baesystems.com/government

# Helping Secure Government Organisations Establish Integrated Low-side/High-side Working Practices

BAE SYSTEMS

# 1 Introduction

In recent years, in response to rapidly changing market dynamics, government organisations with protectively marked networks – even those operating almost entirely within air-gapped, siloed environments - have sought to implement a new operating architecture: the division of operations between a secure, 'high-side' network, and a network of lower security classification – a 'low-side' network where users have access to the internet and to a wider range of new digital technologies. Under this new architecture, classified work is still conducted on the high side under the strictest of policies, however depending on the risk appetite of an organisation, a significant percentage of daily operations and the development and support of applications can be conducted on low-side networks.

BAE Systems is a global leader in helping secure government organisations establish low-side to high-side working practices. In this white paper we introduce considerations for low-side working, summarise key benefits for customers and discuss how BAE Systems can help secure government customers move workloads, application development and some mission capability to low-side environments. The paper has the following structure:



# 2 What is Low-Side Working?

Traditionally, the majority of daily operations and mission capabilities of secure government organisations have been conducted in secure 'air-gapped' high-side environments. However, there is a growing realisation that not all aspects of high-side work need governed by the same security policies. When examined through a different lens, it is possible to break down day-to-day operations into different groupings. Some of these will always by default and necessity be subject to the most stringent of policies.

However, it may be possible to identify activities which could be conducted within environments with lower security classifications and by staff with lower security clearances. If so, many of the historic restrictions surrounding those activities could be relaxed when they are transferred to low-side operating environments. In addition, even though at a macro level some individual activities may appear to require a top security classification, it may be possible to break down those activities into bite-size components where some elements could actually be performed within low-side environments.

# 3 The Benefits of Low-Side Working

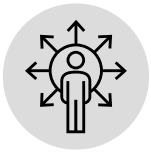
There are significant benefits for those able to implement secure low-side working practices within secure low-side environments. These include:

**Greater access to new technologies**
An ability to benefit from new technologies and recent technology shifts including increasing use of public cloud environments, Infrastructure as Code, containers, cloud-native tools, microservices and automated security testing.

**Faster development times**
In comparison to high-side environments, engineering teams operating on the low side are able to take greater advantage of modern engineering methodologies such as DevSecOps[1] and Agile working, which when combined with greater access to new technologies, facilitates the more rapid development of new applications and systems. By using Continuous Integration/Continuous Delivery (CI/CD) pipelines integrated across the low-side to high-side boundary, application code can then be synced and deployed on the high side in a relatively fast and seamless fashion.

**Lower Cost**
In general, the costs of working on low-side networks should be lower than those conducted within high-side environments. For example, developers working on the low side can make use of SaaS tools and have easy access to Open Source libraries.

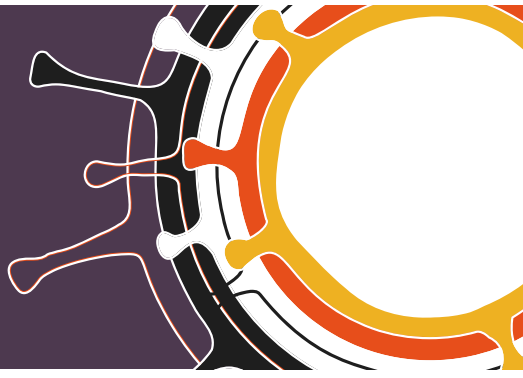
**Access to more staff**
High-side environments require experienced, vetted staff with appropriate clearances. Employees must work onsite and live locally. This limits the available talent pool, increases staff costs and reduces flexibility to respond to changing working conditions. In comparison, low-side working is not limited to a specific geography, and can be established where talent is plentiful and more affordable.



**Flexibility**
Low-side working enables significant flexibility in business operations. Managers have greater flexibility to allocate resources according to changing working conditions, and mission requirements.

**Staff morale and retention**
As the digital revolution continues, finding and retaining appropriately skilled cleared staff has become increasingly difficult for many government organisations. Organisations that operate within siloed environments have found it harder to retain staff who wish to enjoy the same digital capability within their working environments as they do at home. By switching to low-side working practices, employees may be granted more digital privileges: this contributes to staff morale and helps organisations retain staff.

