HMICFRS

His Majesty's Inspectorate of Constabulary and Fire & Rescue Services

National Crime Agency inspection

An inspection of the effectiveness and efficiency of the National Data Exploitation Capability

Contents

Summary

The National Crime Agency (NCA) is the UK's lead agency in the fight against serious and organised crime (SOC). In 2018, the NCA formed its National Data Exploitation Capability (NDEC) as a five-year programme. The NDEC's purpose is to help the NCA respond to SOC by analysing or exploiting bulk datasets.

During this inspection, we couldn't establish the final cost of the NDEC programme, having received contradictory evidence in documents and interviews. However, the NDEC team told us the final cost of the programme was about £92 million.

At the time of our inspection, the NCA hadn't authorised the NDEC's annual budget for the financial year 2024/25.

Our inspection considered:

- how valuable the NDEC's contribution to the NCA is, and how well the NCA uses it;
- whether the NDEC makes effective use of the data it has access to;
- whether the NDEC has the technological capabilities and other resources to fulfil its role; and
- how efficiently and effectively the NCA co-ordinates and prioritises the NDEC's work.

IT capability and resourcing

The NCA knows many of its IT systems need updating

For several years, the NCA has known that many of the IT systems it relies on are outdated and unfit for purpose. The NCA recognises and understands the problems these legacy IT systems present.

A lack of investment in IT infrastructure means the NCA is burdened with technical debt – that is, the increasing cost of replacing outdated systems when fast solutions have been prioritised over long-term solutions.

The NCA has also been slow to fully embrace the benefits of cloud-based technology, which has adverse practical consequences. For example, personnel can't automatically transfer data between computer systems operating on each of the three security tiers of the Government Security Classifications Policy. This is a significant limitation, given the sensitivity of some of the material the NCA routinely handles.

The NCA should improve its access to and management of bulk datasets

At the time of our inspection, the NDEC had access to a number of bulk datasets which form its data catalogue. The NCA's use of bulk datasets is controlled by a data access panel, chaired by the NCA's chief data officer. The NCA's processes mean its use of any bulk datasets must be authorised by the panel.

However, we believe that there are some obvious SOC-related datasets omitted from the data catalogue. For example, the catalogue contained no datasets from the nine regional organised crime units (ROCUs). We were also told that there were no plans to allow the NCA to routinely carry out bulk analysis of data held by the Law Enforcement Data Service (LEDS) which is due to replace the Police National Computer in 2026. We were also concerned to find that the NCA doesn't have an effective system of version control for the datasets in use across the organisation. This means there is potential for flawed data analysis and use in operational decision-making.

The NCA should establish a more rigorous approach to data management. This is especially important for the datasets the NDEC includes in its data catalogue.

We received inconsistent information about staffing levels

We found confusion among NDEC personnel, including leaders, about the approved staffing levels for the NDEC, with the NCA giving us inconsistent and contradictory information. In interviews, managers highlighted a lack of personnel as one of the major problems for the NDEC.

Five previous NCA reviews of the NDEC have identified resourcing as a problem needing urgent attention. None of these reviews have led to a clear action plan to resolve this issue.

Any future NCA resourcing plan for the NDEC should adopt the Government Digital and Data Profession Capability Framework to bring it into line with relevant technical units in other government departments.

The NDEC should improve the way it works with partner organisations

The NDEC acknowledged to us that it hadn't fully achieved its plans for formal partnership working with industry, academia, and other government departments and law enforcement agencies. We found that the partnerships that were in place had developed through personnel from each organisation knowing each other already or from having worked together on operations. There was a lack of structured engagement with other organisations also working in the fields of data science and data exploitation.

There was an absence of well-established arrangements with all ROCUs, and other government departments and agencies.

NDEC personnel understand the relevant frameworks relating to ethics and standards

The NCA publicises its data protection policies on its intranet. We found that NDEC personnel understood the legislation governing their work and were knowledgeable about the processes in place to report data breaches.

The NCA has no powers under the Investigatory Powers Act 2016 in relation to personal and communications data. This means that it isn't subject to the regulatory regime required by the Act, and independent oversight of its use of that data isn't required by statute. In 2020, at the NCA's invitation, the Information Commissioner's Office carried out a consensual audit of the NDEC's data-handling processes. The audit concluded that the NDEC's processes "mirrored" requirements contained in the Investigatory Powers Act 2016 and its Code of Practice.

We were encouraged by the NCA's decision to request an audit, despite it being under no statutory obligation to do so. However, auditing the NDEC's processes shouldn't be wholly reliant on the NCA's willingness to give consent. A more systematic, robust arrangement would be preferable.

Progress against objectives

The NDEC's initial business case (unpublished) refers to nine deliverables, or objectives, it should achieve during its first five years. The business case contains a list of areas in which investment was needed for the NDEC to be successful.

Regrettably, the NDEC's recording and understanding of these objectives was confusing and inconsistent. We couldn't identify a single, authoritative document that defined the intended outcome, progress or timeline for completing each objective. In our view, some of the objectives overlapped, or weren't suitable for the NDEC to achieve.

However, we consider that the NDEC has achieved, or partially achieved, six of the original nine objectives.

During its five-year existence, the NDEC has been the subject of at least five unpublished internal reviews. None have led to any documented management intervention. In addition, these reviews fell well short of being comprehensive, insightful evaluations of the quality, importance or value of the NDEC's work.

Governance, management and performance

The NDEC didn't record or assess performance well enough

NDEC personnel at all levels told us that the NDEC didn't record or assess its performance effectively. About six months before our inspection, and at least four years after the NDEC's inception, senior leaders put in place a process for recording performance data. This allowed analysts to show some of the tangible benefits the NDEC brings to the NCA.

NDEC personnel need a better understanding of the work allocation system

The NDEC has an official process for allocating work to personnel. However, we found that some were unaware of this, instead using an unofficial process, which they referred to as "back-door".

In the six months before our inspection, the NCA had introduced a new work-tracking system. This should improve how well the NDEC can manage and monitor its demand. It is much needed.

The value of the NDEC

One of our terms of reference required us to consider: "How valuable is the NDEC's contribution and how effectively does the NCA use it?"

For the reasons explained above, we conclude that its potential remains unfulfilled.

Recommendations and areas for improvement

We make nine recommendations and we have identified one area for improvement.

Recommendation 1

By 30 September 2025, the National Crime Agency, working with the Home Office, should make sure its ten-year IT strategy includes a timeline, indicative budget and priority order for removing, replacing, developing or merging its legacy IT systems.

Recommendation 2

By 30 September 2025, the National Crime Agency, working with the Home Office, should develop a plan, including a timeline, to allow it to automatically move information between the three tiers of government security classification.

Recommendation 3

By 30 June 2025, the National Crime Agency should review the National Data Exploitation Capability data catalogue and identify other datasets suitable for inclusion. As soon as reasonably possible, it should add those datasets to the catalogue.

Recommendation 4

By 30 June 2025, the National Crime Agency, working with the Home Office, should develop a plan, including a timeline, to allow it to routinely carry out bulk data analysis of the Law Enforcement Data Service dataset.

Recommendation 5

By 30 March 2026, the National Crime Agency should make sure that:

- the datasets in use across the National Crime Agency are correctly version controlled; and
- the National Data Exploitation Capability establishes a data management policy to provide a consistent methodology, and a single structure and pathway for all the datasets it imports.

Recommendation 6

By 30 June 2025, the National Crime Agency should adopt the Government Digital and Data Profession Capability Framework.

