and signposted staff to the People Protection Risk Team (PPRT), line managers, integrity leads, and reporting and referral channels. The team within Border Force responsible for providing the training told inspectors that following delivery of a session, there was often an influx of referrals and queries from participants to PPRT. Staff who had undertaken the course spoke highly of it. However, some staff who spoke to inspectors were unaware of its existence.

12.4 NPSA advises making "the security messages at induction meaningful and relevant, focusing on the first 12 months of the employee lifecycle".[70] However, a Border Force senior leader told inspectors that new recruits no longer had to sign the Officials Secrets Act on their induction course and therefore may not understand the security culture of the organisation. Border Force officers commented that there was a lack of "respect" for the role among new recruits and that the lack of being bound by the Official Secrets Act had "lost its gravitas".

12.5 The need to make the security measures relevant and timely was emphasised by a Border Force senior leader. They provided an example of a Border Force officer on their first day in the job, walking into a Border Force building while recording a selfie video on their phone. The senior leader went on to describe the importance of making staff understand that as a law enforcement officer, they are a target.

12.6 Staff at Dover told inspectors that recent recruitment campaigns had led to a large intake of new recruits within International Trade at Dover. A senior leader described that the team "effectively went from 40 to 400 overnight". Due to the rapid expansion of staff, an inexperienced management structure was trying to understand a new area of work while dealing with multiple disciplinary cases. Border Force Operational Assurance Directorate worked with local managers to "upskill and raise awareness" of insider threat. As a result of the increased awareness and focus on security messaging in the local area, staff at Dover felt that they were now "ahead" in mitigating the risk of insider threat activity.

Exit procedures

12.7 How an individual exits an organisation is important. Border Force determines whether the employee is leaving Border Force on good terms through an optional exit questionnaire. The process, which is confidential, is completed via Metis with a link to undertake the survey sent to an employee within 28 days before they leave.[71] Guidance on Metis states: "We use your anonymous feedback as quantitative evidence to help improve our attraction, retention and progression strategies."

12.8 Like Human Resources data, information relating to how an employee feels at the point they leave Border Force could potentially be useful in assessing insider risk, particularly any evidence

[69] Approximately 7,000 staff from circa 9,000 total staff.

[70] NPSA website, Learning and Resources, NPSA Insider Risk Mitigation digital learning, Module 6 – Ongoing Personnel Security, https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

[71] Metis is the Home Office Human Resources system.

in relation to disaffection, highlighted by the NPSA 'Insider Data Collection Study' as a key element of many insider cases.[72]

12.9 Border Force line managers told inspectors an exit 'tick-box' checklist was available to guide the manager through the actions that needed completing. Other mitigations which could increase understanding of an employee's experience of working for Border Force are not in place. These could include an exit interview with senior leaders or a mandated de-brief from a line manager. Mitigations that could possibly improve the terms on which someone leaves Border Force could include a certificate of service or a thank you message.

12.10 Cancelling of IT access upon departure is not an automatic process. Managers must identify which systems the employee has access to and request these access rights are revoked. Access to buildings should be revoked as security and building passes are returned; however, if buildings can be entered without the need for a pass, using for example a combination code, then different measures would need to be taken.

12.11 A Border Force officer told inspectors that there is currently no operational assurance of exit procedures, explaining "it doesn't seem to have been an issue that we have come across". The exit checklist is reliant on managers' knowledge of the systems a member of staff had access to, the building access they had, the uniform and equipment they had been issued during their employment, and is reliant on management discussions with the employee and any local records held.

Summary

12.12 In contrast to NPSA advice, current induction and exit procedures appear largely administrative and location specific. There is no central Border Force policy to include insider threat training during induction, and so local variations exist. Exit procedures lack person-to-person interaction that might allow Border Force to take more account of human factors. An absence of focus on the link to insider threat in both the induction and exit procedures is a missed opportunity to embed critical security messages with staff and build and maintain a good security culture. Incidents at Dover highlighted the need to focus these messages during the first 12 months of the employee lifecycle and highlight the potential consequences when this doesn't happen.

