Through Technology

Namespace Security

G-Cloud 15 (RM1557.15) - Service Definition Document

enquiries@throughtechnology.uk

January 2026

Namespace Security and External Attack Surface Management are complementary services which discover, assess and monitor your organisation's presence on the internet. Giving you monitoring and centralised control over external digital assets such as domain registrations, web content, applications, IP addresses, and certificates.

Through Technology are experts in this field, and bring processes and the industry leading solutions proven at national scale to help your organisation mitigate the financial and reputational risks involved.

Exec Summary

Namespace Security refers to the practices and technologies employed to protect domain names and other digital identifiers from unauthorised access, manipulation and misuse.

At the time of writing (March 2024) this is a new and rapidly growing method of attack and one which many major international brands have already been impacted by.

The ease with which new domains and sub-domains can be created for projects, test environments and services has led to unprecedented growth in public sector namespaces, and with it an increased burden to manage and monitor them effectively.

Without effective namespace monitoring and management, communications with the public and other organisations can be disrupted or intercepted, access to public services can be impaired, traffic can be redirected to fraudulent sites and your organisation's identity can be misused in onward cyber attacks.

Attacks on your namespace cannot be detected with traditional tooling as they work by exploiting mistakes and poor lifecycle management in Public DNS, enabling traffic to be redirected or faked without passing through your on-premise or cloud infrastructure.

The National Cyber Security Centre have identified namespace security attacks as a growing concern and recommend that public sector organisations monitor their namespaces for vulnerabilities and unexpected change[1]. This is in addition to, not replacing or duplicating the NCSC's own "MyNCSC" tools such as Mailcheck and WebCheck.

The purpose of this service is to provide the tools and expertise necessary for that essential monitoring and management tooling and to help your organisation use them effectively.

1.1 Why do we need to manage namespace security?

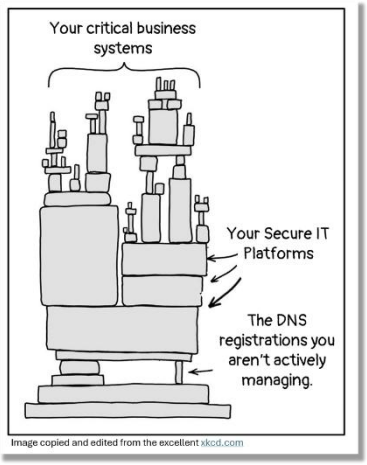


Image copied and edited from the excellent xkcd.com

- Attacks occur entirely outside your network boundary, where most current security tooling will never see them
- Attacks impact your genuine organisation identity, eroding public trust in your digital services and those of other public sector organisations in the same top-level domain (gov.uk, nhs.uk etc)
- This is a new and growing area of security risk, which is already impacting major organisations in the private sector
- NCSC Guidance is clear: organisations need to monitor DNS for unauthorised changes and misconfiguration.

[1] https://www.ncsc.gov.uk/guidance/managing-public-domain-names

1.2 Why select this service?

1.2.1 Pedigree

Through Technology have extensive experience in securing UK Public Sector domains. As well as securing hundreds of public sector domains to meet the Minimum Cyber Security Standard, we have also worked in the past with the Government Digital Service (now Central Digital & Data Office or CDDO) improve security across all of the .gov.uk namespace, developing namespace security tooling, communicating issues to public sector bodies and preparing contracts for new UK Government DNS Services.

1.2.2 Capability

We are an SME, but with enterprise-level experience working with the largest government departments and leading their incumbent suppliers managing their critical infrastructure services.

