



# NATIONAL POLICING CYBER SECURITY STRATEGY

**This strategy, commissioned by the National Police Chiefs' Council's (NPCC's) Digital, Data and Technology Coordination Committee (DDATCC), sets out the context of cyber security in policing. It defines objectives, strategic priorities and concludes with a set of transformation proposals designed to increase policing's cyber resilience.**

## Contents

# FOREWORD

## Policing in the digital sphere presents opportunities and challenges."

Cyber threats and risks are ever present dangers, where our officers and staff have to be ready and able to respond, often at a moment's notice. These kinds of incidents are often unseen, but can have a major impact and compromise our ability to keep the public safe.

The National Policing Cyber Security Strategy is a significant step forward for policing to face these challenges and work together to defend our people, systems, and the service, as a whole, from the threats that we face. Aligned with the Government's National Cyber Security Strategy, this new Strategy supports our wider work to ensure that we are ready and able to face current, new, and emerging threats from criminals and cyber incidents.

I am delighted with the response from the policing community and partners that have engaged with this important work. It highlights that we are all committed to the continuous improvement of the service to build our cyber security capability across the board.

I fully support the key themes in the Strategy and would like to thank the Information Assurance Portfolio, led by Assistant Commissioner Peter O'Doherty, and the Police Digital Service for their work and continuing support for policing.

**Chief Constable Gavin Stephens**
**Chair of the National Police Chiefs' Council**

# FOREWORD

> Harnessing modern digital, data and technology capabilities is critical to our policing mission; allowing us to effectively tackle crime and ensuring that we can meet demand. The data that we hold is our most valuable asset and accordingly, any compromise of our information security will undermine our capability."

Everyone in policing has a part to play in keeping information secure. Without the assurance that we can be trusted to do this, public trust will be eroded and support from communities to tackle crime will be reduced.

Cyber criminals have a wide range of methods that they use to target organisations and they are relentless in their efforts to target and attack any vulnerability. We must be diligent in our approach to cyber security and agile in our responses to issues that arise; ensuring that our management of data, the systems we use and the way we work, places safety and security at the forefront of our thinking and actions. This is a shared responsibility across all policing organisations, partner agencies and suppliers.

I welcome and endorse this National Policing Cyber Security Strategy and I am pleased that it highlights the importance of information security roles. It reflects the importance of strengthening capability in this area by developing skills and supporting the cyber security profession. The strategy will support our wider work to drive up professional standards and draw in expertise to enable policing to work consistently in cyber security matters.

**Rob Carden**
**Chair, NPCC Digital, Data and Technology Coordination Committee (DDaTCC)**
**Chief Constable, Cumbria Constabulary**

"The police's ability to protect the public relies on the availability of data and several critical IT systems. Ensuring the security of these services and the data the public entrusts with us is, therefore, crucial for enabling policing to deliver its core function."

We know that policing is an attractive target for malicious cyber actors because of the sensitive information it holds. Equally technology plays a crucial role in supporting an emergency response. Therefore, having a high level of cyber resilience is essential for reducing the risk of disruption to police operations.

Satisfying this requirement at scale is not without its challenges but at the National Cyber Security Centre (NCSC), we are pleased to support this strategy, which clearly defines what policing must achieve to mitigate the risk of suffering a cyber attack.

Central services such as those delivered by the Police Digital Services and its National Management Centre are already improving cyber resilience, and under this new strategy, these services will continue to evolve, providing forces with access to the cyber expertise they need, supporting their implementation of consistent and repeatable processes, and, at a national level, providing better visibility of policing systems to help with oversight.

This strategy also aligns to the Government Cyber Security Strategy and in particular the objective of enabling public sector bodies to come together to offer an overall cyber defence that is greater than the sum of its parts.

The NCSC works hand in glove with law enforcement to protect citizens and organisations and our continued collaboration is vital for our overall ability to do that. I look forward to seeing how the implementation of this strategy will improve cyber security outcomes and strengthen our relationship so we can continue keeping the UK safe online.

**Ian McCormack**
**Deputy Director for Government, NCSC**

# FOREWORD

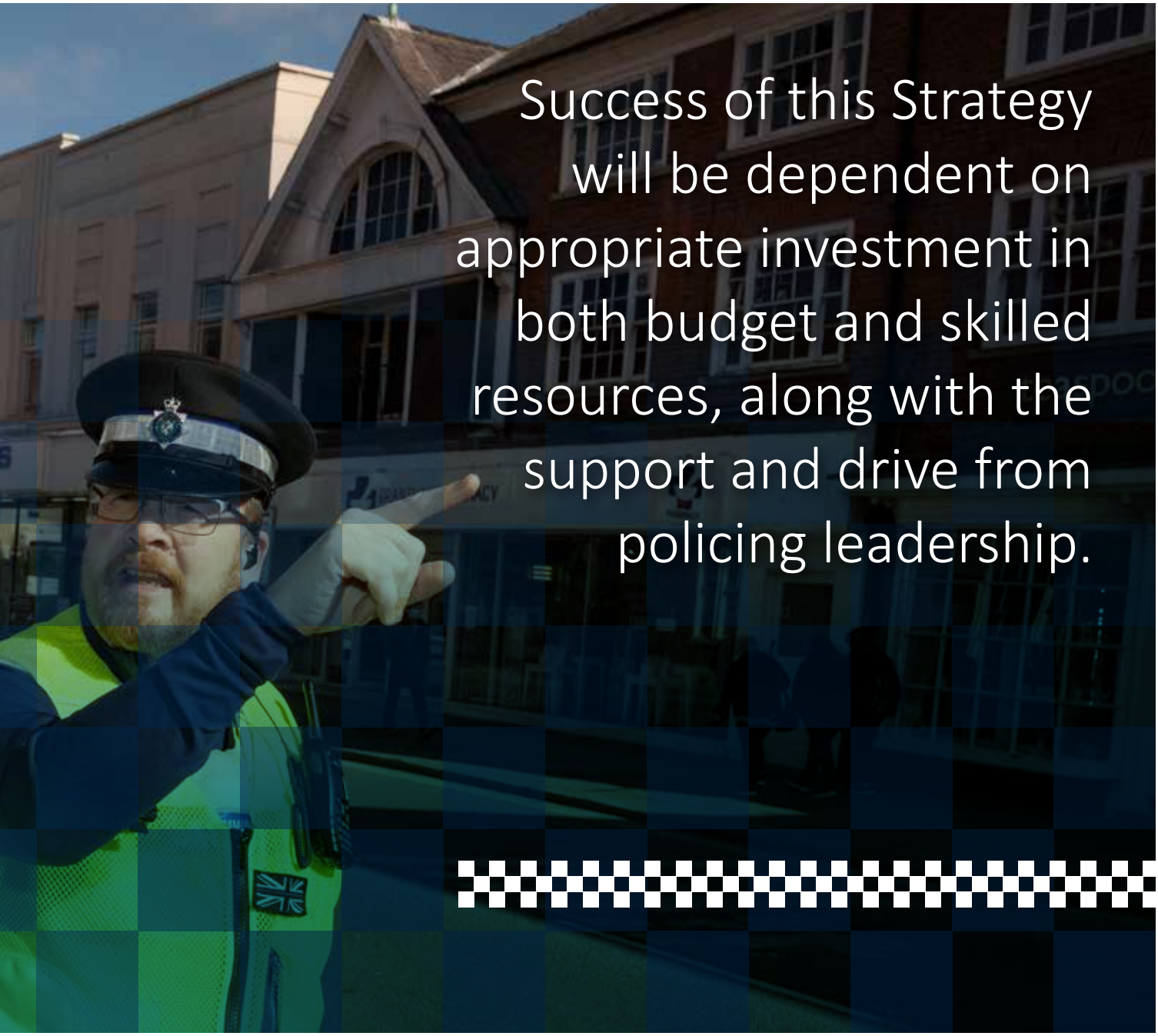
## Improving consistency and professional standards across policing is a key focus of our work at His Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS)."

I welcome the introduction of a National Policing Cyber Security Strategy. Cyber security is a significantly increasing area of risk for the police service. For the police to protect the public, critical IT systems and the data they contain must be protected.

This means cyber security practices and standards need to be effective at a national, regional and local level. The National Policing Cyber Security Strategy reflects the need to take a unified approach to how cyber security is led, and aims to meet the challenges of new and evolving threats.

In the future, it is highly likely that we will inspect the effectiveness of forces' cyber security practices and the contribution of this strategy.

**Andy Cooke QPM, DL**
**His Majesty's Chief Inspector of Constabulary HMICFRS**



Success of this Strategy will be dependent on appropriate investment in both budget and skilled resources, along with the support and drive from policing leadership.

