Government
Security

Government Security Centres (GSeCs)

Three-Year Plan - FY 25/26 to 27/28

Government Security Group (GSG)

Executive Summary

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

Over the past three years the GSeCs have established themselves and proven their ability to provide expert, scalable services that are not cost-effective for departments to replicate. Now is the time to set a new three year plan, and clear strategy and priorities, to guide the evolution of the GSeCs over the coming years.

The public sector faces persistent and evolving security threats across all domains. Key vulnerabilities in physical and personnel security, alongside an escalating cyber threat environment, contribute to a critically high risk exposure for the Government. The NTAs report a deteriorating threat landscape which is now more complex and interconnected than ever. In addition to increased conventional threats, we confront hybrid warfare tactics, such as cyber attacks and misinformation aimed at undermining democracy.

The Government currently faces numerous external threats including espionage, state actors, serious organised crime, terrorism, state sponsored threats and cyber crime, amongst many others. Changes in daily life - like hybrid working, international lifestyles, the cost of living crisis, and rising debt - further increase these risks, with lasting effects that are difficult to predict.

It is crucial for the Government to proactively enhance its security capabilities to address evolving threats over the next decade. The GSeCs play a vital role in supporting these efforts.

Our Opportunity

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. Supporting Government departments in this endeavour is the primary focus of the GSeCs. They provide expert guidance and advice, training programmes, and facilitate collaboration within the Government security community. Additionally, as multipliers for the National Technical Authorities (NTAs), they assist the Government security community in implementing NTA guidance, enhancing resilience against growing threats.

Our ambition is for the GSeCs to become the primary contact for any Government department seeking specialist security advice. From 36 organisations in 2021, the GSeCs have expanded to 69 organisations today, yet many more Government departments still seek support in increasing their security capability.

Our plan for the next three years has 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. These products and services will assist departments in identifying and implementing effective mitigation measures to underpin departments' ability to deliver Government’s missions and priorities.

- **Creating Strategic Interventions:** The GSeCs will create targeted security interventions, to make the Government more secure and resilient, collaborating with Government Security Group (GSG), the NTAs, and Government organisations, and in doing so enhancing their role as the central point of contact for security expertise and guidance across Government.
- **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’, making it easier for departments and organisations to draw on services once and well. Strengthening resilience and integrity in Government operations, ensuring a unified security strategy that integrates diverse capabilities.

