Ministry of Justice

Cyber Security Strategy

2023 - 2028

September 2023

Contents

Foreword

At the Ministry of Justice (MoJ), we protect sensitive data to deliver crucial work for citizens. This includes information on victims of crime, on those in the prison and probation system, on our own staff, and information involving thousands of organisations with whom we work with across the justice system.

The ambition of our Digital Strategy 2025[1], to make MoJ the most data-led and digital Department, means that our dependence on technology is increasing. Building our resilience against cyber-attacks is a challenge for everyone in the Department. We must work together to use the skills and knowledge from across the Department, and our partners, to keep our services secure.

I am pleased to introduce the new MoJ Cyber Security Strategy which outlines our ambition to be government-leading in the provision of secure services.

Our strategy is focused on threats we are most likely to face, and the most critical technology systems that the MoJ rely on. The strategy is not just about technical security measures, it is also about having the right people and the right culture in place to embed security into everything the Department does.

Antonia Romeo

Permanent Secretary, Ministry of Justice

September 2023

[1] https://www.gov.uk/government/publications/ministry-of-justice-digital-strategy-2025

Executive Summary

Vision and Aim

As a department, the Ministry of Justice (MoJ) has a unique role. Our organisation's size, complexity and the volume of sensitive information held and processed across our many IT systems, organisations, suppliers and partners present many security challenges. A successful cyber-attack places this data, and the vital work of the department at risk. Effective cyber resilience in all that the department does is vital to counter this threat.

The MoJ's Strategic Vision for Cyber Security

Every critical Justice service is resilient to cyber-attack.

The MoJ's Strategic Aim for Cyber Security

To embed 'Secure by Design' thinking into everything the department does, ensuring everyone working in Justice can confidently perform their security responsibilities.

Our intent is to set the context for the initiatives within this strategy in the coming years, and to establish an implementation programme to provide them.

Context

Strategic Context

The Government Cyber Security Strategy (GCSS)[2], published in 2022, sets out a bold vision to ensure core government functions are resilient to cyber-attack. The aim is that critical functions in government will be significantly hardened against cyber-attack by 2025, and the whole public sector will be resilient to known cyber-attacks no later than 2030.

The GCSS describes two pillars:

- To build **a strong foundation of organisational cyber security resilience** – requiring departments to have the right structures, mechanisms, tools and support in place to ensure that they can manage their cyber security risks. This will be underpinned by genuine accountability, so government has confidence in its cyber resilience, both at an organisational and cross-government level – through a programme known as "GovAssure".

- To '**Defend as One'** - harnessing the value of sharing cyber security data, expertise and capabilities across government to present a defensive force disproportionately more powerful than the sum of its parts.

This Cyber Security Strategy therefore seeks to support these ambitions by setting out the MoJ's vision, putting 'secure by design' at the heart of what we do within the department and across the wider justice sector. The key headlines are captured in Figure 1 below.

Figure 1 - strategic context

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf

Ministry of Justice Context

Like any organisation, the Ministry of Justice relies on an extensive range of technology systems, and tech-enabled processes and suppliers, to support our important services across the nation. We are entrusted with sensitive information on some of the most vulnerable people in society and must ensure that it is protected against cyber-attack wherever it is held and used in the justice community.

The MoJ technology landscape is complex and fragmented, both technically and organisationally. There are over 1000 IT services used to run large operational processes; under 100 are judged to be modern digital services. The legacy services have many different support models, commercial arrangements and rely on different underlying technology. Teams must make difficult priority decisions about operating existing systems, building required features, and undertaking security improvements; deferring investment in maintenance and support leads to vulnerabilities.

A vast number of spreadsheets, databases and applications are used to manage the work of the department. The department has over 350 terabytes of unstructured digital data, processes over 37 million emails a month, and has over 100 million files - excluding those in case management systems. This context is captured in Figure 2.

