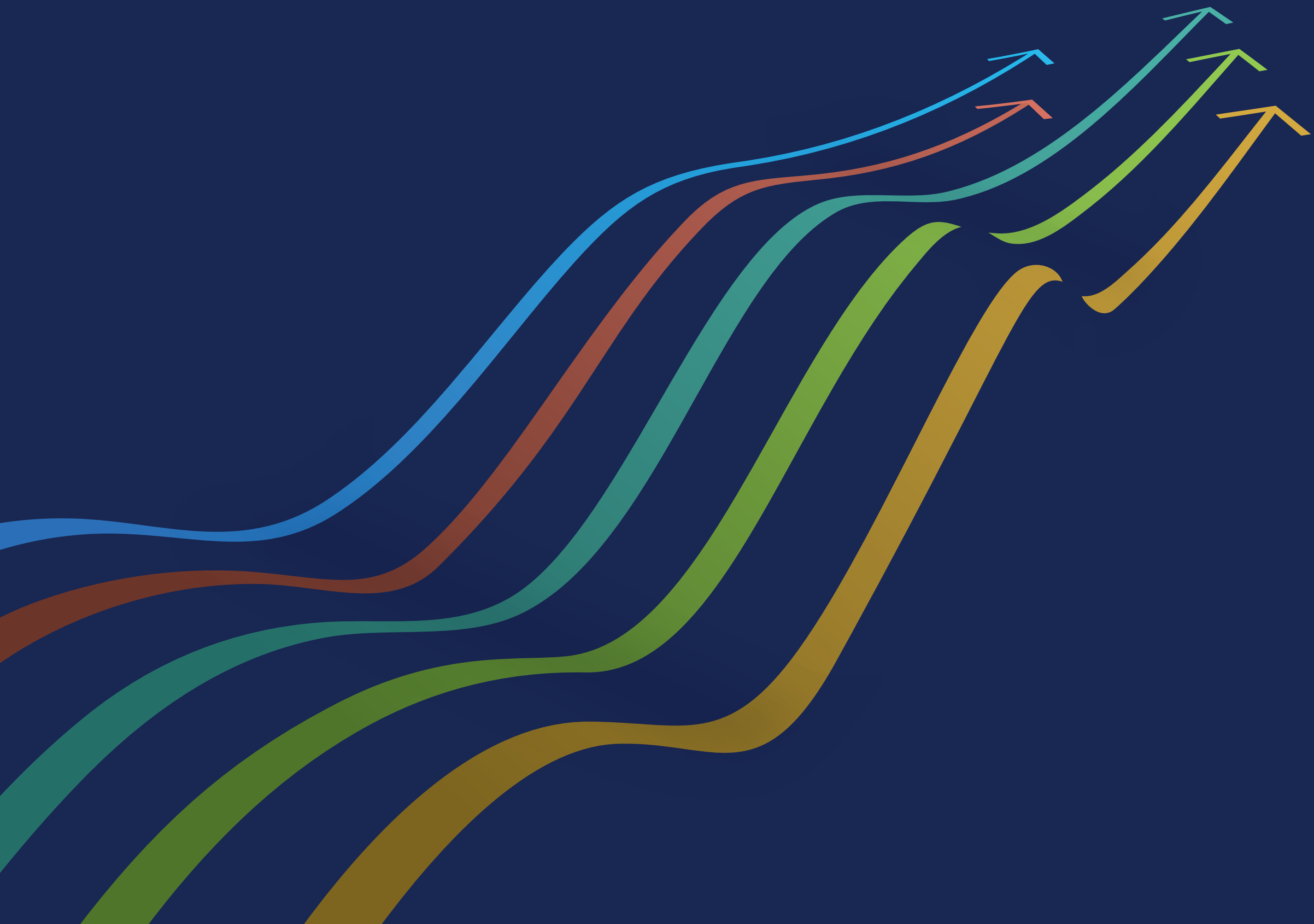
Government
Security

Government Security Centres 2024/25 in Review

Simpler. Smarter. Streamlined.



Contents

Introduction from the Government Chief Security Officer

This has been another successful year for the Government Security Centres. Over the past 12 months the GSeCs have continued to provide expert, scalable services to a growing number of public sector organisations. They are firmly part of the security landscape, supporting us all in improving resilience and driving up standards, whilst delivering excellent value for money.

The GSeCs provide a model for how we should do business in the security function:

- They are a key vehicle to grow and share our professional expertise;
- They enable us to raise standards and performance right across Government, in large and small departments, in the centre and in our Arms Length Bodies.
- And, critically, they enhance our efficiency and productivity by providing scalable, expert services that it would not be affordable or cost-effective to replicate across all departments.

This year will see the publication of a new GSeCs three year plan, endorsed by the Government Security Board, which will guide activity out to 2028. The plan has three key pillars of activity:

- supporting departments and organisations;
- creating strategic interventions; and,
- building converged capability

The plan also sets out the key priorities for GSeCs over the next three years. These include:

- Government Cyber Security Strategy;
- Supply Chain Security;
- Insider Risk management;
- Asset Management; and,
- Security Culture