12.13 Border Force Operational Assurance Directorate does not currently assure exit procedures, which are delivered locally at each port. The reasons why an employee might be leaving Border Force do not appear to be being captured routinely. Additionally, access to critical IT and physical assets are not easy for managers to restrict when an employee leaves Border Force's employment. Having more robust processes in place would allow Border Force to prevent any insider behaviours during the notice period and beyond.

12.14 Figure 24 summarises what inspectors consider to be working well and what requires further attention.

[72] NPSA website, Learning and Resources, NPSA Insider Risk Mitigation digital learning, Module 1 – Resources, NPSA Data Collection Study, (published April 2013), insider-data-collection-study-report-of-main-findings.pdf (npsa.gov.uk)

Figure 24: Ongoing personnel security summary table

Working well	Further attention required
Border Force insider threat awareness training well received by staff, delivered to over 7,000 staff as of January 2023	Border Force insider threat awareness training is not mandatory
	Border Force not assuring exit procedures
	Exit procedures are focused on the administrative process and are not targeted to identify any disaffection

Annex A: Role and remit of the Independent Chief Inspector

The role of the Independent Chief Inspector of Borders and Immigration (until 2012, the Chief Inspector of the UK Border Agency) was established by the UK Borders Act 2007. Sections 48-56 of the UK Borders Act 2007 (as amended) provide the legislative framework for the inspection of the efficiency and effectiveness of the performance of functions relating to immigration, asylum, nationality and customs by the Home Secretary and by any person exercising such functions on her behalf. The legislation empowers the Independent Chief Inspector to monitor, report on and make recommendations about all such functions and in particular:

- consistency of approach
- the practice and performance of listed persons compared to other persons doing similar activities
- the procedure in making decisions
- the treatment of claimants and applicants
- certification under section 94 of the Nationality, Immigration and Asylum Act 2002 (c. 41) (unfounded claim)
- the law about discrimination in the exercise of functions, including reliance on paragraph 17 of Schedule 3 to the Equality Act 2010" (exception for immigration functions)
- the procedure in relation to the exercise of enforcement powers (including powers of arrest, entry, search and seizure)
- practice and procedure in relation to the prevention, detection and investigation of offences
- the procedure in relation to the conduct of criminal proceedings
- whether customs functions have been appropriately exercised by the Secretary of State and the Director of Border Revenue
- the provision of information
- the handling of complaints; and
- the content of information about conditions in countries outside the United Kingdom, which the Secretary of State compiles and makes available, for purposes connected with immigration and asylum, to immigration officers and other officials.

In addition, the legislation enables the Secretary of State to request the Independent Chief Inspector to report to her in writing in relation to specified matters.

The legislation requires the Independent Chief Inspector to report in writing to the Secretary of State. The Secretary of State lays all reports before Parliament, which she has committed to do within eight weeks of receipt, subject to both Houses of Parliament being in session.

Reports are published in full except for any material that the Secretary of State determines it is undesirable to publish for reasons of national security or where publication might jeopardise an individual's safety, in which case the legislation permits the Secretary of State to omit the relevant passages from the published report.

As soon as a report has been laid in Parliament, it is published on the Inspectorate's website, together with the Home Office's response to the report and recommendations.

Annex B: ICIBI ‘expectations’

Background and explanatory documents are easy to understand and use (e.g. statements of intent (both ministerial and managerial), impact assessments, legislation, policies, guidance, instructions, strategies, business plans, intranet and GOV.UK pages, posters, leaflets etc.)