Recommendation 7

By 30 June 2025, the National Crime Agency should establish partnership arrangements with relevant bodies. These should include:

- all regional organised crime units;
- police forces that face major challenges in tackling serious and organised crime; and
- other government departments and agencies.

Recommendation 8

By 30 June 2025, the Home Office should secure a systematic, robust arrangement (which may require legislation) for regular audits of the National Crime Agency's use of bulk personal datasets. This should include:

- retention
- disclosure
- security
- destruction.

Recommendation 9

By 30 June 2025, the National Crime Agency should establish a programme of consensual audit by the Information Commissioner's Office, as permitted by section 129 of the Data Protection Act 2018. These audits should meet the requirements of section 229 of the Investigatory Powers Act 2016 and its Code of Practice.

Area for improvement

The National Crime Agency should introduce changes to its training, performance and recruitment processes for the National Data Exploitation Capability.

Introduction

About us

His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) independently assesses the effectiveness and efficiency of police forces, fire and rescue services, and some other law enforcement agencies, to make communities safer. In preparing our reports, we ask the questions the public would ask. We use our expertise to interpret the evidence and make recommendations for improvement.

Section 11 of the Crime and Courts Act 2013 requires us to inspect the National Crime Agency (NCA). Following an inspection, we must report to the Home Secretary on the NCA's efficiency and effectiveness.

Paragraph 3 of Schedule 6 to the Crime and Courts Act 2013 requires the Home Secretary to arrange for every HMICFRS report commissioned under the Act to be published in a manner they consider appropriate.

The legislation also allows any part of the relevant report to be excluded from publication if it:

- would be against the interests of national security;
- could prejudice how crime is prevented or detected, how offenders are apprehended or how offences are prosecuted; or
- might jeopardise the safety of any person.

In February 2025, we gave the Home Secretary our report on the inspection of the NDEC. That report included detail of operational matters that weren't suitable for the public domain. As a result, and in consultation and agreement with the NCA and the Home Office, we have prepared this version of the report with the relevant operational matters excluded. The Home Secretary subsequently asked us to publish this version of the report.

About the NCA and the National Data Exploitation Capability

The NCA is responsible for leading, supporting and co-ordinating the approach to serious and organised crime (SOC). It has several statutory functions, explained in section 1 of the Crime and Courts Act 2013.

The NCA supports police forces, government departments and other law enforcement agencies. This support can come from various parts of the NCA, including its intelligence and investigations directorates.

The National Data Exploitation Capability is part of the NCA's intelligence directorate

The National Data Exploitation Capability (NDEC) is part of the NCA's intelligence directorate. It was formed in 2018 as a five-year programme. The programme was jointly funded by the Home Office, the NCA, the Economic Crime Levy, which is managed by His Majesty's Treasury, and Project Invigor.

We couldn't establish the final cost of the NDEC programme, having received contradictory evidence in documents and interviews. The NCA gave us further figures after our fieldwork had ended which contradicted the financial data the NCA had previously given us. As a result, we haven't been able to determine their accuracy. However, the NDEC team told us the final cost of the programme was about £92 million.

At the time of our inspection, the NCA hadn't determined the NDEC's budget for 2024/25. However, we understand that in April 2024, the NDEC submitted a funding request to the NCA for £22 million.

The NDEC's purpose is help the NCA address SOC by analysing or exploiting bulk datasets. The NDEC does this to support intelligence-led operations. It works alongside the NCA's National Assessment Centre and National Targeting Centre.

The NDEC includes the following teams:

- **Data and analysis operations team** – this team is responsible for carrying out the NDEC's bulk data exploitation work. It is made up of analytical and intelligence personnel.
- **Data acquisition and management office** – this team is responsible for working with other organisations holding datasets that may be of use to the NDEC. Personnel in the data acquisition and management office are also responsible for maintaining the NDEC's data catalogue. This is the collection of all the datasets the NDEC has access to.
- **Datalab** – this team is responsible for developing new data exploitation techniques and services. This includes creating new productivity software, which the NDEC calls "production tools". These tools make creating, editing, viewing and processing information easier, helping to increase efficiency. They are created by data scientists and engineers.

Terms of reference

We addressed the following questions:

- How valuable is the NDEC's contribution and how effectively does the NCA use it?
- Does the NDEC make effective use of all the data it may lawfully access?
- Does the NDEC have all the technological capabilities and other resources it needs, now and for the foreseeable future?
- How efficiently and effectively does the NCA co-ordinate and prioritise the NDEC's work?

Methodology

Our inspection took place in January and February 2024. We visited NCA offices and spoke to personnel in the teams relevant to this inspection and carried out reality testing. We also carried out interviews in partner organisations.

We went to NCA premises to view case material and examine data. While we were there, the NCA gave us briefings about investigations involving sensitive techniques.

We carried out:

- a case file review, in which we examined nine case files;
- a review of other case-related material, such as presentations;
- interviews and focus groups with NDEC and other NCA personnel;
- interviews and focus groups with representatives of partner organisations, such as the Cabinet Office, Merseyside Organised Crime Partnership, and the National Police Chiefs' Council's Tackling Organised Exploitation team; and
- a review of the NDEC's development against its initial objectives and subsequent reviews.

Explanations

To help readers understand concepts and terminology in this report, we have included this explanatory section.

Bulk personal and communications datasets

Bulk personal datasets are collections of personal information about a large number of people, most of whom will be of no interest to the NCA. Many organisations across the public and private sectors hold datasets such as this. Examples of these datasets include the electoral roll, telephone directories and travel-related data.

Bulk communications datasets are collections of information about the use of communication systems, such as mobile phone networks. Commercial organisations known as communication service providers hold datasets such as this. Examples of these datasets include extensive information showing when, where and by whom the service was used. Importantly, these datasets don't include the contents of communication, such as what was said or written.

Legislation

The NCA doesn't have powers under the Investigatory Powers Act 2016 to access bulk personal and communications datasets. Instead, the NCA relies on section 7 of the Crime and Courts Act 2013 (the Act) to facilitate access to this data.

The Act allows the NCA to apply to the owner of a specific bulk dataset, such as a government department. Once the owner has received that application, unless there is a legal restriction, it can share that dataset with the NCA.

Analysis of bulk datasets

Bulk datasets are essential in helping the NCA identify lines of enquiry or individuals who surface during the course of an investigation. Analysis or exploitation of the datasets, combined with other intelligence the NCA obtains, helps to establish links between individuals and groups. It helps the NCA understand a person's behaviour and connections, and to quickly exclude anyone who isn't of investigative interest. Bulk datasets help the NCA focus on individuals involved in SOC or organised crime groups.

IT capability and resourcing

This chapter includes our observations on:

- the National Crime Agency's (NCA) IT capability and its consequences for the National Data Exploitation Capability (NDEC);
- the NDEC's access to and management of datasets;
- the NDEC's approved staffing levels and resources;
- training and accreditation of personnel;
- partnership arrangements; and
- the NDEC's approach to ethics and standards in the way it manages data.

Problems with the NCA's IT capability

For several years, the NCA has known that many of its IT systems are outdated and unfit for purpose. When the NCA was created in 2013, it inherited much of its IT capability from its predecessors, such as the National Crime Squad and the Serious Organised Crime Agency.

In 2015, we published 'An inspection of the National Crime Agency'. This was our first report on the (then newly formed) NCA. In that report we said:

> "The NCA faces very significant challenges concerning science and technology. As a result of a history of under-investment in technology […] the NCA has: poor connectivity between different information systems; a paucity of mobile computing capability; certain critical applications in a fragile state; and (because of the need to maintain especially high levels of information security) very limited internet connectivity. This all has a materially detrimental effect on the NCA's efficiency and effectiveness."