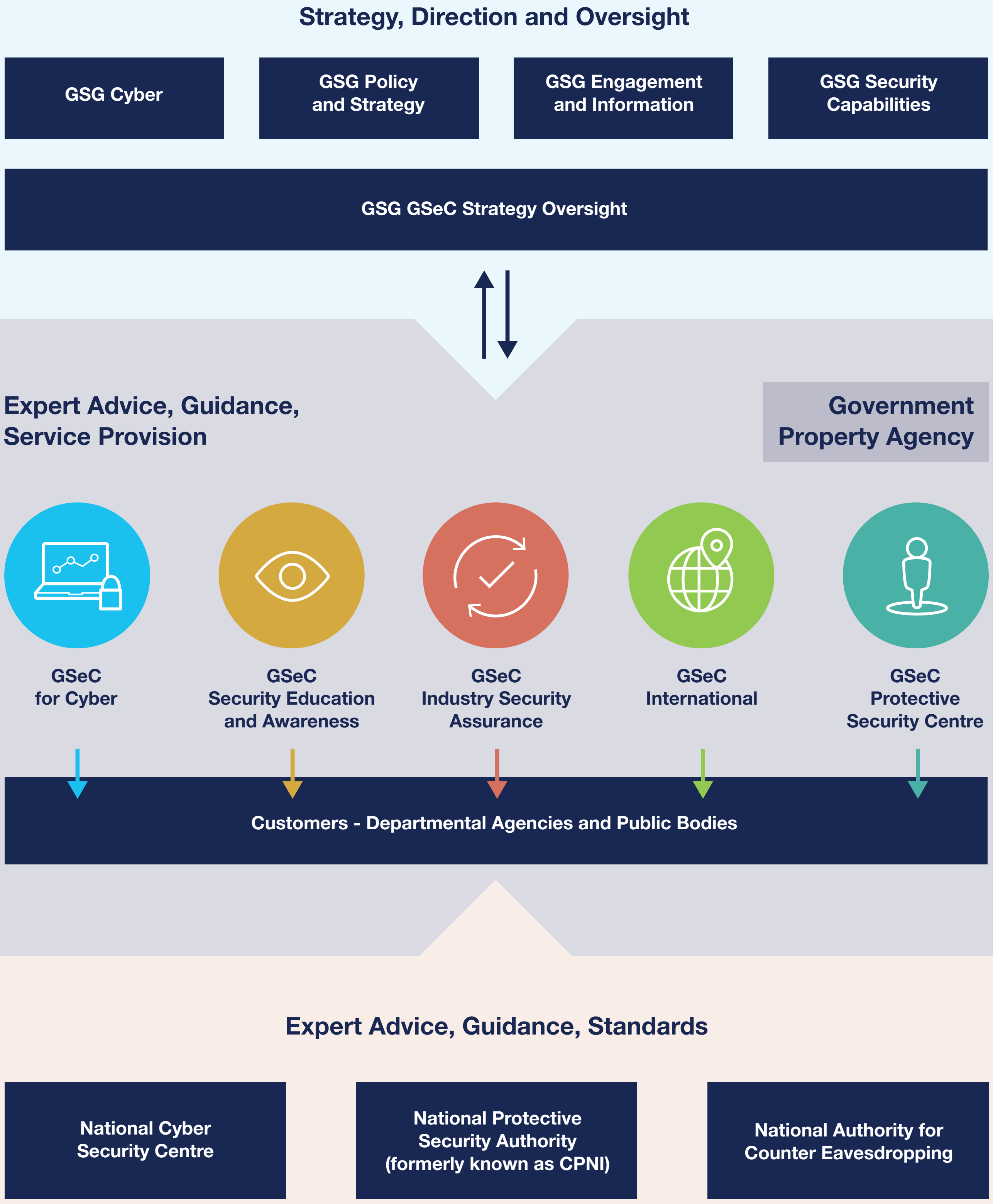
The success of the GSeCs largely depends on the support and buy-in from Government organisations who continue to recognise their value and use their services and guidance.

Thank you to all those who have contributed to the continuing achievements of the GSeCs model.

Vincent Devine

Government Chief Security Officer

The Government Security Centres Ecosystem



Strategy, Direction and Oversight

- GSG Cyber
- GSG Policy and Strategy
- GSG Engagement and Information
- GSG Security Capabilities

GSG GSeC Strategy Oversight

Expert Advice, Guidance, Service Provision

Government Property Agency

- GSeC for Cyber
- GSeC Security Education and Awareness
- GSeC Industry Security Assurance
- GSeC International
- GSeC Protective Security Centre

Customers - Departmental Agencies and Public Bodies

Expert Advice, Guidance, Standards

- National Cyber Security Centre
- National Protective Security Authority (formerly known as CPNI)
- National Authority for Counter Eavesdropping

Government Security Centres in Numbers

GSeCs Customer Survey High Level

81%

of survey respondents said they think the GSeCs ‘provide’ or ‘somewhat provide’ Value for Money services.

78%

of respondents have, or are intending to, implement recommendations from the GSeCs.

73%

of respondents believe that receiving recommendations improved or somewhat improved their ability to communicate security improvement requirements to stakeholders in their organisation.

Security Education and Awareness Centre (SEAC)

5,917

documents downloaded from Knowledge Hub and **480** active members.

250,000

users accessed Security and Data Protection eLearning from **over 100** departments.

1,700

line managers from **70** departments attended Personnel Security campaign webinars.

1,373

downloads of **‘Share With Care’** campaign materials.

Protective Security Centre (PSC)

20,000

insider risk cases handled through aftercare services.

150

interventions to help build security capabilities, **up 285%** on 23/24.

4,700

views or downloads of pieces of Thought Leadership, a **115% increase** from 23/24.

250+

attendees from 115 departments at the annual PSC conference.

96%

of customer responses agreed that ‘PSC is good value-for-money’ (87% in 23/24).

Government Security Centres in Numbers

Industry Security Assurance Centre (ISAC)

277

companies IPSA assured, to Feb '25.

700+

Facility Security Clearance provided to 700+ sites.

107

companies scheduled for assurance March – Nov '25.

Security Centre for International

400+

HMG staff briefed prior to attending COP29.

280

missions overseas feeding into GSeCI's products.

257

Post Security Fact Sheets continually updated and available through security.gov.uk.

Security Centre for Cyber

63

GovAssure engagements successfully completed.

70

engagements enabling departments to adopt security controls to prevent email spoofing and man-in-the-middle attacks.

13

government organisations received the in-depth Purple Teaming service.

324

Engagements Completed.

Collective Benefits of the GSeCs

The GSeCs play a vital role in building cross-government security capability and support the improvement of HMG's security posture through the following collective benefits:

Supporting the rollout of new security standards, guidance and policy, as well as National Technical Authority (NTA) products as they become available and future services as a result of development activity.

Improving health check performance. Taking up GSeC services demonstrates, and provides clear evidence, that an organisation is taking steps to meet standards through follow-up and engagement on the Departmental Security Health Check (DSHC) results.

Enabling organisations to have access to an expert crossgovernment capability. GSeCs ensure that SMEs take learning across a range of different organisations, ensuring services are developed in line with crossgovernment best practice.

Designed to complement and enhance existing security within organisations. Providing value-adding, sustainable services and products to better protect organisations' people and assets.

Support the maturing of the security function by improving security resilience and capability, in line with the government benchmark - Functional Standard GovS 007: Security.

Working collectively to defend HMG as one. Supporting GSeCs helps us collectively defend against a range of threats, providing the ability to apply what works well for departments facing higher threats, across multiple organisations.

Provide a trusted network and range of services to organisations. GSeCs are hosted by the largest government departments with long-established expertise in critical areas of security. This supports quality of service and value-for-money for less self sufficient organisations.

Committed to growing internal professional talent, now and in the future, providing HMG security staff with the opportunities to widen their knowledge and expertise across government. This grows our expertise, reduces reliance on external contractors and enables economies of scale.

Services are dynamic and continue to evolve in response to learning from live use, and to the ever-changing threat and risk landscape. Customer organisations can influence the direction and development of shared services.