In early 2020, the COVID-19 pandemic forced many organisations to shift from office-based to home-based working. Organisations practising low-side working were able to continue many aspects of their operations, progress engineering projects, and minimise impact to their mission capability.



# 4 Considerations for Low-Side Working

**Protect High-Side Environments**
Understand and remediate the threat: The fundamental consideration for all low-side working initiatives is to protect the security, integrity and operational capability of high-side operations. Ultimately, there is a balance to be found between the benefits which low-side working can bring, versus any possible risks that may be introduced.

To do this, organisations must understand what is proposed to be done on the low side and the threats against which they need to protect, who they may need to protect themselves from, why attackers may wish to attack them, and how they might try to do this. For example, threats may arise from:

- Initiating a new attack surface through establishing a connection across an air-gap to an external network
- Enabling the importing of data/code from the low side to the high side which could carry malware, establish exploitable vulnerabilities or underpin new attack-vectors which could be taken advantage of by external threat actors
- The loss of sensitive data or valuable intelligence on the high-side mission/infrastructure through the deliberate or accidental export of data to the low side.

**Cross domain communications between low-side and high-side environments:**
For low-side working to be practical and efficient, secure data links and communications must be established between those working on both sides of the low-side/high-side divide. This includes:

- Ability to export/import data securely (e.g. output from DevSecOps developments/software patches and software upgrades to infrastructure on the high side.)
- Secure voice and video teleconferencing
- Secure emails
- Messaging (e.g. of system health) transmitted between a high-side and low-side network which enables support of high-side applications from the low side.

## Shaping and managing low-side engineering projects

Engineering projects conducted on the low side need to be scoped by experienced engineers with sufficient knowledge, clearance and exposure to high-side mission working to understand what elements of any project can be conducted on the low side. Likewise, when projects are underway on the low side, oversight must be applied to both ensure that the scope of the work does not stray into more securely classified areas, and that the work once complete, will match high-side mission requirements. This can often only be achieved by supplying engineering staff on the low side who have high-side clearances and a working knowledge of high-side mission requirements and operational capabilities.

During the process of shaping the work that low-side teams can perform, it will be necessary to review any content that is transferred to the low side and ensure that that any information or business logic elements of higher classification are obfuscated, redacted or removed. In the development of the workflow, a 'plug-in' application framework may be constructed which utilises configuration-based data models. This can then facilitate the output of low-side workstreams to be inserted into the framework on the high side, or in reverse, for high-side classified modules to be added to low-side outputs when transferred across the low-side/high-side divide.