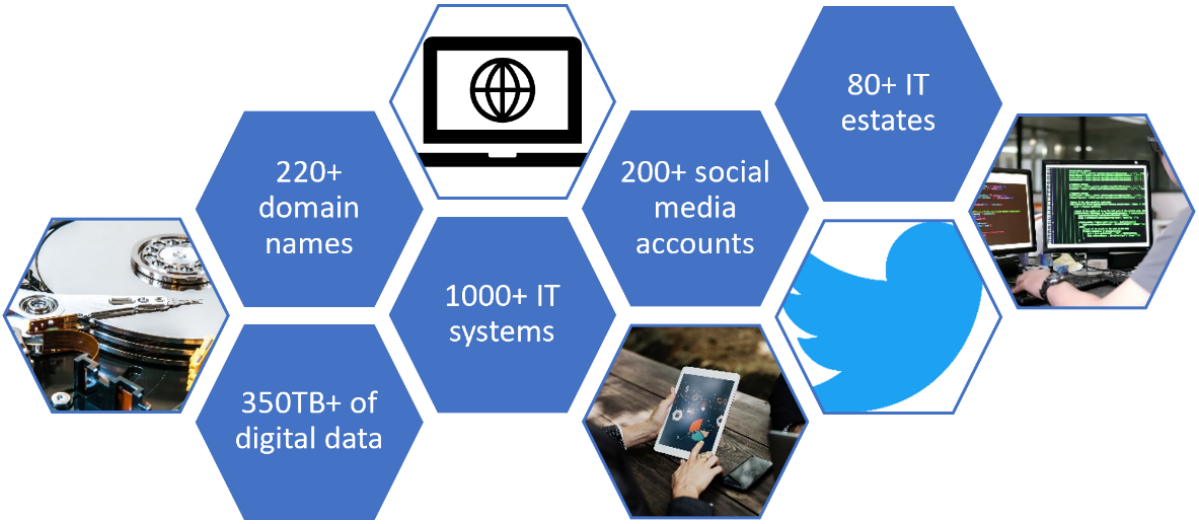


Figure 2 - scale of the challenge

Most of the cyber security threats the MoJ faces are not esoteric or exotic – they are the same challenges which large organisations worldwide deal with every day.

However, the unique nature of the MoJ's role in Government means there are more specific threats that need to be considered in some contexts. For example, the threats associated with deploying IT solutions into prison environments are ones that lack parallels in other departments. The In-Cell Technology programme (where prisoners have access to laptops) exemplifies this – it required careful consideration of layered defences, and operational security techniques to ensure a suitable security approach. This helps ensure that despite giving devices to those with the time, the motivation, and the capability to attack them, we have confidence in the overall solution.

As a government department, we are naturally a target for foreign state attackers seeking intelligence gains. The operational costs associated with preventing a successful cyber-attack is significant. Ensuring our investment is proportionate to the level of risk we face, our focus is preventing non state actor level attacks[3], as this will provide the best return on investment for the taxpayer.

[3] The individuals within organised criminal groups who conduct high end cyber-attacks – distributed denial of service (DDoS) and ransomware – frequently operate with the tacit approval of the state.

Delivering Success

In recent years, the MoJ has demonstrated that a considered, agile approach to cyber security in government pays dividends. The department has an appetite for innovation – greater digital change, and adoption of new technology and approaches for our services. Getting cyber security right in such an environment is challenging, but vital.

Success in cyber security means we have confidence in connecting our systems to others to share data and collaborate effective, we are relaxed about using the fullest range of modern tools available, and we can quickly identify and respond to potential security problems before they become critical issues.

The MoJ family of organisations contains huge numbers of complex, interrelated and interdependent systems, providing a massive range of vital services to citizens and businesses. We know that excellent cyber security will take time to achieve and requires concerted effort within this environment.

The MoJ is committed to meeting the two strategic pillars of the GCSS as described in the Strategic Context. Our progress so far is described below:

- We are making progress on the first – to **build a strong foundation of organisational cyber security resilience**. Our responsibility for cyber security stretches beyond the MoJ. The department does not operate in isolation, but succeeds through partnerships, contractual or otherwise, with thousands of organisations providing services across the justice sector.