# EXECUTIVE SUMMARY

**The National Policing Digital Strategy stems from policing's ambition to exploit digital capability in support of tangible, positive and measurable outcomes for both law enforcement and the public. The National Policing Cyber Security Strategy represents a fundamental pillar, underpinning that Strategy.**

Trust and confidence of the public, partners, officers and staff in policing's ability to store and process data safely and securely are paramount and at the heart of information assurance. Policing's adoption of digital capabilities continues to grow in depth and breadth. Without a corresponding and proportionate focus on cyber security and its associated disciplines, policing runs the risk of a significant information security breach that could negatively impact on critical policing services and the privacy rights of individuals whose data we store.

Policing has made significant progress in recent years regarding cyber security, however there is much more to be done. This is reflected in the Security Assurance for Policing (SyAP) scores used to measure policing's current level of maturity regarding cyber security.

Policing's approach to risk management and mitigation across local and national technology portfolios is inconsistent. Insufficient sharing of best practices across policing, as well as with wider government and industry, is leaving local security teams in forces over-stretched and isolated. There is insufficient linkage between the way policing is measured for assurance and how it can protect information, in practice.

In line with the **Government Cyber Security Strategy 2022 to 2030**, this document sets out the following objectives and outcomes for policing:

1. Manage cyber security risk
2. Protect against cyber attacks
3. Detect cyber security events
4. Minimise the impact of cyber security incidents
5. Develop the right cyber security skills, knowledge and culture

The achievement of these objectives in policing is dependent on five strategic priorities:

1. Alignment between cyber security and policing outcomes
2. Skilled, engaged and empowered cyber security personnel
3. Operational consistency
4. Nationally aligned technical capabilities
5. Nationally available services

This Strategy contains a programme of transformation proposals designed to address these areas of strategic priority, thereby improving policing's cyber security maturity over the period of Q1 2024 to Q4 2026. A steering group, reporting to the Police Information Assurance Board (PIAB), will be stood up to oversee the working groups leading each of the strategic priority areas. This steering group will include membership from the NPCC's DDaTCC and its supporting portfolios.

Success of this Strategy will be dependent on appropriate investment in both budget and skilled resources, along with the support and drive from policing leadership.

# CONTEXT

## The National Policing Digital Strategy

Information is the lifeblood of policing. Achieving today's policing outcomes requires the ability to effectively make the most of the available data at ever-increasing scale and speed.

The National Policing Digital Strategy sets out five key digital ambitions for policing:

1

### Seamless citizen experience

We will deliver seamless, digitally enabled experiences. The public will have more choice in how they engage with us, using channels, media, or devices most relevant to them. We will be able to connect citizen interactions, information, and data across departments, and across forces to build a more credible and richer intelligence picture, all whilst maintaining public trust by ethically acquiring, exploiting, and sharing their data.

2

### Addressing Harm

We will harness the power of digital technologies and behaviours to identify the risk of harm and protect the vulnerable in the physical and digital world. We will deliver earlier, more precise, and targeted proactive policing approaches and early interventions through the application of digital technology.

3

### Enabling officers & staff through digital

We will invest in our people, from leadership through to the front-line, to ensure they are equipped with the right capabilities (knowledge, skills, and tools) to deal with increasingly complex crimes. We will establish digital leadership and ways of working to allow our workforce to focus on critical and value-adding activities.


4

## Embedding a whole public system approach

We will foster a philosophy of openness and deepen our collaboration with our public sector partners to jointly design and tackle complex public safety issues – sharing data insights and making use of digital tools to work more effectively across the public safety system, ensuring we do so in an ethical way to safeguard public trust.

5

## Empower the private sector

We will strengthen our relationships with the private sector to empower it to appropriately share in public safety responsibilities. The private sector, and the users of its services, have always shared responsibility for elements of public safety and, as technologies become easier and more accessible, there are new ways to safely empower those with an active desire to help.

Building and maintaining the trust of the public, partners, officers and staff in policing's ability to store and process information safely and securely is at the very heart of these ambitions. Policing's adoption of digital capabilities continues to grow in depth and breadth. Without a corresponding and proportionate focus on cyber security and its associated disciplines, the risk increases of a significant information security breach impacting critical policing services and the privacy rights of the individuals whose data we store.

Policing must therefore ensure that as its digital 'attack surface' broadens, its resilience to cyber attacks also continues to mature.

## The threat landscape

The scale and diversity of information stored and processed across policing's digital platforms presents a high-value target to threat actors, from nation states to cyber criminals. Whilst attackers' capabilities and techniques continue to evolve and diversify, the commoditisation of offensive cyber tools and services increasingly lowers the capability threshold required for anyone seeking to disrupt or undermine UK policing.

Government and public services remain an attractive target for a broad range of malicious actors. Approximately 40% of the 777 incidents, managed by the National Cyber Security Centre (NCSC) between September 2020 and August 2021, affected the public sector.[1] This is expected to increase.

The threat from nation state actors is of considerable concern. Nearly half of nation state activity is being targeted at governments across the world, with the UK being the third most targeted country behind the USA and Ukraine.[2] Equally, the dramatic rise of ransomware[3] attacks and recent high impact incidents demonstrate both the scale of impact and the diversity of organisations affected, from government departments to wider public sector organisations. The targeting of healthcare, education and other essential services (either directly or to expose system vulnerabilities) continues to prove the severity of such cyber attacks. These types of attacks can cause significant disruption to the delivery of essential public services and also pose a real risk to public safety.

In the time it has taken to prepare this Strategy, policing has been subject to several cyber incidents, ranging from supply chain data losses due to ransomware to nation state infiltration of a policing hosted system. There is no doubt that cyber threats are a very real and present danger.

[1] **Government Cyber Security Strategy 2022-2030, page 7**

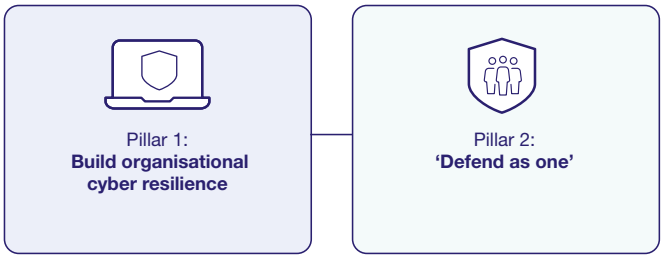
[2] **Microsoft Digital Defense Report 2021, page 53**

[3] Ransomware - a type of malicious software designed to block access to data on a computer system until a sum of money is paid.

## The Government Cyber Security Strategy

The **Government Cyber Security Strategy 2022 to 2030** provides a set of cyber security objectives and outcomes for all public sector organisations, underpinned by the core pillars of 'Building Organisational Cyber Resilience' and 'Defend as one'.

The 'Defend as one' principle recognises that the scale and pace of the threat demands a more comprehensive and joined up response. The government will harness the value of sharing cyber security data, as well as, the expertise and capabilities across its organisations to present a defensive force disproportionately more powerful than the sum of its parts. This principle can be extended directly to policing.




The government's Strategy sets out an assurance framework aligned with the **NCSC Cyber Assessment Framework (CAF)** and a system of independently assessed self-reporting for **Government departments and Public Services (GovAssure)**. It sets a specific aim for critical functions to be significantly hardened to cyber attack by 2025, with all government organisations across the public sector to be resilient to known vulnerabilities and attack methods, by no later than 2030.

## Legislation and regulation

Policing needs to protect its information assets and the systems that it depends on to meet its obligations. These are not just aspirations. The UK has, in fact, put in place legislation and regulations that make it mandatory for policing to protect its data and systems. Failure to comply with the relevant legislation could result in fines and sanctions, neither of which will be beneficial to policing or its mission.

Examples of relevant legislation and regulations include the:

- Data Protection Act 2018;
- General Data Protection Regulation (UK) 2021;
- Network & Information Systems Regulations (NIS Regulations) 2018;
- Computer Misuse Act 1990;
- Telecommunications (Security) Act 2021; and
- Human Rights Act 1998 – with reference to right to privacy.

## Policing's cyber security maturity

Policing has made significant progress in recent years regarding cyber security. The standardisation of technical security controls across productivity platforms has ensured a better understanding of our attack surface and ensured consistent controls. The establishment of the PDS NMC, as a centre of cyber security capability has provided a huge leap forward for policing on its journey towards defending as one. The NMC ensures greater visibility of cyber activity and enhanced threat intelligence, detection, and hunting capability. Bringing together several security capabilities into the national PDS Cyber Services has also provided a focal point for cyber, building a body of knowledge for use across policing. The replacement of the Governance and Information Risk Return (GIRR) with Security Assurance for Policing (SyAP), has provided a more dynamic and transparent maturity and risk reporting structure. This has strengthened defences and empowered the Police Information Assurance Board (PIAB) with increased visibility of risk and an improved ability to effect change. The development of strong working relationships with the National Crime Agency (NCA), the NCSC and other key government cyber bodies has further united the law enforcement community.

