Funding and acknowledgements

The study on which this document is based was undertaken with financial support from the Prevention and Fight Against Crime (ISEC) Programme of the European Union, European Commission DG - Home Affairs Award [JLS/2009/ISEC-FP-4000000592] and was undertaken by members of the Scottish Centre for Crime and Justice Research (SCCJR) and the Scottish Institute for Policing Research (SIPRI).

The research project team gratefully acknowledge the participation and support of Strathclyde Police and Police Scotland in providing the access to undertake the research on which these guidelines are based. We are particularly grateful to all those – in Scotland, Europe and South Africa – who participated in interviews or who responded to the research project.
INTRODUCTION

Security has become a defining feature in bid preparation, planning and the delivery of mega-events.

This document contains findings from the research, which included a review of relevant international research and literature, particularly focusing on security planning arrangements for major events. It also included observation at G2014 security planning meetings, and interviews with individuals from a range of organisations with professional responsibilities in relation to the planning and operationalisation of security arrangements.

The purpose of the document is to provide guidance across key planning and implementation areas that are likely to be common to the successful undertaking of security planning and provision for sporting mega-events. It is important to note however that the broader political and bureaucratic contexts within which such planning takes place, and the diversity of social and institutional risks encountered, mean that guidance is likely to require modification and adaptation to inform policy, strategy and tactics in different national or local contexts. A model for understanding these key planning and implementation areas is given opposite.

Table 1: A model for understanding planning and implementation for mega-events.

### Preparation: Principles and Precursors

| Governance frameworks, partnership and vision |
| Strategic decisions |
| Communications |
| Testing and exercising |

### Risk Identification (including horizon scanning)

### Risk Mitigation

Figure 1: A model for understanding planning and implementation for mega-events.

### Scope

Adoption of vision / normative framework

| Requirement for holistic thinking / recognising inter-dependencies between actors/ agencies |

Flexibility of actors/agencies to respond to emerging challenges facing one or more actors/agencies |

### External factors underpinning influencing each stage |

- Global, local, political, economic, environmental, social |
“The fundamental drivers of the process [of establishing the security strategy] were the huge scale of the event and its impacts on almost every part of the community. This will be true of every other host city. Managing the preparation and staging of an event of this magnitude draws on the full range of resources of the host - intellectual, financial and physical.”
(Official Report for the Sydney 2000 Olympic Games)(iii)

Principles and precursors
Hosting an international sporting mega-event is a very large and complex undertaking that requires several years of planning, extensive budgets, the involvement of multiple state and non-state actors and organisations, and the input of thousands of people to plan and deliver. While the rationales behind expending the very considerable effort required to stage an event of this scale varies from host to host - whether realising ambitions of economic, social and physical transformations or a form of nation-building - all hosts maintain a primary objective of delivering the mega-event safely and securely. The wide range of global and local security risks, perceived and real, combined with the importance of host cities in providing a safe and secure environment has meant that security planning is a key early priority.

For many host cities and countries, it is important that security arrangements do not interfere with the ‘spirit of the games’. Security at mega-events therefore ideally operates as an ‘absent presence’, apparent to attentive citizens seeking reassurance but inconspicuous enough that the spectacle of security does not itself terrorize the public or undermine the spirit of the sporting event(iv). This task of creating ‘inconspicuous security’ is problematic considering the number of security personnel involved. For security planners, it is essential that security operations do not overshadow the events so finding the balance between security and spectator enjoyment poses a continuous challenge.

Mega-events incorporate security, intelligence, and law enforcement agencies on the national, state and local levels, along with their emergency services counterparts. There is a call for these agencies and services to be prepared to respond to any eventuality that may threaten the security of the event or the safety of the wider general public during the event, including terrorist threats, inclement weather, disease outbreak, critical infrastructure failure, natural disasters, and more. For some hosts, the event is regarded as their largest, most expensive and most intricate ever.