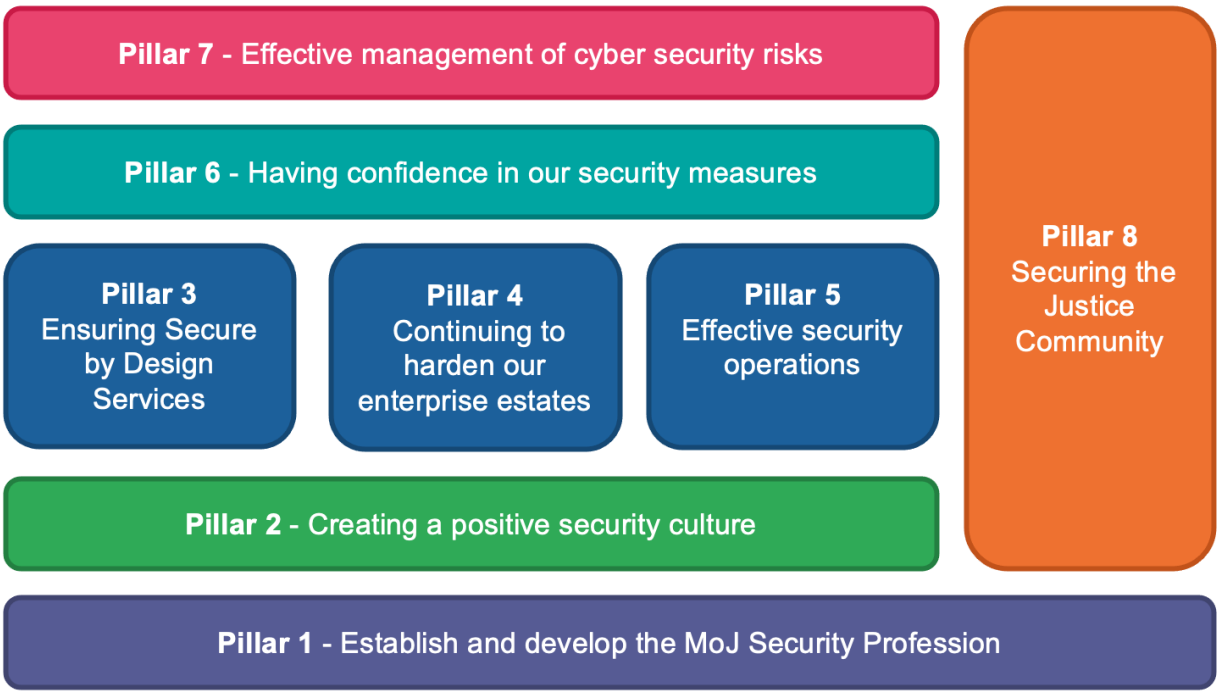
- Our role includes representing the justice sector in cross-government cyber strategy discussions, as well as ensuring appropriate security in all our executive agencies, Arm's Length Bodies (ALBs) and our complex supply chain. In this regard, the MoJ is also addressing the second strategic pillar set out in the GCSS, to '**Defend as One'**.

This strategy therefore sets out our aspirations for the future of cyber security within the MoJ, with a clear focus on investing appropriately in people, process and technology at every step of that journey. If we achieve these aspirations, we will meet the relevant government standards for cyber security and provide senior leaders, partners, and the public with assurance that the MoJ is resilient to cyber-attacks.

The strategy aligns to the Government Functional Standard GovS 007: Security.

Our Strategic Pillars

The MoJ's Cyber Security Strategy is formed of eight related strands of activity.



Pillar One: Establish and develop the MoJ Cyber Security Profession

The department is known across government for its knowledgeable and approachable cyber security staff. This reputation has been hard-earned. The positive support for and implementation of cross-government development schemes within the MoJ, to build an effective cyber security profession, can be seen through the excellent ongoing cyber apprentice and fast streamer schemes.