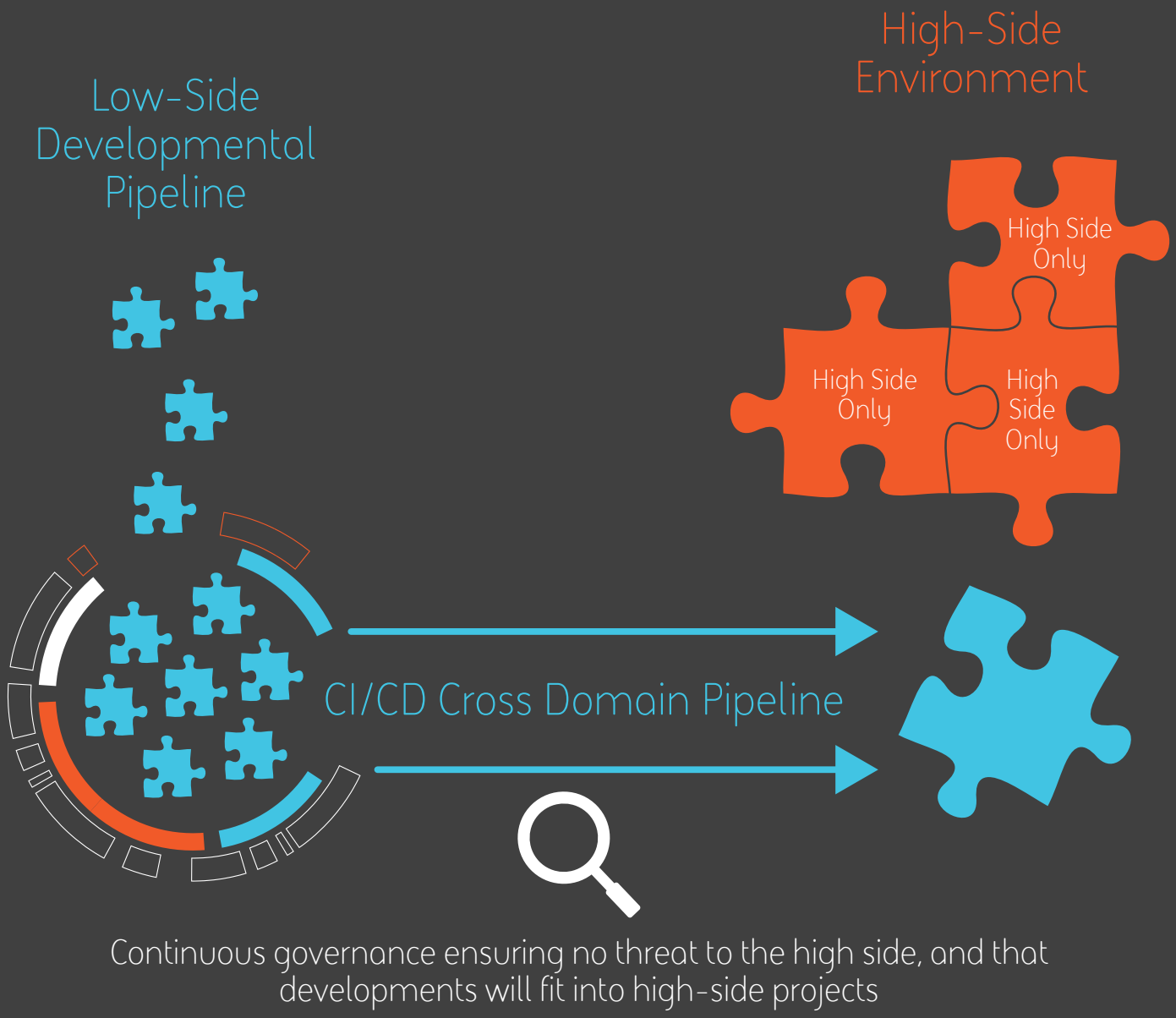



**Figure 1**
A development project may be divided into multiple-sub components, some of which must remain on the high side but others of which can be safely left on the low side and then exported to and assembled on the high side