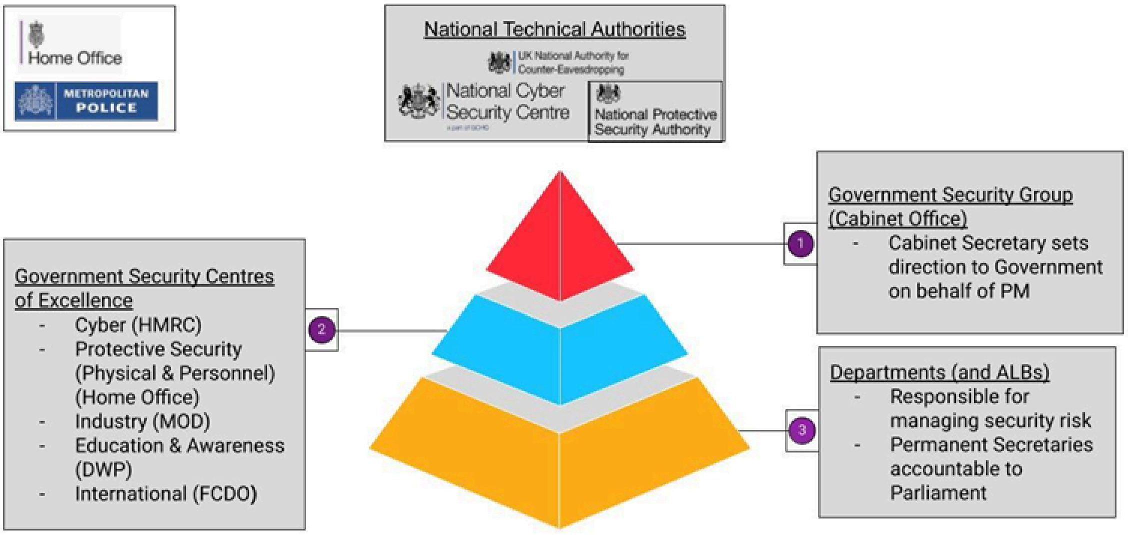
Key Priorities

The continued evolution of GSeC services is critical to support Government to respond to the changes in the threat landscape. The 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:** Building a Cyber Resilient Public Sector is crucial to the UK’s standing as a cyber power. The GSeCs will support Government in delivering functions and services which maintain and promote the UK’s economy and society in a cyber secure way.
- **Supply Chain Security:** Strengthening supply chain security is crucial for protecting Government operations. The Government's supply chain is large and complex and covers a significant number of providers. It is essential that we strengthen the Government's supply chain through targeted activities.
- **Insider Risk Management:** To mitigate the risks from intentional or unintentional insiders, the GSeCs will work with departments to understand their insider risk, and seek to develop interventions to support departments, tailoring to specific departmental requirements.
- **Effective Asset Management:** Enhancing asset management is vital to ensuring the integrity and availability of Government resources. It improves efficiency, enables tracking of security progress and helps prevent issues cascading. The GSeCs will support departments to better understand and protect their assets.
- **Fostering Security Culture:** Fostering a strong security culture is key to ensuring Government personnel are vigilant in safeguarding information. We aim to strengthen resilience by embedding secure practices and enhancing existing security measures.

What Are The Government Security Centres (GSeCs)

Key actors in Government Security:


Home Office
METROPOLITAN POLICE
UK National Authority for Counter-Eavesdropping
National Cyber Security Centre
a part of GCHQ
National Protective Security Authority
1
2
3

National Technical Authorities

Government Security Group (Cabinet Office)
- Cabinet Secretary sets direction to Government on behalf of PM

Government Security Centres of Excellence
- Cyber (HMRC)
- Protective Security (Physical & Personnel) (Home Office)
- Industry (MOD)
- Education & Awareness (DWP)
- International (FCDO)

Departments (and ALBs)
- Responsible for managing security risk
- Permanent Secretaries accountable to Parliament

There are five GSeCs, overseen by GSG, but hosted by a lead department: Government Security Centre for Cyber (HMRC), Protective Security Centre (People and Physical security) (Home Office), Government Security Centre International (FCDO), Industry Security Assurance Centre (MoD) and Security Education and Awareness Centre (DWP).

The GSeCs were created, following the Transforming Government Security programme, to deliver excellence in shared value services that both large and small Government organisations can take advantage of. In particular, they were designed to provide an affordable solution for filling capability and capacity gaps where scarce specialist skills and knowledge are required and by doing so deliver efficiencies across Government.

Hosted by their lead department, they offer:

- **Expert Shared Services & Technical Advice:** They provide expert shared services, including consultancy, briefings, training, and security products. Collaborating closely with GSG and National Technical Authorities (National Protective Security Authority (NPSA), National Cyber Security Centre (NCSC), and UK National Authority for Counter Eavesdropping (UK NACE), they implement uniform standards and specialist advice.
- **Risk Mitigation:** GSeCs focus on building resilience against evolving security vulnerabilities. Their products and services help departments mitigate significant security risks.
- **Value for Money:** The GSeCs deliver targeted services that enhance security capabilities through specialist advisors at a lower cost than similar private sector offerings. These services can be procured for specific tasks without lengthy commercial processes, exemplifying effective Government security practices.

Government Security Centre for Cyber

Mission

Provide technical cyber expertise to help the Government understand and manage cyber security risks, improve cyber resilience, and increase Government defences against cyber related threats; supporting improvement in the Government-wide cyber security posture.