In the 11 years since its inception, the NCA has made only limited progress in dealing with these issues.

The NCA still relies on too many legacy systems

At the time of this inspection, the NCA was still using several of the legacy IT systems that its predecessors used. Many had outdated hardware or software, used obsolete programming languages and had limited flexibility.

While legacy systems may still operate and allow the organisation to carry out its work, they often pose the following challenges:

- higher maintenance costs;
- limited functionality, and incompatibility with other, more up-to-date IT systems;
- not being able to fully exploit datasets from other legacy systems; and
- increased training requirement for new personnel.

The NCA is burdened with technical debt

At the time of our inspection, the NCA had identified that it had 260 legacy IT systems. Each year, the NCA spends 80 percent of its IT budget on servicing its technical debt – that is, the increasing cost of replacing outdated systems when fast solutions have been prioritised over long-term solutions. The NCA rates technical debt as one of the highest risks on its corporate risk register. And its technical debt is growing.

The NCA recognises and understands the problems that its legacy systems present. In 2023, it produced a technical debt strategy (unpublished), stating:

> "The Agency holds a significant but not yet fully known technical debt position. From an IT management standpoint, this results in mounting costs, inflexibility to meet changing business needs and increased risk of service disruption through failure and/or cyber-attack."

We were pleased to see that the strategy contains a plan to resolve the technical debt problems we found during our inspection.

The NCA has recognised that it has been slow to fully embrace the benefits of cloud technology, as set out in the Government's Cloud First strategy. Some other government agencies that manage large amounts of sensitive information told us they have adopted cloud solutions. These may include using, where appropriate, hybrid or combinations of private and commercial cloud services.

The NCA has completed the first phase of its ten-year IT strategy

The NCA told us that in 2020, it began implementing a ten-year IT strategy to improve its technology. At the time of our inspection, the NCA had completed the first phase (at a cost of £250 million).

The second phase had begun, but it is subject to the Home Office's agreement to continue funding. The projected cost was estimated to be between £350 million and £500 million, depending on the accepted options.

We will scrutinise the NCA's IT strategy in a future inspection

As we have shown, our concerns regarding the NCA's IT capability are long-standing. And, although there have been some improvements since our initial report on the NCA in 2015, we remain concerned that the NCA hasn't made enough progress on this issue.

In early 2024, we consulted with the Home Office on a planned inspection of the effectiveness and efficiency of the NCA, due to take place in 2024/25. That consultation identified several priority areas for the forthcoming inspection. These included:

- how the NCA's capabilities match its needs; and
- opportunities to increase the NCA's productivity, efficiency and overall value for money.

When we carry out that inspection, we will scrutinise the NCA's ten-year IT strategy and its progress against it.

Recommendation 1

By 30 September 2025, the National Crime Agency, working with the Home Office, should make sure its ten-year IT strategy includes a timeline, indicative budget and priority order for removing, replacing, developing or merging its legacy IT systems.

The NCA's ageing IT systems create operational problems for the NDEC

The issues that we have highlighted above for the NCA also apply to the NDEC. It has the same basic IT provision and operating systems as the rest of the NCA. The NDEC's only bespoke capability comes from the production tools that the NDEC's personnel create.

The NCA has previously recognised the implications that ageing and outdated IT systems have for the NDEC. In 2019, an NCA review (unpublished) of the NDEC identified: "The current IT estate is considered to be inappropriate for data exploitation due to the aged data interrogation applications provided."

Outdated IT also limits the NDEC's use of modern web-based applications that take advantage of modern technologies. This includes those that provide greater visualisation of data for analysis. The lack of modern IT makes effective data exploitation challenging for the NDEC's personnel, who are using obsolete IT when trying to work on large volumes of data.

In addition, the NDEC's IT systems don't support effective oversight and audit. Later in this chapter, we report on the good ethical culture in the NDEC; we didn't find any specific matters of concern in this area. But there still needs to be effective oversight by senior leaders or independent auditors such as the Information Commissioner's Office (ICO). Use of more up-to-date IT systems would help make sure the NDEC accesses data legally and ethically.

The NCA has introduced IT monitoring software for its core systems

We have commented in other reports on the NCA's inability to audit the access its personnel have to its IT systems.

In our 2023 report 'Vetting and anti-corruption part 1: How effective is the National Crime Agency at dealing with corruption?', we said:

> "By 30 September 2023, the National Crime Agency should make sure that it has IT monitoring capability for all its systems, to effectively protect the information contained within its systems and help it to identify potentially corrupt officers and staff. In the meantime, by 31 December 2022, the National Crime Agency should have IT monitoring for its core systems."

The NCA has completed the second part of the recommendation. It has purchased the IT monitoring software and introduced monitoring on its core systems. But, due to compatibility problems, it can't monitor the other systems. Introducing this process is important and the NCA is working to resolve this problem. It needs to make sure it achieves this, so that the NCA uses data legally and ethically.

The NDEC's access to and management of datasets

The NDEC's IT capability is inextricably linked to its ability to efficiently exploit data. This includes how well it can manage information and data in accordance with its security classification.

The NCA can't automatically transfer data across the three security tiers

Government Security Classifications Policy provides an administrative system to protect information. The system uses three security classification tiers: OFFICIAL, SECRET and TOP SECRET.

At the time of our inspection, the NCA had access to three IT platforms, which corresponded with these tiers. This should make sure the NCA manages, shares and stores information on systems that are appropriate to its security level.

- **Tier one** – the majority of information that the public sector, including the NCA, uses and shares is classified as OFFICIAL.
- **Tier two** – this relates to sensitive information that requires enhanced protective controls. These include the use of secure IT networks. This classification is SECRET.

- **Tier three** – exceptionally sensitive information that usually relates to national security. This classification is TOP SECRET.

The NCA and the NDEC classify most of the information they manage as tier one. But the NDEC regularly gathers information from partners that falls in the tier two category, and sometimes tier three.

In addition, security classifications can change. Information or data originally classified as tier one may be reclassified at a higher tier once it has been analysed or aggregated with other information. Similarly, on some occasions, information or data may have its classification lowered.

In our 2016 report on the NCA's progress against outstanding recommendations, we said:

> "Although it invests in a Tier 2 network, the NCA estimates that between 80 percent and 90 percent of the data held on its network should, given its content, actually be treated as 'official-sensitive' (or Tier 1), thus rendering a Tier 2 network largely unnecessary."

Cybersecurity threats have increased since our 2016 inspection

Since our 2016 inspection, the cybersecurity threats that the NCA faces have increased. These include new threats from state actors and others intent on penetrating and disrupting the NCA's networks. The need to protect the NCA's information means that more information needs to be held at the tier two level. Although most of the NCA's applications operate at the tier one level, the NCA estimates that at least 80 percent of its personnel require regular access to the tier two level.

As a result, it is vital that the NCA has an efficient and secure means of transferring data between computer systems operating on each of the three security tiers. This is an important capability, given the sensitivity of some of the data that the NCA routinely handles.

Regrettably, at the time of our inspection, the NCA's only way of transferring classified information from tier to tier was a manual one. And, although this problem adversely affected the entire NCA, its effect on the NDEC was magnified due to the technical nature of its work.

The NDEC has created an interim IT system for managing tier two information

In 2022, when an anticipated NCA-wide platform for managing tier two information didn't materialise, NDEC personnel created an interim IT system. The NDEC subsequently adopted that system in all its relevant departments.