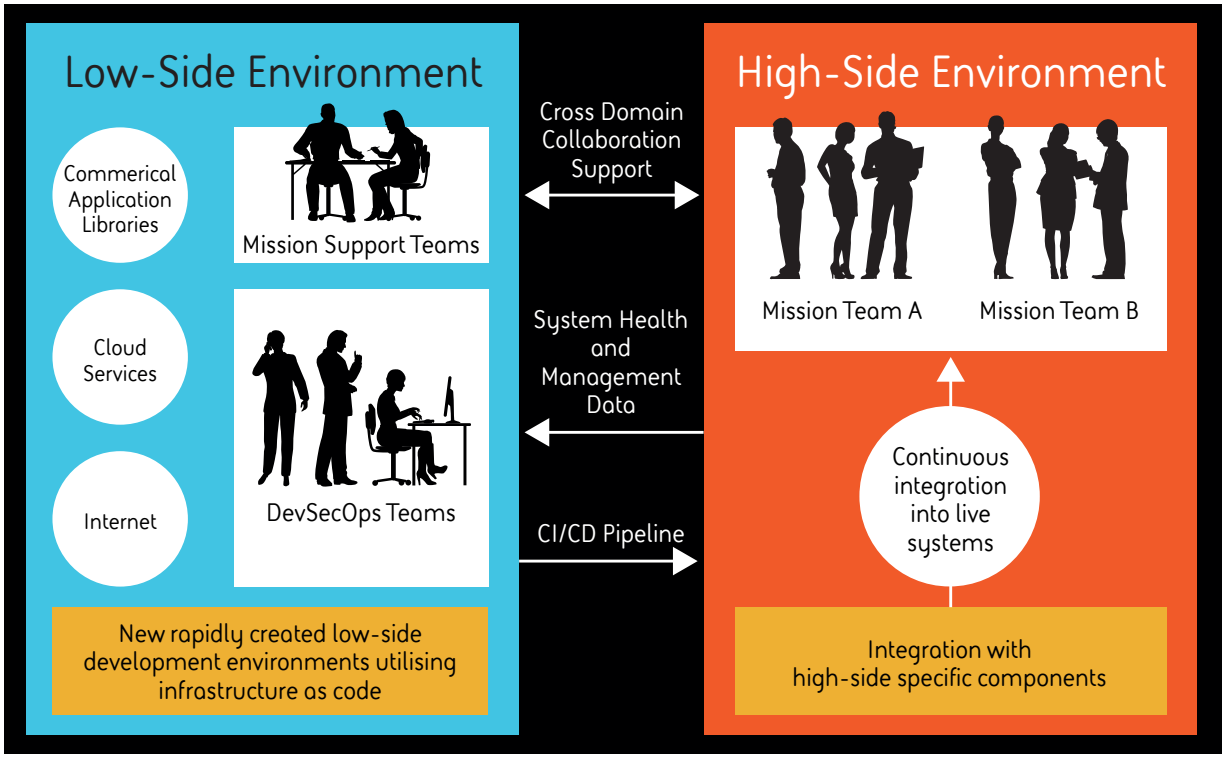
**Working with representative but sanitised data sets on the low side:**
When DevSecOps teams start to build new applications on the low side, it's important any components of their developments that are built to use, process, analyse or display data are supplied with sufficient data which is representative of data that will be used in the finished product on the high side. Typically, such data is manufactured so that it is not protectively marked and can be made available to the low-side engineering teams.

- **Testing:** Under DevSecOps practices, any low-side engineering work would have a suitable level of testing built into it to provide assurance that work completed would be safe, secure and function appropriately. However, in general, low-side testing should not be entirely trusted to protect the high side, and a subset of tests should be repeated on the high side before any code is made fully operational.

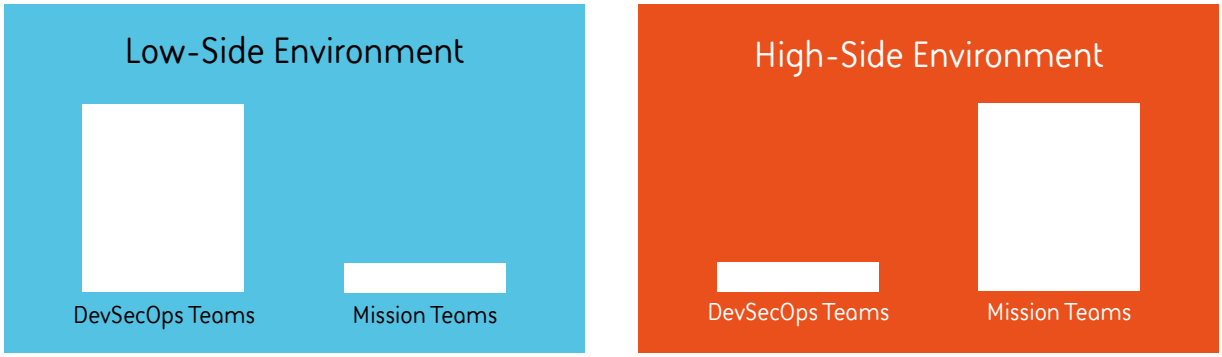
- **Audit:** In all aspects of low-side to high-side working, it is important that a clear audit trail is created and maintained for all decisions, approvals, testing of code releases and data transfers.

- **Patching:** Within new low-side to high-side working practices, new technology and commercial applications/systems may be implemented on both sides of the divide. It is important to ensure that all systems are regularly updated and patched, to guard against known vulnerabilities.

- **Penetration Testing:** To ensure ongoing security, regular penetration testing of existing and new systems/infrastructures is advised.