There are several common trends within the realm of mega-event security planning. Because of their complexity and scale, key amongst these is to start planning from day one(v).

One of the most difficult aspects involved in setting security policy for a mega-event is estimating what threats to the event will arise years in advance of the actual event date. Initial security planning begins during the bid phase, which is usually several years before an event takes place. Nevertheless the early planning stage is of key importance for the taking of early and timely decisions, and developing a full understanding of capabilities and capacities, and ensuring adequate public transparency. It is key for the review of existing legislative frameworks; estimates of resource needs; and the initial development of an overall work plan. It is also a crucial time for establishing buy-in and support from relevant agencies.

Key guidance points
• Early planning for security is crucial
• Relevant existing legislative frameworks used as a basis for agreements between ‘owner-organisers’ and public authorities, as early as possible
• An estimate of the resource needs for planning and implementation
• A credible overall design or blueprint for security needs
• Buy-in and support from relevant agencies, providers and other constituencies likely to be involved in security planning and implementation, with commitment to a holistic process
• An approach guided and informed by the principles of negotiated management, incorporating negotiation, consensus and interaction.
The responsibilities regarding planning and staging of a sporting mega-event are stipulated in contracts between host cities or countries and owner organisations’ like FIFA, the IOC or the CGF, which exercise a controlling function and often require the establishment of specific high level governance structures which in turn entail particular configurations of responsibilities for management of the event.

Governance schemes define the design, planning, hosting and delivery of mega-events, and incorporate the relevant decision making process regarding allocation of resources. Within host countries, responsibilities for overall governance, risk management, financial management and programme management arrangements to ensure successful delivery of the event tend to lie with national and/or local government and a small number of key agencies, which together form the bureaucratic context supporting the setting of security responsibilities and the development of governance structures.

Governance schemes define the design, planning and provision of security for coordinating participation. Robust governance structures are essential, for several reasons: First, global events invariably involve a wide range of state and non-state actors in planning and coordination, management of risk, training of personnel, and the mobilisation of security; in addition to the sharing of intelligence. It is important to recognise the potential number and diversity of actors in this landscape – even within specific agencies – and the challenges that such a constellation of public and private agencies can bring. Security operations take place on a grand scale and require close forms of cooperation at international, national, regional and local levels.

Second, security planning relies on international and national intelligence, working under international governing frameworks and securing international populations. Local security operations have to co-exist alongside a high security complex, concerned with national and international level political aims and objectives, as well as local community-oriented safety and quality of life concerns. Those with responsibility for the planning and provision of security at a national/local level are therefore required to navigate an international landscape and establish mechanisms for working, which requires and necessitates organisational capacity on a huge scale.

Third, governance structures with identified roles and remits for partners, and with clear lines of communication provide mechanisms for transparency and accountability. Multi-agency working requires interdependencies in terms of working arrangements, and the absence of clear governance structures can lead to responsibility and accountability being vague. Crucial to the achievement of successful security planning therefore is the early adoption of appropriate internal governance arrangements, to provide a framework for partner relationships, communications, and the levels of authority and autonomy between different agents and in which they function. As a result, structures for the provision and delivery of security for mega-events tend to be highly complex, incorporating a wide range of stakeholders and partner organisations, with activities co-ordinated through overarching governance arrangements. A shared governmental association is an essential component in establishing the setting of security responsibilities and the development of governance structures.

Different models of security governance have been identified: vertical governance involving hierarchical – usually state-led – processes of steering and coordination (upward or downward) characterised by more formal relationships; corporate governance, and; horizontal (nodal) governance where responsibilities for security are more dispersed between a range of public and private security actors in a network.(v). In reality, these models intersect, and are more complex in form. All however stipulate some form of interaction between the different agencies and institutions, and emphasise inter-organisational relations.

Decisions on the adoption of a particular form of security governance in the context of mega-events need to take account of the broader governance scheme for the design, planning and delivery of the event, the roles of strategic security partners, and the existing networks of relationships between state and non-state security stakeholders at the international, regional and local levels.