We acknowledge the work and innovation of the NDEC personnel who developed the interim system. They dealt with a problem that the NCA and the Home Office had been aware of for several years. An NCA senior leader described the interim system as “groundbreaking”. For tier two information, the interim solution provides useful functionality. But, at the time of our inspection, the NCA still didn’t have an automated electronic means of transferring information across the three tiers.

Several personnel we spoke to were clear that the development of corporate IT systems shouldn’t have been the NDEC’s responsibility. They were also concerned that developing the interim system had distracted personnel from the NDEC’s core function. At time of our inspection, the NCA told us it was developing a corporate tier two system.

Recommendation 2

By 30 September 2025, the National Crime Agency, working with the Home Office, should develop a plan, including a timeline, to allow it to automatically move information between the three tiers of government security classification.

Creating the NDEC has helped the NCA increase the size of its data catalogue

In 2015, in our first report on the NCA, we stated: “Access to databases held by the police, law enforcement bodies and government departments should be improved.”

Creating the NDEC has helped the NCA make this improvement.

Personnel in the NDEC told us that, since 2018, it had acquired access to a number of datasets. The NDEC refers to these datasets as its data catalogue. During this inspection, we examined a list of the datasets. They are a combination of datasets that the NDEC either has direct access to, such as NCA-owned datasets, or those that it has indirect access to, such as datasets owned by other organisations.

In some cases, the NCA has real-time access to datasets. In others, access is limited to part of a dataset, for example a downloaded copy or cut, usually containing data that represents a snapshot in time.

The NDEC has several processes for accessing bulk datasets

We found that the NDEC had several processes to prevent it carrying out unnecessary applications for access to bulk datasets.

These included a pre-application process, which helps the NDEC establish success criteria or performance indicators for acquiring each dataset. This process considers the benefits of acquiring access to a particular dataset, and whether doing so represents value for money. The NDEC also considers the potential threat, risk and harm presented by the subject of the relevant investigation. It follows up the

pre-application process with a request for authorisation by the data authorisation panel (DAP).

The DAP is chaired by the NCA's chief data officer, supported by a legal advisor. The panel's role is to consider the legality, necessity and proportionality of each request for bulk data. By doing so, the panel controls the NCA's use of bulk datasets contained within its data catalogue.

In 2020, the ICO carried out an audit of the NDEC. In its unpublished report, the ICO stated: "The DAP is providing adequate protective monitoring and oversight."

The NCA gave us brief descriptions of what each of the datasets contained. Based on these descriptions, the NDEC's access to datasets appeared proportionate and appropriate. The DAP process allows it to apply for access to further datasets and to add to the data catalogue from time to time.

In our view, there were some obvious limitations in the way the NDEC identified relevant datasets, leading to potential omissions in the catalogue.

The NDEC's function is reactive, not proactive

With few exceptions, a dataset is included in the catalogue because of the NDEC's task-led approach. Usually, investigators elsewhere in the NCA ask the NDEC to carry out bulk data analysis for a specific investigation.

In these cases, the NDEC has a valuable function. However, it is inherently reactive rather than proactive, missing opportunities to identify other potential sources of intelligence from bulk data.

To some extent, the NCA had recognised this. We were told that the NDEC managers had asked personnel for suggestions of datasets that should be considered by the DAP. But this fell short of a comprehensive and structured approach to identifying other bulk datasets that may potentially add to the NCA's understanding of serious and organised crime (SOC).

The NDEC should make sure it has access to a wider range of datasets

In the list of datasets relating to UK policing, none were from the nine ROCUs or forces with particular challenges in relation to tackling SOC. This concerns us; we have highlighted this lack of connectivity before, in several other inspection reports.

There are other bodies which, to varying degrees, deal with SOC. This criminality is multi-faceted, and the groups involved can be skilled at carrying out SOC in multiple forms. We can't say for certain what any analysis of these bulk datasets would show. But we were left unconvinced that the NDEC had sufficiently considered the matter or had plans to do so.

We encourage the NCA to be more imaginative in its approach to identifying bulk datasets for consideration. It should involve, but not solely rely on, the NDEC teams.

Recommendation 3

By 30 June 2025, the National Crime Agency should review the National Data Exploitation Capability data catalogue and identify other datasets suitable for inclusion. As soon as reasonably possible, it should add those datasets to the catalogue.

Some important datasets weren't configured for bulk exploitation

Irrespective of the NDEC's own IT limitations, there are some datasets that it can't access in bulk because of the way they have been configured. The Police National Computer, the Police National Database, and the tax dataset belonging to HMRC are examples of this. Each of these systems were designed for individual checks, not for exploiting bulk data.

These are major limitations, particularly in the case of the Police National Database. The Police National Computer is due to be decommissioned in 2026 and replaced by the Law Enforcement Data Service (LEDS). At the time of our inspection, we were told that NDEC access to bulk data in the LEDS system wouldn't be within the scope of the LEDS implementation process until at least 2026. We strongly encourage the NCA to liaise with the LEDS programme team now, to secure future access to the LEDS dataset, including bulk provision for the NDEC.

Recommendation 4

By 30 June 2025, the National Crime Agency, working with the Home Office, should develop a plan, including a timeline, to allow it to routinely carry out bulk data analysis of the Law Enforcement Data Service datasets.

We found poor version control of datasets

We were concerned to find that the NCA doesn't have full oversight of all the datasets it uses. This means other departments in the NCA have different versions of the datasets held by the NDEC.

Each version may contain discrepancies or different information. They may also have been constructed differently. This results in datasets which look similar, but provide different analytical results. Simply put, there is often no single version of the truth. Although we didn't find any specific examples, there is potential for flawed data analysis being used in operational decision-making.

The dataset versions held by the NDEC in its catalogue should be the stable version – that is, the primary and updated version – held on behalf of the NCA. This would make sure data being analysed stays consistent and dependable over time.

We found that, even within the NDEC, different structures and pathways were used when importing datasets from other agencies. This could be something as simple as the way in which individual names or dates of birth were ordered. We found that the import processes were inconsistent across the NDEC's data catalogue. This makes the analytical process unnecessarily complicated.

The NDEC should make sure it consistently uses common structures and pathways so it can analyse and exploit data more efficiently.

Recommendation 5

By 30 March 2026, the National Crime Agency should make sure that:

- the datasets in use across the National Crime Agency are correctly version controlled; and
- the National Data Exploitation Capability establishes a data management policy to provide a consistent methodology, and a single structure and pathway for all the datasets it imports.

The NDEC's approved staffing levels and resources

The NDEC's approved staffing levels are unclear

Since its creation in 2018, the NDEC has had problems recruiting and retaining personnel. We have highlighted this issue before. In our 2020 report 'An inspection of the National Crime Agency's criminal intelligence function', we said that recruitment and retention problems resulted in "specialist posts not being filled and associated problems".

Senior leaders in the NCA are well aware of this problem. At the time of our 2024 NDEC inspection, the NCA's corporate risk register included recruitment and retention of personnel as one of the top five risks that the NCA faced. We found confusion among personnel, including leaders, about the approved staffing levels for the NDEC.

During this inspection, the NCA gave us information, in interviews and in document form, relating to the NDEC's approved staffing levels. This information was inconsistent and contradictory. To follow are three examples of the numerous pieces of information the NCA gave us before and during our fieldwork:

1. In December 2023, before our inspection, the NCA told us that the confirmed staffing level for the NDEC was 140.5 posts and that 117.6 were filled. This represented a vacancy rate of about 16 percent.