We wish to build on this success, and ensure everyone working in, and alongside, cyber security has the support they need to succeed. The success of this strategy will not only depend on the expertise of those within the security profession – the security analysts and risk advisors – but it will rely on the active support and involvement of colleagues in adjacent professions, such as digital, data and technology.

Our goal is to be recognised as one of the best places to work on real-world cyber security problems in Government, with an expert and enthusiastic security profession made up of people at all stages of their security careers.

To achieve this, we will:

- Establish an MoJ-wide cyber security profession, in line with the Government Security Groups' definitions, covering all related roles across the department. We will unlock a level of professional development support for all cyber security staff, to help one another with challenging tasks, establish a central pool of expertise for more serious incidents, and to help the department to create an effective and positive security culture.

- Expand our help to various initiatives that support people who wish to join the security profession – setting targets for hosting more apprentices, fast streamers, summer interns and industry-year students. We will also investigate other options to support mid-career transfers to cyber security roles.

- Set up a training programme to help develop security skills in those working in 'adjacent' roles – e.g., technical architects, DevOps staff, and HR teams.

- Investigate, in conjunction with our industry partners, a scheme to help develop positive cyber skills for those in prison and on probation, to bolster cyber skills and provide opportunities for them to join the nation's cyber workforce.

Pillar Two: Creating a positive security culture

The MoJ is known across the public sector for high quality security policy and guidance material. We will build on this success as we continue to develop and refine our portfolio of policies and guidance to support staff, suppliers and partner organisations to understand their responsibilities and requirements, and ensure they remain fit for purpose.

In addition, in the last eighteen months, we have formalised our work to develop an effective and positive security culture within the department, through a range of activities including training, education and awareness-raising events and our 'Security Champions' network. We will accelerate our work at all levels of the department, to improve the maturity of our approach to put in place long-term, sustained cultural change[4] through the implementation of new technology and by adopting a 'little and often' approach to address behavioural and cultural change.

Our goal is to have a government-leading portfolio of excellent security policies and guidance, coupled with a 'secure by default' culture across the entire department.

To achieve this, we will:

- Build on existing board-level cyber security engagements to ensure senior leaders regularly discuss security topics and the benefits of a positive 'fail secure'[5] culture.

- Provide joined-up training and awareness appropriate for all levels and roles in the department, working with colleagues in related areas, such as the Data Protection Team, Information Services and Group Security areas. This will include both foundational and bespoke training material.

- Develop our network of Security Champions within our security culture programme, empowering key individuals to become the focal point for colleagues on security matters: helping to disseminate security messages; providing feedback on security initiatives and new concepts quickly; and supporting awareness-raising activities.

- Continue our government-leading work on open security policies and guidance, to ensure they reflect major initiatives like the Supplier and Partner Security

[4] As measured using the SANS Security Awareness Maturity Model (https://www.sans.org/security-awareness-training/resources/maturity-model/)

[5] An environment in which tolerance is applied to enable individuals to learn from their mistakes.

Framework, the introduction of GovAssure, and changes in wider HMG policies and guidance.

Pillar Three: Ensuring Secure by Design Services

We will seek to quickly meet, if not exceed, the Baseline CAF Profile for all new MoJ services, as codified in our policy portfolio. Our IT estates have significant technical debt, so for existing services and products the service teams will be supported in understanding deviations from the new standards and given help in mitigating risks wherever possible.

Our goal is to ensure that all MoJ IT systems are protected against common cyber-attacks and are resilient to the threats we actually face.

To achieve this, we will:

- Adopt a ‘secure by design’ approach, with security architectures that minimise the trust we need to place in individual components. We will further enhance the Justice Digital Application Security Programme. This programme provides automation, bespoke training for developers, and additional tooling and support to embed security in all aspects of digital development, significantly reducing the number of preventable vulnerabilities that reach production systems.

- Ensure that ‘secure by design’ is occurring in the choices digital teams are making. For example, additional security checks and balances will be added to internal governance regimes, such as service assessments, where teams will need to demonstrate their positive approach to security, and how they are discharging their security responsibilities.

- Adopt existing common security patterns and establish automated guard rails to help teams develop and operate in a secure environment by design. In line with the strategic pillars in the GCSS, and as a government leader in technology, the MoJ will ‘Defend as One’ by continuing to share such material for use by other departments. These configurations will include the default controls – such as encryption, data minimisation, and access control – which similar services need to adopt. We will continue to play our part in the cross-government Secure by Design work to share our expertise and learn from good practice elsewhere in government.

Pillar Four: Continuing to harden our enterprise estates

Our enterprise IT estates are the technology environments that underpin so many core services the department provides. Whether it is email, mobility, productivity services, collaboration or providing the means for other services to operate, the security of these estates is vital. The department can harness the improved security of modern technology and move away from legacy security thinking.

Our goal is that our enterprise technology is consistently resilient against cyber-attacks, with significantly improved staff security experiences – such as how we authenticate to systems or get help with suspicious emails.

To achieve this, we will:

- Building on our previous Joiners, Movers and Leavers improvement project, we will significantly improve our identity and access management approach to ensure that the majority of staff access to critical systems will be through a single identity, enabled through strong passwordless technology. Through this, and the introduction of a common password manager for staff, we will dramatically reduce the number of passwords that colleagues need to remember to access the technology they use every day.

- Conduct a review of existing enterprise security capabilities which are provided in a federated measure – such as PKI services, and identity and access management – to understand where there might be realisable efficiencies and benefits from estate-wide consolidation.

- Review privileged access management practices for improvements, across both enterprise and digital services. We will also ensure that all privileged management is undertaken from authorised – and where possible – dedicated devices, with appropriate auditing and logging of management activity.

- Introduce technical solutions to improve efficiency for MoJ staff users in managing their own security within the business-as-usual working environment e.g., introducing an option to report suspected phishing emails.

- Migrate the small number of above OFFICIAL systems on which the department relies onto the cross-government Rosa[6] platform. Where this is not possible, we will create a new oversight group to ensure existing classified systems are operated and maintained to the highest possible standards.

[6] Rosa is the cross-government SECRET IT service.

Pillar Five: Effective security operations

With an ever-expanding reliance on technology, and a corresponding growth in the number of systems the MoJ relies upon, it has been a challenge to provide an appropriate and consistent level of investment into security operations.

Designing and implementing effective security controls into our technology estates is a necessary first step, but not sufficient to ensure that security is maintained throughout the lifespan of a system or service.

Good security operations ensure that: potential security incidents are investigated swiftly with action taken quickly to minimise harm; proactive steps are taken to improve the security of live systems; change is well managed in technology systems to avoid introducing new security problems; and general security maintenance is routinely undertaken.

Realistically, given the diverse range of technology systems and services the MoJ manages, and the breadth of technology solutions across our multiple IT estates, it is unlikely the department will ever have sufficient in-house security operations effort to cover all these effectively. Our in-house expertise therefore needs to be focussed on MoJ-specific problems, rather than on addressing commodity security operations challenges. Individual digital and technology teams across the department need to be supported in embedding security operations into their routine activities, and new mechanisms explored to support these.

Our goal is to have confidence in the robust security monitoring we've put in-place to protect against likely cyber-attacks on our most vital services.

To achieve this, we will:

- Continue to use our Red Team, recognised as an excellent pan-government capability, to undertake offensive security operations across departmental systems to find weaknesses before they become vulnerabilities. The team will also publish more of their tools and techniques and collaborate further with other departments to help others benefit from their work.

- Refresh our approach to the regular security testing of systems beyond the work of our red team, building on attack simulation tools, automated vulnerability discovery tooling and using IT Health Checks in a more structured way, to bolster confidence in our security controls. We will use standard reporting formats to better track how

discovered issues are being addressed across the disparate areas of the department.

- Refresh processes and policies around security incidents, to ensure greater consistency of approach across all areas in terms of escalation and visibility of incidents. We will review incident management playbooks for all critical services to ensure they have been captured in a consistent format to improve management and response to potential incidents.