Achievements

Over the past three years, Cyber GSeC has provided services to improve security across lead departments and their ALBs through services such as, but not limited to:

- **Purple Teaming:** In 2024/25 provided exercises and recommendations to 13 departments. Findings have provided evidence to board-level sponsors to successfully seek funding and improve resilience.
- **Supply Chain Security Consultancy (SCSC):** Developed to guide departments in secure procurement and contract management. It has delivered 32 engagements since its inception, supporting departments to reduce supply chain risk.
- **Met Office Supercomputer:** Cyber gained the accreditation of the £1.2bn; 'Met Office weather and climate Supercomputer – something the private sector was unable to undertake. Met Office feedback: "*Your diligence, knowledge and experience resulted in a number of changes to the better that would not have occurred had you not been involved in the process."*

Looking to the Future

Over the next three years Cyber GSeC aims to continue to deliver their pre-exisiting products as well as developing the following:

- **Secure Clouds Configurations Support (SCCS):** Mapping of existing secure cloud configurations and to provide departments with the support to implement such configuration templates.
- **Cyber Uplift Service:** Building on the existing Deployable Cyber Enablement (DiCE) pilot to develop remediation teams that can be deployed to departments.
- **Purple Teaming:** Development of the existing service incorporating tools such as automation, with an aim to reduce the cost of the exercise allowing more for less.
- **Optimising Microsoft Security Solutions (OMSS):** Continuation and development of the cyber contribution to tackling insider risk and support data loss prevention (DLP) and data leakage.
- **Asset Management:** The continued participation in the collaboration of the GSeCs to attempt to address low asset management maturity levels across Government.
- **GovAssure Enhancement:** Expanding the existing GovAssure offering in line with the Cyber TOM to cover a much wider scope of Government estate.
- **Cross Government Response to Cyber Threats:** Facilitate and lead cross-government tabletop incident response exercises to encourage a collaborative and 'Defend as One' approach in to exercise cross-government cyber incidents.

Protective Security Centre (PSC)

Mission

To deliver services, capability building and thought leadership to drive down the protective security risk to the Government. We work with our customers and help them protect people, information and assets. We blend customers' local business and risk knowledge with our cross-government insights to deliver tailored support, promoting best practice and influencing HMG Policy.

Achievements

Over the past three years we have supported departments to improve security by:

- **Physical Security:** Launched the Terrorist Incident Checklist (TICC) to assist organisations in assessing their preparedness for a terrorist incident and facilitate the review of necessary measures and policies in their Counter-Terrorism planning.
- **Consultancy Services:** Launched of a Technical Security programme, developed with UK NACE, to mitigate the risk from threat actors using espionage and close access technical attacks to steal Government information.
- **Standards Development:** Co-authored the Physical and Personnel Standards, Lockdown Framework for Government Hubs and the Surveillance Equipment Policy.
- **Training:** Launched See, Check and Notify (SCaN) training to help departments identify and disrupt hostile reconnaissance and the Espionage Essentials: Technical Security (EE:TS) programme alongside UK NACE to mitigate the risk to government information.
- **Customer Satisfaction & Value-for-money:** Created 600 Thought Leadership pieces that have been viewed and downloaded over 10,000 times, and PSC's site survey costs are 75% less than the private sector.

Looking to the Future

Over the next three years, our focus will be on achieving concrete outcomes by:

- **Advising:** Guide and support customers on security risk management controls.
- **Assisting:** Aid the implementation of controls through services or capacity building.
- **Evaluating:** Assess the effectiveness of implemented controls.
- **Capability Building:** We will focus on using our expertise to enhance departments' in-house security capability and capacity whilst continually improving our own capabilities to maintain best practices by developing hybrid skills approaches, implementing new digital solutions and refining current processes.
- **Thought Leadership:** Leveraging expert knowledge in protective security to educate and influence Government security professionals. It aims to promote best practices from various sectors to enhance Government security.
- **Partnership Mindset:** We will maintain a 'partnership mindset' which continues the move away from a catalogue-based approach towards jointly constructed customer profiles and support plans.
- **Developing the Protective Security Apprenticeship:** Promoting security convergence across Government and the private sector, expected to launch in Summer 2025.