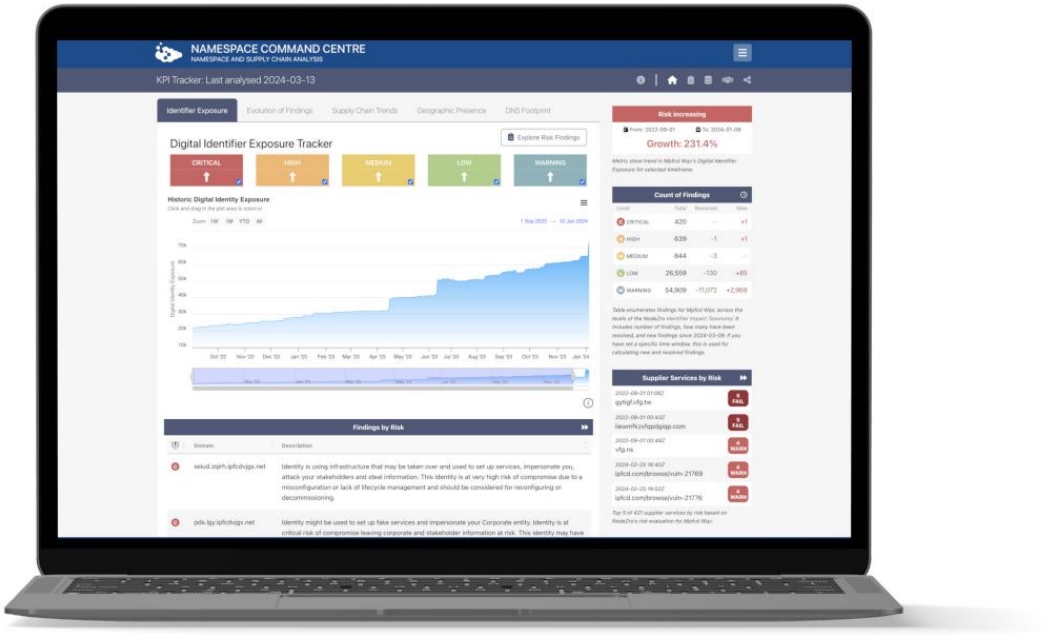
1.2.3 Products

The two main products we use for this service are both in use at National Scale, protecting public sector digital services:

1.2.3.1 Nodezro

We utilise Nodezro Namespace Command Centre to deliver this service. A secure Software as a Service platform that requires minimal setup and no integration with your infrastructure. It gathers data from the public internet, analyses it and presents information on your namespace directly into a simple and secure web interface, or via an API if required.

Figure 1 - NodeZro Command Centre Portal



With no integration effort required, real actionable data about your namespace security is available from the first time you engage with us.

1.2.3.2 Detectify

Detectify is a world-class External Attack Surface Management (EASM) SaaS Solution, not only discovering your digital assets but also providing the capability to interrogate them and discover the underlying technologies and assess their vulnerability to known and emerging Common Vulnerabilities and Exposures (CVE). Alerting you when your assets are misconfigured or when patching fails, leaving your solutions exposed to existing or new vulnerabilities.

1.2.4 Flexibility

We recognise that G-Cloud customers have a broad range of scale and capability when it comes to securing digital services. For this reason, we offer a high level of flexibility in this service with a range of options including.

Software Only – Where we supply NodeZro Command Centre software licensing only as either a G-Cloud Lot 2 – Cloud Software offering or via the Technical Products & Services Catalogue.

Implementation Support – Where we provide expertise to educate your team and help remediate the issues in your namespace, while also creating and instilling effective namespace lifecycle management to avoid problems recurring.

Managed Service – Where you outsource namespace security to Through Technology to manage and monitor on your behalf.

1.2.5 Cultural Fit and Social Value

Through Technology was founded by two individuals who had worked for multi-national IT companies and then provided oversight of similar businesses while working directly for HMG Departments. Our business is founded on (and has proven) the theory that focus on our customers needs, open and direct communication, technical excellence, proactive knowledge transfer and clean exit make a real difference.

People and relationships deliver projects. We work hard to find and retain the very best people who then build and maintain effective working relationships with relevant parties at all levels.

We believe in "working in the open" and typically do so using shared file storage, chat channels and plans with our customers (e.g. on shared Microsoft Teams). This was our progress and products are always available to view.

As a business, we are certified as Carbon Negative. Meaning that we have removed more CO2 from the environment than we have added and this applies to all services that we deliver via the G-Cloud Framework.

We also have a strong focus on adding value…. And recognise the need for the UK Public Sector to deliver high quality and value for money to taxpayers. So much so that we have a documented process for how to deliver added value, quantify it and report back to our customers.

Please refer to the G-Cloud 15 portal for further information on our Social Value approach and measures across all 5 categories.