- They are written in plain, unambiguous English (with foreign language versions available, where appropriate)
- They are kept up to date
- They are readily accessible to anyone who needs to rely on them (with online signposting and links, wherever possible)

Processes are simple to follow and transparent

- They are IT-enabled and include input formatting to prevent users from making data entry errors
- Mandatory requirements, including the nature and extent of evidence required to support applications and claims, are clearly defined
- The potential for blockages and delays is designed out, wherever possible
- They are resourced to meet time and quality standards (including legal requirements, Service Level Agreements, published targets)

Anyone exercising an immigration, asylum, nationality or customs function on behalf of the Home Secretary is fully competent

- Individuals understand their role, responsibilities, accountabilities and powers
- Everyone receives the training they need for their current role and for their professional development, plus regular feedback on their performance
- Individuals and teams have the tools, support and leadership they need to perform efficiently, effectively and lawfully
- Everyone is making full use of their powers and capabilities, including to prevent, detect, investigate and, where appropriate, prosecute offences
- The workplace culture ensures that individuals feel able to raise concerns and issues without fear of the consequences

Decisions and actions are ‘right first time’

- They are demonstrably evidence-based or, where appropriate, intelligence-led
- They are made in accordance with relevant legislation and guidance
- They are reasonable (in light of the available evidence) and consistent
- They are recorded and communicated accurately, in the required format and detail, and can be readily retrieved (with due regard to data protection requirements)

Errors are identified, acknowledged and promptly ‘put right’

- Safeguards, management oversight, and quality assurance measures are in place, are tested and are seen to be effective
- Complaints are handled efficiently, effectively and consistently
- Lessons are learned and shared, including from administrative reviews and litigation
- There is a commitment to continuous improvement, including by the prompt implementation of recommendations from reviews, inspections and audits

Each immigration, asylum, nationality or customs function has a Home Office (Borders, Immigration and Citizenship System) ‘owner’

BICS ‘owner’ is accountable for

- implementation of relevant policies and processes
- performance (informed by routine collection and analysis of Management Information (MI) and data, and monitoring of agreed targets/deliverables/budgets)
- resourcing (including workforce planning and capability development, including knowledge and information management)
- managing risks (including maintaining a Risk Register)
- communications, collaborations and deconfliction within the Home Office, with other government departments and agencies, and other affected bodies
- effective monitoring and management of relevant contracted out services
- stakeholder engagement (including customers, applicants, claimants and their representatives)

Annex C: Glossary

Glossary	
ACCIU	Anti-Corruption Criminal Investigation Unit
AO	Assistant Officer
ASC	Additional security check
BFITIC	Border Force Insider Threat and Integrity Committee
BF ITIT	Border Force Insider Threat and Integrity Team
BF OAD	Border Force Operational Assurance Directorate
[Redacted]	[Redacted]
COP	Central Operating Platform
CPNI	Centre for the Protection of National Infrastructure
CTC	Counter Terrorism Check
DAT	Drug and Alcohol Testing
DDaT	Digital, Data and Technology
DV	Developed vetting
EO	Executive Officer
GRS	Government Recruitment Service
HMRC	His Majesty's Revenue and Excise
HORC	Home Office Resourcing Centre
HR	Human Resources
IOPC	Independent Office for Police Conduct
IVA	Individual voluntary arrangement
JACIT	Joint Anti-Corruption Intelligence Team
LEA	Law enforcement agency
MOJ	Ministry of Justice
MoRiLE	Management of Risk in Law Enforcement
NCA	National Crime Agency
NPCC	National Police Chiefs' Council
NPSA	National Protective Security Authority
PNC	Police National Computer

Glossary	
PND	Police National Database
PPRT	People Protection Risk Team
PSU	Professional Standards Unit
[Redacted]	[Redacted]
SC	Security check
SEO	Senior Executive Officer
SIP	Single Intelligence Platform
SSB	Senior Strategy Board
SSG	Strategic Security Group

Acknowledgements

The inspection team is grateful to the Home Office for its co-operation and assistance during this inspection and for the contributions from the staff who participated. We are also grateful to the stakeholders who contributed.

Inspection team members

Inspection Oversight:	Dan Cartwright
Lead Inspector:	Rachael Wood
Project Manager:	Louise Milligan
Inspector:	Peter Brown
Inspector:	Philip Hallwood

978-1-5286-4393-1
E02956811