2. During our fieldwork, the NCA gave us an NDEC document titled 'NDEC TOM [target operating model] Summary', dated June 2022. The document stated that "the original NDEC TOM expected NDEC to need 307 officers". The 2022 document reiterated that expectation. It also recognised that, at that time, the NDEC had approximately 100 vacancies – a 33 percent vacancy rate.
3. We asked for clarification on the actual levels of staffing across the NDEC, and the NCA gave us a spreadsheet. This detailed the vacancy rates across NDEC units. It showed the total number of posts as being 202. It also stated that the vacancy rate for the NDEC was 40 percent.

Regardless of these varying official figures, it was clear that personnel (including some at senior levels) believed that the expected staffing level for the NDEC remained 300 posts. They pointed to the lack of personnel as one of the NDEC's major problems. In doing so, they also said vacancy rates across the NDEC's units averaged 50 percent.

Personnel were clear that the failure to meet the anticipated workforce level had significantly reduced the NDEC's capacity and capability to meet demand. In our view, this is worsened by poor performance management in the NDEC, which we highlight in 'Governance, management and performance'.

We were told that personnel shortages were so severe that, at one stage, the NDEC senior leaders prevented personnel from making lateral moves to other departments in the NCA. We were also told that specialist personnel, recruited for specific reasons, were often deployed into roles that they felt didn't make the best use of their skills. Personnel told us this often caused dissatisfaction.

The NCA has reviewed the NDEC five times, but we found a lack of clarity on the NDEC's target staffing level

During its first five years, the NDEC has been reviewed by the NCA five times. We provide details of these reviews in 'The NCA's reviews of the NDEC programme'. But none of these reviews gave us any clarity on approved staffing levels.

As a result, we haven't been able to establish exactly how many personnel the NDEC should have and how that decision was reached. Specifically, we have been unable to determine:

- when the decision to reduce the target approved staffing level of the NDEC was taken;
- what, if any, information and data was used to support that decision;
- which, if any, objectives were discarded in light of that decision;
- where, if anywhere, that decision was recorded; and
- how it reflects on the agreed levels of funding that the NCA historically received to create the NDEC.

The NCA should determine the NDEC's staffing level and convey its decision, including its rationale, to all the NDEC's personnel.

When recruiting, the NCA must compete with the private sector and other government departments

The NDEC requires highly qualified and specialist personnel to manage and analyse data. The recruitment market in the area of technology and analysis is highly competitive. This places the NCA in competition with the private sector and other government departments.

We recognise there are limits to the salaries and benefits the NCA can offer recruits. However, there are some actions the NCA can take.

The recruitment process takes too long

We were told that the time it takes to recruit is a significant factor in the NDEC's failure to successfully fill posts with new personnel.

We were told about numerous examples of people waiting more than six months to take up a post. On several occasions, the prospective recruits had found alternative employment and declined the NCA's job offer.

We found a lack of understanding of recruitment and retention

During our inspection, the NCA gave us data showing the personnel attrition rate (the percentage of employees who leave an organisation within a defined time frame). Broadly speaking, the NCA has good retention of personnel, with an attrition rate of only 7.5 percent. But digital, data and technology personnel (which includes the NDEC) have an attrition rate of 12 percent. This might reflect the high demand for qualified personnel in the analytics field.

However, the NCA didn't give us any attrition data that related specifically to the NDEC. And, despite the confusion about the correct staffing level for the NDEC, all the managers we interviewed said it was understaffed. They also stated that they struggled to fill specialist posts.

Each one of the five NCA reviews cited above identified resourcing as an issue that required urgent attention. But none resulted in an action plan to tackle the situation. The NCA should create one.

Area for improvement

The National Crime Agency should introduce changes to its training, performance and recruitment processes for the National Data Exploitation Capability.

Training and accreditation

In general, the NCA provides good training for personnel in the NDEC. We found most personnel were satisfied with the training, and they thought it had improved in the 12 months leading up to our inspection. But they also told us the NCA's central training team should improve the internal training it gives technical personnel.

This is an area in which improved partnership working would also be beneficial. We highlight the benefits of working with the Government Analysis Function later in this chapter.

There is mandatory training for all personnel. This includes data ethics and relevant legislation. Personnel have five development days each year.

The NCA provides relevant personnel with biometrics training. This includes considering the ethical challenges that arise from using this type of data.

Technical personnel don't receive formal accreditation

Although the NDEC's analytical and intelligence personnel receive formal accreditation within their roles, this wasn't the case for technical personnel, such as data scientists and engineers.

The Government Digital and Data Profession Capability Framework provides a structure through which technical personnel can gain accreditation that is recognised across government. We were surprised that the NDEC hadn't fully adopted the framework. Senior leaders told us they believed it didn't apply to NDEC personnel. We disagree. Adoption of the framework would provide NDEC personnel with a clear continuing professional development model. It would also record their training and bring the NDEC into line with relevant technical units in other government departments.

Recommendation 6

By 30 June 2025, the National Crime Agency should adopt the Government Digital and Data Profession Capability Framework.

Partnership arrangements

The NDEC, through its data acquisition and management office, had good processes in place to initiate working arrangements with partner organisations and to acquire access to bulk datasets. And we found evidence of the NDEC's ambition to develop effective partnerships. But, after five years of the programme, we expected to see more evidence of established partnerships with industry, academia, and other government departments and law enforcement agencies.

We found that the partnerships that were in place had often come about because personnel from each organisation knew each other already, or because they had worked together on operations. There was a lack of structured engagement with other organisations also working in the fields of data science and data exploitation. Working with other organisations would offer opportunities to share production tools, technology and good practice, and it would improve organisational learning.

For example, we found that the NDEC's analysts weren't routinely working with the Government Analysis Function – a network for all civil servants working in government analysis. As a result, the NDEC personnel weren't accessing a valuable network of people who could support them in their professional development.

This lack of communication can also lead to duplication of effort. For example, the NDEC had developed a single-language translation tool. It was useful, but another government organisation had already developed a multilingual translation tool. The NDEC personnel we spoke to didn't know about this other development. This was a missed opportunity for them to benefit from others' learning.

The NDEC acknowledged to us that it hasn't fully achieved its plans for formal partnership working. NCA personnel described the reasons for those delays as the NCA's internal bureaucracy, its lack of resources and "commercial challenges". These challenges included the NDEC's inability to communicate with IT suppliers directly. In one manager's view, the delays were increased by the (understandable) requirement for IT procurement to be centralised.

The NDEC also told us of its plans for partnerships with ROCUs. The aims of these potential partnerships were:

- to give intelligence to the ROCUs using a self-service process;
- to give the ROCUs access to the data exploitation capability; and
- to identify joint data exploitation opportunities.

However, at the time of our inspection, activity was limited to discussions with a single ROCU. In these discussions, the NDEC had explored the possibility of collaborating on a data cloud infrastructure and exploiting some datasets.

Again, after five years, we were surprised not to see well-established arrangements with all ROCUs. Similarly, several police forces face major challenges in tackling SOC, particularly those covering urban areas. They would benefit from close partnership arrangements with the NDEC.

Recommendation 7

By 30 June 2025, the National Crime Agency should establish partnership arrangements with relevant bodies. These should include:

- all regional organised crime units;
- police forces that face major challenges in tackling serious and organised crime; and
- other government departments and agencies.

The NDEC's approach to ethics and standards in the way it manages data

The right to privacy is protected in law. Article 8 of the European Convention on Human Rights provides a right to respect for an individual's "private and family life, his home and his correspondence". Any breach or interference with that right must be in accordance with the law.