Figure 2 - Through Technology Professional Certifications & memberships

2 Lot 2 - Service Description

2.1 NodeZro Namespace Command Centre

Our service is built around the product and our long-standing partnership with the leading namespace security vendor "NodeZro". Their Namespace Command Centre (NCC) is the core tool we use internally for namespace security and with our Lot 3 Service (see section 3 of this document). It is also available from us via the Crown Commercial Service Purchasing Platform Catalogue.

The Namespace Command Centre (NCC) uses specialized AI agents to provide comprehensive namespace security across a guided transformation journey: Discover → Identify Gaps → Analyse Root Causes → Establish Governance → Ensure Compliance. The platform delivers zero-integration discovery across 8 asset categories in less than 24 hours. Namespace information is refreshed on a weekly or optionally daily cadence, enabling customers to monitor the status and growth of their namespace, and changes to it, including identifying attempts to misuse their domains.

2.2 Asset Discovery

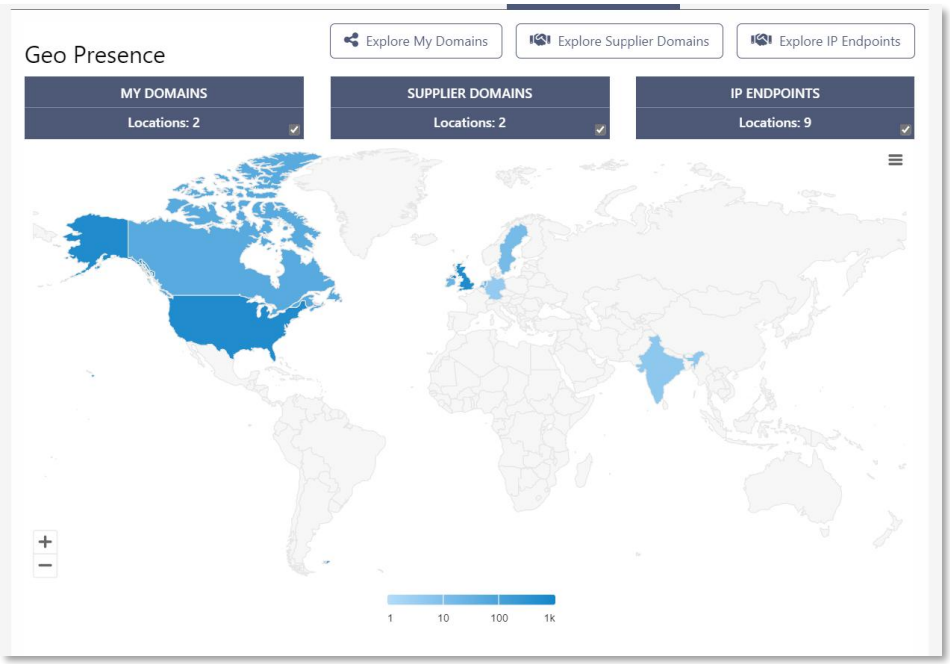
NCC discovers 8 asset categories: DNS (domains, subdomains, zones, records), Public certificates (TLS/SSL), Email (SPF, DMARC, MTA-STS, MX records), Content (web pages, published media), Technologies (frameworks, libraries, tech stacks), Brand (lookalikes, typo squatting), Suppliers (DNS providers, CAs, CDNs, hosting, SaaS), and IP Addresses (with geolocation and reputation scoring).

This in itself provides valuable information and is often – in our experience – the first-time customers get a true picture of their digital service footprint.

Data is presented in a simple web portal including numerous views and reports, such as:

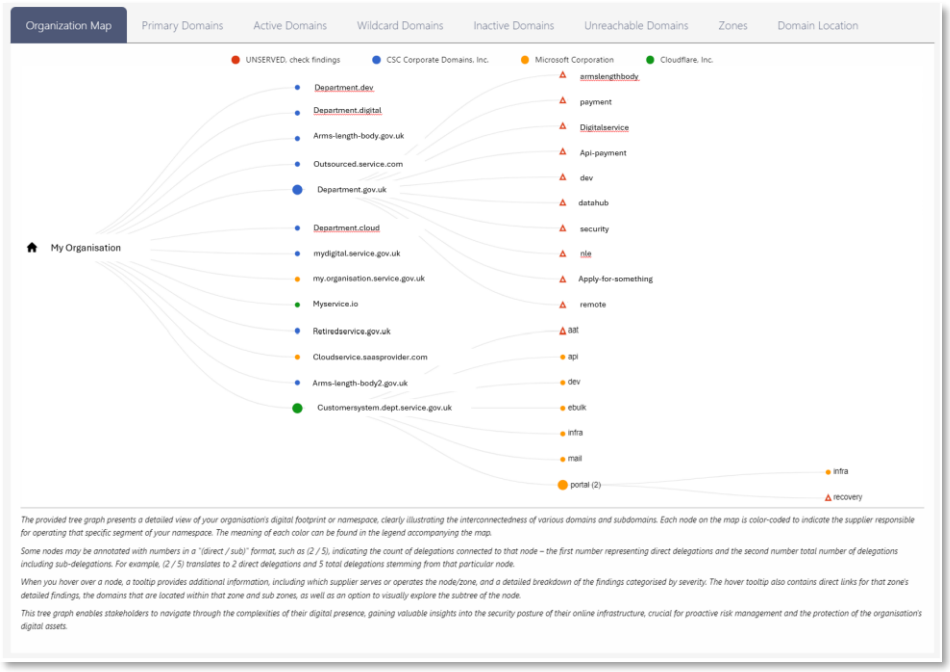
Figure 3 - DNS Footprint - Domain types and trends

Figure 4 – DNS Footprint - Geographic Presence



Geographic mapping allows you to quickly see where your domains are registered, where the IP endpoints for them are located and where your supply chain operates from. Changes in these patterns can be a clear indication of compromise.

Figure 5 - Organisational Mapping



Organisational mapping provides insight into how your digital presence is structured and managed. Providing real insight into your organisation's entire digital footprint.

In addition to these views, command centre provides detailed lists and reports with filter and search capabilities.

2.3 Vulnerability Management

NCC provides multi-dimensional risk scoring across exploitability, business impact, and Single Point of Failure (SPOF) exposure. Prioritized remediation queues deliver Next Best Actions for both tactical fixes (dangling CNAMEs, expired certificates, weak ciphers) and strategic transformation initiatives.

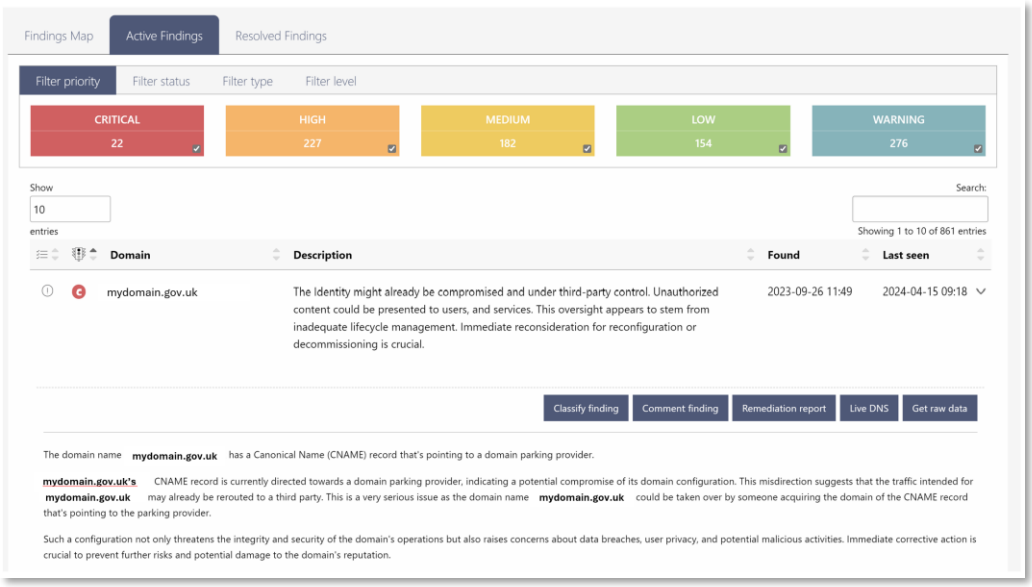
Vulnerabilities can be seen in organisational map view or as a detailed list with filters for the criticality, type, domain-level and status.