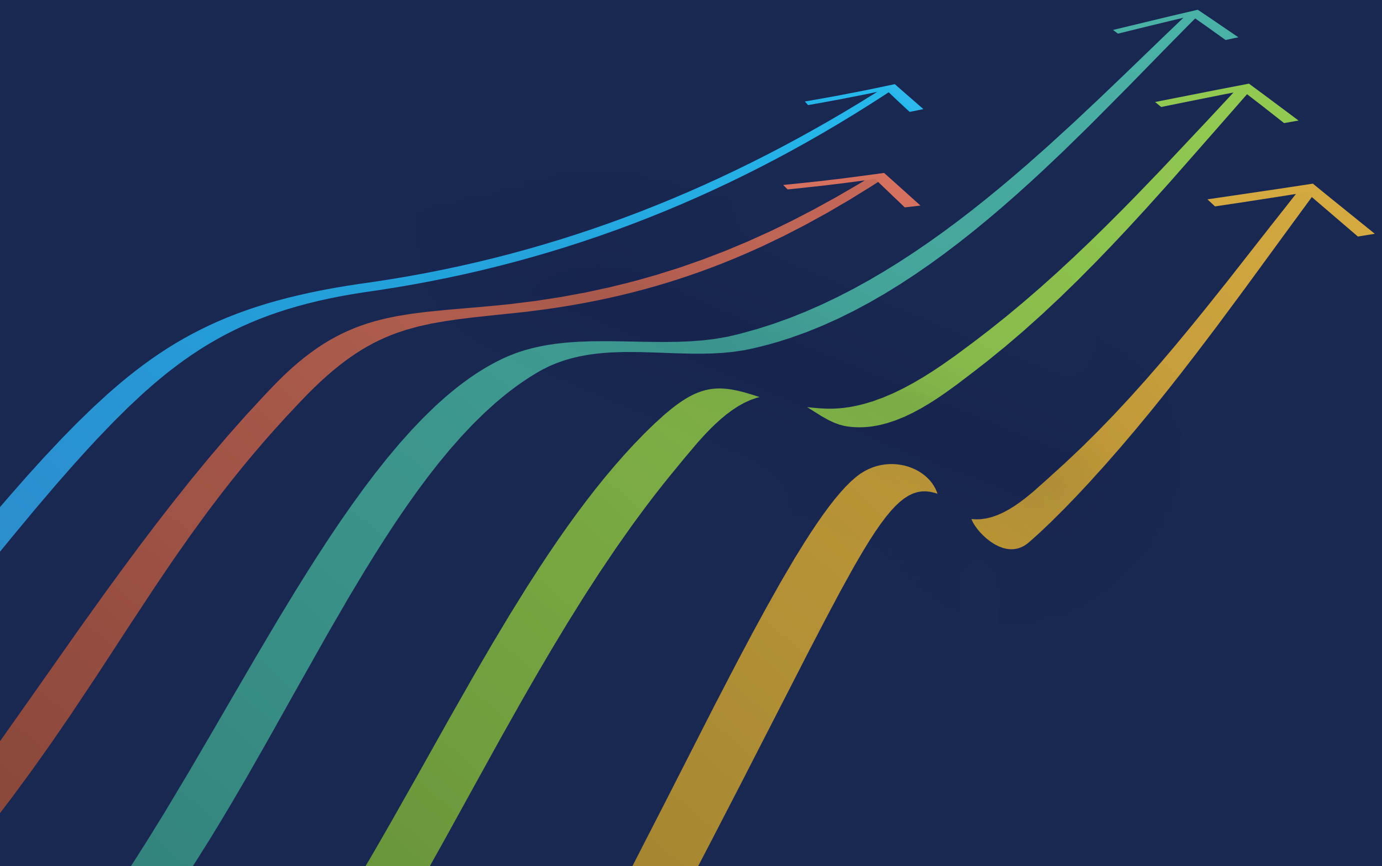
Working collectively to defend HMG as one

A new Three Year Plan for the GSeCs

With the support of the Government Security community, the five Government Security Centres (GSeCs) were created in 2020/21 as part of the Transforming Government Security programme. The GSeCs have become a core part of the Government security landscape, supporting ministerial departments, non-ministerial departments, as well as arm's length bodies, and the National Technical Authorities (NTAs).

Over the past three years the GSeCs have proven their ability to provide expert, scalable services that are not cost-effective for departments to replicate. The initial three year plan that guided the GSeCs since inception concluded within the last 12 months. So, a new three year plan has been set, along with a clear strategy and priorities, to guide the evolution of the GSeCs and their services over the coming years. This has been fully endorsed by the Government Security Board.

Much remains to be achieved and as the threat landscape evolves, the need to 'Defend as One' is as vital now as when the GSeCs were established. They provide expert guidance and advice, training programmes, and facilitate collaboration within the government security community.



The new plan sets out three central pillars of focus:

- **Supporting Departments and Organisations:** The GSeCs will work with Government departments and organisations to provide them the tools and products needed, and share best practice, to enhance their resilience and address security concerns, delivering a high quality service to customer departments.
- **Creating Strategic Interventions:** The GSeCs will create targeted security interventions, to make the Government more secure and resilient.
- **Building Converged Capability:** The GSeCs will work together when creating interventions to build holistic and converged capabilities across cyber, physical and personnel security. Building solutions that support 'Defending as One'.

The continued evolution of GSeC services is critical in supporting Government to respond to the changes in the threat landscape. The five core strategic priorities the GSeCs must focus on, informed by departments, the Government Strategic Security Risk Register, assurance data, and GSG strategies are:

- Government Cyber Security Strategy
- Supply Chain Security
- Insider Risk Management
- Effective Asset Management
- Fostering Security Culture

The plan identifies three key areas that will support the GSeCs; governance, effective KPIs and communications. We remain committed to transparent reporting and will continue to seek a secure and stable financial model for the GSeCs. The GSG GSeC team will work closely with the GSeCs to agree and set KPIs which will be quantifiable measures used to evaluate the success and performance of the GSeCs in relation to the strategic goals and objectives. The team will also develop a communications plan throughout the three year period to increase the reach of campaigns and to build understanding of GSeC services across Government. All three areas will be aligned to the Government's key priorities.

The GSeCs continue to provide excellent Value for Money:

- GSeC services are cheaper than using commercially procured alternatives. For example a physical security site survey is 90% cheaper than private security companies and a Surreptitious Threat and Mitigation Process Assessment is 600% cheaper.
- A GSeC subscription gives access to a significant catalogue of Security Education and Awareness material to promote security, and access to all annually developed campaigns, negating the need to have to design and pay individual campaigns.
- GSeCs give access to FCDO's security network overseas through the International GSeC to support staff security while travelling - this is something that simply cannot be replicated commercially.

In an ever more challenging fiscal landscape the need for effective shared services is not in question. However, those services can only remain in place if they are taken up. Thank you to all customer departments who have continued to use the GSeCs – we look forward to working with you again in this coming year.

Government Security Centre: Protective Security Centre

The Protective Security Centre (PSC) exists to drive down the protective security risk to government. We provide guidance and operational services to customers across government, including central departments, ALBs, devolved administrations and other public bodies.