It is important that law enforcement agencies acting on behalf of the state, such as the NDEC, act in a manner that is not only lawful but also ethical.

Managing bulk data presents ethical challenges

In our view, the ethical challenges that need to be considered when managing bulk data include:

- the protection of people's privacy;
- making sure data is secure; and
- minimising the risk of losing data.

The NDEC has been audited by the Information Commissioner's Office

As we explained earlier, the NCA has no powers under the Investigatory Powers Act 2016 (IPA) in relation to bulk personal and communications data.

This means that it isn't subject to the regulatory regime required by the Act, and independent oversight of its use of that data isn't required by statute. But section 129 of the Data Protection Act 2018 permits the Information Commissioner's Office (ICO) to carry out "consensual audits" to establish if an organisation is "complying with good practice in the processing of personal data".

In 2020, at the NCA's invitation, the ICO carried out a consensual audit of the NDEC's data-handling processes. We recognise the NCA's decision to request an audit despite being under no statutory obligation to do so.

The audit concluded that the NDEC's processes "mirrored" requirements contained in the IPA and its Code of Practice.

Although this finding was reassuring, there had been only one such audit in four years.

We think that the auditing of the NDEC's processes shouldn't be wholly reliant on the NCA's willingness to give its consent.

Section 229 of the IPA requires the Investigatory Powers Commissioner's Office to "keep under review (including by way of audit, inspection and investigation)" the exercise by public authorities of the powers enabled by the IPA. This includes the "acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service". Similarly, section 244 of the IPA requires the ICO to audit the integrity, security or destruction of acquired communications datasets.

The regular examination of the NDEC's processes shouldn't be left to chance. We believe a more systematic, robust arrangement is needed. In our view, this would make sure that the NCA's processes and data handling are audited appropriately. This would demonstrate a similar level of compliance with Part 7 of the IPA in respect of retaining and using bulk personal data.

Recommendation 8

By 30 June 2025, the Home Office should secure a systematic, robust arrangement (which may require legislation) for regular audits of the National Crime Agency's use of bulk personal datasets. This should include:

- retention
- disclosure
- security
- destruction.

In the meantime, the NCA should make sure that the practice of making itself subject to audit, as permitted by section 129 of the Data Protection Act 2018, continues on a timely and regular basis.

Recommendation 9

By 30 June 2025, the National Crime Agency should establish a programme of consensual audit by the Information Commissioner's Office, as permitted by section 129 of the Data Protection Act 2018. These audits should meet the requirements of section 229 of the Investigatory Powers Act 2016 and its Code of Practice.

General awareness of data protection policies is good among NDEC personnel

The NCA publicises its data protection policies on its intranet. The NCA policies we reviewed were up to date and included relevant information. Importantly, the NDEC personnel we spoke to knew about the policies and understood their contents. We were also told that all NCA personnel, during their initial training, receive information on data management.

NDEC personnel also understood the legislation that governed their work in the management of data. This helped them manage ethical considerations. For example, personnel in the biometrics team had a good understanding of important definitions of biometric data. These are contained in section 28 of the Protection of Freedoms Act 2012 and the ICO's report 'Biometrics: insight'.

Personnel know how to report data breaches

The NDEC personnel we spoke to were knowledgeable about the processes in place to report data breaches. We found that they were confident that senior managers would focus on dealing with any breach, as opposed to placing undue blame on any individual. This helped to encourage an ethical culture in data management. We found that the NDEC personnel worked well with the NCA's Information Asset Owner.

At the time of our inspection, the NDEC had experienced one data breach in the previous 12 months. A member of NCA personnel accidentally sent a dataset to the wrong internal email address. This was categorised as a low-level breach. We agree with that assessment. The breach was reported immediately.

Progress against objectives

This chapter includes our observations on:

- the National Data Exploitation Capability's (NDEC) initial objectives;
- the National Crime Agency's (NCA) reviews of the NDEC programme; and
- the objectives the NDEC has achieved.

The NDEC's initial objectives

As explained above, the NDEC programme was formed in 2018. The initial business case, which the NDEC showed us, established nine "deliverables", or objectives, that the NCA expected the NDEC to achieve during its first five years.

This business case doesn't explain the nine objectives, other than by way of a brief heading. Below, you can see in bold the objectives as they are listed in the initial business case. They are accompanied by our own explanations, based on commentary from personnel we interviewed:

- **NDEC service partner** – creating the data acquisition management office as a single point of contact, helping NCA units and external organisations to communicate with the NDEC.
- **Identity and access management** – intended to provide all NCA personnel with a single means of accessing and using information and data across the NCA's three tiered IT platforms.
- **Initial capability delivered** – establishing the NDEC's basic capability.
- **Tier one cloud environment** – providing a cloud service appropriate for sharing and managing information classified as tier one, or OFFICIAL.
- **Tier two cloud environment** – providing a cloud service appropriate for sharing and managing information classified as tier two, or SECRET.
- **Mediated access for partners** – an electronic means of allowing authorised NCA units to access exploited data.
- **Data exploitation centre of excellence** – a proposal to pursue recognition as a data exploitation centre for excellence.
- **Data academy training** – providing training to NCA personnel by the NDEC and the NCA's chief data officer.

- **Partner support and comms** – providing support and communication for other NCA units or external agencies.

Regrettably, we found during our inspection that the NDEC's recording and understanding of those objectives was confusing and inconsistent.

Then, in September 2024, the NCA gave us a different set of "deliverables" for the NDEC, which it told us superseded the previous set. This second set bore little resemblance to the initial "deliverables" the NCA had given us during our fieldwork.

The NCA didn't explain how or why it had replaced the original objectives. For the purposes of this report, unless otherwise specified, references we make to specific objectives are to those the NCA initially gave us at the time of our inspection.

We provide further information about the apparent lack of governance of NDEC objectives below.

Irrespective of which set of objectives the NCA considers to be the definitive ones, during our inspection we couldn't identify a single, authoritative document that defined the intended outcome, progress or timeline for completing each objective.

Based on our understanding of the objectives, some of them overlapped or weren't suitable for the NDEC to achieve. For example, some related to ongoing NCA IT projects which, at the time the initial business case was created, were the responsibility of the NCA's corporate IT department.

The NDEC personnel we interviewed couldn't give a consistent explanation of the NDEC's objectives or whether they had been completed.

We have been told that, in 2020, the NCA followed up the business case by creating a target operating model for the NDEC. The model was intended to be a framework that defined how the NDEC would operate to achieve its strategic objectives. The NCA set out the design, structures, processes, capabilities, technologies and governance needed to implement the model.

During our inspection, we weren't given the original version of the target operating model. Instead, we were given a "refreshed" version of the model, written in 2022. We report below on the NCA's record-keeping in relation to the NDEC's implementation.

We didn't find any evidence that the NCA was routinely using the initial business case, or either version of the target operating models, to assess the NDEC programme.

The NCA's reviews of the NDEC programme

Since 2018, the NDEC has been the subject of at least five unpublished internal reviews. In date order, they were:

- 'NDEC Strategic Delivery Update', February 2019;

- ‘National Data Exploitation Capability Blueprint’, draft, March 2019;
- ‘NDEC Programme Objectives 2021–22 Mid-Year Review/Stock Take’, 2021/22;
- ‘NDEC Target Operating Model – Summary of the Refresh TOM Draft’, June 2022; and
- ‘GMPP (Governments Major Projects Portfolio) Transformation Portfolio Quarterly Review’, October 2023.

We recognise that this list doesn’t include the 2020 target operating model. As we stated above, this wasn’t given to us during our inspection.