Security Education & Awareness Centre (SEAC)

Mission

To improve security culture behaviour, build Security Education and Awareness (SEA) capability across Government and reduce human risk in line with the Government Security Strategy, through the provision of a centrally coordinated, streamlined approach to Government security education and awareness, providing high quality, high impact SEA campaign material and best practice products.

Achievements

Over the past three years we have supported departments by delivering:

- **Personnel Security Campaign:** SEAC has delivered Personnel Security webinars to over 1,700 line managers from 58 Government departments and trained 32 SEA leads from 24 departments to conduct the webinars. After attending, 99% of line managers felt motivated to act, with a reported 73% increase in knowledge.
- **Share With Care:** A cross-Government Information Security campaign, launched in November 2024, after collaborative work with Government Security Group which includes a video, several digital screens and guidance products, has been downloaded a total of 1373 times on Knowledge Hub.
- **E-Learning:** SEAC's Security & Data Protection eLearning has been completed by more than 253,493 people across 126 departments since its launch in 2024. And the classification eLearning product has been completed by more than 21,201 people across 77 departments with feedback showing a 73% positive experience.
- **SEA Community:** Built a community of practitioners, with 80 active members joining working groups.
- **Escape Rooms:** Delivered sessions across government, alongside Civil Service Live events, promoting and advocating good security behaviours.

Looking to the Future

Over the next three years, our focus will be on:

- **Campaigns:** Producing value-adding pan-Government SEA campaigns, products and best practice material to improve SEA standards across Government. The Campaigns Plan for FY 2025/2026 is included at Annex A.
- **Aligning Outcomes to the Cyber Security Strategy:** Deliver SEA interventions linked to the outcome of the Government Cyber Security Strategy.
- **Increasing Cyber Skills:** Continue to enhance SEA skills, knowledge, and capabilities across Government by implementing initiatives that improve cyber capabilities within the Civil Service. Additionally, promote the development of SEA programmes across Governmental organisations and establish mechanisms for tracking SEA performance evaluation.
- **Implementation of SEAC Data and Analysis Strategy:** Implement a data driven SEA strategy that evaluates the impact of campaigns and demonstrates value for money using a range of criteria.
- **Grow and Scale:** A collaborative community of SEA practitioners by developing SEA skills, knowledge and capability across Government to help SEA practitioners deliver SEA programmes.
- **In House Development:** Bring all SEAC development in house, increasing capability and reducing the need for external creative agencies.

Government Security Centre for Industry Security Assurance (ISAC)

Mission

The Industry Security Assurance Centre (ISAC) works to increase the security of the Government supply chain. Currently operating within the Defence sphere, work is underway to begin expansion of ISAC services across Government.

Achievements

Industry Personal Security Assurance Framework (IPSA), is now a recognised assurance service across Defence industry partners. As IPSA's reputation grows, so does the uptake in companies seeking 'IPSA only assurance'.

This is a positive, as it reduces the number of companies requiring Facilities Security Clearance (FSC) and holding classified material unnecessarily.

- ISAC serves the MOD whilst looking for appropriate opportunities to support other Government departments.
- Provides an assurance service across Defence industry partners.
- Supports and enhances security of the Government supply chain.
- Over 500 private sector organisations FSC assured and 191 IPSA assured to date by ISAC, to reduce vulnerabilities in our supply chain.