Monitoring governance processes

Mechanisms that allow for the auditing and monitoring of preparation and planning processes, decision-making and implementation, including the appropriateness of structures for delivery, are considered good practice. Audit information on the operation of governance structures, alongside the appropriate means for the capture and use of meaningful data to provide authoritative, evidence-based analysis is essential for transparency and accountability and assists in collective learning and knowledge management processes.

Key guidance points

- A core recommendation is that stakeholders focus collaborative efforts on creating or strengthening institutional mechanisms that enable security planning structures to develop in a dynamic and sustainable manner;
- Early establishment of robust, yet flexible, governance structures for security planning:
  a. with a clear remit and responsibilities;
  b. to provide oversight and co-ordination for strategic, tactical and operational levels, as well as accountability for decision-making;
  c. that is able to achieve specific tasks, whilst retaining an overall unity of purpose;
- A structure for making decisions and holding each part of the system accountable for meeting its responsibilities;
- A designated high calibre leader of appropriate authority;
- A set of measurable performance standards to identify where the system and its elements are and are not operating according to their objectives;
- Inclusion of robust mechanisms to monitor preparation processes, in order to enhance transparency and accountability and which;
  a. report on actions taken and results achieved, lessons learnt;
  b. provide recommendations for future events.
Security is now increasingly provided by partnerships that straddle the public, voluntary and business sectors. These include high-level strategic partnerships with primary responsibility for planning and management, and sub-level working groups consisting of partnerships with operational responsibilities. High levels of co-ordination and cooperation between diverse agencies is crucially important for planning and delivery of mega-event security. Security planning needs to be co-ordinated effectively with diverse partners to ensure that they complement each other. Notable features of these events recognised as successful are the organisational approach and high levels of inter-agency co-operation and professionalism. For example, a defining feature of the organisational approach in the lead up to and during the FIFA World Cup in South Africa was the mobilisation and smooth co-ordination of various agencies and networks (vii).

Yet partnership working can be challenging, particularly in relation to the very lengthy, complex and often fraught planning stages necessary for mega-event security. The fixed deadlines for the readiness of venues and the production or completion of other security facilities can place undue stress on professional working relationships. The unprecedented scale of mega-event preparation and the high reputational stakes can severely undermine professional relationships.

It is important to be aware of the number of empirical challenges relating to the routine, day-to-day activities and logistics of partnerships and the parameters within which they operate. Each partner is likely to have different needs, priorities, technologies, and ways of thinking. Different approaches may lead to conflict. A further challenge is that of sustaining partnerships throughout the often very lengthy period of preparation. Partnerships may sometimes be driven by particular personalities, and equally may be destroyed by them. Partnerships also have to deal with power issues, which may be legal or symbolic.

Complex co-working structures and arrangements can sometimes blur boundaries of responsibilities. A clear framework and specificity of purpose is essential based on a shared vision of what is meant by security, and a clear understanding of the respective roles and remits. Aligned to this is the need for ‘whole system thinking’ in order to develop a common language and approach. There is a clear risk that partnership working, involving multiple actors from state, public, and private sectors, as well as local communities, compromises holistic thinking. This risk can be reduced by the adoption of a shared set of values and the encouragement of a culture of collaboration between all partners.

Of key importance for security planning are strong international relationships, particularly in relation to intelligence. Possessing a robust national intelligence community is a substantial advantage when preparing for and hosting a mega-event. Equally, if a host country is lacking in the area of national intelligence capability, the setting up a dedicated working partnership with other nations whose capacity is more advanced can go some way to rectifying this deficiency.

Another important area of partnership concerns the engagement and utilisation of international consultants specialising in providing guidance and management of sporting mega-events to share the knowledge that they have built up. This is a recognised feature of planning practices. It is also a recognised risk. Key issues here relate on the one hand, to the management and resolution of differences of opinion between local and global experts in terms of security priorities and planning and, on the other the risk of high turnover in relatively short time periods, which can affect planning and result in a loss of knowledge.