Each of these reviews correctly identified the problems the NDEC faced at the relevant time. Unsurprisingly, they are broadly the same personnel and IT issues we have highlighted in this report. However, the NCA appeared to have done little to either rectify the situation or identify appropriate amendments to the initial NDEC business case.

Each review the NCA showed us during our inspection followed a different format, with no clear link to the previous one. Of the five, four were in the form of Microsoft PowerPoint presentations. We concluded that these had been used for briefing senior managers. These documents identified that some of the initial objectives for the NDEC, or elements of them, were unachievable. But these objectives weren’t removed or amended to help the programme develop. In some cases, the reviews added more objectives without any obvious decision-making process, associated budget, timeline or evidenced understanding of the programme.

At best, these reviews only served to confirm the obvious. At worst, they added to the confusion about the NDEC’s objectives. None resulted in documented management intervention. And all these reviews fell well short of a comprehensive, insightful evaluation of the quality, importance or value of the NDEC’s work.

In September 2024, the NCA told us that the Infrastructure and Projects Authority had also reviewed the NDEC. The authority carried out its review in February 2024, shortly after our fieldwork had ended. In September 2024, we saw a copy of the authority’s report. The authority’s findings were broadly similar to ours. It stated that “capability has been delivered […] but it is limited in functionality below what had been expected”.

The NCA didn’t give us programme records for the NDEC

We tried to better understand the process for the NDEC’s development. We requested minutes or other records of the NDEC’s implementation board or similar governance arrangement. For example, we asked about the briefings for which the PowerPoint presentations we referred to above were prepared.

The NCA didn't give us any of these records, nor have we received any explanation for their absence. Therefore, we concluded that these documents were either never created, can't be found or no longer exist.

There is a lack of clarity about the status of the NDEC

Based on the evidence the NCA gave us, it appears that there is some confusion about the status of the NDEC programme.

In March 2024, after we had completed our fieldwork, the NCA told us that the NDEC programme had been finalised and had become a "business as usual" function.

This surprised us because during our inspection the NCA didn't give us any evidence that it had subjected the NDEC programme to a robust evaluation, or even had plans to do so. (It was only in September 2024 that the NCA told us about the Infrastructure and Projects Authority review.)

This meant that the NCA didn't appear to have a good understanding of whether the NDEC had achieved its objectives. And a senior leader told us that the NDEC target operating model originally formed part of the NCA's financial savings plans.

In September 2024, the NCA told us that the NDEC hadn't become a "business as usual" function, although it had decided to remove formal programme support for the NDEC. The practical implications of this decision include the NDEC no longer having access to a programme manager to oversee its implementation.

The NCA hasn't given us any rationale for this decision.

The objectives the NDEC has achieved

Based on the evidence we found during our inspection, we consider that, of the original nine objectives, the NDEC has achieved or partially achieved six.

These are the provision of:

- NDEC service partner;
- Tier one cloud environment;
- Mediated access for partners;
- Data academy training;
- Partner support and comms; and
- Initial capability delivered.

In the case of the final objective, due to the absence of any clear criteria for its completion, we can't say whether the NDEC has achieved the objective in full.

At the time of our inspection, the NDEC hadn't achieved three objectives:

- **Identity and access management** – this was, at the time of the initial business case, the responsibility of the NCA's corporate IT department. We understand that the NDEC hasn't had a role in this initiative, nor have we seen any evidence that suggests it should have had a role. At the time of our inspection, an identity and access management system of the kind envisaged wasn't in place and there wasn't an agreed timeline for its completion.
- **Data exploitation centre of excellence** – we understand that this objective was discontinued after the NCA recognised that several similar centres of excellence already existed in other government agencies. We have reported on the NCA's lack of meaningful communication with the Government Analysis Function.
- **Tier two cloud environment** – distinction should be made between this and the NDEC's creation of the interim IT platform (explained above). This platform is a critical stepping stone in creating a tier two cloud environment.

The NDEC's cited achievements didn't appear to match its objectives

We asked the NDEC managers to give us a list of what they considered the NDEC had achieved. Only one item on the list had been included in the initial business case list of intended objectives for the NDEC.

As any programme develops, it may be legitimate for its objectives to evolve. However, as we explained above, the NCA hasn't given us any recorded rationale for a change in the NDEC programme's objectives.

The achievements the NDEC managers highlighted were:

- **Tier one cloud environment** – the NDEC has rolled out a tier one cloud environment. In line with the Government's Cloud First strategy, this involved working with a commercial company and developing several bespoke production tools.
- **Some partnership working** – the NDEC has developed formal partnerships with two of its four intended partners. We described above the shortcomings in the NDEC's partnership arrangements.
- **Connectivity with Police National Computer and the Police National Database** – the NDEC has access to both the Police National Computer and the Police National Database. But this access is limited to individual checks, not bulk data. The NDEC's access to these systems is comparable to that of police forces.
- **Access to datasets** – as we explained above, the NDEC has acquired access to a number of datasets to help it target serious and organised crime. Some of these datasets are more valuable to the NDEC than others.
- **Creation of an interim system for managing tier two information** – NDEC managers also cited the development of the tier two platform interim system.

NDEC managers also told us what they thought the NDEC hadn't achieved

We also asked the NDEC managers to give us a list of what the NDEC hadn't achieved. Once again, the items listed didn't correlate with the objectives set out in the initial business case or the target operating model. They included:

- full partner collaboration;
- mapping (or listing) all potential stakeholders to identify suitable datasets for the NDEC to acquire; and
- developing all the planned production tools which the NDEC should have access to.

The final point supports the observation we made above, that the NDEC may not have completed achieved the "initial capability delivered" objective.

The NDEC managers also included what they referred to as the "enterprise team" in the list of unachieved objectives. They highlighted it as a reason the NDEC hadn't achieved all its other intended objectives.

Plans for an enterprise team hadn't been realised

Personnel at all levels in the NDEC told us that the initial business case for the NDEC included a plan for an enterprise team. This team's purpose would have been to maintain the production tools created in the Datalab by the NDEC's data scientists.

During interviews, we were told they had understood that production or support engineers would staff the enterprise team. But, because the team wasn't created, the maintenance demand had fallen to personnel in the Datalab. In their view, this extra demand had severely reduced their capacity to develop tools for extracting and analysing bulk data.

It was also clear to us that the perceived failure to create the enterprise team was the source of great frustration for personnel. They believed that, as a result, they or their teams were carrying out functions that didn't make the best use of their skills or qualifications.

The initial business case contained an NDEC organisational structure described as being "under development". But, with one exception, we didn't find any reference to the enterprise team in that document or in subsequent review material.

There was a single reference in the 2022 refresh of the target operating model. That document refers to "enterprise service deployed and supported". We didn't find any evidence to support that statement.

We don't doubt the NDEC personnel's understanding of the situation. Providing a maintenance capability strikes us as a sensible proposal. But, once again, there is clearly a disconnect between the understanding of personnel and managers, and what is recorded.

Governance, management and performance

This chapter includes our observations on:

- performance management;
- allocation of the National Data Exploitation Capability's (NDEC) workload;
- governance structures; and
- the value of the NDEC.

Performance management

Personnel at all levels told us that the NDEC didn't record or assess its performance effectively. Many people, including managers, struggled to explain how they collected or used performance data.

About six months before our inspection, and at least four years since the NDEC's inception, senior leaders put in place a process for recording performance data. Before this, team managers may have recorded some performance data on spreadsheets. But this was unco-ordinated and not a universal practice across the NDEC.