Looking to the Future

Over the next three years our goal is to expand our current ISAC assurance service across Government to further secure supply chains. The process for this will include:

- Establishment of pan-Government need and scope requirement to create a unified framework or approach to address issues.
- Review changes to Government policy, primarily GovS 007 and its Supporting Documents, to establish the appropriate security environment with the potential to include the development and implementation of Government Conditions (GovCons) as a replacement to DefCons.
- Increase resources, including but not limited to financial, personnel and technology, to support, facilitate and enable conduct of Industry ISAC and IPSA pan-Government.
- Pan-Government oversight and management of the ISAC and IPSA performance (potentially by review of Management Information by GDC, establishment of a Steering Committee or similar) to ensure a consistent security baseline.

Government Security Centre International

Mission

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. The 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.

The 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.

Achievements

Over the past three years we have assisted Government departments by:

- Regularly updating and uploading products, including 257 Post Security Fact Sheets, to share via security.gov.uk.
- Briefing HMG staff before travelling to COP summits and Commonwealth Heads of Government Meetings (CHOGM), in the face of significantly heightened and dynamic threats overseas.
- Developing and delivering the Espionage Threat Awareness Course for all HMG staff deploying to high threat Espionage Posts and a HMG wide Espionage Threat Collection, Analysis and Risk Assessment.
- Effectively transitioning the Post Security Fact Sheet library from FCDO's previous electronic platform (GLO) to the new security.gov.uk site.
- Working collaboratively with other GSeCs on many projects to ensure a consistent and coherent approach to content with an international travel dimension.

Looking to the Future

Over the next three years, will seek to build upon the solid foundations by focusing on:

- **Espionage:** Continue to actively track the sustained and ever evolving increase in the targeting of civil service staff to gain access to information, building and systems, or cultivate our people as an 'Insider Threat'.
- **Advisory Gateway:** Secure the position as the first point of contact for any HMG Official seeking security advice for travelling overseas.
- **Build Stability:** continue to enhance our support to HMG departments in understanding overseas risks, building resilience to them and implementing mitigation measures to combat them.
- **Develop Security Culture:** further embed awareness of the dynamic and varied international threats and the proactive security practices set to mitigate them across all HMG departments when travelling overseas.
- **Increase Confidence:** Among HMG officials in the security arrangements and consistency of those arrangements across departments when participating in overseas travel.

Our Plan for Delivery

Governance

Over the past three years, the GSeCs have evolved from a proof-of-concept model to an established delivery framework, necessitating an update to our governance to meet this growth. This will enhance customer service, improve performance, and create further opportunities for the wider security function.

We remain committed to transparent reporting and will continue to seek a secure and stable financial base for the GSeCs. To achieve this, we will:

- Coordinate the GSeCs through the central GSG/Cabinet Office team, driving further collaboration, and the building of holistic and converged capabilities, with all activities endorsed by GSG.
- Maintain endorsement processes through the GSeC Delivery Committee and Government Security Board.
- Ensure the GSeCs' annual delivery plans are approved by the GSeC Delivery Committee at the start of each financial year.
- Oversee the GSeCs' financial allocation and reporting through GSG/Cabinet Office, including quarterly financial reports and timely invoice submissions.
- Pursue additional funding streams to enhance the GSeCs' services and reach.

Communications

Communication with our customers and stakeholders is vital to ensure customer centric delivery and increase the visibility of GSeC services. We will develop a communications plan throughout the three year period to increase the reach of our campaigns and to build understanding of GSeC services across Government. The success of our communications relies on getting the right messages to the right people at the right time in the most impactful way.

We will more closely align our communications with the best campaign management principles and will seek to improve evaluation methods to help gather greater insights and evidence of the behavioural benefits of the GSeCs' activities and campaigns. The GSeCs team will work closely with the GSeCs' communications colleagues to deliver clear, timely and informative materials to promote the GSeCs and their work - this will support the individual communications work of the GSeCs throughout each year of the plan. To deliver this:

- The GSG GSeC team will engage in meaningful communications to raise the profile of the GSeCs across Government through targeted communication plans with stakeholders and wider Government.
- The GSG GSeC team will develop and issue a regular GSeC bulletin, providing an overview of the work of all five GSeCs.
- The GSG GSeCs team will work with the GSeCs to embed an evaluation model into our communications to understand the reach and behavioral changes they drive.