When working with different partners with specific responsibilities, it is essential to have a contingency plan in case one partner – or one aspect of security – fails to deliver or becomes redundant. For example, the spectacular failure of the global private security organisation G4S to deliver on its security responsibilities not only jeopardised the venue security arrangements for London 2012 Olympics, it also became a significant matter of public concern and national embarrassment. In multi-agency structures, as responsibilities and accountabilities become more dispersed a clear danger is for agencies to become scapegoats when things go wrong. Creating audit trails has become a prominent feature in the management of security to reduce the chances of ‘scapegoating’ that can occur through the blurring or abrogating of responsibilities.

Conventionally, a linear approach is taken to security planning but, given the range of partners involved in mega-event security and the size and scale and complexity of the tasks, concurrent approaches sometimes need to be adopted whereby different inter-related security activities are progressed simultaneously.

In recent mega-events, strategic decisions have taken to co-locate those with responsibility for security planning and implementation within the same physical location. Creation of a centralised co-ordination centre has become standard practice. This is intended to ensure close and efficient working practices, provide economies of scale but also to foster professional working relationships, and encourage an atmosphere of unity, focus, and hard work.

3 PARTNERSHIP WORKING AND A SHARED VISION FOR DELIVERY

High levels of co-ordination and cooperation between diverse agencies is crucially important for planning and delivery of mega-event security.
Effective strategic decision-making on key issues is integral to security planning and provision

The security arrangements at mega-events seek to achieve maximum levels of security through the implementation of governance structures and practices that support risk management, incorporating the identification, assessment and mitigation of risk. The governance structures supporting risk management for G2014 were highly complex, encompassing a wide range of both stakeholders and potential risks.

Given the scale and complexity of security planning and provision at mega-events—which inevitably go beyond the routine planning and provision at mega-events—there is a natural tendency towards a more serious and reluctant to discard identified risks. Additionally, risk assessment in advance of mega-events can also be used by security actors and agencies as a stratagem: escalating the priority of a risk can potentially provide leverage to unlock the provision of a larger share of security programme resources.

Processes of risk management inevitably raise issues of governance and accountability. These issues become increasingly important under the conditions of international attention and scrutiny associated with mega-events, whereby risks can become reputational to the host city or country. Any failure to deal satisfactorily with such risks can result in both domestic political embarrassment and a loss of confidence from international partners.

Effortive strategic decision-making on key issues

The results of such an exercise can result in both domestic political embarrassment and a loss of confidence from international partners. External communication, that is the discussion with communities, groups and organisations beyond the fields of politics and security, is vital to security planning and provision. Strategic decision-makers should ensure that full use is made of all channels of communication with host communities who will be most affected by the mega-event. Communities can not only help identify risks but they can also be co-opted to help prevent risks associated with domestic extremism or political activism. This style of proactive security was evident at the 2012 London Olympics, where police protect liaison groups were active in communities, and similar efforts were made at G2014.

Exercising

Exercising security in advance of a mega-event provides an opportunity to test the decision-making of key security actors, and assess the effectiveness and resilience of structures, agencies and processes. It also provides an opportunity to plan for, and test responses to, emerging risks that have not yet previously appeared on the threat horizon, and have thus not yet been ‘experienced’.

The system for exercising security in advance of G2014 evolved from existing structures in Scotland (linked to the wider UK network) and capitalised upon the similar work undertaken for the London 2012 Olympic Games. Developing an exercising regime in advance of a mega-event allows strategic decision-makers to address any weaknesses in planning, response, resourcing, interoperability, or resilience.