We couldn't find any evidence of how the NDEC's managers then used that information to improve performance.

At the time of our inspection, the data and analysis operations team had begun to record basic data on the NDEC's performance. This helped analysts demonstrate some of the tangible benefits that the NDEC brings to the NCA.

For example, each month the team recorded:

- the number of bulk searches completed;
- the number of entities (names, addresses or telephone numbers) included in those searches; and
- the number of identified links to serious and organised crime (SOC).

This is encouraging, but the NDEC didn't begin gathering this type of information until just before our inspection. Had it had done so from the beginning, it may have collected a greater body of evidence to show its value to the National Crime Agency (NCA).

The NDEC needs to do more to gather evidence on the value of its support. At the time of our inspection, it couldn't describe the outcomes of any of the links the NDEC analysis made or show what the NCA did with those links. For example, the number of suspects targeted or arrested, and the amount of assets, firearms or drugs recovered. We think the NDEC should collect this type of information more systematically.

We expected to find the NDEC carrying out more recorded activity to disrupt organised crime groups

The NCA uses the agency and partner management information system (APMIS) to monitor disruptions of organised crime groups. NCA units use the system to record whether they have taken a lead role or supported other NCA units, police forces or agencies in each disruption. Many of the personnel we interviewed believed that the NDEC didn't fully record its involvement in the NCA's disruption activity. We agree.

We recognise that the NDEC's role is mainly to support other NCA units. But we would have expected there to be more activity recorded. We understand that the revised performance monitoring should lead to a more accurate reflection of the NDEC's involvement. Managers should make sure this data is recorded accurately on APMIS.

Figure 1: The NDEC's annual recorded disruption activity data, as either the lead unit or supporting other NCA units

Year	Lead	Supporting other NCA units
2021	0	200
2022	3	184
2023	1	166
2024 (Q1)	0	19

Source: Data collection from the agency partner and management information system

Allocation of the NDEC's workload

The NDEC has an official process for allocating work to personnel, but it needs to be auditable and applied more consistently. We found that, in practice, an unofficial process ran alongside the official one.

The NDEC has an official process for allocating tasks

The NDEC's official process for allocating tasks requires service users to submit a tasking request form. Each request is assessed and, if it relates to an NCA priority, it is considered at a weekly meeting chaired by the lead of the data and analysis operations team. Those present at the meeting assess and, if appropriate, allocate each task to the relevant team in the NDEC.

The meeting is also used to prioritise each request. Those considered to be non-priority are placed in a backlog queue. At the time of our inspection, the backlog extended to 12 weeks. The NDEC personnel refer to this process as "front-door tasking".

NDEC personnel told us there is also an unofficial process for allocating tasks

Nearly all the personnel we spoke with also referred to a "back-door" process for assigning work. This means that service users in the NCA routinely circumvented the official process by approaching NDEC personnel directly.

We were told that, at the time of the inspection, some personnel who had worked in the NDEC for more than two years had only recently found out about the official task allocation process.

This means NDEC managers were potentially unaware of whether tasks completed by their personnel met the correct criteria for action or were being correctly prioritised. It also means that managers didn't have an accurate way of understanding the demand on the NDEC or how effectively it responded to that demand.

The NDEC should make sure the unofficial, back-door process of assigning work ends. The only approved process used by personnel should be the official process. This should be auditable, and the work assigned according to threat, risk and harm.

The NCA has introduced a work-tracking system

In the six months before our inspection, the NCA had introduced a work-tracking system. Prior to that, managers used spreadsheets to co-ordinate workload.

Although IT incompatibility issues had disrupted the system's implementation, it was in use during our inspection. From the evidence we saw, it appeared to be working well. This was reassuring as it was much needed.

But we found that, despite its availability, it still wasn't being used across all the NDEC's teams. Managers told us that for this to happen, a "culture change" would be required. The benefits of a single system to assign and track work should be clear to all. It would:

- provide a clear and auditable record of the NDEC's work;
- make sure each task the NDEC carries out is necessary, proportionate and appropriately prioritised; and
- help the NDEC's managers to end the culture of back-door allocation of work.

Feedback on the NDEC's work is rare

The NDEC's personnel rarely receive feedback from service users on their work. This prevents the effective evaluation of the NDEC's role in disrupting SOC. Managers estimated that, in the nine months before our inspection, fewer than ten instances of feedback had been given.

Although the official task request form includes a section for feedback, NDEC service users hardly ever complete it. And the prolific use of back-door allocation of tasks clearly undermines the process.

At the time of our inspection, NDEC managers were considering building a requirement for feedback into the work-tracking system form. We would encourage them to do so.

Leadership and governance

At the time of our inspection, the NDEC had an established governance structure. It was supported by routine strategic and operational meetings. These meetings appeared to be run well.

The NCA should communicate better with NDEC personnel

As we have shown, particularly in relation to the NDEC's approved staffing levels and the lack of an enterprise team, communication with personnel needs to be improved.

There were further examples. Some personnel we interviewed spoke of the confusion that followed the merger of two of the NDEC's teams in June 2023. During our inspection, about six months later, some NDEC personnel were still unaware of the merger. And several of the personnel we spoke to were unclear about the organisational structure and their roles within it. For example, personnel in one team considered themselves to be service users of the NDEC, rather than integral members.

NDEC personnel highlighted several problems with leadership

Throughout our inspection, NDEC personnel frequently raised the issue of leadership. This related to a high turnover of programme managers, a lack of strategic and technical support, and insufficient performance management.

We were told that in the five-year span of the programme, there had been five programme managers. Some personnel attributed this turnover to the "challenging nature" of the programme.

We have highlighted the apparent absence of plans to deal with the strategic resourcing issues the NDEC has continually faced. One senior leader told us they were employed as a technical expert, not a strategic leader. In their view, it wasn't their responsibility to respond to strategic challenges. We disagree.

Some junior personnel also told us they were frustrated with the lack of communication, direction and leadership from senior managers outside the NDEC.

We were told that some senior managers didn't understand the technical nature of the NDEC's work, and that they dismissed some matters as being "too technical" for discussion.

The NCA has been aware of this issue for some time. The 2019 National Data Exploitation Capability Review (unpublished) said: "Varying levels of [IT] literacy amongst officers in leadership roles means that the true value of data exploitation cannot be fully realised to the benefit of the agency."

At the time of that review, the NCA classified this as an amber risk. We aren't aware of any action taken to remedy the situation.

We concluded that the NDEC had a tier of management unwilling to intervene in strategic issues, and another without the technical understanding to be involved in tactical matters. This situation was frustrating for NDEC personnel. We recognise that at the time of our inspection, a new senior leader had recently been deployed to the NDEC.

The value of the NDEC

One of our terms of reference required us to consider: "How valuable is the NDEC's contribution and how effectively does the NCA use it?" The shortcomings in the programme's implementation, governance and management have made answering the question far from straightforward.

We were unable to establish any record of clear and universally accepted objectives for the NDEC. Nor were there any apparent records relating to the NDEC's implementation or to strategic decisions made during the implementation process.

As we have identified, until six months before our inspection, the NDEC had no meaningful performance management regime. Other NCA units routinely circumvented the official process to allocate work.

We recognise, however, the hard work and dedication of the NDEC's personnel. Their work is shown in the examples we have included in this report. These are an illustration of the potential benefits that a well-resourced and well-led NDEC can bring to the NCA and other law enforcement agencies. But they shouldn't be taken as evidence that the NDEC has become either of those things. As yet, its potential remains unfulfilled.

hmicfrs.justiceinspectorates.gov.uk