- Validate that all critical systems (including data, configuration items, software, processes, key knowledge etc) are frequently backed up offline and that disaster recovery plans are comprehensively tested.

- Achieve the 'baseline' level of security logging and monitoring maturity[7] for every new MoJ technology system, with all business critical systems reaching at least 'enhanced' maturity.

- Conduct at least one tailored cyber security tabletop exercise for every team supporting a business-critical system (approximately 50), to ensure security incident practices remain relevant to, and understood by, all relevant personnel. The department will also undertake a 'silver command' level cyber incident exercise annually and a 'gold command' cyber security-related exercise every two years.

- Improve asset management across the department so that technology and data assets, inventoried in federated solutions, will be regularly audited to ensure accuracy of records. To help meet Objective 2 in the Government Cyber Security Strategy[8], we will extend existing active automated asset discovery and management tooling across all areas of the department to ensure a clear picture of the hardware and software that is in use.

[7] https://security-guidance.service.justice.gov.uk/security-log-collection-maturity-tiers/#security-log-collection-maturity-tiers

[8] Protect against cyber-attack: Understanding of cyber security risk informs the adoption of proportionate security measures with centrally developed capabilities enabling protection at scale.

Pillar Six: Having confidence in our security measures

To allow the department to operate effectively we need to have confidence in all the security measures we have. These might be the controls in our internal systems, or those provided by the many suppliers and partners we work with to support the objectives of the MoJ.

Cyber security in the MoJ has previously been assessed through the Departmental Security Health Check (DSHC), against the Minimum Cyber Security Standards (MCSS)[9]. GovAssure is the new cyber security assurance approach that is replacing the cyber security element of DSHC. GovAssure uses the National Cyber Security Centre's Cyber Assessment Framework (CAF)[10] to provide an objective, coherent understanding of cross-government cyber security[11].

Our goal is to be an exemplar across Whitehall in how we assure our internal systems', and external supply chain's, security measures, providing assurance to senior leaders and partners that our security controls are working effectively.

To achieve this, we will:

- Build on the work that began in FY22/23 to improve supplier and partner assurance. We will implement our assurance framework for the third-party organisations the department relies upon. We will ensure our suppliers and partners, both existing and newly onboarded, are clear on the security requirements they need to achieve to protect our information and systems.

- Update policies and procedures to support continuous assurance to provide confidence in the security of our technology, people and processes through the implementation of the Cabinet Office's GovAssure programme.

- Build on our successful MoJ pilots of GovAssure, to become a government-leading department in how we undertake internal security assurance and compliance effectively and pragmatically.

[9] https://www.gov.uk/government/publications/the-minimum-cyber-security-standard

[10] https://www.ncsc.gov.uk/collection/caf

[11] The MoJ, along with three other government departments, is participating in the Cabinet Office's GovAssure pilot programme.

Pillar Seven: Effective management of cyber security risks

The MoJ will ensure we have clear, effective, and well-understood cyber security risk management processes, governance arrangements, and defined responsibilities in place. This will be led from board-level, with regular discussion of security risks and controls occurring throughout the MoJ family of organisations.

Our goal is that security risk decisions are being taken at the most appropriate level, by well-informed and empowered individuals across the MoJ, with excellent visibility of strategic security risks at senior level to help guide investment decisions and business priorities.

To achieve this, we will:

- Identify a senior responsible owner for the security of every MoJ IT system, who has delegated security decision-making authority to the most appropriate level.
- Refresh our processes and guidance to ensure that all security risks are identified, analysed, prioritised and managed, including deployment of a central governance, risk and compliance solution.
- We will ensure that Agency CEOs, functional leads, and SROs all have clear security accountabilities. This will be accompanied with bespoke training for key roles to ensure those making decisions about security risks are equipped to make effective choices.
- Introduce automation to provide senior leaders with greater insight into security performance across the entire department, by drawing cyber security metrics and measures together into a performance dashboard.
- Ensure that all security decision-making and risk management is informed by a good understanding of the true threats to systems, and by a clearly stated and communicated cyber security risk appetite statement.