Key guidance points

- The robust identification of risks becomes essential to security planning and provision.
- The formation of groups from a diverse range of security providers in order that they try and identify as many risks as may be associated with the mega-event.
- Identify appropriate risk assessment methodology used to facilitate prioritisation of risks.
- Awareness and understanding of the challenges posed by risk assessment processes.
- Strategic decisions can assist in improving communication between partner agencies.
- Integration between security agencies facilitate enduring inter-agency cooperation beyond the conclusion of the mega-event.
- Ensure full use is made of all channels of communication with host communities who will be most affected by the mega-event.
- Develop an effective exercising programme, involving ‘real-time’ and ‘table-top’ exercises, to test the decision-making of key security actors.

The scale, complexity and provision at mega-events—which inevitably go beyond the routine planning and provision at mega-events—there is a natural tendency towards a more serious and reluctant to discard identified risks. Additionally, risk assessment in advance of mega-events can also be used by security actors and agencies as a stratagem: escalating the priority of a risk can potentially provide leverage to unlock the provision of a larger share of security programme resources.

Processes of risk management inevitably raise issues of governance and accountability. These issues become increasingly important under the conditions of international attention and scrutiny associated with mega-events, whereby risks can become reputational to the host city or country. Any failure to deal satisfactorily with such risks can result in both domestic political embarrassment and a loss of confidence from international partners.

Additional risk assessment in advance of mega-events can be used by security actors and agencies as a stratagem: escalating the priority of a risk can potentially provide leverage to unlock the provision of a larger share of security programme resources.

Processes of risk management inevitably raise issues of governance and accountability. These issues become increasingly important under the conditions of international attention and scrutiny associated with mega-events, whereby risks can become reputational to the host city or country. Any failure to deal satisfactorily with such risks can result in both domestic political embarrassment and a loss of confidence from international partners.

Internal communication between security agencies and providers is essential to the proper functioning of any security model for mega-events. Beyond the necessary technological requirements for communication, including command and control systems, strategic decisions can assist in improving communication between partner agencies, for example through the provision of resources for the co-location of staff. However, the effectiveness of any such endeavour hinges on the integration of people, processes and practices between organisations. Where effective channels of communication between security partners are established, and integration occurs this has the potential to facilitate enduring inter-agency cooperation beyond the conclusion of the mega-event.

Communications

Internal communication between security agencies and providers is essential to the proper functioning of any security model for mega-events. Beyond the necessary technological requirements for communication, including command and control systems, strategic decisions can assist in improving communication between partner agencies, for example through the provision of resources for the co-location of staff. However, the effectiveness of any such endeavour hinges on the integration of people, processes and practices between organisations. Where effective channels of communication between security partners are established, and integration occurs this has the potential to facilitate enduring inter-agency cooperation beyond the conclusion of the mega-event.

External communication, that is the discussion with communities, groups and organisations beyond the fields of politics and security, is vital to security planning and provision. Strategic decision-makers should ensure that full use is made of all channels of communication with host communities who will be most affected by the mega-event. Communities can not only help identify risks but they can also be co-opted to help prevent risks associated with domestic extremism or political activism. This style of proactive security was evident at the 2012 London Olympics, where police protect liaison groups were active in communities, and similar efforts were made at G2014.

Exercising

Exercising security in advance of a mega-event provides an opportunity to test the decision-making of key security actors, and assess the effectiveness and resilience of structures, agencies and processes. It also provides an opportunity to plan for, and test responses to, emerging risks that have not yet previously appeared on the threat horizon, and have thus not yet been ‘experienced’. The system for exercising security in advance of G2014 evolved from existing structures in Scotland (linked to the wider UK network) and capitalised upon the similar work undertaken for the London 2012 Olympic Games. Developing an exercising regime in advance of a mega-event allows strategic decision-makers to address any weaknesses in planning, response, resourcing, interoperability, or resilience.