There is, nonetheless, much more to do. Whilst awareness of cyber security risks across policing has improved, continued maturity assessments highlight the gap between policing's current cyber resilience and the achievement of a consistent minimum baseline. Policing's approach to risk management and mitigation across local and national technology portfolios is inconsistent. Insufficient sharing of best practices across policing, as well as with wider government and industry, is leaving local security teams in forces over-stretched and isolated. The size and diversity of policing's supply chain makes it challenging to manage associated cyber security risks, particularly given duplication of effort. Policing's legacy technology base still leaves it too exposed to vulnerabilities, increasing risk outside of tolerance. There is currently insufficient linkage between the way policing is measured for information assurance, which impacts on its ability to protect information.

Furthermore, as with the wider public sector, policing struggles to compete with the private sector to attract and retain the required cadre of diverse and skilled cyber security professionals, despite positive efforts to date. This extends beyond technical cyber security skills, including the broad range of professional functions that require cyber security knowledge and awareness.

Improving and adapting policing's approach to cyber security is much more than a technology consideration. It requires policing to pool expertise, implement flexible but repeatable practices, collaborate effectively across forces, wider government, academia, and industry, and make policing an attractive sector for the best cyber security talent.

## Cyber security vs cybercrime

Cybercrime and cyber security are distinct from one another. However, within the policing community these themes are sometimes both abbreviated as 'Cyber'. For clarity, the focus of this Strategy is **cyber security**, i.e. the protection of policing's information assets and the systems on which they reside.

**Cybercrime** is an umbrella term used to describe two closely linked but distinct ranges of criminal activity. The **Government Cyber Security Strategy 2022 to 2030** defines these as:

*"Cyber-dependent crimes - crimes that can be committed only through the use of Information and Communications Technology ('ICT') devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity).*

*"Cyber-enabled crimes - traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft)."*

Tackling cyber-dependent and cyber-enabled crime is a policing priority. This operates as part of an integrated response coordinated by the NCA's National Cyber Crime Unit (NCCU), delivering intelligence-led response to all forms of cyber attacks against individuals, organisations, or whole sectors.

**Cyber security** is how individuals and organisations reduce the risk (likelihood and impact) of cyber attack. This Strategy focuses on how policing achieves this through the defence of its systems and information assets.

Cyber security considers how the confidentiality, integrity and availability of information is maintained, through the following broad objectives:

- Managing information security risk;
- Protecting against cyber-attacks;
- Detecting cyber security events;
- Minimising the impact of cyber security incidents; and
- Developing the right cyber security skill, knowledge, and culture.


# Cyber security considers how the confidentiality, integrity and availability of information is maintained

# VISION, OBJECTIVES AND OUTCOMES

## Vision statement

Policing functions are resilient to cyber attack, improving on and maintaining public trust and confidence in policing services.

### Objectives and outcomes

These objectives and outcomes have been derived directly from the Government Cyber Security Strategy 2022-2030 and adapted, where appropriate, for policing.

## Objective 1 – Manage cyber security risk

Effective cyber security risk management processes, governance and accountability enable the identification, assessment, and management of cyber security risks across policing.

### Outcomes

| | |
|---|---|
| 1 | Policing has established governance arrangements with clear accountability, enabling effective management of cyber risks across all levels of policing. |
| 2 | Policing has comprehensive visibility and understanding of its digital assets, enabling it to identify and manage vulnerabilities and the cyber security risks they present. |
| 3 | Policing has comprehensive visibility of the information it handles and shares, so that it can appropriately assess and respond to the risks it presents. |
| 4 | Policing understands and manages risks emanating from third parties, including commercial suppliers, partners, and consumers of policing systems. |
| 5 | Through optimised sharing of threat intelligence, policing understands the threat it faces relative to its functions to plan appropriate mitigations across all policing entities. |
| 6 | Decision makers at all levels of policing have timely access to relevant and actionable risk data that enhances their ability to make effective risk management decisions. |
| 7 | Cyber security assurance provides policing with the visibility it needs to make effective decisions and the confidence that it has appropriate cyber security measures in place to manage the risks to its functions. |
| 8 | Strategic partnerships with the private sector are further embedded to enhance proactive defence. |

## Objective 2 – Protect against cyber attack

Understanding of cyber security risks informs the adoption of proportionate security measures with nationally developed capabilities, enabling protection at scale.

## Outcomes

1. Policing adopts a common approach to 'Secure by Design' to ensure that appropriate and proportionate cyber security measures are embedded within the technology used by policing and that the security of digital services is continually assured throughout their lifecycle. It will be a hybrid of existing methodologies, including the **Government Secure by Design Framework**, made suitable for policing.
2. Policing entities deploy cyber security controls commensurate with their risk profile and, where appropriate, in accordance with nationally agreed standards, to ensure that risks to their functions are managed proportionately.
3. Technology is appropriately configured, with standard profiles for common technology and architectures being developed and continuously updated.
4. Shared capabilities, tools, and services that can tackle 'common' cyber security issues at scale.
5. Policing data is classified appropriately and handled and shared in a way commensurate to the risk it presents.

## Objective 3 – Detect cyber security events

Comprehensive monitoring of systems, networks and services enable cyber security events to be managed before they become incidents.

### Outcomes

1. Policing networks, systems, applications, and end points are monitored to provide proportionate internal detection capability to deliver risk treatment.
2. Shared detection capability provides detection at scale across all police critical systems.
3. Policing's detection capabilities will be enhanced to allow for earlier detection of threats and attacks.

## Objective 4 – Minimise the impact of cyber security incidents

Cyber security incidents are swiftly contained and assessed, enabling rapid response at scale.

### Outcomes

1. Policing is fully prepared to respond to cyber incidents, including people, process, technology and an appropriate schedule of testing and rehearsal.
2. Policing rapidly responds to cyber incidents, using a coordinated and consistent local and national response and recovery process.
3. Policing has the capability to quickly restore systems and assets affected by cyber security incidents and resume the operation of its functions with minimal disruption.
4. Lessons learned from cyber incidents drive improvements in cyber security across the whole of policing.

## Objective 5 – Develop the right cyber security skills, knowledge and culture

Sufficient, skilled, and knowledgeable professionals fulfil all required cyber security needs, extending beyond technical cyber security experts to the breadth of professional functions that must incorporate cyber security into the services they provide. This is all underpinned by a cyber security culture that promotes sustainable change.

### Outcomes

1. All policing cyber security skills requirements are understood.
2. Policing attracts and retains the diverse cyber security workforce it needs to be resilient.
3. Policing continuously develops its cyber security workforce to ensure that it has and retains the skills it needs.
4. Sufficient cyber security knowledge and awareness across policing's professional functions ensures that cyber security is actively taken into consideration.
5. Policing has a cyber security culture that empowers its people to learn, question and challenge, enabling continuous improvements in behaviours and resulting in sustainable change.


# Sufficient, skilled, and knowledgeable professionals fulfil all required cyber security needs

# STRATEGIC PRIORITIES

## To achieve the strategic objectives set out above and, at the same times demonstrate economy, efficiency, and effectiveness, policing's cyber security operating model must evolve.

Policing organisations differ in their scale, operational priorities, and internal cyber security capabilities. It is therefore important to acknowledge that a 'one-size-fits-all' approach to cyber security is unlikely to succeed.

Achievement of the strategic objectives will undoubtedly challenge capacity in some areas of policing, particularly in smaller forces where constrained funding and resources must be prioritised towards front-line policing. In this case, more use will be made of centrally provided cyber security services, alleviating some of the need to recruit and retain skills locally and removing single points of failure, whilst still retaining critical local contextual knowledge of information, systems, and the digital attack surface.

In areas of policing that have the capacity and scale to warrant local cyber security capability, this will be maintained. However, these forces will still be able to leverage and benefit from nationally developed solutions, services, and best practices, to achieve consistent outcomes across policing.

## Strategic Priority 1: Alignment between cyber security and policing outcomes

Organisations increasingly acknowledge that the benefits associated with effectively protecting information extend well beyond simply complying with legislation. Stakeholders' confidence, in particular the willingness to share data, is increasingly influenced by their perception of how well that data will be protected. At a time where there has never been a greater need for public trust and confidence in policing, along with an ever increasing operational dependency on digital capabilities, there is a clear link between policing's ability to maintain and improve its own cyber resilience and the achievement of wider policing outcomes and public trust.