We are hosted by the Home Office but are entirely revenue funded. We charge our customers just what we need to cover our annual operating costs - around £11M in 25/26. Approximately a third of this is covered by customer subscriptions collected by the Cabinet Office and passed on to us in the form of an annual settlement. The remainder we raise ourselves through direct sales of services to customers. Our prices are benchmarked against and considerably lower than comparable private sector offerings[1].

We know that our customers know their risk areas best. We blend that local knowledge with the insights we gain from operating across government. We advise our customers on the most effective controls for their particular security challenges, help our customers implement those controls and help them check that the controls are working. As part of this process, we've delivered 114 assessments to help customers identify and manage their critical assets and 50 site security assessments. We have a particular expertise in the handling of classified information, providing advice on Tier 3 builds and directly managing STRAP services for some departments.

Insider risk management is another core element of our customer offer. We've played a leading role in the treatment of insider risk, mediating between GSG and customers to ensure that the new personnel security policies and standards are robust but also as proportionate as possible.

We've delivered role-based risk assessments for our customers and handled 20,000 insider risk cases through our aftercare services. We've also helped HMG mitigate insider risk at point of entry by delivering 52,000 vetting applications and answering 55,000 enquiries on insider risk management and vetting processes. And we've helped UK Security Vetting (UKSV) understand how vetting transformation proposals affect departments and acted as the independent assessor of Stage 2 complaints about the vetting process.

We also work hard to build up our customers' capacity to manage their security risks. In 24/25 we delivered 150 capacity-building interventions to help build departments' own security capabilities in 2024/25, up 285% on the previous year. These include:

- **20 training sessions** on the surreptitious and insider threat to sensitive information assets.
- **30 Protective Security Risk Management** (PSRM) training programmes.
- **Help for customers** establishing their own vetting teams, including policy development, process set-up, training and shadowing opportunities.
- **45 'See Check and Notify'** (SCaN) training sessions across government.
- **58 training programmes** to build customers' ability to mitigate the technical threat to government information and assets.

[1] The PSC measures its cost-effectiveness through a basket of services (including the Surreptitious Threat and Mitigation Process (STaMP) Assessment, Full Site Survey and Operational Requirements) that are also available to government departments via the commercial sector. Comparisons have identified that this cost for the basket of services is circa 14% of what the commercial sector charges. 96% of customers who responded to the PSC's post-work completion survey agree with the statement that 'The PSC is good value-for-money,' up from 87% last year

Our work with customers across the breadth of government gives us a unique overview. Over the past year we've written over 200 guidance notes, cementing our position as **thought leaders** on the operationalisation of personnel and physical security in government. Subjects covered have included the Internet of Things, Martyn's Law, security convergence, physical harm to the UK, hosting external and visiting delegates, doxing, addressing and managing insider risk and threats and dealing with protests. We also ran our third annual protective security conference, which drew 250 delegates from 115 departments gathering in London to hear speeches from the Security Minister, DG MI5 and the Government Chief Security Officer and included presentations from across government, academia and industry. We have been working hard to make sure our message is accessible to everyone. Our weekly newsletter is read by 115 organisations across the public sector. Our revamped online portal has welcomed 250 new users and seen a 30% increase in traffic over the year. Our thought leadership pieces have been viewed or downloaded 4,700 times, a 115% increase from last year.

We are also committed to increasing diversity within our profession, making it as accessible as possible and investing in our pipeline of new talent. Our prime focus here has been the ground-breaking **Protective Security Apprenticeship** we've developed with the NTAs and industry to establish a universal standard of learning. We have strong support and have passed the initial approval stages. The next step is to work out a route to procurement. The Home Office has agreed to provide one-off funding of £120K to help with initial procurement costs providing the Cabinet Office cover the run costs, so we hope to make this available to departments soon. We are also working on a corresponding Level 4 qualification as an alternative route to this learning for those who don't want to do an apprenticeship.

Finally, we remain committed to **continuous improvement**. We led the expansion of the Personnel Security Minimum Standards to cover insider risk in its entirety and provided webinars and interactive sessions to support the GSG launch. We've played a core role in shaping operational insider risk management and future vetting requirements. We're also developing a range of new services to help customers improve their physical security. These include the Espionage Essentials: Technical Security programme developed with the UK National Authority for Counter Eavesdropping (UK NACE) to mitigate the risk of close access technical attacks to steal government information. We've also developed the Terrorist Incident Checklist (TICC) to help organisations understand how prepared they are for a terrorist incident and what they can do to manage it – like the apprenticeship, another example of an initiative that we've designed for industry as well as government.

PSC Forward Look

Over the next three years we'll continue to evolve services to focus on concrete outcomes for our customers and help them win the value-for-money argument with their finance colleagues. This means that all our services will either:

- Advise customers on the controls necessary to manage their security risks.
- Help customers implement controls – this might be through direct service provision, advice on operationalisation or capacity building.
- Help customers check whether those controls are working.

We'll maintain a 'partnership mindset' which continues the move away from a catalogue-based approach towards jointly constructed customer profiles and support plans. We'll also continue to provide thought leadership on physical and personnel security issues, using its increasingly well-established brand to convene discussion, shape policy and share best-practice across government. The PSC annual conference will remain a critical part of this. And our portal will be redeveloped to improve the user journey and functionality, increase the PSC's digital presence and explore how AI can assist with enhancing service delivery.

An important enabler to all this work will be the maturing of the PSC's task management and business support mechanisms. The PSC will develop systems to find and exploit the data available to them to make sure that our interventions are focussed where they can have most impact.

CASE STUDY

Civil Nuclear Constabulary (CNC): Delivering Concrete Outcomes and Value for Money

When CNC first became our customer, they identified insufficient stakeholder buy-in and limited resources as areas needing our help. We started by providing advice on the controls we judged they needed to put in place. We used our Insider Risk Indicator Tool (IRIT) to identify vulnerabilities and recommend controls. This assessment highlighted the need for a more robust security framework with senior leadership and strong governance built in.

We then helped CNC to implement those controls, providing services, advice and capacity building. This bespoke approach included on-site assessments, interviews, and document reviews to ensure compliance with nuclear-specific security regulations to tailor solutions to CNC's specific needs. For example, we helped CNC to develop an incident management system for their control room, ensuring it met the required Personnel and Physical Security Standards.

We also helped the CNC check that its controls were effective by conducting follow-up assessments and ongoing support. This included role-based risk assessments (RBRA) to evaluate the appropriateness of security clearances and access controls and insider risk briefings to educate staff on potential threats. This continuous engagement helped CNC maintain a high level of protective security management and adapt to evolving risks.

The PSC's work with CNC not only improved their security standing but also demonstrated significant value for money. Our advice helped them avoid unnecessary costs by ensuring that security was integrated into the design of their new control room from the start. Our advice also helped the CNC security team make the case for the extra resources they needed to sustain security improvements over the long term.

> The PSC's work with CNC not only improved their security standing but also demonstrated significant value for money

The Protective Security Centre (PSC) exists to drive down the protective security risk to government. We provide guidance and operational services to customers across government.