Key guidance points

- The robust identification of risks becomes essential to security planning and provision.
- The formation of groups from a diverse range of security providers in order that they try and identify as many risks as may be associated with the mega-event.
- Identify appropriate risk assessment methodology used to facilitate prioritisation of risks.
- Awareness and understanding of the challenges posed by risk assessment processes.
- Strategic decisions can assist in improving communication between partner agencies.
- Integration between security agencies facilitate enduring inter-agency cooperation beyond the conclusion of the mega-event.
- Ensure full use is made of all channels of communication with host communities who will be most affected by the mega-event.
- Develop an effective exercising programme, involving ‘real-time’ and ‘table-top’ exercises, to test the decision-making of key security actors.
Security threats to mega-events can be diverse, and the list of potential targets expansive. Security planners responsible for staging mega-events face huge challenges, which require the design and implementation of the most effective and suitable security strategies possible.

Security operations for mega-events tend to be specific to the geographical conditions surrounding the event, the particular threats involved, and the capabilities and philosophy of the host government responsible for security. Generally, however, key security threats taken into account in mega-event security operations are: terrorism, spectator and/or political violence, and urban crime, including localised risks such as robbery, drug dealing, and interpersonal violence. Each of these requires strategic security planning and effective security during mega events.

The risks and potential targets associated with a mega-event are numerous and varied. Potential terrorist targets may include everything from the main event stadium to critical infrastructure like public transportation networks, and power, water and electricity grids. Indeed, any event and any venue may become a potential target. Athletes’ accommodation; hotels housing event staff; and, areas within the host city and country that are not directly connected with the event. These include metropolitan areas outside of the host city; public transport anywhere in the country, national borders, airports and ports; governmental building, societal and symbolic icons, national infrastructure. The list of potential targets is expansive, thus the security planners responsible for staging an event face huge challenges. To achieve this, requires designing and implementing the most effective and suitable security strategies possible.

In general, security planning processes include three main steps;

1. **Intelligence gathering**
2. **Development of preventative measures**
3. **Crisis management**

### Common security measures for sporting mega-events

Counter-terrorism and general security strategies tend to be based on existing national security plans. The focus of security planning of mega-events internationally has been on prevention, drawing primarily on situational crime prevention approaches, by using techniques of surveillance and control to reduce the opportunity to commit crime (i) and the application of defensible space theory (ii) to the design and co-ordination of security planning. The international research literature and official event reports provide information on common security measures used in mega-events, although these vary in terms of scale.

#### Intelligence-led security:
- Creation of a specialised event-focused intelligence centre
- Building, developing and enhancing strong international political and intelligence sharing relationships
- Development of internal governmental structures and inter-agency collaboration domestically
- Co-location of those with responsibility for security planning and implementation within a centralised co-ordination centre.

#### Risk
- Use of risk and threat assessment methodologies, which also include qualitative forecasting
- Formulation of ‘families’ of risk
- Identification of owners of risk with responsibility for monitoring and mitigating
- Frequent, numerous – and as event draws closer – daily, risk and threat assessments conducted.

#### Internal resilience and preparedness
- Protection of critical infrastructures (power, water, transport)
- Strengthening of potential targets, including both hard and soft targets (soft targets include schools, restaurants, hotels, public transportation etc.).

#### Training and exercising
- Enhances training for law enforcement personnel (on crowd management, fire arms, etc.)
- Extensive use of simulation exercises to test readiness and contingency
- ‘Table-top’ and ‘real-time’ exercises.

#### Venue security
- ‘Island site’ security concepts
- ‘Concentric rings’ principles
- Perimeter fencing
- Perimeter and in-venue patrols
- CCTV surveillance networks
- Vehicle restrictions around venue site
- Vehicle accreditation and inspections on entry to venue.
- Venue security and person searches (according to level of risk for event/venue)
- Entry security personnel and events stewards
- Crowd management personnel in venues
- Access and entry security (personal searches, bag searches, magnetometer gates)

#### Transport
- Use of intelligence analysts to support transport security
- CCTV monitoring of transport networks
- Restricted parking around venues
- Restrictions on certain vehicle categories
- Dedicated event transportation routes

#### Border Controls (land, ports, and aviation)
- Enhanced border controls
- Amplified passport checks
- Enhanced international entry accreditation procedures for individuals entering the country during event-time increased levels of security personnel present at borders, ports, airports
- Addition of military vehicles, vessels, submarines
- ‘No-fly’ zones over main stadia.

### VIP policies (heads of state, royalty, athletes)
- Protective measures, including site inspections, advance escorts, separate venue entrances, patrolling guards at accommodation sites, monitoring of transportation routes,
- Use of close personal protection teams (usually own personal security services).

### Public reassurance
- Community consultations
- Community engagement strategies
- Involvement of residents groups in some aspects of decision-making.
The security planning for mega-events often moves beyond merely securing the event. Just as mega-event preparation has the potential to create lasting legacies through investment in physical regeneration and the transformation of urban space through infrastructure preparation, and the creation of new or improved sporting venues, stadia, parks, and housing built specifically for the event, legacies emanating from security planning can have an impact and consequences beyond the duration of the event itself.

### Security legacies

Due to their exceptional nature and their ability to unlock resources, mega-events can leverage the integration of technological, informational and human capabilities to deter and detect crime and security risk that might otherwise not occur. The cross-sectoral partnership arrangements necessary for delivery of security, alongside often massive capital investments and the deployment of new security and surveillance configurations can therefore lead to enduring security legacies.

Security is an important feature not only for the duration of the mega-event, but also in its aftermath, producing a legacy for crime prevention, community safety, security and regulation.

**Resource legacies** concern the knowledge and experience gained and applied by key actors and stakeholders, and the insights drawn from relationships and partnerships that are forged and negotiated in planning and implementation. Here, security planning and delivery forms a valuable ‘memory bank’ or resource for the sharing of knowledge and experiences on how best to conduct security at subsequent events.

**Professional legacies** include the upgrading and up-skilling of existing professional security apparatus, such as modernisation of equipment, comprehensive training for police and/or military personnel, and private security contractors. This also might include the training that is given to the large number of local volunteers and semi-professionals servicing security, which was an explicit aim of G20. Mega-events can also enable the development of specialist expertise, which can be applied globally, through training seminars and professional conferences, and appointments as consultants and advisers.

**Physical security legacies** include preventative security measures permanently built into the physical infrastructure of new buildings and venues, and their adjacent spaces, such as CCTV infrastructure, fencing, access control, locks and alarms, lighting and architectural design which materially transform the physical environment. For example, permanent securitisation measures as part of the legacy of 2012 London Olympics; the retention of CCTV in Cape Town, and in and around Turin following the 2006 Winter Olympics. Securitisation is not always retained post-event; whilst there was an expansion of security measures in the twelve host cities of the 2006 World Cup in Germany, only two cities retained CCTV cameras following the event’s conclusion, although surveillance remained within the stadia.

### Legislative/regulatory legacies

The organisation of mega-events is generally subject to existing national legislation and local rules on the organisation of sporting events; on international conventions, such as the European Convention on Spectator Violence and Misbehaviour at Sports Events; and particular contractual requirements of organising authorities. Compliance with these requirements may require legal and/or regulatory change, some with permanent effects. For example, prior to the 2006 FIFA World Cup, laws were changed to extend the use of CCTV, the extension of custody for suspects, and to allow for wire-tapping and automatic number plate recognition.

In South Africa, in advance of the 2010 FIFA World Cup a raft of local bye laws were introduced, and prior to the XXVII Olympic Games in Sydney 2000, laws were introduced aimed at increasing the control of public gatherings to stem possible protests.

### Consider legacy implications

Increasingly plans for the laying down of security legacies are incorporated into bid development for mega-events. Careful consideration of the type of security legacy likely to emanate from a mega-event is key to early planning, with significant implications for budgetary considerations. The nature and implications of particular types of security legacy are immensely important not only for the reputation of the host countries but also in terms of their long-term effects on the local communities that are likely to be subject to them.

Valuable legacies include those security investments that help (re)build the host’s physical and social infrastructure, that improve national and local intelligence capabilities, that build better legal frameworks to improve the ability to achieve security while respecting civil liberties, and that ensure effective judicial and legislative security oversight.

The introduction and retention of new or more extensive security technologies, practices and infrastructures runs a high risk of ‘security creep’, where security built or implemented for one purpose, is used for another purpose, and can have potentially significant consequences for civil liberties and human rights.

### Key guidance points

- Early consideration of the type and, importantly, the implications of security legacies, which include financial considerations.
- Adopt a discerning and contextually grounded approach to security planning and implementation to avoid ‘security creep’.

The retention of extensive security apparatus and expanded legal powers implemented for events, can pose serious questions of legitimacy and democracy. The costliness of permanently embedding security apparatus can also have devastating financial outcomes for host countries, as in the example of the Olympic Games held in Athens in 2004.
LIST OF KEY GUIDANCE POINTS

Preparation
1. Early planning for security is crucial.
2. Relevant existing legislative frameworks should be used as a basis for agreements between ‘owner-organisers’ and public authorities, as early as possible.
3. An early estimate of the resource needs for planning and implementation to be provided.
4. A credible overall design or blueprint for security needs, as early as possible.
5. Obtain Buy-in and support from relevant agencies, providers and other constituencies likely to be involved in security planning and implementation, with commitment to a holistic process.
6. Adopt an approach guided and informed by the principles of negotiated management, incorporating negotiation, consensus and interaction.

Governance Frameworks
7. A core recommendation is that stakeholders focus collaborative efforts on creating or strengthening institutional mechanisms that enable security planning structures to develop in a dynamic and sustainable manner.
8. Early establishment of robust, yet flexible, governance structures for security planning:
   - with a clear remit and responsibilities;
   - to provide oversight and co-ordination for strategic, tactical and operational levels, as well as accountability for decision-making;
   - that is able to achieve specific tasks, whilst retaining an overall unity of purpose.
9. A structure for making decisions and holding each part of the system accountable for meeting its responsibilities.
10. Appointment of a designated high calibre leader, of appropriate authority.
11. Development of a set of measurable performance standards to identify where the system and its elements are, and are not, operating according to their objectives.
12. Inclusion of robust mechanisms to monitor preparation processes, in order to enhance transparency and accountability and which:
   - report on actions taken and results achieved, lessons learnt;
   - provide recommendations for future events.

Partnership Working and Shared Vision for Delivery
13. The creation of a common objective and the adoption of a set of shared values to enable a clear vision of security provision.
14. Development of a culture of collaboration between all partners involved in the security planning process.
15. A clear framework and definite purpose for each security function.
16. Aim for participatory accountability in trying to address complex security plans and arrangements.
17. Co-location of those with responsibility for security planning in a centralised location.
18. Robust contingency planning from an early stage, to mitigate against delay, or failure to deliver by one partner.
19. Monitoring of management information from partners.

Strategic Decisions
20. The robust identification of risks is essential to security planning and provision.
21. The formation of groups from a diverse range of security providers in order that they try and identify as many risks as may be associated with the mega-event.
22. Identify appropriate risk assessment methodology used to facilitate prioritisation of risks.
23. Awareness and understanding of the challenges posed by risk assessment processes.
24. Strategic decisions can assist in improving communication between partner agencies.
25. Integration between security agencies facilitate enduring inter-agency cooperation beyond the conclusion of the mega-event.
26. Ensure full use is made of all channels of communication with host communities who will be most affected by the mega-event.
27. Develop an effective exercising programme, involving ‘table-top’ and real-time exercises, to test the decision-making of key security actors.

Planning for Security Legacies
28. Early consideration of the type, and importantly, the implications of security legacies, which include financial considerations.
29. Adopt a discerning and contextually grounded approach to security planning and implementation to avoid ‘security creep’.

USEFUL RESOURCES

ENDNOTES