Chief officers posing the timely question **'Is this secure?'** will encourage the necessary behavioural change to enable growth in the maturity of cyber security across policing. This alone is an essential precursor to all strategic priorities and associated transformation proposals.

To enable this, policing leaders will be equipped with education and data related to cyber risk. This includes:

- timely and effective information risk training, that provides the requisite knowledge to correlate information and cyber risks to downstream operational risks and policing outcomes;

- access to skilled and knowledgeable information and cyber risk specialists to provide trusted counsel;
- information and cyber training and education to be incorporated into the long-term training pathways for future chief officers;
- timely, relevant, and consistent cyber security risk data that enables informed decision making; and
- an appropriate and consistent set of metrics and measures relating to cyber resilience incorporated into local, regional, and national governance and reporting.

Improvement in these areas will enable chief officers and other senior leaders with accountability and responsibility for information risk, to be better informed, understand the impact on operations of an information risk materialising, and be more confident in providing the decisions required to protect operational policing activities from cyber disruption.

## Strategic Priority 2: Skilled, engaged and empowered cyber security personnel

Achieving this Strategy's vision and objectives will not be possible without appropriately skilled people operating at all levels and across all policing organisations.

Policing will be an attractive choice of employer for new and established cyber security professionals looking to build their careers. Competition for cyber talent is fierce, however as an employer, policing provides a unique, challenging and rewarding proposition for applicants.

To establish and maintain a competent and capable cyber security community, policing will establish:

- a positive working culture that values the importance of the cyber role and recognises its successes;
- flexible working arrangements (where appropriate) that meet both employee and employer needs;
- clear opportunities for career progression, both locally and nationally across policing and the public sector;
- a fair rate of compensation, that reflects the level of demand for competent cyber security and risk professionals and is consistent across policing;
- training and developing our cyber security and risk professionals to become and remain an effective and efficient first line of defence against our adversaries;
- a positive profile in the cyber security talent market, where policing is seen as a great place to work, learn and develop, with excellent career prospects and somewhere you can make a difference;
- a supportive environment where cyber security and risk professionals have access to experienced and knowledgeable professionals, who can guide, coach and mentor them during their working life with policing; and
- a cyber community, to provide a sense of belonging, and a support network of peers, for sharing challenges and successes, and a comprehensive living knowledge base.

To achieve an appropriate and sustainable level of demand placed on cyber security and risk personnel, force-level cyber security operating models will leverage national capability wherever this is possible and practical to do.

## Strategic Priority 3: Operational consistency

Cyber security is achieved through the consistent delivery of internationally recognised controls. To effectively realise these control objectives, policing must maintain clear definitions on how they are achieved in both a local and national context.

Rather than continuing to work in isolation across forces, policing will move towards a common set of cyber security policies, standards, processes, procedures, patterns, and guidelines that are:

- simplified;
- documented;
- normalised;
- integrated;
- repeatable; and
- consistent.

Furthermore, these artefacts will be:

- readily available to the communities that need them, through shared platforms;
- maintained, kept up to date, and continuously improved by subject matter experts, including representatives from forces;
- relevant to the people, data, systems, and environments they are written to protect; and
- demonstrably utilised in the protection of policing's information.

This will create efficiency by removing duplication of effort, enable local Information Security Officers to focus on their most pressing local priorities and achieve a level of consistency and maturity across policing.

As processes and procedures mature, they will increasingly enable automation and orchestration of operational cyber activities.

## Strategic Priority 4: Nationally aligned technical capabilities

Technology will play a significant part in achieving the objectives defined in this Strategy, primarily by maximising policing's value from technologies specifically designed to provide protection from cyber security threats.

The market is awash with cyber security technology solutions. Significant time and resources are required to evaluate, assure, and select technology solutions, in addition to ensuring secure configuration and deployment.

Policing will work collaboratively regarding the selection, deployment, and operation of cyber security technology. The development of a nationally agreed catalogue of technology solutions and its broad adoption across policing will improve efficiency and economy through:

- aggregated procurement volumes, achieving great economies of scale;
- national product assurance positions that can be re-used across policing;
- common and repeatable configuration and deployment practices;
- design, development, and deployment following Secure by Design methodologies;
- enabling automation and orchestration of processes and procedures;
- ensuring that technology solutions are integrated with policing's security monitoring and detection capabilities;
- use of proven solutions that provide a robust cyber defence capability for policing;
- supporting operational and risk reporting in real-time, where possible;
- increasing cyber visibility and cyber situational awareness through integrated capabilities;
- enabling intelligence-led prevention and detection through focusing on a reduced technology footprint; and
- improving policing's ability to respond quickly and effectively in the event of a cyber incident through common awareness of tooling and capabilities.

## Strategic Priority 5: Nationally available services

There is a subset of activities needed to underpin the outcomes described in this Strategy that for many police forces can be more effectively and economically consumed as a service rather than delivered using in-house resources.

To avoid forces duplicating effort by going to market for these services independently, a subset of these identified services will be delivered as national services to policing, building on the model already established with PDS NMC.

Policing will build a portfolio of effective, efficient and value for money services that can be consumed by forces, reducing siloed working, and freeing up valuable local cyber security resource to focus on local activities that cannot be addressed at a national level.

Policing will specifically look to develop national cyber security services that enable:

- optimal utilisation of investment in people and technology, through economies of scale and consistency of operational practices;
- intelligence-led outcomes across all service areas;
- continuous improvement of the speed to protect, detect and respond;
- consistent risk assessment and risk management across key services;
- more effective integration with the broader government cyber security functions, with clear lines of accountability and responsibility;
- improved collaboration with industry partners to improve cyber resilience and gain early insights into threats that may impact policing; and
- policing to 'Defend as One'.

# MEASURING SUCCESS

## Realisation of our vision of '*Policing functions are resilient to cyber-attack, maintaining public trust and confidence in policing services*', will be achieved through successfully delivering the five objectives listed in this Strategy document.

Delivery of the strategic priorities will contribute to the achievement of these objectives. It is believed that the implementation of the strategic priorities will lead to cost efficiencies and cost avoidance through economies of scale and write once for the benefit of many principle. These are, however, difficult to measure as the baseline data is not available today.

Policing does have baseline data in the form of SyAP scores. These provide the current maturity state for policing's cyber security controls and will be the primary measure of this Strategy's success.

SyAP data, along with other information security risks will be provided to the PIAB, which will have a significant role in tracking progress and steering policing to increased cyber maturity.

## What is SyAP?

Security Assurance for Policing, better known as SyAP, was introduced in 2022 as a replacement for the Governance & Information Risk Return (GIRR) and legacy Codes of Connection (CoCo). Like the wider GovAssure scheme, it is aligned to the NCSC's Cyber Assurance Framework (CAF) and also aligns to the National Institute of Standards and Technology Cyber Security Framework (NIST CSF).

All policing entities that provide or connect to national systems are required to self-assess using SyAP. With a maturity matrix of 0-5, rather than the GIRR's red, amber, green ratings, it provides greater granularity of the cyber and risk positions of policing entities.

It is run by the PDS Cyber Services Audit, Risk and Compliance Team and provides a single point of contact for each organisation and national system, fostering continuous improvement through a collaborative approach.

The success of this Strategy will primarily be measured through an increase in the SyAP maturity ratings.

## Additional measures

The table below illustrates which objectives are met by each strategic priority and details additional measures.

**List of objectives (as set out in the Strategy)**

1. Manage cyber security risk
2. Protect against cyber attack
3. Detect cyber security events
4. Minimise the impact of cyber security incidents
5. Develop the right cyber security skills, knowledge and culture

| STRATEGIC PRIORITY | | | | |
|---|---|---|---|---|
| **Alignment between cyber security and policing outcomes** | **Skilled, engaged and empowered cyber security personnel** | **Operational consistency** | **Nationally aligned technical capabilities** | **Nationally available services** |
| **Manage cyber security risk** | | | | |
| ✓ | ✓ | ✓ | ✓ | ✓ |
| **Protect against cyber attack** | | | | |
| ✓ | ✓ | ✓ | ✓ | ✓ |
| **Detect cyber security events** | | | | |
| ✓ | ✓ | ✓ | ✓ | ✓ |
| **Minimise the impact of cyber security incidents** | | | | |
| ✓ | ✓ | ✓ | ✓ | ✓ |
| **Develop the right cyber security skills, knowledge and culture** | | | | |
| ✓ | ✓ | | ✓ | ✓ |
| **Measurements** | | | | |
| % SIROs completing training.<br>% SIROs attending PIAB. | Implementation of people related transformation proposals.<br>% Improvement in Cyber Security Personnel.<br>% Improvement in skills base. | % Core Cyber Standards available to forces.<br>% Core Processes & Procedures available to forces.<br>% adoption of the above by forces.<br>Operational effectiveness. | Implementation of technical proposals.<br>Additional measurement will be defined as part of proposal deliverables. | Implementation of services proposals.<br>Additional measurement will be defined as part of proposal deliverables. |

# IMPLEMENTING THE STRATEGY

**The delivery of the objectives and priorities detailed in this Strategy, will require pragmatism to achieve a vision where cyber security practices implemented with policing are proportional to the threats it faces. It will also require investment and a business case that will follow this Strategy to secure the necessary funding.**

This section will cover the recommended transformation proposals, a high-level implementation plan, and the proposed governance model.