Every finding has simple controls to enable the customer to:

- Classify, set a status on, and comment on each finding.
- View the DNS data that resulted in the finding.
- View the current live DNS data to see any changes
- View a PDF Remediation Report explaining the finding in further detail and how it can be exploited.

Customers can classify and comment on findings to track their status as they are addressed.

Figure 6 - Vulnerability Management



Crucially, customers can also see historic data on **Resolved Findings.** When a domain that has been left unmanaged suddenly changes in configuration, this can be because your team has resolved the issue, or because it has been exploited and its traffic is being redirected elsewhere.

"Using your own tools or a commercial service, you should monitor critical DNS records for unexpected changes"

NCSC Guidance - Managing Public Domain Names

2.4 Certificates & Cryptographic Security

Certificate Inventory and Expiry Monitoring

NCC maintains a comprehensive inventory of certificates across your namespace, tracking both certificates actively in use and those issued via Certificate Transparency logs. Automated expiry monitoring ensures certificates can be renewed before they impact service availability.

TLS Connections Monitoring

Beyond certificate inventory, NCC monitors the actual cryptographic endpoints where TLS is negotiated across your infrastructure:

1. Web endpoint monitoring (HTTPS) with multi-port coverage
2. Email endpoint monitoring (SMTP/TLS on port 25 and related services)
3. TLS version detection (identifying deprecated TLS 1.0/1.1 requiring elimination)
4. Cipher suite analysis with identification of weak or broken configurations
5. Post-Quantum Cryptography (PQC) readiness indicators tracking ML-KEM/X25519 hybrid support

Post-Quantum Cryptography (PQC) Planning

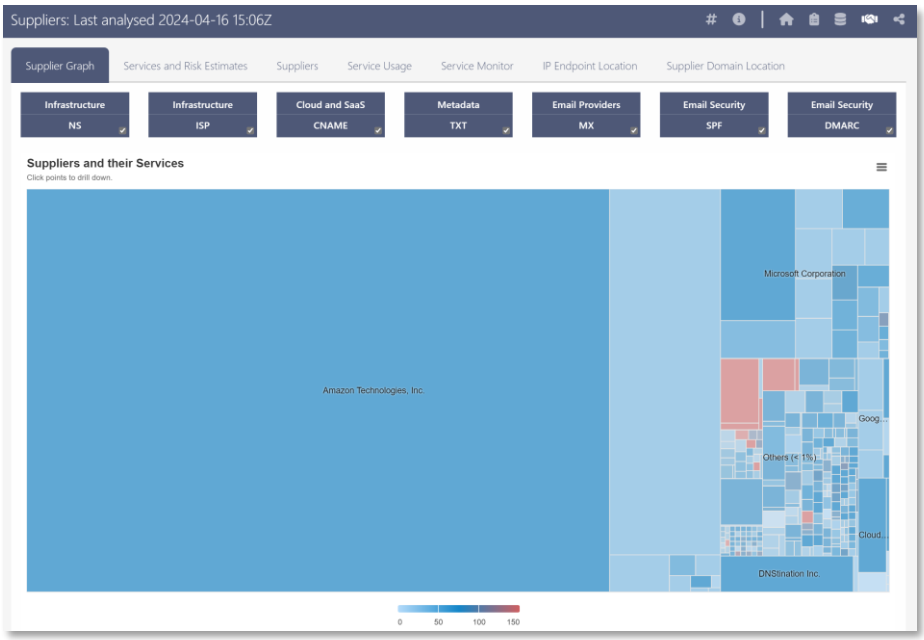
With NIST announcing deprecation of current algorithms by 2030 and disallowance by 2035, NCC supports your PQC migration planning by identifying which endpoints support quantum-safe key exchange. This addresses the 'harvest now, decrypt later' threat where adversaries collect encrypted traffic today for future decryption.

