



Cybernetica Solutions Limited Cyber Security Network and Cloud Consultancy Services

G-Cloud 15 Service Definition Lot 3 Cloud Support

G-Cloud 15 Service Definition Lot 3 Cloud Support

Contents

1. Introduction.....	1
Company Overview	1
Value Proposition.....	1
What the Service Provides	2
Overview of the G-Cloud Service	3
The Cybernetica Approach	6
2. Data Protection	9
Information Assurance	9
Data Backup and Restoration	9
Business continuity statement/plan.....	9
3. Using the service	10
Ordering and Invoicing	10
Availability of Trial Service	10
On-Boarding, Off-Boarding and Service Migration	10
Training.....	10
Implementation Plan	11
Service Management	11
4. Provision of the service	13
Customer Responsibilities	13
5. Our experience	15
Case Studies.....	15
6. Clients	21
7. Contact Details	22

1. Introduction

Company Overview

Cybernetica Solutions Limited provide Security and Network consultancy and professional services for Enterprise technology to all parts of the UK Government. Equipped with over 45 years of combined experience across public and private sectors, the Cybernetica team have a verifiable track record of successfully delivering complex projects. At the core of Cybernetica's ethos are attention to detail, transparency, honesty, a willingness to go the extra mile and ultimately feel pride in delivering services that meet clients' requirements.

Value Proposition

Whether it be setting strategy and vision, scoping requirements, selecting suitable products, producing high and low-level designs, performing implementation activities, conducting testing, finding or retaining suitably skilled and experienced technical employees is a challenge for many organisations.

Cybernetica Solutions Limited brings real-world Security and Networks technical transformation project experience obtained across multiple sectors to help public sector clients realise their business visions whilst battling with specialist resource constraints across many levels in their organisation.

At Cybernetica we are competent and experienced in a number of enterprise technologies including but not limited to:

- Aruba
- AWS
- Azure
- Check Point
- Cisco
- F5
- Fortinet
- Linux; Red Hat, CentOS, Debian, Ubuntu
- Meraki
- Oracle OCI
- Palo Alto
- VMware
- Zscaler

We offer the full end-to-end solution lifecycle or discrete components such as technical design or implementation services. Whatever the request we work collaboratively with the client team to ensure that requirements are understood by all parties, key stakeholders are identified and engaged early, responsibilities are documented and dependencies

called out as early as possible. Adopting this approach from the outset ensures there is no ambiguity and all parties have a strong understanding of both their and the others responsibilities.

What the Service Provides

Cybernetica Solutions Limited provides a number of service offerings across security, network and Wi-Fi enterprise technologies all of which are based on real-world project experience working across both the public and private sector, as follows:

- Delivery of full end-to-end solution lifecycles
- Requirements definition
- Product selection consultancy
- Proof-of-concept, proof-of-value, pathfinder and pilot projects
- Procurement assistance
- High Level Design (HLD)
- Low Level Design (LLD)
- Implementation services
- Testing services
- IT Health Check (ITHC) scope definition
- Enablement of ITHC test activities
- Assessment of ITHC report findings
- Remediation of ITHC findings
- Integration services with existing security and monitoring toolsets
- Education and handover to live service operations
- Ongoing operational support
- Assurance services to review ongoing operational support effectiveness, configuration reviews and supplier support agreements
- Network and security consultancy services across an array of enterprise technologies
- Secure Access Service Edge (SASE)
- Network and security transformation services encompassing multiple enterprise technologies
- Secure Remote Access Services (RAS)
- Secure Network Access Control (NAC)
- Secure Wireless LAN (WLAN)
- Next Generation Firewall Services (NGFW)
- Secure Web Gateway (SWG)
- Software Defined Access (SDA) and Software Defined WAN (SD-WAN)
- Continual hardware and software refresh services

Overview of the G-Cloud Service

Full end-to-end Solution Lifecycle

Cybernetica leverages our experience with complex technical transformation projects to ensure that such engagements with our clients are a success. We can operate to our own solution lifecycle methodology or can dovetail into a client's preferred approach. Defining functional, non-functional and security requirements are the first step in the journey to realising a successful project engagement. Adherence to defined requirements is tracked through the life of a project through Requirements Traceability Matrices.

Where new technologies are part of an overall solution, we offer product selection consultancy to ensure that technical requirements are met, alignment with existing operating models is adhered to, good value commercial deals are realised and service models with new suppliers are effective. Proof of concept, proof of value, pathfinder and pilots can be managed to support product selection.

Delivery activities provide high level designs with supported bills of materials. Subsequent low-level detailed designs elaborate upon the high-level designs into something tangible that can be realised through the implementation phase. All designs are subject to clients' existing governance processes.

Testing services follow to ensure that functional, non-functional and security requirements are met.

Where required, IT Health Check (ITHC) Services can be managed on behalf of the client, including scope definition, enablement of ITHC testing, assessment of report findings and subsequent remediation activities.

Prior to handing over any new technology solutions to a client's operational teams, integration with existing or new operational and security monitoring systems is conducted.

Full knowledge transfer activities are delivered to a client's existing operational capability prior to a new system go-live. Extended operational support is available from Cybernetica to assist until a client's operational functions are comfortable in managing any new technologies. The level of extended support ramps down accordingly.

The approach to Project Management can encompass Agile or Waterfall methodologies provided by Cybernetica, or our specialist architect and engineering resources can form part of existing clients' internal project or delivery management teams.

Ongoing business as usual assurance services are available to review ongoing operational support effectiveness, conduct configuration reviews and assess the effectiveness of vendor technology supplier support agreements.

Secure Access Service Edge (SASE) Services

Secure Access Service Edge (SASE) Services encompass traditional on-premise security controls hosted as cloud-native converged services. Gartner predicted that by 2024 40% of companies will have strategies to adopt SASE services. Cybernetica have real world project experience in migrating traditional on-premise security controls to SASE services (Palo Alto Prisma, Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA)).

SASE services can support the realisation of SD-WAN initiatives and Software-as-a-Service applications such as Office365, ServiceNow, Skype for Business and Microsoft Teams.

Secure Remote Access Services (RAS)

Enabling remote and mobile work forces saw a dramatic rise in importance during 2020 because of the restrictions on human movement during the COVID-19 pandemic. Once considered as a luxury to increase productivity and reduce costs associated with real-estate, Secure RAS services have become a necessity to keep organisations operating productively. Cybernetica resources were at the heart of keeping one of the largest UK government's departments RAS service operating during COVID-19 in addition to increasing its capacity to cater for a substantial growth in the remote user base to support the department's reactive actions to the crisis.

Secure Network Access Control (NAC) services

Network access control, or NAC, solutions support network visibility and access management through policy enforcement on wired and wireless devices and users of corporate networks.

A NAC system can deny network access to noncompliant devices, place them in a quarantined area, or give them only restricted access to computing resources, thus keeping insecure nodes from infecting the network.

Ensuring that only authenticated access devices are permitted to connect to organisational networks.

Secure Wireless LAN (WLAN) services

Enable corporate and guest mobility for the on-premise based workforce to aid productivity and collaborative working. Wi-Fi 6/6E/7 802.11ax/be deployments supporting end user device speeds up to 10Gbps.

Next Generation Firewall Services (NGFW)

Provide consolidated network security services to secure networks, systems and applications through on-premise, cloud hosted and VMware deployments.

Secure Web Gateway (SWG) Services

Provide controlled access to Internet resources for employees through on-premise or cloud- based SaaS deployments.

Software Defined Access (SDA) and Software Defined WAN (SD-WAN)

Software-defined networking (SDN) is designed to make a network flexible and agile. SDN lets you design, build, and manage networks, separating the control and forwarding planes. SD-WAN is a cloud-first architecture that separates data and control planes. You can quickly establish an SD-WAN overlay fabric to connect data centres, branches, campuses, and co-location facilities to improve network speed, security, and efficiency.

System Integration Services

Integration of new network, Wi-Fi and security technologies with existing or new organisational toolsets, including health and availability, time source, DNS and authentication systems.

Security Integration Services

Integration of new network, Wi-Fi and security technologies with existing or new organisational security toolsets, including Protective Monitoring Security Incident and Event Monitoring (SIEM) systems and vulnerability management scanning systems.

Refresh Services

Provide regular Software refresh, and less often Hardware refresh/upgrade services for security, network and Wi-Fi technologies to reduce the burden from already constrained operational resources.

The Cybernetica Approach

Our approach to delivering successful and comprehensive solutions to clients follows a four- phase methodology. The services available are modular, in any combination or all may be consumed as per client needs.

Define

Under the define phase Cybernetica can provide the following:

- Strategy definition
- Assistance with business cases
- Discovery activities
- Requirements definition
- Product selection advice and support
- Proof of concepts, proof of value, pathfinder and pilot schemes
- Outline project planning
- Resource allocation and scheduling
- Identification and engagement of key stakeholders

Design

The design phase takes the output of the define phase in order to create the overall solution design in readiness for actual implementation, including:

- Detailed project planning
- Determine migration approach
- Creation of requirements traceability matrices
- Creation of RACI matrices
- Creation of project risk log
- Creation of high-level design artefacts
- Creation of low-level design artefacts
- Design governance reviews
- Detailed bill of materials
- Input to risk assessments
- IT Health Check or penetration testing scoping support
- Creation of test plans

Implement

Based on the output from the design phase, the Implement phase leverages engineering resources to create tangible solutions, including:

- Physical and logical build and configuration activities
- Functional system testing
- Non-functional system testing
- Security Testing
- User acceptance testing
- Integration with existing or new:
- Protective monitoring systems
- Health and availability monitoring systems
- Central authentication systems
- Vulnerability assessment systems
- System backup services
- Support for IT Health Check activities
- Support for migration activities

Operate

The focus of the Operate phase is to ensure that the client's operational functions are able to transition in new services with the minimum ease. Early engagement with operations, as identified during key stakeholder mapping during the define phase, is a key component of a smooth transition, which includes the following:

- Technical handover workshops with operation support teams
- Operational support guides
- On-site or remote assistance as required
- New supplier introductions
- Contribution to lessons learnt workshops



Figure 1: The Cybernetica design and build methodology

2. Data Protection

Information Assurance

Cybernetica brings a wealth of industry experience in delivering secure network and cloud consultancy services across the public and private sectors. The organisation currently holds the UK National Cyber Security Centre's Cyber Essentials certification and is committed to continual improvement of its security posture, with plans to achieve Cyber Essentials Plus.

Data Backup and Restoration

Cybernetica adheres to industry best practice for data back-up and restoration, utilising a combination of on-premise and cloud-based enterprise solutions in line with applicable protective markings. Client-specific requirements are agreed in advance and confirmed prior to order placement to ensure alignment with security, compliance, and operational needs.

Business continuity statement/plan

Cybernetica maintains a documented and regularly reviewed Business Continuity Plan (BCP) designed to support the continued delivery of services in the event of a disruptive incident. The plan covers governance, roles and responsibilities, communication arrangements, and the recovery of critical business and technical functions. Cybernetica's Business Continuity Plan can be made available to buyers on request, subject to appropriate confidentiality considerations.

3. Using the service

Ordering and Invoicing

Cybernetica professional services can be ordered in line with the G-Cloud framework call off-terms and by sending an email to ukhmg@cybernetica-solutions.co.uk.

Resource rates are defined within the SFIA rate card and invoices are raised one month in arrears for the resource days worked including VAT and any agreed expenses if applicable.

Cybernetica payment terms as standard are 30 days.

Availability of Trial Service

Cybernetica Solutions do not provide trial services however are happy to engage with prospective clients' in a pre-sales capacity to understand business requirements and help form the initial high-level scoping objectives.

Proof-of-concept and proof-of-value exercises can be provided using the resource rates defined within the SFIA rate card.

On-Boarding, Off-Boarding and Service Migration

Cybernetica's approach to on-boarding, off-boarding and service migration is flexible to ensure a smooth process and varies from customer to customer. A suitable approach is agreed with prospective clients in order to meet their specific requirements prior to orders being placed.

Training

Cybernetica Solutions Training services are tailored around the specific enterprise vendor technologies that we have accumulated real-world subject matter expertise in and accompanied with supporting accreditations and certifications.

All training is scoped accordingly to ensure that it aligns with a client's operational set up and capability. It includes information on foundational knowledge of a particular technology product which is supplemented with targeted focus on the product's features leveraged in a particular solution rather than everything that it is capable of.

Training can be delivered on site at a client's premises or through online collaboration services.

Cybernetica views the enablement of a client's operational function to effectively manage new services that contain new technology of great importance and a critical part of a solution lifecycle. As a result, and at client discretion, a thorough handover to operations is always factored into our statements of work.

Implementation Plan

A detailed implementation plan can be provided to the buyer on request.

Service Management

Cybernetica's Information Technology Service Management (ITSM) framework is founded on ITIL best practice and is designed to deliver reliable, secure, and continually improving services. Our ITSM capability is structured around five integrated stages, supported by clear governance, reporting, and continual service improvement:

Service Strategy

Defining service value, aligning IT services to business outcomes, and setting clear service objectives.

Service Design

Designing services, service catalogues, policies, and processes to meet agreed requirements and performance expectations.

Service Transition

Managing change, release, and deployment activities to ensure controlled, low-risk introduction of new or modified services.

Service Operation

Delivering day-to-day operational excellence through service desk, incident, problem, and asset management.

Continual Service Improvement

Measuring performance, reporting outcomes, and driving ongoing improvement across services and processes.

These stages are underpinned by robust knowledge management, clear policies and procedures, and actionable reporting dashboards, ensuring transparency, control, and continual optimisation of service delivery.



Figure 2: Cybernetica ITSM Processes

Support can be provided on-premise or remotely and during normal business office hours; 09:00-17:00, Monday-Friday, excluding UK national holidays.

Out-of-hours support, including weekends and UK public holidays carries a premium charge, as defined in the rate card.

Service Levels

Cybernetica's standard Service Level Agreement provides a 2-hour response time during normal business office hours; 09:00-17:00, Monday-Friday, excluding UK national holidays.

Bespoke Service Level Agreements can be formulated based on specific client requirements.

4. Provision of the service

Customer Responsibilities

Customers to provide:

- An appropriate work area if on-site working arrangement is required
- A safe working environment
- Appropriate access to basic facilities when working on client premises. For example, toilets, canteen and kitchen areas
- Internal executive level governance approval board for decision making, issues resolution, agreeing strategic directions and providing strategic inputs into delivered solutions or agreed delivery timeline
- Access to key stakeholders throughout the engagement, including any third-party suppliers
- Secure computer and/or mobile equipment should the client's security mandate the use of their own managed equipment
- Where possible secure remote access to the client's infrastructure
- Access to secure data centre environments where required

Technical Requirements and Client-Side Requirements

During the inception of any new project, Cybernetica will work in conjunction with the clients to identify key stakeholders and dependencies. Where access to key stakeholders, whether internal or third-party resources, is critical to the delivery of a project or service, any delays or the inability to make these available to Cybernetica will need to be addressed and managed by the client. Where significant delays are incurred to the project as a result of key identified stakeholders or resources not being available then subsequent costs will need to be absorbed by the client as per the Cybernetica SFIA rate card.

Outcomes/Deliverables

Client deliverables will vary depending on the agreed scope of an engagement, its complexities and outcomes expectations. For most engagements design artefacts will be produced by Cybernetica which are the intellectual property of the client.

After-sales Account Management

Cybernetica will sponsor clients to attend vendor supported events and seminars, where appropriate. In addition to these, Cybernetica also hosts events to discuss future business requirements and goals in social environments.

Termination Process

Cybernetica will support the clients in the off-boarding process in a controlled manner, with consideration for business continuity, knowledge retention, value creation and relationship management.

The termination process will follow the G-Cloud framework call-off terms and conditions and Cybernetica Termination clauses and process.

5. Our experience

Case Studies

802.1x Network Access Control (wired and wireless) for UK Government Department

Design, implement and operate an 802.1x NAC solution to secure both wired and wireless endpoints for a large Government Department.

This solution provided a highly available, fault tolerant ISE cluster to service over 10,000 wired and wireless connections. Extending the network trust boundary to the network edge and continually monitoring and securing the network boundary for anomalous behaviour and unknown network access devices. Exporting SIEM logs securely to a data lake for monitoring and inspection.

The AAA service also provided device administration (TACACS+/RADIUS) granular Role Based Access Control, integration with Protective Monitoring systems, integration with Vulnerability Management technology and processes and securely hosted various enterprise management toolsets.

GovWiFi Guest Wi-Fi services for inter-Government roaming

Design, implement and operate an 802.1x GovWiFi guest Wi-Fi network to secure guest wireless endpoints for a large Government Department.

This solution was initially a pilot which went into production to provide an Eduroam style, secure guest Wi-Fi service for Government employees and third parties requiring secure guest internet-only access. Enabling users to roam between Government departments and remain securely connected to the internet.

Endpoints are authenticated to ISE as an AAA proxy and forwarded securely to GovWiFi AAA servers for authentication and authorisation.

Secure Gateway Service for large UK Government Department

Design, build, implementation, test, IT Health Check management and handover to operational support for a new Secure Gateway Service for the second largest UK government department.

The solution provided a secure gateway between circa 100,000 internal users, systems and applications with resources hosted in AWS, Azure, PSN, SaaS- based Internet services (O365, ServiceNow, Skype for Business), Secure Access Service Edge (SASE) services, the PSN, multiple third-party organisations and inbound Remote Access.

