OSCE Organization for Security and Co-operation in Europe

PROTECT

TECHNICAL GUIDE
ON PHYSICAL SECURITY CONSIDERATIONS FOR PROTECTING CRITICAL INFRASTRUCTURE FROM TERRORIST ATTACKS

2025 Release

Critical infrastructure provides essential services that enable daily life across the entire OSCE area, from potable water, energy and electricity to transportation and banking services. Given their central role in society, critical infrastructure sites have historically been, and continue to be, targeted by violent extremist and terrorist organizations. This has been recognized by the OSCE participating States, which, in the 2012 OSCE Consolidated Framework for the Fight Against Terrorism, called on the Organization to pursue activities to enhance co-operation and build capacity to "[i]mprove the security of international transportation and of other critical infrastructure".[1]

Addressing this persistent yet evolving threat is why the OSCE's Project PROTECT developed the *Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks*. This *Technical Guide* is a consolidation of experience and expertise from across the OSCE area and beyond.

This Technical Guide aims to support OSCE participating States and critical infrastructure owners/operators to meet the evolving terrorist threat head-on and enhance the physical security of their critical infrastructure sites. It provides structured guidance on practices, principles and considerations that can enhance the physical security of permanent critical infrastructure sites and facilities, with a view towards preventing, better preparing for and mitigating terrorist attacks.

WHERE CAN I FIND THE GUIDE?

To access the Guide in English and Russian, go to www.osce.org/project/PROTECT or scan this QR code. Hard copies are available for interested parties upon request.

1 OSCE Permanent Council Decision No. 1063 OSCE Consolidated Framework for the Fight Against Terrorism.

WHY IS THIS GUIDE NEEDED?

With the exception of highly regulated critical infrastructure sectors, many OSCE participating States do not have detailed instructions on the physical security measures to be implemented at the site level. What often exists is a complex collection of practices, principles and non-binding guidance documents, which governments, critical infrastructure owners/operators and those with security duties at critical infrastructure facilities (including private security providers) must sift through and examine in order to ensure effective physical security for sites and facilities under their care.

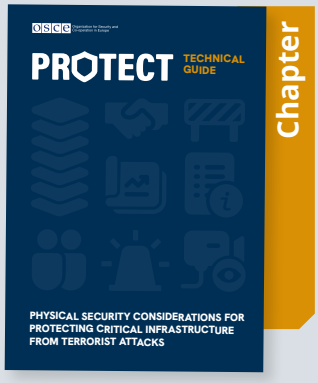
Rather than dictating a single approach to physical security, this Guide presents a range of publicly available practices that reflect the diverse approaches that currently exist. Most of the practices cited throughout this Guide are from OSCE participating States, showcasing the vast wealth of knowledge present in the OSCE's membership.

WHO IS THIS GUIDE FOR?

Effective physical security at critical infrastructure facilities requires buy-in and commitment from a range of stakeholders:

- **Senior government policymakers and senior critical infrastructure owners/operators:** While not the direct implementers of physical security measures at the critical infrastructure site level, government policymakers provide the legal and strategic framework around which effective physical security is built. Insights that may be particularly valuable are in Chapter 2 on Strategic and Legal Frameworks for Critical Infrastructure Protection, Chapter 3 on Human Rights Considerations, and Chapter 4 on Public–Private Partnerships.
- **Technical practitioners with physical security duties:** The Guide offers an essential strategic framework for physical security missions in Chapters 1 through 3. Chapters 5 through 10 provide detailed descriptions of real-life policies, case studies and practices that enhance physical security at a range of different critical infrastructure sites.

WHAT IS IN THE GUIDE?



1 Introduction
2 Strategic and Legal Frameworks for Critical Infrastructure Protection
3 Human Rights Considerations
4 Public–Private Partnerships
5 Terrorism Threat and Risk Assessment
6 Physical Security Measures
7 Security Planning and Target Hardening
8 Insider Threat Management
9 Training and Exercising
10 Enhanced Threat Escalation Options

FURTHER DETAILS

If you would like to learn more about this *Technical Guide* or Project PROTECT, email the Action against Terrorism Unit of the OSCE Secretariat's Transnational Threats Department at atu@osce.org.

FUNDERS

Project PROTECT is funded by the United States of America's Bureau of Counter-terrorism and the Federal Republic of Germany.