## Number of Teams



# 5 BAE Systems' Capability

Our experience has evolved from helping government customers develop low-side working practices to become more competitive, embrace new technologies and expand their talent pool. From this privileged position, we have not only been able to help develop new working practices and learn from the journey, but we have been able to develop new reusable business and technical patterns that enable more efficient and secure low-side to high-side working.

## What we've already learned

**The importance of mission knowledge**
An understanding of the mission is critical in defining and employing low-side working practices. Through our close relationship with our customers, we have been able to tailor our best working practices to each customer and their mission, maximising efficiency and minimising risk to the organisation.

**How to make low-side to high-side working secure:**
To enable secure low-side/ high-side operations, the inclusion of Cross Domain Solutions is key. To protect the high side, these solutions need to be approved for use at the highest level. Over the past decade BAE Systems has worked with Governments and the Five Eyes community to design, test, build and put into operation a range of hyper-secure FPGA-enabled Cross Domain Solutions which currently underpins many such low-side to high-side working environments, supporting the secure import/export of data, collaboration and secure browse between networks.

**To mitigate the risk of malicious or unauthorised transport of data between domains (accidental or deliberate) in low-side to high-side environments, BAE Systems has built additional controls into its Cross Domain Solutions:**

- To check the content of data transmissions (e.g. keyword scanning) against policy and authorised content (white lists/black lists)
- To alert when unauthorised content is detected
- Which applies business logic for quarantine or release control when suspicious content is detected and needs additional authorisation. All transfers and human actions are audited.

**Understanding the role of security-cleared staff:**
Low-side to high-side working provides greater flexibility in the employment of vetted staff. When designing engineering workflows and work practices, we understand how to optimise the use of the full range of cleared or non-cleared staff across the span of projects, without threatening the security of a customer's mission. On a day-to-day basis, due to the nature of our exposure to government clients, we have an extensive pool of cleared and vetted staff which we can use to support government clients, as required. During the Covid-19 pandemic, we were able to help triple the number of staff working with government clients on low-side working, thus helping our customers to maintain operational capability.

**DevSecOps Experience:**
The establishment of new low-side to high-side working practices goes hand-in-hand with new engineering methodologies. Over the past decade, we have helped our customers to adapt modern methodologies such as DevSecOps to a secure environment.