## Transformation proposals

The following 17 proposals have been designed to address the requirements of policing today, as illustrated in the strategic outcomes. Some of these proposals are already in development but have been included here as, when delivered, they will contribute to the achievement of the objectives of this Strategy.

Across policing there are already many examples of notable practices that have the potential to be leveraged on a wider scale. There are also examples outside of policing, such as initiatives driven by the Cabinet Office via their Cyber Skills Programme.

Except for the few that are already at some stage of development, the proposals are just that – proposals. A programme of work will be built around this Strategy and the subsequent business case, with the goal of delivering it. Each proposal will be required to consider the best approach to its delivery, whether it be the expansion of some good work already done in a force, or the creation of a new national service. For those which require more specialist resources or for those areas where recruitment and retention could be problematic, this could be an outsourced model.

The **Government Cyber Security Strategy 2022 to 2030** calls for critical systems to be resilient to cyber attack by 2026. All the proposals will, in some way, improve resiliency, and the proposed implementation plan has been structured to deliver this element of the Government Strategy for critical policing systems.

| **STRATEGIC PRIORITY:** *Alignment between cyber security and policing outcomes* | | |
|---|---|---|
| **TRANSFORMATION PROPOSAL** | **DETAIL** | **BENEFITS** |
| ***Cyber Services Training Framework**** | Deliver refreshed training for SIROs, ISOs and IAOs, fit for modern policing, and in a way that can be consumed efficiently and effectively by busy officers and staff. The people holding the three key roles will be better equipped to handle their responsibilities. | The ability for leaders to have a better understanding of the impact on operational services through the materialisation of cyber risks, will lead to more effective resource allocation (funding and personnel), better detection of threats, increased protection, and reduced impact. |
| ***Enhanced training from the College of Policing*** | The College of Policing have a central role in the training of all officers, from guidance on how things are done, to delivering their own courses.<br>Working with the College of Policing to build cyber security into the syllabi and course content from the start of officers' careers, will enable them to consider cyber implications on operational activities by default. | Increasing cyber security knowledge and awareness across policing ensures that cyber security is actively and continuously taken into consideration, reducing the human risk factor.<br>Policing will develop a cyber security culture that empowers its people to learn, question and challenge, thereby enabling continuous improvements in behaviours that contribute to improved cyber hygiene. |

**Note**

*Work is already underway on this deliverable, but it is included in this Strategy for awareness. This applies to deliverables, marked out in the same way, throughout this section of the Strategy.

| **STRATEGIC PRIORITY:** *Skilled, engaged and empowered cyber security personnel* | | |
|---|---|---|
| **TRANSFORMATION PROPOSAL** | **DETAIL** | **BENEFITS** |
| ***Cyber Support Function*** | Design, build and recruit a centrally managed, geographically diverse team of experienced senior cyber staff that will:<br>• provide ISO cover for forces;<br>• work with forces to develop Cyber Operating Models aligned to their requirements;<br>• develop nationally consistent cyber role descriptions to meet forces' cyber needs, incorporating the work of the UK Cyber Security Council;<br>• support the recruitment of cyber professionals;<br>• develop and maintain baseline Training & Development plans for the policing cyber community; and<br>• support, coach and mentor the policing cyber community.<br><br>Develop a cyber toolbox for use with forces. For example, templated target cyber operating models and a library of common cyber role descriptions, standards, processes, and procedures. | Cyber security skills requirements will be understood and continuously developed, ensuring policing has a skilled cyber workforce that can competently manage cyber threats.<br><br>By continually investing in the people, policing will attract and retain the diverse workforce it needs for resilience.<br><br>Having skilled, knowledgeable, and well-trained cyber professionals, will ensure policing can optimise the benefits of its cyber tooling in protecting its networks, systems, applications, and end points. This will reduce cyber risks and gain improved return on investment, through a more effective use of cyber solutions and services. |
| ***CyberNet*** | Design, build and deploy an online hub for the policing cyber community to:<br>• access policies, standards, processes, procedures, guidelines, methodologies, and templates;<br>• provide a hub for the policing cyber community to communicate and share challenges and successes; and<br>• share cyber career opportunities across the policing sector. | Ease of access to cyber colleagues and readily available best practice documentation and advice will improve the effectiveness and efficiency of our cyber personnel.<br><br>Availability of career opportunities across policing will significantly contribute to the retention of the cyber workforce. |
| ***NPTC People Group Retention Workstream**** | Work with National Police Technology Council (NPTC) People Group Retention Workstream to ensure cyber roles are adequately represented. Support the Workstream with achieving its outcomes aligned to the people strategic objective, which will benefit all personnel within its scope. | Policing will attract and retain the diverse cyber security workforce that it needs to be resilient. |

| STRATEGIC PRIORITY: *Operational consistency* | | |
|---|---|---|
| **TRANSFORMATION PROPOSAL** | **DETAIL** | **BENEFITS** |
| ***Policy & Standards Acceleration*** | Secure a temporary dedicated team, to create a comprehensive base set of standards, that cover the bulk of controls required to meet the SyAP control objectives. Existing governance will be followed for approval of any new standards.<br><br>Design, select and build a solution for the hosting, management and searching of cyber policies and standards, e.g. a 'Cyber Wiki'. Ensure the current Policy and Standards (P&S) function is adequately resourced to maintain the policies and standards required for policing, ensure lessons are learned and factor in the rapidly changing cyber landscape for the P&S product set. | Comprehensive standards aligned to industry best practice will allow technologies to be appropriately configured, with standard profiles for common technology and architectures being developed and continuously updated.<br><br>A fit for purpose hosting service will increase efficiencies through ease of access to all resources. |
| ***Process & Procedures Creation*** | Define and document a set of common processes and procedures, that can be used and adopted by policing entities. Examples include, but are not limited to:<br>• Secure by Design (SBD) methodology for policing entity use; and<br>• Identity and Access Management (IDAM) Framework.<br><br>Further processes and procedures will be developed and deployed alongside other proposals within this table. | Adopting a common approach to SBD will ensure that appropriate and proportionate cyber security measures, are embedded in the technology used by policing, and that the security of digital services is continually assured throughout their lifecycle.<br><br>Cyber security controls commensurate with their risk profile and, where appropriate, in accordance with national agreed standards will ensure that risks to their operational functions are managed proportionately. Common and consistent processes and procedures will reduce the necessity for locally developed inconsistent processes and procedures, saving time and resources, and reducing risk. |
| ***ISRMF and ISRAG Deployment**** | Work with forces to deploy the recently approved Information Security Risk Management Framework (ISRMF) and Information Security Risk Assessment Guidance (ISRAG) consistently across the policing community.<br><br>Develop and deploy an information security risk management tool for collation and management of these kinds of risks for use by forces. This will also provide a national view of information security risk. | Decision makers at all levels of policing will have visibility of and timely access to relevant and actionable risk data that enhances their ability to make effective risk management decisions, which could impact on operational activities.<br><br>Policing will have a consistent taxonomy for risk management, providing consistency and easier comparisons. |

| STRATEGIC PRIORITY: *Nationally aligned technical capabilities* | | |
|---|---|---|
| **TRANSFORMATION PROPOSAL** | **DETAIL** | **BENEFITS** |
| **Roadmap & Catalogue*** | Continue the work already underway (supported by PDS) to identify current cyber technology stacks used across policing to create a cyber solution catalogue. The roadmap and catalogue will seek to:<br>• gather policing requirements to ensure suitable cyber solutions are selected for use across policing;<br>• build the cyber solutions list within the catalogue in a prioritised order that provides greatest benefit to policing from a risk reduction perspective;<br>• take a 'once for the benefit of many' approach to cyber solution selection;<br>• benefit from cost savings by economies of scale through selecting cyber solutions at a national level;<br>• assure solutions once for policing, for use by many forces;<br>• reduce future force deployment timeframes, by negating the need for local tender processes and supplier assurance and by providing deployment patterns, operating processes and procedures; and<br>• provide downstream efficiencies, with normalised cyber solutions, that will enable centres of excellence for support and simplified protective monitoring set-up. | Policing will work with strategic partners in the private sector in a more pragmatic way to further enhance proactive defence capabilities across policing.<br><br>This approach will provide significant savings in time, resources and costs in the selection, purchase, and deployment of future cyber solutions. This will ensure a more effective use of the resources available to manage cyber risk. |
| **Automated compliance checking** | Design, select and build an automated compliance checking solution that enables forces to check that their technical implementations are consistent with current and future blueprints and patterns.<br>The solution will:<br>• monitor and test compliance against agreed configurations (blueprints/patterns);<br>• notify forces of deviations, to enable prompt remediation or risk acceptance;<br>• help to reduce manual checking;<br>• reduce the risk of uncontrolled drift from the assured blueprints and patterns; and<br>• provide both a local and national view of compliance. | Policing will be able to check that technology is appropriately configured, in line with current and future standards, as architectures are being developed and continuously updated, ensuring policing is not exposed to unnecessary risk. |

| **STRATEGIC PRIORITY:** *Nationally available services* | | |
|---|---|---|
| **TRANSFORMATION PROPOSAL** | **DETAIL** | **BENEFITS** |
| **Cyber Education and Awareness (E&A)** | Design and develop a service that delivers a policing specific set of E&A materials centrally, which can be consumed and delivered locally by policing entities. This will include both mandatory information security training for officers and staff, and a set of targeted cyber materials for rolling campaigns throughout the year.<br><br>The service will ensure the materials are maintained and remain relevant to policing and the evolving threat landscape.<br>Similarly, additional training for privileged users and for those likely to be targets of whaling and spear-phishing attacks could be provided through the same means. | Sufficient cyber security knowledge and awareness across policing's professional functions will ensure that cyber security is actively taken into consideration, reducing the risk of cyber related incidents.<br><br>Cyber resources can be focused on the delivery and effectiveness of the education and awareness, rather than its creation, ensuring more effective use of cyber resources.<br><br>Selecting one solution/service for all of policing ensures increased economies of scale and, therefore, improved value for money. |
| **Vulnerability Management Enhancement*** | Design, build and deploy a near real-time vulnerability and scanning management service, which can be applied to both local and national systems, to provide a joined-up view of vulnerabilities, and allow policing to take a more structured and strategic approach to addressing those vulnerabilities.<br><br>The solution will also provide the National Management Centre (NMC) with visibility to allow for enhanced monitoring and alerting for high priority issues. | Policing will have comprehensive visibility and understanding of its digital assets enabling it to identify and manage vulnerabilities and the cyber security risks they present.<br><br>Additionally, it will provide the necessary visibility of vulnerabilities to make effective decisions and the confidence that it has appropriate cyber security measures in place to manage the risks to its operational functions.<br><br>Shared capabilities, tools and services will tackle 'common' cyber security issues at scale. |

| STRATEGIC PRIORITY: *Nationally available services* | | |
|---|---|---|
| **TRANSFORMATION PROPOSAL** | **DETAIL** | **BENEFITS** |
| **Third Party Assurance for Policing (TPAP)*** | Build upon the current TPAP proof of concept and deploy a national third-party assurance platform, accessible to all forces.<br>Develop and deploy a training and certification program to ensure policing has sufficient numbers of trained cyber specialists to conduct and maintain assurance of third-party suppliers to policing.<br>Develop and build the necessary operating model and team to support and maintain the ongoing management of the TPAP service. | Policing will better understand and manage the risks emanating from third parties, including commercial suppliers, partners, and consumers of policing systems.<br>Policing will have comprehensive visibility of the data it shares with third parties, so that it can appropriately assess and respond to the risks it presents. |
| **Security Testing** | Design, develop, build, and deploy a range of security testing services to enhance vulnerability identification.<br>Services will include:<br>• a national IT Health Check and Penetration Testing service, where policing entities can request testing services without the need to go to tender; and<br>• a 'Red Team' service of highly skilled penetration testers who can test policing systems real-time, outside of normal testing cycles, with the latest tools, techniques and processes that are used by our adversaries. | Comprehensive, regular, and robust security testing will provide further visibility of cyber vulnerabilities, enabling policing to assess the risk and take appropriate action to reduce that exposure in a timely fashion.<br>A dedicated service within policing means that the testers will be familiar with policing and its systems, allowing for more context to be derived from the testing.<br>A 'Red Team' can react quickly to threat landscape changes, looking for any exposure to policing systems, complementing the national vulnerability management solution and further reducing risk exposure. |

| STRATEGIC PRIORITY: *Nationally available services* | | |
|---|---|---|
| **TRANSFORMATION PROPOSAL** | **DETAIL** | **BENEFITS** |
| **Cyber Incident Response Improvement** | This proposal will look at 3 areas of Cyber Incident Response (CIR):<br>1. Cyber Incident Response Plan (CIRP) Testing<br>2. Advanced CIR Team<br>3. Cyber Insurance<br><br>1. Design and develop a service that delivers a policing specific set of CIRP materials centrally, which can be either consumed locally by policing entities, where skills and knowledge is available, or delivered locally from the centre, where necessary. The service will provide:<br>• CIRP templates;<br>• CIRP testing materials;<br>• CIRP testing processes and procedures; and<br>• CIRP testing delivery services, including reporting, improvement recommendations and tracking.<br><br>2. Design and implement a service that goes beyond PDS NMC current capability for Cyber Incident Response. The service needs to be accredited by the NCSC and will provide advanced cyber investigative capability in the event of a serious incident.<br>Today, forces are either individually agreeing third party contracts for this type of service or purchasing in the event of an incident, when there is no opportunity to negotiate.<br>This service seeks to provide a cost-effective national capability for use by all of policing.<br><br>3. Review policing's cyber insurance requirements, identify and implement a national cyber insurance offering that represents value for money for policing and reflects policing's current cyber maturity. | Policing will be fully prepared to respond to cyber incidents, through people, process, and technology, via an appropriate schedule of testing and rehearsal, enabling policing to respond more effectively to future incidents, reducing the impact on policing operational capability.<br><br>Lessons learned from cyber incident response testing will drive improvements in cyber security across the whole of policing.<br><br>Policing will have the optimum services in place to allow it to be fully prepared to respond to cyber incidents. This will enable policing to respond to cyber incidents more rapidly, using a coordinated and consistent local and national response and recovery process.<br><br>Policing will be in a better position to restore systems and assets affected by cyber security incidents and resume the operation of its functions with minimal disruption.<br><br>Policing will have an insurance policy, that is tailored to its current cyber maturity and provides value for money. |

| **STRATEGIC PRIORITY:** *Nationally available services* | | |
|---|---|---|
| **TRANSFORMATION PROPOSAL** | **DETAIL** | **BENEFITS** |
| **Advanced Detection Capabilities** | Review current Cyber Threat Intelligence capability and identify opportunities to move policing from a reactive to a proactive detection stance.<br><br>Work with industry experts to assist in the development of the above.<br><br>Policing will work with organisations such as the Government Cyber Coordination Centre and Scottish Cyber Coordination Centre to enhance detection capabilities throughout the public sector. | Advancing policing's detection capabilities to inform and enhance prevention will reduce the percentage of successful breaches against the number of attempts. This will in turn, reduce the potential number of cyber incidents and related costs that need to be managed, across policing. |
| **Strategic Partnership Coordination** | Formalise an engagement plan to ensure policing has a coordinated approach to working with partners in the public, private and academic sectors.<br><br>Policing will identify and work with strategic partners and industry groups to help remain at the forefront of cyber resilience. | Strategic partnerships with the private, public and academic sectors, and industry groups will be further embedded into the policing ecosystem to enhance proactive defence. |

Adopting a common approach to 'Secure by Design' will ensure that appropriate and proportionate cyber security measures are embedded within the technology used by policing