Government Security Centre: Cyber

The Cyber GSeC is hosted by HMRC and provides consultancy and advice services to improve cyber security posture across HMG, supporting lead government departments and their Arm's-length bodies (ALBs).

In 2024/25, Cyber GSeC's services to Government organisations included GovAssure Support, Purple Teaming, Supply Chain Security Consultancy (SCSC), Optimising Microsoft Security Solutions (OMSS), Active Cyber Defence and Open Standards Adoption (ACD&OS), and Bespoke Consultancy. These service lines helped organisations to make progress in areas defined in the Government Cyber Security Strategy (GCSS). For detailed information on each service, please see Cyber GSeC's all services brochure [https://www.security.gov.uk/wp-content/uploads/2025/03/government-security-centre-cyber-services-capabilities.pdf].

Alongside its core services, Cyber GSeC supports high-priority partner projects and initiatives from authorities including NCSC, GSG and Government Digital Service (GDS). In 2025/26, this remit will continue to evolve to best serve the needs of government and the GCSS in the ever-changing threat landscape.

Overview of the last year & key achievements

During 2024/25, Cyber GSeC has completed a total of 324 engagements with government organisations: this has included 129 Business partnering engagements; 63 engagements with 19 organisations to support their GovAssure returns; 13 Purple Teaming exercises to identify susceptibilities to attack and upskill the organisations to identify common indicators of compromise; and, 25 SCSC engagements to improve resilience in supply chains. The remainder has primarily been Bespoke support (15 engagements completed, providing uniquely tailored support for individual organisations' security concerns), ACD/OS 82 (protecting domains from phishing and tampering, by improving active cyber defence via a suite of tools and services produced by the NCSC), and 15 OMSS work (utilising Microsoft security and compliance solutions, leveraging existing security tools and features to meet cyber resilience and security objectives whilst saving costs and protecting against insider threat).

Hardening political parties' domains:

In the run-up to the UK general elections in July 2024, the NCSC reached out to the Cyber GSeC's ACD&OS team for urgent support in helping UK political parties to strengthen their active cyber defences.

Through an audit-style review of their existing environment, close collaboration and one-to-one engagements, ACD&OS was able to make tailored recommendations in line with existing NCSC best practice to help address vulnerabilities, successfully enhancing the email and website security of several major political parties – thereby reducing the risk of interference from hostile actors in the UK democratic process.

Senior Officer development programme:

Proficient, adaptable cyber security professionals need a range of technical and non-technical competencies, including the ability to work with others, collaborate and communicate effectively, and understand the wider business context they are operating within.

Over the past year, Cyber GSeC has been piloting a development programme within HMRC, which centres around combining coaching and mentoring, work placement, and learning and development, with the aim of providing a framework which can be tailored to the participants' needs, abilities, and ambitions.

The pilot for the development programme has been a success, with participants demonstrating behaviours and skills at a much higher level than would otherwise be expected, and in many areas they have outshone their peers. Three of the four participants achieved Grade 7 promotion in early 2025. This is an important step towards objective 5 of the GCSS - developing the right cyber security skills, knowledge, and culture.

> In 2025/26, this remit will continue to evolve to best serve the needs of government and the GCSS in the ever-changing threat landscape.

Apprenticeships:

Over the past three years, Cyber GSeC has continued to develop future talent, supporting level-six apprentices with mentoring, support, and challenging work opportunities, helping them to build the skills and experiences required for a successful career in the Cyber Security Profession, directly contributing to achieving objective 5 of GCSS, by creating a supply of cyber security experts for the future.

Assessing Google Gemini AI in a key Department

A key department was seeking to implement Google Gemini for Google Workspace (a generative form of AI), and engaged with Cyber GSeC to help them understand the risks associated with the implementation. The department wished to take advantage of the Enhanced AI Assistance in Workspace Apps via an initial trial covering assistive features in email, documents, spreadsheets and meetings, with the aim of enhancing productivity and user experience. The department's Google platform is provided by a third-party supplier.

Cyber GSeC examined the evidence available from Google, the department, the third party and other sources to produce a report that identified five key risks along with recommended remedial actions. This, subject to assurances from the suppliers, was to enable the department to make an informed decision on their adoption of Google Gemini.

In this way, Cyber GSeC has helped the department to consider the adoption of AI technological advances, with a clear picture of the risks involved and suitable mitigation measures. The experience gained from this engagement is highly valuable and Cyber GSeC is well positioned to share the learning across all organisations, bringing enhanced value and relevant experience to other government organisations that are looking at using AI.

CASE STUDY

Supply Chain Security Consultancy: Met Office supercomputer accreditation

Cyber GSeC was contacted by the Met Office to assist in fulfilling a contractual obligation between the Met Office and Microsoft to accredit the world's most advanced weather and climate forecasting system. The data it will generate will provide more accurate warnings of severe weather, helping to build resilience and protect the UK population, businesses, and infrastructure.

An assessment was carried out by an independent information risk manager/professional appointed by the Met Office, which resulted in an accreditation decision. Accreditation provides the risk owner (the Met Office) with the basis to make an informed decision to accept or plan to remediate any risks balanced against the business needs.

> "I just wanted to say a massive thank you for all the time and effort that you put into reviewing the Supercomputer RMADS last year. Your diligence, knowledge and experience resulted in a number of changes to the document for the better that would not have occurred had you not been involved in the process. It's quite a large, complex programme and your ability to take on board the information, review it and make recommendations in the time frame that you did is nothing short of incredible – really impressive."
>
> **Met Office**

Given the gravitas of this request, there was an expectation from the Met Office that the role would be fulfilled by a senior security practitioner with accreditation and audit skills. Cyber GSeC met this requirement deploying one of its Senior Cyber Security Consultants, through the SCSC service line.

Cyber GSeC worked closely with the Met Office and Microsoft to ensure any details provided could be corroborated and supported by verbal and written evidence. The accreditation was underpinned by a series of phone calls, extensive email dialogue, virtual walk-throughs, and a large volume of supporting documents.

Cyber GSeC acted as an impartial and independent assessor, ensuring the risks associated with the adoption of the supercomputer, including its service and business processes, were acceptable to the Met Office. Cyber GSeC ensured the risk management process followed Met Office internal and sector-specific security and quality assurance standards, that the depth and rigour required was proportionate whilst meeting Met Office business needs.

Cyber GSeC's positioning and ability to both understand Met Office's risk appetite and the business impact of accepting risks, while providing an independent view, was a real strength in this instance. Cyber GSeC provided a service that the private sector was reluctant or unable to undertake, and gave the Met Office clear sight of the risks and recommended mitigation measures for their new supercomputer.

The Cyber GSeC is hosted by HMRC and provides consultancy and advice services to improve cyber security posture across HMG, supporting lead government departments and their Arm’s-length bodies (ALBs).

Key Numbers

63 GovAssure engagements successfully completed, supporting organisations to: identify and plan targeted remedial action; reduce cyber risk; and increase cyber resilience in support of the GCSS published goals. This support enables organisations to drive forward a targeted approach to identified shortfalls and take corrective action in line with the 'defend as one' and 'increased resilience' GCSS pillars – all at a cost of around an average of £47k per submission, significantly cheaper than a similar service from a Big Four private sector equivalent, and tailored to government.

11 OMSS engagements successfully completed, with 18 more under way and a further 21 enquiries pending – improving protective monitoring and data governance across HMG by leveraging existing Microsoft security licensed capabilities.

16 SCSC engagements successfully completed, giving government organisations greater visibility into, and improved security throughout, their supply chains.

5 level-six apprentices supported through Cyber GSeC's future cyber security early talent scheme, 4 having already achieved promotion in 2024/25 – providing them with mentoring, support, and challenging work opportunities so they can build the skills and experiences required to build a successful career in the Cyber Security Profession.

13 Purple Teaming exercises delivered – executing real world cyber incident exercises to provide valuable recommendations reports on further defensive measures government organisations can take to increase cyber resilience. One government organisation fed back that the outcome from the Purple Teaming exercise was instrumental in securing funding for critical work.

38 departments adopted DMARC security controls to prevent email spoofing by malicious actors, and **32 departments implemented MTA-STS email security measures** to prevent man-in-the-middle tampering of government communications thanks to Cyber GSeC's support.

Cyber GSeC's Forward Look

Joining up planning across government security:

Cyber GSeC is committed to supporting the delivery of the GSeC three-year plan and the Cyber Target Operating Model interventions by:

- Serving the future pipeline for Purple Teaming services, to support government organisations in testing responses to attack scenarios;
- Fostering a culture of security awareness and convergence;
- Building the OMSS service to combat insider risk, data loss, and aid asset management;
- Collaborating with delivery partners (including GSG, GDS, NCSC, GSeCs); and
- Regularly updating services to mitigate evolving risks to government cyber security.

Subject to funding allocation and strategic direction, these goals will be delivered by:

- A converged approach to asset management (AM). Cyber GSeC, in collaboration with SEAC and PSC, will address GovAssure findings, departmental feedback and NAO audit findings where AM maturity levels across government are low.
- Exercising cross government response to cyber incidents. We will facilitate and lead cross-government tabletop incident response exercises to encourage a collaborative and 'Defend as One' approach in cross-government cyber incidents. Output of the exercises will be disseminated across government.
- Continuing to provide support to government organisations for the five stages of GovAssure; conducting the refresh of Cyber Assurance Framework profiles; and delivering new services in collaboration with GSG.
- Enhancing support for supplier security assurance (cyber and protective) capability, with a stronger focus on existing supplier contracts, utilising the existing SCSC service and Supplier Assurance Framework Toolkit (SAFeT).

- Owning and operating the delivery of the Cyber Uplift Service following the integral role in the pilot initiative (DiCE). This will seek to improve cyber resilience through central team activities with support for hands-on interventions. Cyber GSeC is working with the Cabinet Office Strategic Projects team to form the best delivery approach.

Notable information

Deployable Cyber Enablement pilot

Cyber GSeC undertook assurance reviews of remediations proposed during the Cabinet Office's Deployable Cyber Enablement (DiCE) pilot, forming a strong relationship with the project team and its supplier and utilising previous experience of working with the pilot departments to help inform activities and implementations. The pilot has been a model in collaborative delivery – surpassing expectations in its achievements. Cyber GSeC will now own and operate the delivery of the Cyber Uplift Service.

> 63 GovAssure engagements successfully completed, supporting organisations to: identify and plan targeted remedial action; reduce cyber risk; and increase cyber resilience in support of the GCSS published goals.

Working with key suppliers for cross-government benefit:

During this last year, Cyber GSeC has worked with major suppliers including Google and Microsoft to influence the product road maps and security offerings available to government organisations – MTA-STS policy file hosting is one such example, seeking to leverage the Crown Commercial Service's five-year memorandum of understanding with Microsoft (the SPA24 agreement) to drive security improvements for all government bodies.

Cyber GSeC support for the Government Cyber Coordination Centre:

The Government Cyber Coordination Centre (GC3) and Cyber GSeC both work to deliver elements of the GCSS, with GC3 providing services to constantly manage and support responses to incidents across government, providing information about threat intelligence, and highlighting vulnerabilities.

Cyber GSeC has supported the maturity and growth of GC3 since before its inception with a soft launch in September 2023. During the past financial year, Cyber GSeC has led projects to build resilience and capability within GC3, and provided dedicated resource to head the GC3 Operations Team.

Cyber GSeC support for the Secure by Design Programme.

Cyber GSeC has been a pivotal contributor to x-Gov Secure by Design – helping to structure the initiative, authoring 30% of guidance activities on security.gov.uk, creating the SbD implementation checklist and supporting 50% of departments in Phase 1 SbD implementation via departmental champions.

Government Security Centre: Security Education and Awareness

SEAC provides ready-made, editable and pan-government campaign material and centrally agreed Security Education and Awareness (SEA) messages for departmental use. SEAC provides central representation in response to current and emerging threats, risks and policy changes. It also offers access to SEA expertise and capability via dedicated security platforms and a thriving SEA community. The service SEA provides removes duplication of effort, saving time, resources and money across Government.

Overview of the last year & key achievements

Building on the success of the previous Security & Data Protection e-Learning product and leveraging the valuable feedback received; SEAC developed the course to strengthen and re-purpose it for new joiners to provide a comprehensive introduction to security and data protection. The name was changed from the Security and Data Protection (S&DP) eLearning course to Security and Data Protection Fundamentals to reflect the change.

In addition, SEAC has also developed a new, shorter Security and Data Protection Refresher Course. This can be used for regular training purposes, ensuring staff are reminded of essential security and data protection practices and good behaviours.

The course also includes recommendations from the latest ICO report on Information Security in Government.

To coincide with peak leave last summer, the refreshed Travel Securely products, with a focus on personal travel, were also uploaded onto our sharing platform, Knowledge Hub. These included a guide for Security Advisers, e-mail footer, one-page information guide and digital screens, editable where possible for departments to tailor.

SEAC worked with Cabinet Office and a cross-government working group to create three complementary Induction videos to reinforce good security behaviours.

Three videos were uploaded to the new security.gov.uk platform in support of Government Security Induction after the DSHC identified a lack of resource in this area. Two shorter videos for Civil Servants and Suppliers give a general overview of risks, threats and people's responsibilities. A longer video goes into greater detail regarding risks and threats and how to mitigate against them.