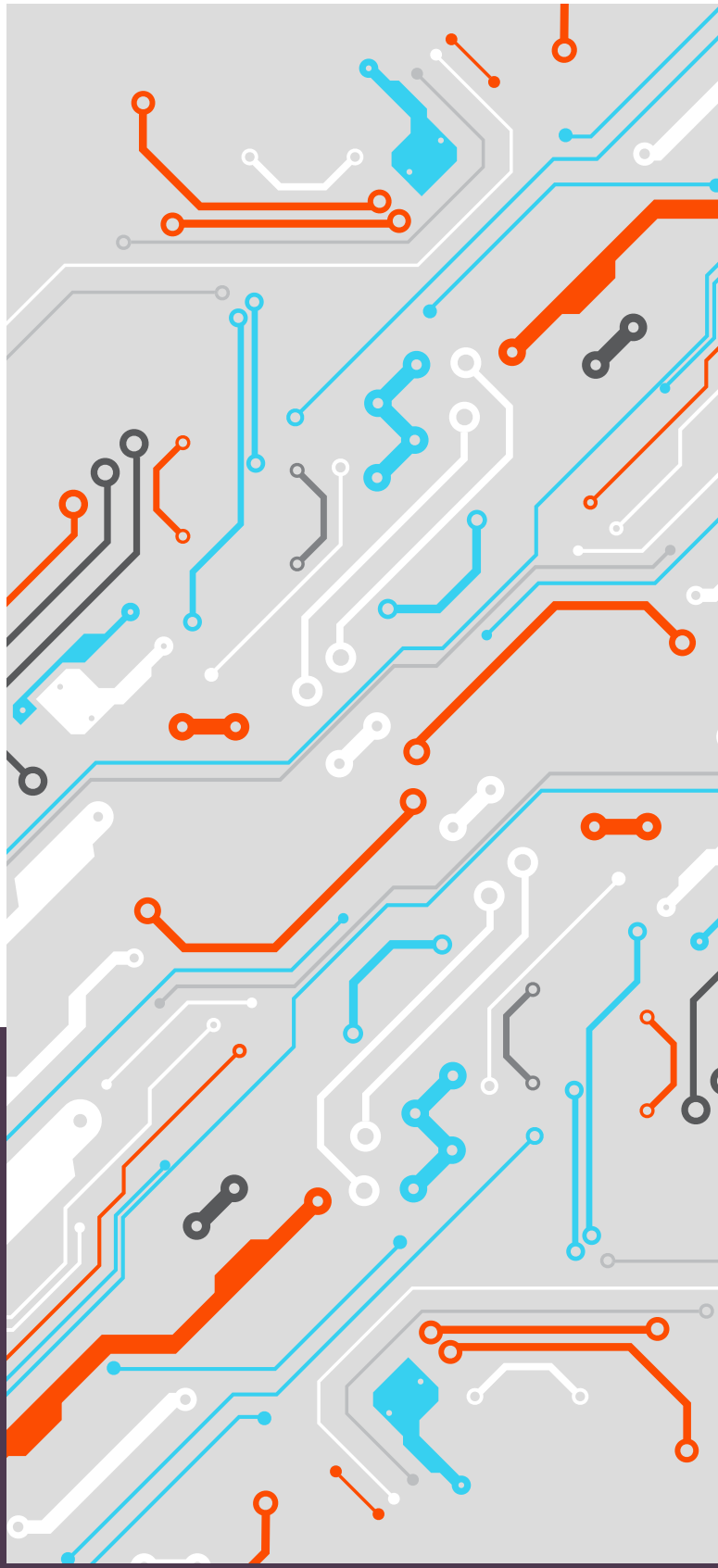
**A threat-based approach to cloud security:**
Acknowledging that each customer is different, we have developed approaches to cloud security which help organisations evolve from taking a traditional risk avoidance approach, to actively managing the risk, and enabling low-side working where appropriate. In this process, we analyse and assess the cyber risks and threats relating to each proposed use-case and business process, along with the wider business context. This, along with an in-depth technical understanding of the technologies and platforms in use, enables us to determine the appropriate controls and mitigations to ensure the risk is managed, and that it may be evidenced to wider auditors or accreditors. This helps organisations to balance the cost and efficiency benefits with the cyber and mission risks of carrying out low-side work.

# New technical enablers

**Building Infrastructure as Code for low-side environments:**
Stemming from our experience in DevSecOps engagements we are now delivering projects which use Infrastructure as Code to instantiate the development environment. In these projects we are automating the creation and configuration of secure development infrastructure, enabling engineers to spin up a virtual, reliable and secure, accredited development environment in minutes rather than days or weeks.

**Building Cross Domain Enabled Low-Side/High-Side offices of the future:**
A recent focus of development has been enabling the secure and efficient operation of office tools between low-side and high-side domains (e.g. syncing of confluence pages between domains (with appropriate redaction), use of Atlassian tooling across domains, and secure browse down. (For further examples please contact us.) Combined with our expertise in cross domain collaboration solutions and our developments in Infrastructure as Code, we are now developing frameworks for complete office environments tailored to low-side or high-side working.

**Common Development Services:**
Enforcing security best practices: establishing common services, such as code pipelines, secret management and artefact repository management which encapsulate cloud and security best practice can be a force multiplier allowing multiple teams to benefit from re-use of trusted services.