# IMPLEMENTATION PLAN

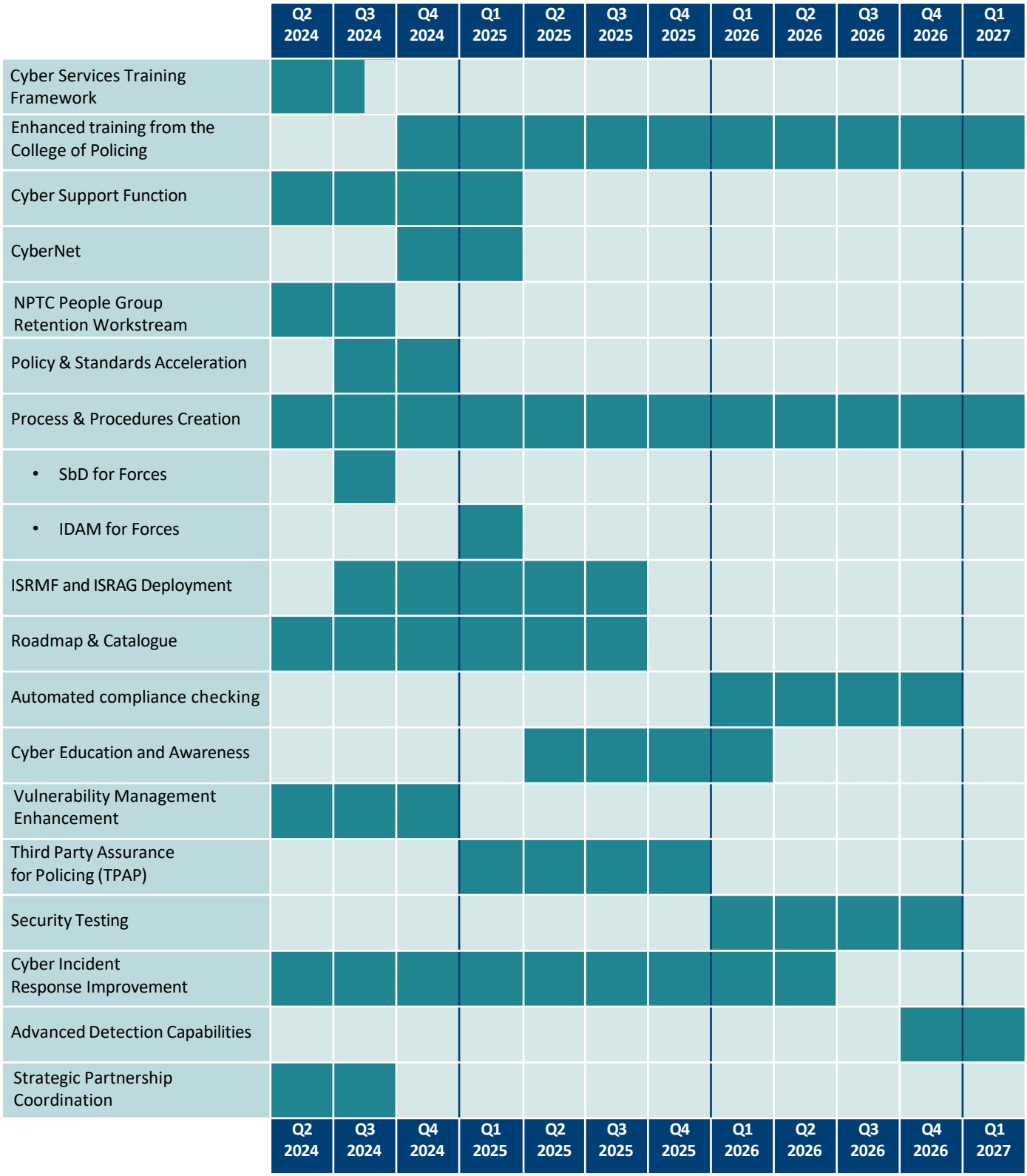
**The diagram on the next page, shows an indicative plan to deliver each of the transformation proposals. It has been designed to allow for each proposal to be implemented within the 3-year period covered by this Strategy. All of these proposals are subject to the availability of resources to deliver and many are subject to funding applications being approved, so consequentially could have start dates moved.**

The plan starts with the work that is currently ongoing, plus those proposals that provide pre-requisites or a foundation for others to build from. The remainder have been prioritised and staged to start at an appropriate point, aligned with the necessary funding periods and resource availability.

While it is possible to condense the timescales and deliver all the proposals quicker, subject to funding and resources being available, it is felt that forces would not be able to adopt the outputs at such a pace. As such, spreading them over the Strategy period, allows forces to adopt them at a pace more appropriate to their capability and capacity.

The bars on the diagram show the approximate timeframes needed to design and implement. The majority will then transition into a business as usual (BAU) service which is not shown in this diagram.

# High level indicative plan



## Governance

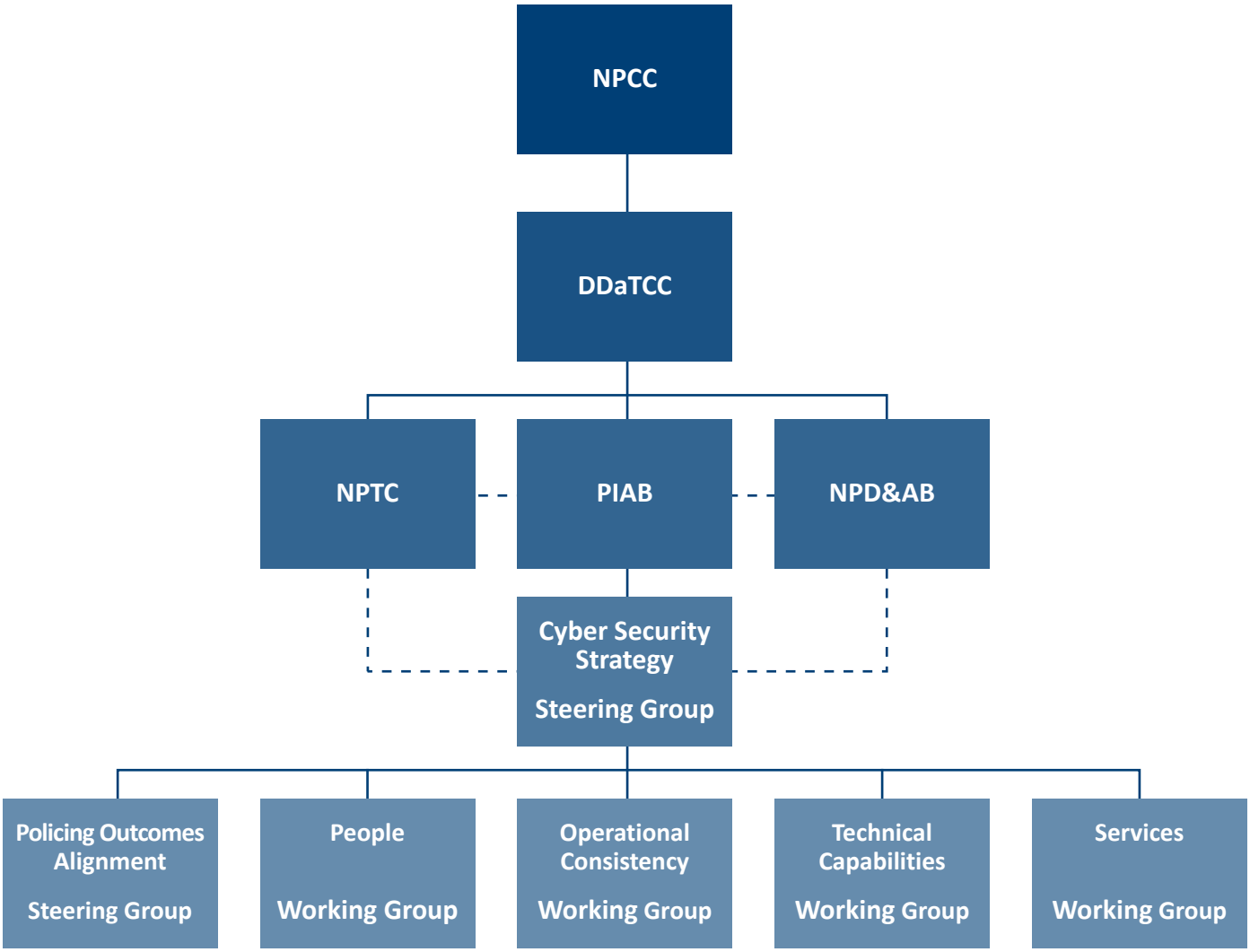
This Strategy seeks to drive an uplift in the maturity of cyber security across policing. To achieve this vision, strong governance will be required to direct, support and track progress.

Ultimate accountability for this Strategy sits with the NPCC. The sub governance groups of the DDaTCC will provide specialist know-how within their fields of expertise. The National Police Technology Council, National Police Data and Analytics Board and Police Information Assurance Board operate with mutual influence, supporting DDaTCC in driving delivery against the strategic objectives.

To support these committees and boards, a 'Cyber Security Strategy Steering Group' will be created to provide direct oversight of the implementation of the Strategy. The Steering Group will be responsible for reporting to the higher-level committees and board.

Day to day management of the Strategy workstreams will be managed by Cyber Security Strategy Working Groups, aligned to the five strategic priorities.

The Cyber Security Strategy Steering Group will have senior representation from across policing, and other key organisations, such as the APCC and the Home Office, whilst the working groups will require a more hands on level of participation, with knowledge and expertise in the areas of strategic priority.



## Glossary

| | |
|---|---|
| **APCC** | The Association of Police and Crime Commissioners |
| **BAU** | Business as Usual |
| **CAF** | Cyber Assessment Framework |
| **CIRP** | Cyber Incident Response Plan |
| **CIRT** | Cyber Incident Response Team |
| **CoP** | College of Policing |
| **DDaTCC** | Digital, Data and Technology Coordination Committee |
| **E&A** | Education and Awareness (Training) |
| **GIRR** | Governance and Information Risk Return |
| **HMICFRS** | His Majesty's Inspectorate of Constabulary and Fire & Rescue Services |
| **IAO** | Information Asset Owner |
| **ICT** | Information and Communications Technology |
| **ISO** | Information Security Officer |
| **ISRMF** | Information Security Risk Management Framework |
| **NCA** | National Crime Agency |
| **NCCU** | National Cyber Crime Unit |
| **NCSC** | National Cyber Security Centre |
| **NMC** | National Management Centre |
| **NPCC** | National Police Chiefs' Council |
| **NPD&AB** | National Policing Data & Analytics Board |
| **NPTC** | National Police Technology Council |
| **NSIRO** | National Senior Information Risk Owner |
| **OCiP** | Operational Communications in Policing |
| **P&S** | Policy and Standards |
| **PDS** | Police Digital Service |
| **PIAB** | Police Information Assurance Board |
| **SIRO** | Senior Information Risk Owner |
| **SME** | Subject Matter Expert |
| **SyAP** | Security Assurance for Policing |
| **TOM** | Target Operating Model |
| **TPAP** | Third Party Assurance for Policing |

# APPENDICES

## Appendix 1 – Mapping of Transformation Proposals to Strategic Objectives

**Mapping of proposals to objectives**

| | OBJECTIVES | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | MANAGE | | | | | | | | PROTECT | | | | | DETECT | | | MINIMISE | | | | DEVELOP | | | | |
| | Outcomes | | | | | | | | | | | | | | | | | | | | | | | | |
| **PROPOSAL** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **1** | **2** | **3** | **4** | **5** | **1** | **2** | **3** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **5** |
| Cyber Services Training Framework | x | | | | | | | | | x | | | x | | | | x | x | | | x | x | x | x | x |
| Enhanced Training from the College of Policing | x | | | | | | | | | | | | x | | | | x | x | | x | | | x | x | x |
| Cyber Support Function | x | | | x | x | | x | | x | x | | x | x | | | | x | | x | x | x | x | | x | |
| Cybernet | | | | | x | | x | | x | x | | | | | | | | | | | | x | | | |
| NPTC People Group Retention Workstream | | | | | | | | | | | | | | | | | | | | | x | x | x | x | x |
| Policy & Standards Acceleration | | x | x | | | | x | | x | x | x | | x | x | | x | | | x | x | | | | | |
| Process & Procedures Creation | x | x | x | | x | x | x | | x | x | x | x | | x | | x | x | x | x | x | | | | | |
| ISRMF Deployment | x | x | x | x | | x | x | | x | x | | | | | | | | | | x | | | | | |
| Roadmap & Catalogue | | x | | | | | | x | | | x | x | | | | | | | | x | | | | | |
| Automated Compliance Checks | | x | | | | x | x | | | x | x | x | | x | x | x | | | | | | | | | |
| Cyber Education & Awareness | | | | | | | | x | | | | | | | | | x | x | | x | x | x | x | x | x |
| Vulnerability Management Enhancement | | x | | | | | x | | | | x | x | | x | x | x | x | | | x | | | | | |
| Third Party Assurance for Policing (TPAP) | | x | x | x | | x | x | x | | x | | x | | | | | x | | | x | | | | | |
| Security Testing | | x | x | | | x | x | | | | | x | | x | x | x | x | | | x | | | | | |
| Cyber Incident Response Improvement | | | | | | | | | | | | x | | | | | x | x | x | x | | | | | |
| Advanced Detection Capability | | | | | | | | | | x | | x | | x | x | x | x | x | | | | | | | |
| Strategic Partnership Coordination | | | | | | | | x | | | | | | | | | | | | | | | | | |

The above table provides an indication of which objectives and outcomes are addressed by each transformation proposal.

The full text for each objective and outcome can be found in 'Vision, Objectives and Outcomes', in the main body of this Strategy document.

# Appendix 2 – How this strategy was developed

## Initiation

The creation of a National Policing Cyber Security Strategy was requested by DDaTCC in response to the Government Cyber Security Strategy and the increasing cyber threat to policing. The action to facilitate production of this Strategy was assigned to the Police Digital Service (PDS).

## Consultation

Under the oversight of a steering group comprised of representatives from NPTC, PIAB and PDS, during June and July 2023, PDS conducted thirty-nine half-day workshops with representatives involved in the delivery of cyber security outcomes across policing. A full list of organisations involved in the workshops is shown below. Workshops were well attended by forces' Information Security Officers and Heads of ICT, with 98% of invited organisations accepting and attending the workshops.

The workshops focused on policing's current cyber security maturity and the steps needed to improve it for the five specific objectives set out in the **Government Cyber Security Strategy 2022 to 2030**:

1. manage cyber security risk;
2. protect against cyber attack;
3. detect cyber security events;
4. minimise the impact of cyber security incidents; and
5. develop the right cyber security skills, knowledge and culture.

Specifically, the workshops' participants were asked the following questions in relation to each of the government objectives:

**How well do you think we're achieving this objective, both locally and nationally?**

**Please provide an estimated score for national SyAP (0-5) and explain why you provided that estimate.**

**What SyAP (0-5) score do you think we should be achieving nationally for this objective?**

**Where we fall short of this, how do you think we could collectively improve our capability?**

*Note - The SyAP (Security Assurance for Policing) maturity ratings, currently used by forces, were used as a common taxonomy for the workshops.*

The following organisations took part in the workshop discussions or consultations:

Avon and Somerset Police

Bedfordshire, Cambridgeshire & Hertfordshire police forces

British Transport Police

Cheshire Constabulary

City of London Police

Civil Nuclear Constabulary

Cleveland Police

College of Policing

Counter Terrorism Police

Cumbria Constabulary

Derbyshire Constabulary

Devon, Dorset & Cornwall Police

Durham Constabulary

Dyfed-Powys Police

Gloucestershire Constabulary

Greater Manchester Police

Guernsey Police

Gwent Police

Hampshire and Isle of White, and Thames Valley police forces

HMICFRS

Humberside Police

Isle of Man Constabulary

Kent and Essex police forces

Lancashire Constabulary

Leicestershire Police

Lincolnshire Police

Merseyside Police

Metropolitan Police Service

National Crime Agency

NCSC

Norfolk & Suffolk police forces

North Wales Police

North Yorkshire Police

Northamptonshire Police

Northumbria Police

Nottinghamshire Police

Police Scotland

Police Digital Service

Police Service of Northern Ireland

Royal Gibraltar Police

South Wales Police

Scottish Police Authority South

Yorkshire Police

Staffordshire Police

States of Jersey Police

Surrey and Sussex police forces

Warwickshire Police

West Mercia Police

West Midlands Police

West Yorkshire Police

Wiltshire Police

## Drafting

Drafting of the Strategy took place during July and August 2023, incorporating ideas and feedback that had been captured during the consultation process. The first draft of the Strategy was shared with the steering group in August and was subsequently shared with NPTC and PIAB for review in September and October 2023 respectively.

## Stakeholder engagement

Throughout the consultation, development and writing of the Strategy the National Policing Cyber Security Strategy Team have kept informed and sought opinion from multiple stakeholders, which have included:

- APCC
- Ministry of Justice
- Blue Light Commercial
- Crown Prosecution Service
- NCA
- Capability Reform Unit
- NPD&AB
- PIAG
- Home Office Cyber Security (HOCS)
- NCSC
- Scottish Police Authority (SPA)
- Cabinet Office
- HMICFRS
- OCIP & Business Change Council
- PIAB
- DDaTCC

## Final approvals

The National Policing Cyber Security Strategy Team have sought support and/or approval from:

| BODY | STATUS | DATE |
|---|---|---|
| National Policing Cyber Security Strategy Steering Group | Approved | 15 Sept. 2023 |
| NPTC | Supported | 28 Sept. 2023 |
| PIAB | Supported | 12 Oct. 2023 |
| DDaTCC | Supported | 5 Dec. 2023 |
| NPD&AB | Supported | 11 Jan. 2024 |
| NPCC | Approved | March 2024 |


POLICE
DIGITAL
SERVICE


NPCC
National Police Chiefs' Council