2.5 Supply-Chain Risk Analysis

The DNS system is hierarchical. With each domain that you own registered with a Registrar and ultimately with a registry. The recent Cloud First policy in government and most public sector organisations has led to extensive adoption of Amazon and Microsoft DNS services, but most organisations will still have multiple suppliers in your DNS Supply Chain. This can lead to significant risks in terms of manageability and vulnerabilities where your suppliers themselves may have poor security or misconfiguration.

NCC provides supply chain risk analysis. Mapping the vendors in your DNS supply chain by type and scale of adoption and providing trust scoring based upon analysis of their namespaces.

Figure 7 - Supplier Graph View –at a glance see the breadth and risk of your supplier base



Customers can also view risk analysis scoring of each supplier, the geographic location or their IP endpoints and domain registrations and crucially, which of their domains are reliant upon which suppliers.

This allows customers to make informed decisions to simplify (or add resilience to) their supply chain and move away from those suppliers which may put their digital services at risk.

2.6 AI-Powered Intelligence

NCC's AI agents generate actionable intelligence packages tailored for different audiences: audio briefings (AI-narrated summaries on-demand), automated collateral (executive summaries, reports, and presentation decks in PPTX, PDF, CSV.

2.7 Progress Tracking

Where NCC tracks the changes to your namespace and its security risks overtime, organisations can clearly see the progress they are making and the tangible improvement in the resilience and security of their digital and technology services as a result.

2.8 Zero Integration

NCC is run as a Software-as-a-Service cloud solution which gathers its data from the publicly available sources and services on the Internet. The only connection required to your systems is to allow single-sign-on (SSO) from your organisation's Google or Microsoft identity provider, which also allows for multi-factor authentication using your organisations chosen configuration.

2.9 API Access

Your namespace data is also accessible through a maintained and documented API, featuring:

- **Streamlined Access:** Organized around REST, our API ensures quick, efficient transfers of your critical data. Navigate your namespaces and fetch analysis results with ease, thanks to our predictable URLs and JSON-encoded responses.
- **Robust Security:** We prioritise security without compromise. Access is strictly via HTTPS, ensuring your data is protected with encryption during transit. Additionally, with dual-layer security involving API keys and IP allow-listing, your data remains secure, accessible only to authorised users.
- **Efficient Integration:** Our Quick Start Guide facilitates rapid integration. Whether pulling the latest findings or fetching detailed issue descriptions, our commands are designed for optimal data retrieval, minimizing redundancy and maximizing relevance.
- **Comprehensive Documentation:** Each feature of our API is supported by detailed documentation that guides you through every aspect of integration and usage. Our clear, concise, and comprehensive instructions ensure you can harness the full potential of our API with minimal learning curve.

3 Lot 3 – Service Description

Namespace Security is new to many organisations, as it is a growing risk which most organisations (including national governments and multi-national enterprise customers) have only just started to fall victim to and address.

As well as offering NodeZro's Namespace Command Centre, Through Technology also provide a flexible service to address the immediate vulnerabilities in your infrastructure and help establish the knowledge and process required to prevent them recurring.

3.1 Service Options

Across the UK public sector, there are organisations of all sizes with digital, technology and security teams of all sizes and capabilities, along with managed service providers running outsourced IT systems.

For this reason we offer flexible support tailored to each customer's needs, based around two options:

- Namespace Command Centre (only): For organisations that do not require any additional capacity, assistance or training to implement or improve your namespace security. We offer NodeZro's Namespace Command Centre as software only through G-Cloud Lot 2 and the Technical Products and Services Framework.
- Namespace Security Improvement: Aimed at those organisations that wish to manage namespace security internally, or have it run by your incumbent supplier. We offer additional support and training to resolve vulnerabilities in your estate and implement effective namespace lifecycle management to prevent their recurrence.
- Namespace Security Service: For those organisations that lack the internal capacity or capability to manage this themselves and wish to have it addressed via a managed service, we offer a full outsourced option, where Through Technology will monitor your namespace for issues or unauthorized change and work with your teams to resolve any issues.
- Namespace Security & External Attack Surface Management Service: This service adds CVE monitoring to our namespace security solution. Identifying more of the underlying technologies (and their versions) that your organisation exposes to the internet and actively testing them for Common Vulnerability and Exposure (CVE) risks

All services include licensing of Namespace Command Centre for your organisation as well as comprehensive knowledge transfer and exit arrangements.