Pillar Eight: Securing the Justice Community

The Government Cyber Security Strategy articulates an important role for lead government departments such as the MoJ. The department must ensure all EAs and ALBs are well-supported in staying safe and secure online, and to provide security leadership for the justice sector.

The department has previously demonstrated this role through the creation of the Criminal Justice Secure (e)Mail (CJSM) service in the 1990s. At its launch, it was a significant step forward to help the wider justice community – from public sector, the legal sector, commercial organisations, and charitable bodies – to communicate safely and securely together.

The sector now needs an active voice to represent it in cyber policy debate across government, and to help raise the bar in justice-wide security practices. It is also important that the department takes a more active role in questions relating to cyber and justice policy.

Our goal is to better understand the role we can play in providing cyber security leadership to the Justice Sector, and what supporting this community effectively requires.

To achieve this, we will:

- Devote effort to define the problem and then establish a roadmap that begins to address this issue over the lifetime of the strategy. We recognise that we will not solve the problem in the short term, but we will dedicate resource to begin working on how to address it.

- Establish a small cyber and justice policy team to collaborate with other government departments, the wider justice sector and academia.

Implementing the Strategy

The initiatives within this strategy require prioritisation for the purposes of:

- Timing. In order to identify when each initiative will be introduced into service within the lifetime of this strategy (out to 2028).

- Funding. To ensure the various project costs are captured and sufficient resource allocated to ensure their introduction into service within the specified timeframe.

The initiatives will be categorised as follows:

- Short Term. Some of these initiatives are already under way and are funded activities. Others that have not yet started are likely to be prioritised in the next Spending Review and will be completed within 12 months of the publication of the strategy.

- Medium Term. These initiatives have not commenced but will be important transformational activities that will attract a higher priority during subsequent Spending Reviews. As these initiatives will be multi-year programmes of work, those deemed transformational in nature for the MoJ will need to attract sufficient funding to initiate the programmes, which are likely to be cross-cutting in their impact and complexity.

- Long Term. These initiatives are currently unfunded aspirations and subject to decisions in later Spending Reviews.

Appropriate measurement of success criteria will be embedded in each project and defined by the overall implementation programme.

A Cyber Security Action Plan will be developed, outlining the key initiatives, responsibilities and partnerships required to achieve this strategy. Collaboration within and beyond the department will be vital to achieving its aspirations.

Measuring Success

As we implement the MoJ Cyber Security Strategy, it is important that we remember the landscape does not remain static. Cyber threats will come and go; the department will adapt to new challenges and opportunities; the technology we use will evolve; the suppliers and partners we work with will change; as will our people. The level of cyber security risk we are willing to tolerate will also change, both within agencies and ALBs, and at an enterprise level. It is therefore essential that we monitor our cyber resilience, and improvement progress, effectively.

We will build on existing board-level reporting to develop improved outcome-based performance indicators for cyber security. These will be underpinned by activities described above, such as our enterprise-wide use of the Cyber Assessment Framework and GovAssure regime.

Annex A

Mapping the GCSS to the MoJ Cyber Security Strategy

GCSS Objective 1. Manage cyber security risk

- MoJ Strategy Pillar Six: Having confidence in our security measures
- MoJ Strategy Pillar Seven: Effective management of cyber security risks

GCSS Objective 2. Protect against cyber-attack

- MoJ Strategy Pillar Three: Ensuring Secure by Design Services
- MoJ Strategy Pillar Four: Continuing to harden our enterprise estates
- MoJ Strategy Pillar Eight: Securing the Justice community

GCSS Objective 3. Detect cyber security events

- MoJ Strategy Pillar Five: Effective security operations

GCSS Objective 4. Minimise the impact of cyber security incidents

- MoJ Strategy Pillar Five: Effective security operations

GCSS Objective 5. Develop the right cyber security skills, knowledge and culture

- MoJ Strategy Pillar One: Establish and develop the MoJ security profession
- MoJ Strategy Pillar Two: Creating a positive security culture