- The GSG GSeCs team will work closely with GSeC Comms teams, GSG Comms and the Government Communication Service to increase the reach of our products and services to wider Government and beyond.

Measuring Success

To ensure accountability and transparency a yearly review of the three year plan will be undertaken to measure progress against our key pillars and KPIs. As part of this delivery, we will also engage regularly with our key strategic partners and GSG to ensure we have a coordinated approach. To deliver this:

- At the start of every financial year, the GSG GSeC team will work closely with the GSeCs to agree and set KPIs. These will be quantifiable measures used to evaluate the success and performance of the GSeCs in relation to the strategic goals and objectives and will be aligned to the Government's key priorities.
- We will ensure that quarterly reporting takes place to the GSeC Delivery Committee and that all KPIs are Aligned; Relevant; Measurable; Achievable; Timely and Visible.
- We will use these to track progress and identify areas for improvement as well as informing future business planning and funding opportunities and revise them when needed.
- We will agree KPIs annually to ensure they remain relevant and replace them where appropriate. The GSeCs will report against these KPIs monthly with quarterly reports being made available at GSeC Delivery Committees.

Funding Model

The GSeCs are currently funded via either burden share or the Integrated Security Fund (ISF) or a combination of both. This model is dependent on two factors:

- Departments continue to subscribe to the service.
- Successful bids to ISF.

The dependencies within the model are acknowledged, as are the potential risks to service delivery, long-term sustainability of critical programmes and workforce capability.

The GSG GSeCs team will support and mitigate against this with a proactive approach to identifying funding solutions. To deliver this:

- The GSG GSeCs team will continue to identify opportunities for funding routes for growth and standalone projects and continue our work to secure a stable funding platform for the GSeCs.
- The GSG GSeC team will seek out ways to provide additional funding streams to enhance the GSeCs' services and reach.

Risks & Issues

Identified risks and barriers to successful delivery have been identified as: changes to funding; changes to threat profile; and changes to resource requirements. It should also be noted that this plan has been created ahead of any possible machinery of Government changes, and the outcome of the Cyber Target Operating Model (TOM).

- **Changes to Funding:** Due to the nature of GSeC funding as it is now, we will conduct regular financial reviews, taking action where necessary to address any change to funding.
- **Changes to Threat Profile:** As the threat profile is constantly evolving we will implement a system to regularly assess emerging threats. This will allow us to quickly adapt our strategies and deploy mitigation measures to ensure operational resilience.
- **Changes to Resources:** Considering both of the above points, we will regularly assess requirements, capacity and availability. We will put adaptive measures in place to reallocate or optimise resources as needed, ensuring our operations remain effective and uninterrupted.

Annex A

Government Security Campaigns Plan for FY 2025/26

	Government Security Campaigns Plan 2025/2026			
	Q1 (Apr - Jun)	Q2 (Jul- Sep)	Q3 (Oct - Dec)	Q4 (Jan - Mar)
Key Campaigns	Theme: Personnel Security	Theme: Physical Security	Theme: Cyber Security	Theme: information Security
	Travel Campaign Personnel Security webinars for line managers New sessions (relaunch) Vetting changes	Travel Campaign Personal travel material (reuse) Potential promotion of the updated Travel Policy?	AI campaign (pending the launch of the AI Policy) Improving SCS Cyber skills Cyber Skills	WaS awareness "if you're working at SECRET you should be using ROSA"
Training	Security and Data Protections Fundamentals Inductions course aimed at those new to the Civil Service Refresher course - the annual mandatory training for all existing civil servants (for those departments that subscribed to the course only)	IAO refresher training	Cyber awareness month	
Events	GSG Security Conference 1st May			
	10th Jun Glasgow, SEC Centre	Civil Service Live 8th & 9th July London, ICC, Excel		