Our cross-government Information Security campaign, 'Share With Care' launched in November after collaborative work with Government Security Group, the Information Commissioner's Office and National Technical Authorities to raise awareness of the risks associated with data breaches. The campaign aimed to address poor information security behaviours that can lead to the accidental disclosure of sensitive Government information and personal data. This campaign was backed by the Cabinet Office Perm Sec and Civil Service Chief Operating Officer and was used by many departments across Government.

SEAC's Personnel Security (PERSEC) Campaign webinars ended in November 2024, having been a huge success, reaching more than 1700 line managers, and consequently many thousands more staff, across 70 government departments.

In addition, 32 SEA leads from 24 departments attended a Train The Trainer session in September to enable them to deliver the webinars themselves.

As in previous years, SEAC also developed a security game with a festive flavour – 2024's was 'Don't Let The Snowman Melt' and aimed to educate players about security themes, identifying key words and phrases to help keep people and information safe.

Our cross-government Leak Prevention Campaign, outlining what information leaks are with a strong deterrent message to prevent them from happening in future, launched in February. Downloadable materials included a video outlining what constitutes a leak and the consequences for the individual and organisation; posters, Line Manager checklists including business processes and resources; pastoral support and change management; vetting and people and performance management. This is now in the evaluation phase.

SEAC's Doxing Campaign, in collaboration with the Protective Security Centre (PSC) and input from FCDO, was delivered at the end of April as a series of webinars outlining risks and prevention strategies, supported by an eBook and reached more than 1600 colleagues.

2024/25 highlights

We were delighted to welcome more than 50 representatives from 22 Government departments to our annual face-to-face event in London including several new departments who had recently joined the SEA Community and attended for the first time.

Our speakers consisted of the City Of London Police's Cyber Protect Officer who shared details of a major hacking case and how the perpetrators were caught, and the Bletchley Park chief historian, who talked about the significance of Bletchley during WWII and its relevance for today's security.

Delegates' excellent feedback around current risks and threats gave us valuable insights which have helped to inform our products and campaign delivery for 25/26.

We have delivered our security Escape Room concept to hundreds of attendees from seven government departments and have also run Train The Trainer sessions to enable organisations to deliver the sessions themselves.

CASE STUDY

Personnel Security Line Manager Campaign

The Personnel Security Line Manager Campaign was launched in September in light of incidents of unrest and disorder across the UK, which underscored the critical importance of maintaining robust security practices across government departments.

The campaign was designed to equip line managers with the necessary tools and knowledge to foster a security-conscious culture within teams; recognising that line managers are pivotal in upholding personnel security and ensuring compliance with security policies.

A range of assets were developed in support including a comprehensive line manager handbook, poster, digital displays and market stall pack.

The handbook's key content was brought to life in a series of webinars run jointly by SEAC and the Protective Security Centre. It was SEAC's first foray into webinars as a means of extending our reach and was hugely successful, attended by more than 1760 line managers across 70 departments. A further 35 individuals from 24 departments attended a Train The Trainer session to enable them to deliver the webinars themselves.

Having attended, 99% of line managers said they felt motivated to act and reported a 73% knowledge increase. The top five attending departments were HMRC, FCDO, Home Office, UKHSA and DfT.

> Having attended, 99% of line managers said they felt motivated to act and reported a 73% knowledge increase

Key Numbers

- **User Group** – Of 67 subscribing organisations, 84% attended at least one User Group through 2024/25 with January seeing our attendance peak at 106 cross-government colleagues.
- **Travel Securely** – 292 downloads between July and September.
- **5917 documents** were downloaded from Knowledge Hub from 3200 visits and 480 active members.
- **Security Escape Room** concept delivered to more than 200 people from 7 departments.
- **Security and Data Protection eLearning** accessed by over 100 departments, undertaken for circa 250,000 users.

SEAC's Forward Look

Quarter 1 will see the launch of the Security & Data Protection (S&DP) Fundamentals course, an induction course aimed at those new to the Civil Service, removing the burden on individual departments having to deliver this. Additionally, the refreshed mandatory security training for all existing civil servants will be launched, enabling departments to demonstrate their compliance with GOVS007.

Personnel Security webinars for line managers will continue, with a focus on insider risk and the responsibilities of line managers.

Quarter 2 will see Information Assert Owner (IAO) refresher training, an area of focus identified via the DSHC process, and a recommendation following the review of the role.

Personal travel material reminding colleagues of their responsibilities as a civil servant when travelling aboard for holiday will be issued.

To coincide with the Official Travel Policy, SEAC will deliver a campaign that further promotes the security behaviours required when colleagues travel for official business, recognising the ever changing international threat landscape.

An AI Campaign is pencilled in for Quarter 3, pending the launch of the AI Policy and Cyber Awareness Month falls in this period. In addition, recognising Cyber Skills as a deliverable within the Government Cyber Security Strategy, SEAC will deliver targeted SCS awareness awareness to improve Cyber skills.

Future ambition

SEAC are leading the implementation of a data and analysis strategy, which will enable us to further demonstrate the reach and impact of our services, demonstrating the direct link to areas within the DSHC and the positive effect SEA continues to have on improving the security culture across government.

In house development will continue, further demonstrating the value of a share service model, utilising internal skills and capability, to deliver engaging SEA products to all government departments and ALBs.

Notable information

SEAC are also focusing on a deep dive into data, with the creation of a data inventory with almost 300 data points and subsequent dashboard and will be looking into use-case scenarios to provide greater insight into the impact of our delivery and communications.

Following a request from GPA, we have been working with PSC to deliver a physical security awareness week with cross-government delivery of virtual and in-person sessions including webinars delivered by SEAC to raise awareness of the potential threat, risks of working at home and on site and how to mitigate them.

Government Security Centre: International

The Government Security Centre International (GSeC International/GSeCI) enables all civil servants and public servants travelling overseas on official business to have quick access in one place to up-to-date, consistent, overseas security advice and guidance before they travel. This will enable them to better protect themselves and Government information and equipment overseas.

Overview of the last year & key achievements

This has been another busy year for GSeCI. Notable achievements from the last 12 months include;

- Regular updating and uploading of products, including 257 Post Security Fact Sheets, to share via security.gov.uk with all civil servants
- Providing security briefings to over a thousand HMG staff attending COP29 and CHOGM 2024 and providing security briefing packs
- Further development of security.gov.uk platform beta versions, shifting all products from alpha to beta, and driving forward use of MI available
- New ‘one pager’ guidance across whole HMG on:
  - ‘Drink Spiking – Protecting Yourself and Others’
  - Travel Checklists
- Further development of course content and expansion of the Espionage Threat Awareness Course to all HMG staff deploying to high threat Espionage Posts
- HMG wide Espionage Threat Collection, Analysis and Risk Assessment
- Compilation & distribution of Quarterly cross HMG Espionage Reports
- Building, compiling and maintaining and espionage report database

Notable highlights

The mission of the Government Security International (GSeCI) is to become the main point of contact for security expertise and guidance for HMG Officials travelling overseas. GSeCI aims to support the Government Security Group (GSG) and the National Technical Authorities (NTAs) by building and maintaining defences across government and its supply chain, guarding against threats from various capable adversaries.