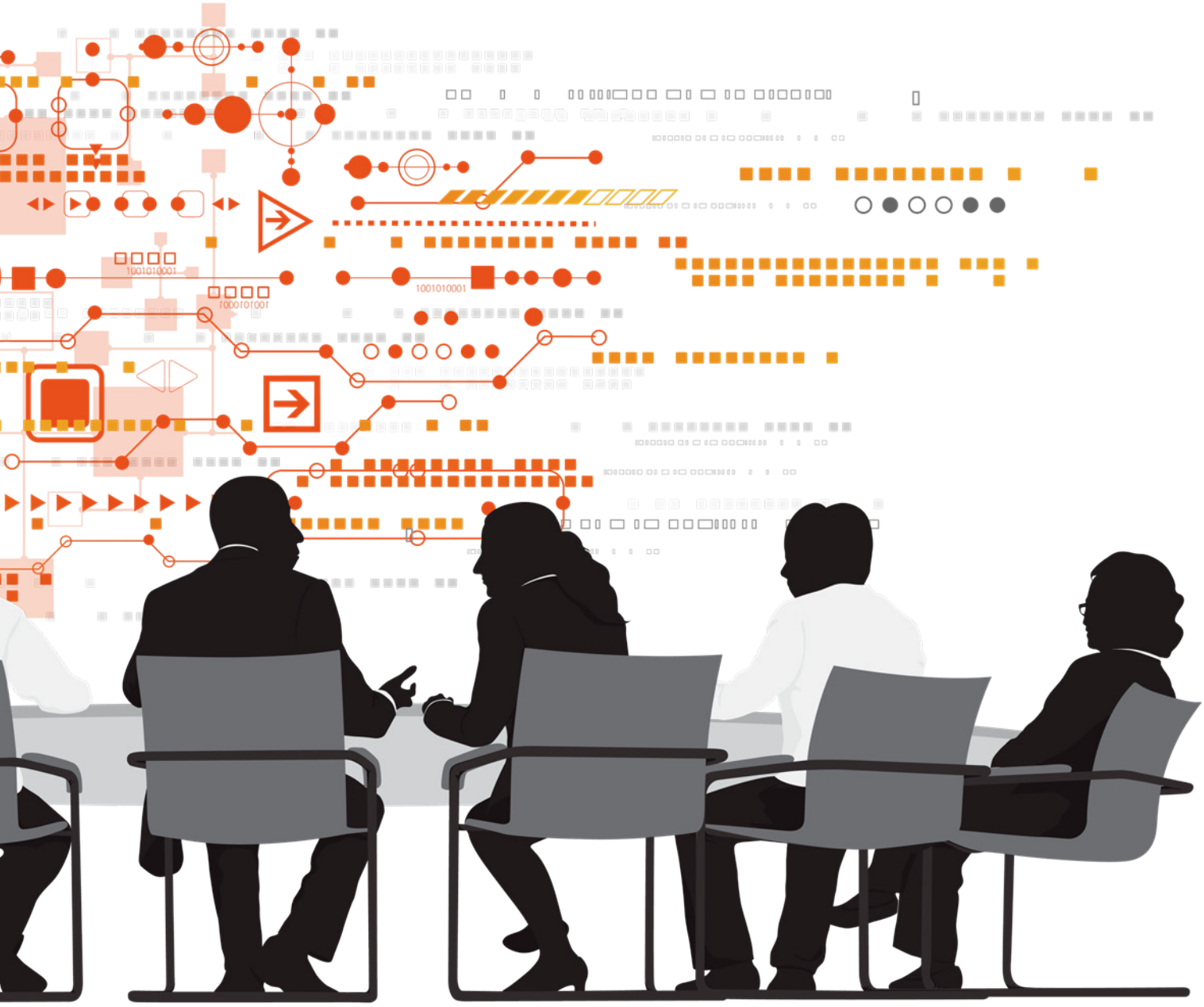
From these and other developments, we are evolving ways of working in low-side environments that package up our experience - combining both new technical components and maturing processes and workflows - that can be reused and reapplied for new customers in other low-side to high-side projects.

# 6 Summary

Hybrid low-side and high-side working will increasingly transform the operational capability of secure government customers. It will enable them to be more agile in the development of new applications, giving them access to the benefits of more efficient and less costly ways of working which utilise modern digital services such as cloud ecosystems and Infrastructure as Code to rapidly spin up new working environments.

For secure government customers interested in making this transition, BAE Systems already has proven excellence in this area. Under normal business conditions we have hundreds of appropriately security cleared developers in low-side development teams who regularly deliver high quality, reliable, performant code onto high-side domains, without the expense and resourcing challenges normally associated with large high-side teams.

**If you are interested in learning how low-side to high-side working can enhance your mission capability, please contact BAE Systems.**



We are

**BAE SYSTEMS**

At BAE Systems, we provide some of the world's most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.


Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 1
14 Childers St
Canberra
ACT 2601
Australia
T: +61 1300 027 001

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000



BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/government

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai