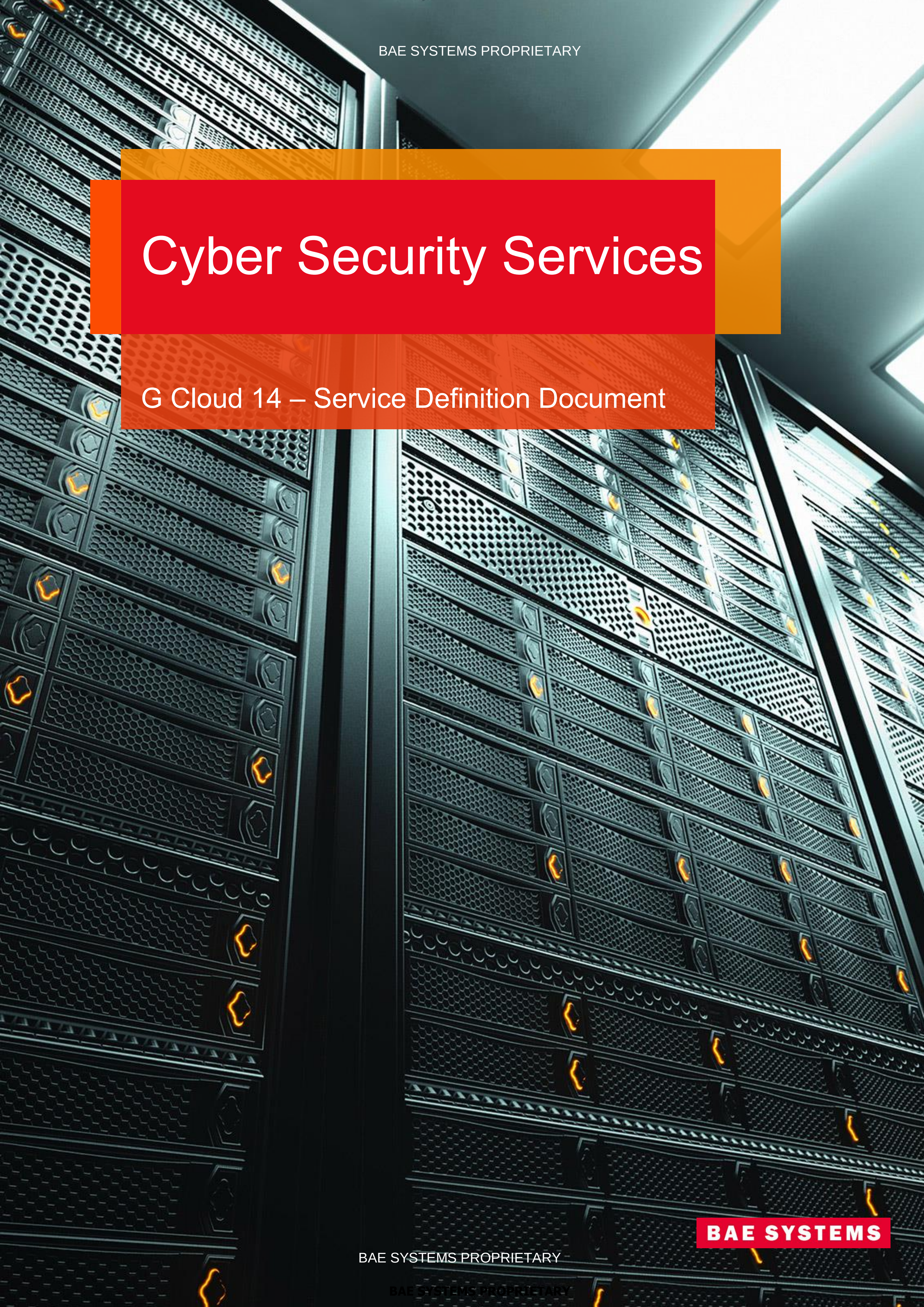

Cyber Security Services

G Cloud 14 – Service Definition Document

BAE SYSTEMS PROPRIETARY

1 Introduction

BAE Systems Digital Intelligence registered as BAE Systems Applied Intelligence Limited delivers solutions to protect and enhance client's critical assets in the connected world. Our solutions combine large-scale data exploitation, 'intelligence-grade' security and complex services and solutions integration. We operate in the following domains of expertise: Cyber Security; Financial Security; National Security; Data Analytics; and Digital Transformation.

BAE Systems is a defence company with a long history of driving successful innovation in massively complex integrated systems. We are well established across HMG as providers of a variety of services all of which are undertaken by a qualified team of experts, experienced in supporting HMG clients and in designing, implementing and managing Cloud Services.

We have a range of Data, Digital and Cyber services available on G-Cloud, to help organisations to define and implement cloud strategies and services, successfully adopt cloud services, manage the change required, defend themselves and manage their security responsibilities when utilising cloud services. This document covers our Cyber Security Services.

2 Risk and Intelligence

The Risk and Intelligence offering enables customers to understand and manage risk in a pragmatic and cost effective manner in light of the changing technology landscape, escalating threat and evolving standards. As providers of both cyber security platforms and a comprehensive suite of cloud security services, our security experts have a deep understanding of threat, risk and the mitigations required to manage the full spectrum of security based risks to an organisation. We enable our customers to understand and manage risks arising from the use of cloud services by combining analytics and our world class threat intelligence to support good risk management decisions aligned with both HMG and international best practice/standards.

It uses the latest threat intelligence and risk knowledge to inform the Board level of an organisation, supporting the risk posture, prioritisation of capability, and strategy for risk management. This flows down to project and live service level engagements to deliver risk analysis, security improvement and implementation assurance through the IT lifecycle for the design, implementation and management of Cloud services.

We work with your business and technical stakeholders to establish the questions you need cyber risk to answer and through our proven methods and analysis provide answers and practical recommendations. We can help you identify the specific questions you want to answer with cyber risk analysis. We assess the security of your business operations to prioritise practical recommendations for risk reduction and use unique insight into current cyber threats to assess the scale and nature of how the cyber risk landscape affects how your organisation operates. We communicate at executive level answers to your questions about cyber risk.

Our risk and intelligence services may cover IT, Operational Technology, organisation, cultural and physical domains and working within the scope of regulatory frameworks including Cabinet Office, General Data Protection Regulations (GDPR), Network Information Security Directive (NIS) and others.

3 Security Engineering

Security Engineering service creates new secure systems for organisations or assesses and improves the security of existing systems. Our capabilities span security architecture, security testing and secure implementation, utilising specialist cyber and cloud knowledge to produce solutions that are secure by design which can protect against specific threats.

Our approach allows you to understand the level and shape of the investment your organisation needs, to identify cost savings and thus ensure that you are spending your security budget on what is right for your organisation.

We help organisations improve their security engineering and organisational robustness, including performing architecture reviews and controls assessment (including in combination with penetration testing) to provide technical assurance of the ability of organisations, Cloud services, or applications hosted in the cloud, to withstand cyber-attack, identifying appropriate measures to ensure the resilience of a platform and developing business-driven, risk focused security architectures that traceably support business objectives using a proven methodology.

Our Security Engineering services may also cover Operational Technology systems and platforms, including industrial, SCADA and transport or defence environments.

4 Security Operations

Our cyber security operations expertise enables organisations to protect against the full range of risks to their cloud-based operations and assets. From providing visibility of the threats, the ability to respond to attacks, through to training and knowledge transfer, our solutions provide an extensive cyber security capability for the cloud.

The Security Operations offering enables customers to define, implement and sustain operational monitoring and incident response capabilities to a level commensurate with the organisation’s risk exposure and focussed on defending its key cloud-based assets. They include a range of advisory and delivery services, including integration with BAE Systems threat analytics technology.

Casual attackers may be defeated by well-maintained defences. But targeted attacks are launched by determined adversaries who use research and repeated attempts to identify weak links and evade safeguards incrementally.

We advise organisations on their security operations, including defining the security operations required based on the threats faced by the client, delivering tailored maturity assessments with associated gap-analysis and developing a security operations roadmap and performing detailed design work to help define the business and/or technical blue prints required to build their security operations capability.

We implement the required security operations within a client organisation, including executing the design, implementation and operation of the security operations capability and helping clients improve their capability, including process and architectural improvements, and demonstrating value from security operations to deliver pragmatic and tangible benefits.

5 Privacy and Trust

Privacy is an evolving and complex landscape. Organisations must build "digital trust" with their users in order to successfully operate in the cloud. We work with our customers to help them manage privacy in a way that builds customer trust and embeds excellent privacy practices into their operations. This requires full engagement with the privacy agenda and proactive engagement with customers and users to build the trust and establish where and how trusted services can gain maximum engagement with their target audiences.

We advise organisations on privacy principles and digital trust, including understanding the art of the possible to enable optimisation within privacy demands and constraints, and investigating the differing requirements for digital identity (citizen, customer, staff etc.) and defining strategic approaches to managing these.

We design and / or implement privacy principles and digital trust, including evaluating business process and data flows to ensure privacy by design principles are implemented throughout the organisation or programme and designing the key elements of end-to-end identity management within a particular business process, in particular integration with identity providers.

Typically we may look at General Data Protection Regulations (GDPR), the Data Protection Act (DPA), Privacy and Electronic Communication Regulations (PECR) and other regulations depending on jurisdiction.

6 Cyber Transformation Programme

Our cyber transformation programme services will support and enable organisations to design, implement, adopt and manage security change and transformation to enhance the overall maturity of an organisations security architecture/practices. Our Security Transformation Services are focussed on ensuring organisations are able to undergo change and transformation, whilst still achieving the targeted security and risk benefits. Our Security Transformation Services enable organisations to:

- Identify, scope, plan, deliver and realise the benefits from security transformation programmes, projects and initiatives.
- The identification and development, benefits identification, tracking, management and realisation, change management, reporting, stakeholder management and delivery.
- Ensure the targeted end-state and security and risks benefits are achieved in the face of changing external threat, technology, competitive and geopolitical landscapes, and internal organisational change and evolution.

Our approach and implementation is tailored to the organisation's own structure, constraints and business context. Our teams integrate into the organisations wider change transformation, security, risk and governance structures, along with internal and external stakeholders to enable delivery as part of the organisation, and its wider supplier ecosystem.

As part of Security Transformation, we may include any of our other services, as necessary to deliver the transformation objectives such as access to our specialists security and cyber capabilities including research, development, penetration testing response advisory and consulting services, whether in the ICT or Operational Technology domain.

Our threat-led and risk based approach ensures the scoping, delivery and management of security programmes remains relevant to the business and organisational challenge and context, and changes in the wider ecosystem.

7 Security Management Services

Our Security Management services offer information assurance, compliance and accreditation management, as well as security and penetration testing and a range of further security-focused capabilities. This service reduces the risk of information compromises and security breaches, and improves response effectiveness in these situations.

We enable customers to scope, run and manage the security of the organisation at any or all of tactical/operational, management and strategic layers. Our Threat-led Security Management Services are integrated into the overall organisational security risk and governance, and internal and external stakeholders, include third party suppliers, to continuously:

- Review, assess and manage the risk to your organisation. Responsibility for management and maintenance of accreditation status and risk across your ICT and Operational Technology (OT) estate.
- Integration and working with internal and external stakeholders and supplier.
- ISMS definition, management and maintenance.
- Provide business relevant reporting, KPIs KRIs and KGIs to leadership and governance team as part overall organisational risk governance.
- Support projects and programmes throughout their lifecycle, and integration into operational and transformational initiative, activities and functions.
- Delivery of security technical design authority, assurance and support.
- Incident management, reporting and response.
- Leadership and strategy.

Each service is scoped and tailored to your operational and organisational context, to integrate into your organisation, as required, to support and augment our current capability. Our services may be delivered to support, bolster or augment existing capability or deliver security management and coverage of dedicated business areas, functions or capabilities. Our Services make use of our capabilities and insight including our threat research, intelligence risk, and specialist cyber capabilities to support the security and risk management of our customers.

Our Service ensure that a consistent and appropriate approach to security is applied across both your ICT and OT domains, through integration and collaboration with internal teams, functions, wider Service Integration partners, Managed Suppliers, Cloud Suppliers and other third party organisations and stakeholders, including regulatory if required. While responsibility for accrediting individual systems rests with the relevant Business Areas or Managed Suppliers, the Security Management Service may retain responsibility for the accreditation status of the overall ICT and OT estate and the risk profile that it presents.