GSeCI continues to achieve this through further establishing itself as the first port of call for overseas security advice, with departments and arm’s-length bodies contacting GSeC International direct for bespoke advice, especially on the use of IT equipment in high threat countries.

GSeCI increased HMG awareness of espionage threats by its reporting across HMG through consultation with key partners.

CASE STUDY

Another successful COP Summit

GSeCI establishes itself as the first port of call for overseas security advice, with departments and arm's-length bodies contacting GSeC International direct for bespoke advice, especially on the use of IT equipment in high threat countries.

The team collaboratively supported security arrangements for COP29. Working with the British Embassy Baku Security Team, the Department for Energy Security & Net Zero (DESNZ) and wider British Embassy team to create and deliver bespoke consistent overseas security guidance for key audiences, namely HMG Security Advisers whose staff were travelling to Baku, and 400 plus HMG staff attending COP29 through five virtual security briefings during October 2024. COP29 HMG overseas security products were also published on www.security.gov.uk.

Key Numbers

Security.gov.uk's alpha site, where all of GSeC International's products sat, had limited ability to provide management information on the use/utility of those products. However, with the continued development of security.gov.uk beta version we hope to have the ability next year to run the following management information data reports:

- The ability to set and compare different time frames e.g. Jan 2024 to Jan 2025 or 12th Jan to 13th Jan, for data availability
- The ability to see the number of visits by different countries or by different departments to identify trends or improvement areas
- Better insights into user journeys (the path that visitors take to get to the information that they're looking for)
- The most popular days that users access the site and average time that is spent on each page or dwell time
- The most searched words in the search bar on the site
- User journey details when moving off the site e.g. gov.uk general pages, NTAs sites
- Popular pages that overseas users view e.g. site user in Mexico looking at the Guatemala GEG page
- In terms of value for money, given the size of FCDO's overseas network (280 missions) and the unique access our mission staff, including 60 Regional and Country Security Advisers, have to national and local governments overseas and the information thus obtained, there is no corporate body that could replicate the precision or breadth of the overseas security guidance GSeC International provides.

GSeC International's Forward Look

In the next three years, the GSeCI will:

- Secure the position as the first point of contact for any HMG Official seeking security advice for travelling overseas
- Support HMG departments to understand overseas risks, build resilience and implement mitigation measures
- Further development and wider provision of the Espionage Threat Awareness Course for those deploying to high threat locations around the world
- Develop Security Culture by increasing awareness and proactive security practices across all HMG departments when travelling overseas
- Enhance HMG asset management and strengthen supply chain security
- Work closely with Five Eyes partners to develop the founding principles of the Letter of Intent. This collaboration will focus on enhancing the security framework and ensuring consistent security practices across all partner nations. Benefits being:
  1. Improved security protocols for HMG officials travelling overseas, ensuring their safety and well-being
  2. Enhanced information sharing and cooperation between Five Eyes partners, leading to more effective threat detection and response
  3. Standardisation of Threat Assessments, Training, staff security support programmes and security measures to provide a cohesive and robust defence against hybrid security threats
  4. Increased confidence among HMG Officials in security arrangements during overseas travel.

Government Security Centre: Industry Security Assurance Centre

The Industry Security Assurance Centre (ISAC) works to increase the security of the Government supply chain, currently operating in the Defence sphere. We do this by providing the administration and provision of Facility Security Clearance (FSC) and Industry Personnel Security Assurance (IPSA) to defence industry partners contracted to MOD.

IPSA has quickly become a recognised assurance service across our Defence industry partners and as IPSA's reputation grows, so does the uptake in companies seeking assurance.

ISAC continues to deliver key assurance across the defence industry and selected OGDs. FSC is provided to more than 700 sites and IPSA to more than 450 companies.

This demonstrates the team's ability to deliver professional services, in a challenging and high demand area.

IPSA has been welcomed across the defence industry. Our partners have commented how the assurance benefits them, provides a suitable guide for improving and managing their personnel security, and mitigating against the insider threat that so many organisations face in the current climate.

FSC continues to lead on defence industry assurance and provides critical advice and support in ensuring sites that hold sensitive assets and information are properly able to protect such assets.

ISAC maintains up to date advice in the face of ever changing threats and provides a single point of contact to our defence industry, handling in upwards of 100 enquiries a day.

IPSA administration has led to all companies on the FSC database being reviewed at least every 3 years, demonstrating their need for FSC/IPSA provision.

A total of 75 organisations/sites have been removed as they no longer require the provision of such assurance, strengthening resilience through our secure practice, mitigating significant risk.

ISAC continues to deliver key assurance across the defence industry and selected OGDs: FSC is provided to more than 700 sites and IPSA to more than 450 companies.

Key Numbers

- Between Nov 2021 – February 2025, **277 companies** have been IPSA assured.
- **154 companies** have been removed from the schedule or have withdrawn. The majority of these are for following reasons:
  - Expired FSC contracts; FSC relinquished, no requirement for IPSA
  - Contracts only with OGDs, no relationship directly with MoD
  - Applications withdrawn through lack of eligibility or engagement
- Remaining are made up of a combination of duplications, companies covered by a parent organisation, companies where IPSA would not be appropriate (such as sole trader IP Agents), and companies that have dissolved
- The current active pipeline is **96**
- Out of the total **538 companies** initiated, **69** were IPSA-only applications, **8** were NATO affiliated applications
- A further **107 companies** are scheduled for assurance between March – November 2025, including 10 IPSA-only applications and 2 NATO affiliated applications (new FSC initiations, IPSA-only applications, and NATO affiliated applications continue to be added to the schedule)

Industry Security Assurance Centre's Forward Look

The overall output of ISAC has been recognised, our expertise has been acknowledged and we are seeking to utilise these services more widely across government.

ISAC aims to provide a single hub within government for FSC/IPSA, for those working at Secret and above. This will raise adherence to minimum security standards through a greater oversight of how security risks are identified and mitigated in industry, working with industry to put remediation measures in place where organisations are not meeting the standards required.

This will provide assurance to Government Departments on the personnel security applied by its most sensitive supply chains, and will provide greater confidence in the companies that receive UKSV vetting sponsorship rights.

We are identifying ways to deliver ISAC services more widely across government, recognising the positive impact these programmes have on industrial security and the proven expertise of ISAC.

ISAC has demonstrated its value to industry and government and a wider cross-government roll-out is to be considered a significant move forward in enhancing security capabilities.

Wider delivery across government is an exciting and positive step, though not without challenges. Our ambition, with the right tools in place, is to support wider delivery of services.

Government
Security

We are government security.

Government Security is a cross-departmental function of HM Government.

For more information, please contact
GSFInfo@cabinetoffice.co.uk