The service encompassed logical and physical separation, full inspection of encrypted content, mutual certificate-based authentication for system-to-system communication, a resilient high capacity Network, Intrusion Prevention Services, URL Filtering, Anti-bot capability, DNS sinkhole protection, Near zero day malware protection, traditional Anti-

Virus controls, full protocols breaks, certificate-based IPsec remote access VPN, SSL Remote Access VPN, virtualisation of Security gateway technologies and VM ware-based security gateways technologies.

The gateway service was underpinned by a highly secure management network that enforced separation of duties, a granular Role Based Access Control model, integration with Protective Monitoring systems, integration with Vulnerability Management technology and processes and securely hosted various enterprise management toolsets.

Secure Outbound Web Gateway

Design, build, implementation, test, IT Health Check management, migration of 100,000 users from a legacy third party service followed by handover to operational support for a new Secure Outbound Web Gateway Service for the second largest UK government department. The solution was delivered as both a Secure Access Service Edge (SASE) and on-premise deployment and encompassed a combination of resilient, enterprise class forward proxy appliances and multiple layers of Next Generation Firewall technologies.

The service included Kerberos authentication of users, integration with existing directory services, granular URL filtering with different policies for various categories of users, Intrusion Prevention services, Anti-bot capability, DNS sinkhole protection, near zero-day malware protection, traditional Anti-Virus controls, File Blocking profiles, HTTP header insertion and integration with existing Protective Monitoring systems.

Secure Remote Access Virtual Private Network (VPN)

Design, build, implementation, test, IT Health Check management, migration of 20,000 users from a legacy third party service followed by handover to operational support for a new Secure Remote Access Service VPN for the second largest UK government department. The solution was delivered as an on-premise, highly available and virtualised enterprise class IPsec VPN vendor. Authentication of remote users was accomplished using digital certificates and integration with internal directory services.

During the COVID-19 pandemic in 2020, the remote access service was enhanced considerably in order to support the department's contingency plans and enable secure remote home working for up to 65,000 users. The on-premise gateways were transitioned from an active-standby high availability deployment to a load shared active-active configuration to ensure that maximum benefit from the hardware appliances was realised. The number of virtual RAS gateways available to remote users was also increased by fivefold to a total of ten.

As a parallel activity, further remote access capability was deployed using the same vendor technology but hosted in AWS, increasing the overall remote access gateway capability available to users to forty five entry points and 130,000 users.

Global Hardware and Software Refresh Project

On behalf of a global gaming organisation, the network security estate comprising circa 80 gateways and management systems was subject to a hardware and software refresh programme. Deliverables included taking receipt of all new

appliance hardware, storing in a secure facility, creation of a pre-staging environment, initial checks of new hardware for defects, asset tagging new devices, preparing new software versions and hot fixes, migration of existing configurations for each gateway device to the new software version, license application, re-packing and secure distribution to the client for onward global distribution.

Vendor consolidation was also performed in order to standardise the network security estate, with configurations migrated from two other vendors to the chosen, strategic vendor technology.

Arts University, London: LAN, WLAN and Security

Design and Installation of an 8 node ISE distributed deployment.

Solution deployed as highly available and load-balanced for Policy Node access, across 2 data centres.

Migrated authentication services from legacy ACS Platform to new ISE solution.

Immediate requirement for Wireless authentication for 45,000 student and staff endpoints, with the future capacity to handle up to 60,000 endpoints in a fault-tolerant solution.

Asset Management Firm, Edinburgh: LAN, WLAN and Security

Installation of ISE Cluster for 2,500 endpoints at Edinburgh office. Installation of Cisco Prime Infrastructure.

Installation of Cisco Wireless Controller solution at Edinburgh and Singapore with approximately 40 x Cisco Aironet APs.

Configured and deployed Guest access via Sponsor portal.

Configured and deployed on-boarding and profiling services for BYOD certificate enrolment.

Subsequent upgrade to ISE across both sites, and integration of ISE with Citrix MDM solution for BYOD policy enforcement and compliance checking.

Design and installation of remote Cisco Wireless LAN Controller and Aironet Access Points for remote Singapore office deployment.

Asset Management Firm, London: LAN, WLAN and Security

Installation of ISE Cluster for 2,500 endpoints at London office. Installation of Cisco Prime Infrastructure.

Installation of Cisco Wireless Controller solution at London and Edinburgh with approximately 40 x Cisco Aironet Series APs.

Configured and deployed Guest access via Sponsor portal.

Configured and deployed on-boarding and profiling services for BYOD certificate enrolment.

Subsequent parallel installation of ISE Cluster as a distributed deployment across both sites, and migration from legacy ISE without disruption to service.

Subsequent upgrade to ISE Cluster across both sites, and integration of ISE with Citrix MDM solution for BYOD policy enforcement and compliance checking.

Automotive Firm, Sunderland: Greenfield LAN, WLAN, WAN and Security

Design, installation, configuration and support of Service Provider LAN, WLAN and WAN. Installation and configuration of Cisco IOS XE Switches.

Installation and configuration of Cisco Catalyst Switches. Installation and configuration of Cisco SSO WLCs.

Installation and configuration of Cisco Aironet Wireless Access Points. Installation and configuration of APC UPS Systems.

Design and installation of copper and fibre structured cabling.

Design, installation, configuration and support of open-source monitoring platform.

Automotive Firm, Sussex: Greenfield LAN, WLAN, WAN and Security

Design, installation, configuration and support of Service Provider LAN, WLAN and WAN. Installation and configuration of Cisco IOS XE Switches.

Installation and configuration of Cisco Catalyst Switches. Installation and configuration of Cisco SSO WLCs.

Installation and configuration of Cisco Aironet Wireless Access Points. Installation and configuration of Cisco ASA HA Firewalls.

Installation and configuration of APC UPS Systems.

Design and installation of copper and fibre structured cabling.

Food Manufacturer, UK: LAN, WLAN, WAN and Security

Design and installation of Cisco Unified Wireless Network to provide EAP-TLS corporate access, guest Wi-Fi services and factory Wi-Fi access in challenging temperature environments.

Design and installation of separate LAN overlay network for factory LAN and WLAN, secured with Cisco HA firewall pair between corporate and factory infrastructure.

Consultancy, design and installation to upgrade resilient Telco WAN links and upgrading from static routing to fully resilient OSPF dynamic routing across the European WAN.

Law Firm, London: LAN, WLAN and Security

Installation of VSS core switch solution for LAN, with an additional 60 x Cisco Catalyst access switches.

Installation of approx. 100 x Cisco Aironet Series access points.

Integration with existing ISE solution, and troubleshooting / remediation of issues from incumbent installation.

Configured and deployed Guest access via Sponsor portal. Integration with Cisco Prime Infrastructure.

National Animal Welfare Charity, UK: LAN, WLAN and Security

Consultancy to troubleshoot and remediate ISE policies and posture enforcement on an existing ISE Cluster installation of approximately 2,500 endpoints.

Proposed and implemented a parallel upgrade of ISE and fully-managed the migration.

Design, installation and ongoing maintenance of Cisco SSO Wireless LAN Controllers and DMZ Wireless LAN Controllers.

Design and installation of Cisco Prime Infrastructure to manage the UK wired and wireless LAN infrastructure.

Sports/Entertainment Stadium, London: LAN, WLAN, Security and CMX

Design and installation of Cisco Unified Wireless Network to replace aging hybrid solution comprising from Cisco, Xirrus and Motorola autonomous Access Points with Cisco Wireless LAN Controllers and Aironet Series Access Points.

Design and installation of LAN infrastructure refresh project to reutilise and replace the aging LAN estate comprising of Cisco 2900 and 3750 Catalyst switches with Cisco VSS chassis and IOS XE stackable switches.

Hardware Encryption Service

Encompassed build, pre-stage, asset tagging, secure distribution, installation and test activities for circa 200 Enhanced grade hardware encryptors. The solution delivered secure high-speed VPN services to protect assets at Confidential level for a major UK government department operating at legacy Business Impact Level 4.

6. Clients



Department
for Education



dti



Department
for Work &
Pensions



HM Revenue
& Customs



HSE
Health & Safety
Executive



Office for
National Statistics



Home Office

7. Contact Details

Further details on any of the services provided by Cybernetica can be obtained by:

- Calling us on 0330 3112569
- Email to ukhmg@cybernetica-solutions.co.uk
- Online at www.cybernetica-solutions.co.uk



Cybernetica Solutions Limited

7 Victoria Road
Tamworth
Staffordshire
B79 7HS



www.cybernetica-solutions.co.uk
ukhmg@cybernetica-solutions.co.uk
+44 (0) 330 311 2569

Crown
Commercial
Service
Supplier