4 Further Information

4.1 Organisations that trust Through Technology

In the eight years since our founding, we have established a position as a well-known and trusted supplier to the UK central government. Building excellent relationships and undertaking complex and critical projects for organisations such as:

Ministry of Justice	The Ministry of Justice	Architecture Managed Services Legacy Risk Mitigation Email Migration Solution, Delivery & Security Assurance Operational Change Assurance Email Security GCF and GSI Service Exits
Government Digital Service	Cabinet Office - Government Digital Service	Namespace Security Cloud Service DevOps Outreach campaign delivery and management across the UK Public Sector Procurement Strategy & Preparation
Department for Work & Pensions	Department of Work and Pensions	GCF and GSI Email Service Exit
HM Courts and Tribunals Service	HM Courts and Tribunals Service	Modern Device Management solution architecture, security, testing, implementation and support Legacy Risk Mitigation
CPS	The Crown Prosecution Service	Strategic End User Services consultancy and advisory services.
Department for Science, Innovation & Technology	The Department for Science, Innovation & Technology	Namespace Security & External Attack Surface Monitoring.

Department for Business & Trade	The Department for Business & Trade	Data Migration and Management Machinery of Government Change

4.2 Awards, Commitments and Certifications

Crown Commercial Service Supplier	With our experience in public sector procurement and as a supplier on the G-Cloud and Digital Outcomes & Specialists framework, we pride ourselves on our capability to draft and agree contracts rapidly and efficiently.
Carbon Footprint standard Carbon Neutral Organisation	We are Carbon Neutral Plus certified to the PAS2060 standard. This means that our business and our delivery of services through the G-Cloud Framework is **Carbon Negative, far exceeding HM Government's targets for Net Zero.**
bsi ISO 9001 Quality Management Systems CERTIFIED	Our business is certified to the ISO9001 standard for Quality Management and audited annually by the British Standards Institute to ensure we continually maintain and improve.
bsi ISO/IEC 27001 Information Security Management CERTIFIED	All our services on the G-Cloud Framework are delivered using our ISO/IEC 27001 Certified Information Security Management System. Which is audited annually by the British Standards Institute.
Gold Microsoft Partner Microsoft	Through Technology is a *former* Microsoft Gold Partner for cloud collaboration services, demonstrating our expertise with Microsoft365 and security solutions. We are no-longer a gold partner after Microsoft changed this award from being competency based, to mostly driven through license sales.
CYBER ESSENTIALS CERTIFIED PLUS	While we typically work with customer data on our customer's own systems, we maintain our own IT to be secure to similar or greater standard and evidence this through Cyber Essentials and Cyber Essentials Plus certification.
techUK FOR WHAT COMES NEXT	Through Technology is a member of TechUK, the industry body for IT in the United Kingdom and regularly participate in consultations and industry events, helping shape the future of UK Public Sector digital and technology policy and services
ARMED FORCES COVENANT	Through Technology are signatories to the Armed Forces Covenant. We are committed to breaking down the barriers to ex-services personnel working in the public and private sectors.
Prompt Payment Code	The Prompt Payment Code (PPC) is a voluntary code of practice for businesses, administered by the Office of the Small Business Commissioner (SBC) on behalf of BEIS. Our signature to the code demonstrates our commitment to paying our supply chain promptly and supporting the UK economy.

A Great British Business	Through Technology is a **British Small Business** paying all our taxes in the UK, diligently ensuring our compliance with all applicable tax legislation, helping improve public sector ICT services and supporting UK Economic Growth.

4.3 Framework Documents

Pricing Document - See our service page on Digital Marketplace

Terms and Conditions - See our Service page on Digital Marketplace

4.4 Other information

Learn more about our experience with this service	www.throughtechnology.uk/services
Learn more about Through Technology	https://www.throughtechnology.uk
Start a conversation	@through_tech Enquiries@throughtechnology.uk
Read our Modern Slavery Statement	https://www.throughtechnology.uk/msa-statement
Read our Carbon Reduction Plan	https://www.throughtechnology.uk/carbon-reduction

To see our other services on the G-Cloud 15 framework, search for "Through Technology" (including the quotation marks) on digital marketplace.