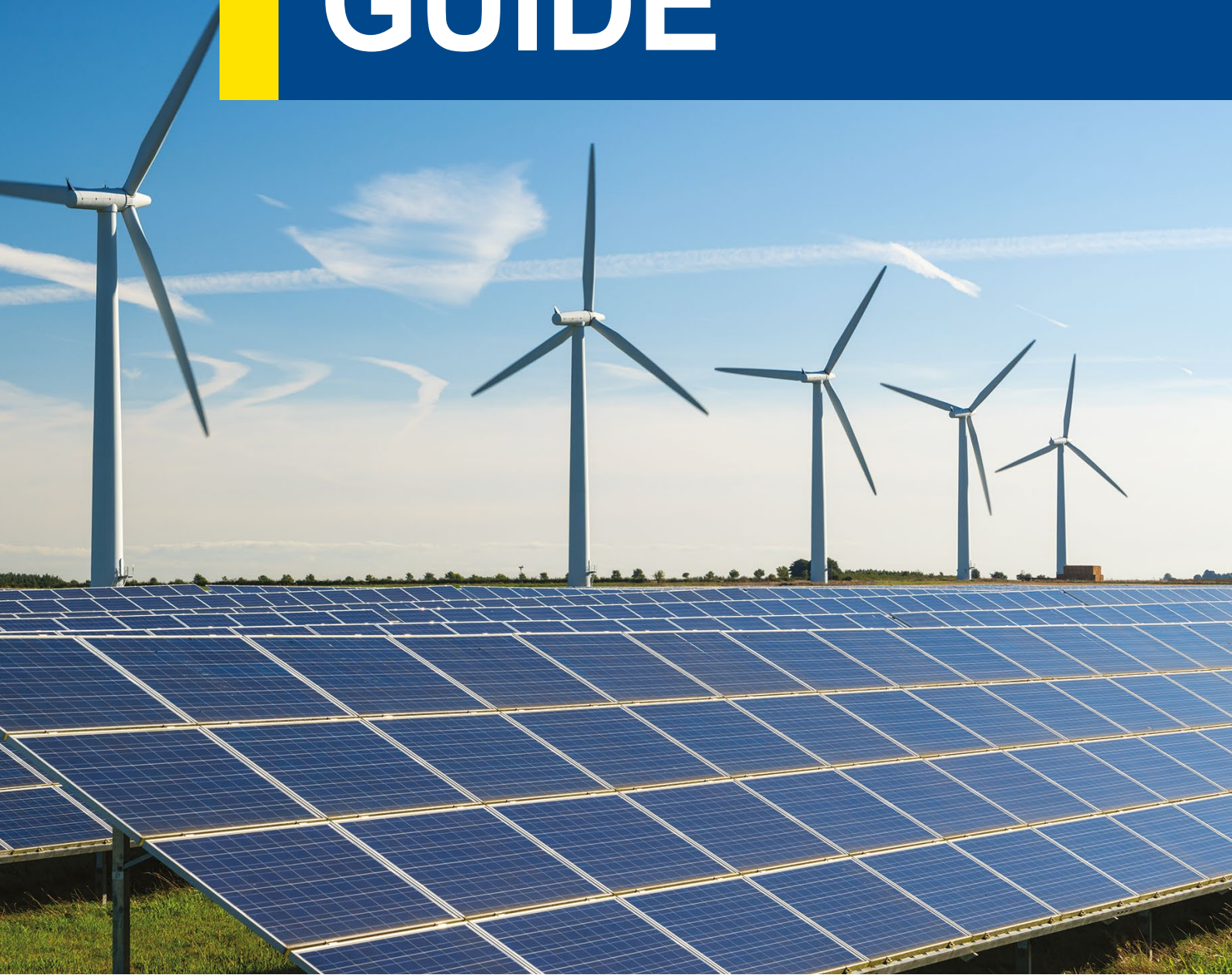


Secured by Design

SOLAR FARM GUIDE



Ministerial Foreword

Solar is at the heart of the Government's mission to deliver clean power by 2030. If we're to achieve this ambition, we'll need to double the amount of solar capacity in the UK.

It is in all of our interests to keep this essential infrastructure secure. Preventing theft and damage ensures that solar farms can keep providing us with clean, cheap power. It prevents developers from having to bear the costs of repairs. And it helps to reassure local residents and planners about the impact of new infrastructure on local areas.

I am grateful to all of those who have contributed to this guidance. I hope it will be of use to developers, local police forces, communities, and planning authorities – all of whom have a vital role to play as we race toward our solar deployment targets.



Sarah Jones MP,
Minister of State for Policing and Crime,
Home Office



Michael Shanks MP,
Minister of State for Energy,
Department for Energy Security and Net Zero

Foreword

It is my pleasure to endorse this joint piece of work between Secured by Design and the National Infrastructure Crime Reduction Partnership (NICRP). This is the culmination of partnership work at its best and I am grateful for both NICRP members and the police service for their collaboration in producing the very best advice in securing renewable energy assets and in particular solar farms and estates.

As the United Kingdom moves ever closer to reliance on renewable energy we must as a collective understand that organised crime affects every sector of our crucial and critical infrastructure. So, to secure the future of everything we rely on to power our homes, businesses, transport network and construction, we need to remain focused and support not only the police service but those charged with securing these resources.

Whilst every contributor went above and beyond in compiling this document, I would particularly like to thank those members of the NICRP who contributed for their unwavering support and boundless assistance.

Andy Wood – NICRP Project Lead
Safer Business Network



Preface

Solar energy now plays a vital role in the United Kingdom's transition to sustainable power. Solar farms and associated installations form part of national infrastructure and must therefore be protected against crime, disruption, and deliberate interference.

This guide has been produced by Police Crime Prevention Initiatives (Police CPI) in collaboration with industry partners, brought together through the National Infrastructure Crime Reduction Partnership (NICRP). Police CPI is the national police organisation that owns and manages Secured by Design (SBD), the official police security initiative, on behalf of the UK Police Service, and NICRP brings together police, government and industry to reduce crime affecting the UK's infrastructure sectors.

The guide is intended for developers, designers, operators, planning authorities, contractors and security professionals involved in the planning, design, construction and operation of solar farms. It provides practical guidance on proportionate, risk-based security measures to support safe and resilient renewable energy developments.

Throughout this guide, reference is made to the police Designing Out Crime Officer (DOCO). The DOCO is a specialist officer within the Secured by Design framework who advises on how to reduce crime and risk through layout, specification and management. DOCOs are professionally trained, nationally recognised as a policing specialism by the National Police Chiefs' Council (NPCC) and required to keep an accredited portfolio of continual professional development. Their role is to assess local and national risk, interpret relevant standards, and recommend proportionate security measures for each site.

Integrating security from the outset reduces crime opportunities, minimises operational disruption, and protects long-term investment while supporting environmental objectives.

If you are already familiar with the Secured by Design application process, go straight to the detailed security measures, which begin at Section 5 on page 17.

PART 1

7

1 Introduction	8
1.1 Purpose	8
1.2 Scope	8
1.3 Context	8
1.4 Proportionate Security	9
1.5 Counter-Terrorism Co-ordination	9
1.6 Data Protection and Privacy	10
1.7 Sustainability and Carbon Considerations	10
2 Designing Out Crime Process	10
2.1 Purpose	10
2.2 Planning Context	10
2.3 Security Overlay to the Royal Institute of British Architects (RIBA) Plan of Work	11
2.4 Planning Policy and Design Quality	11
2.5 Example Planning Condition	11
2.6 Design and Access Statements (DAS)	11
2.7 Role of the Designing Out Crime Officer (DOCO)	12
2.8 Crime-Risk Analysis (CRA)	12
2.9 Integration with Other Disciplines	12
2.10 Documentation	12
3 SBD Award Routes	12
3.1 Overview	12
3.2 SBD Solar Farm Award (New Developments)	13
3.3 SBD Vulnerability Survey (Existing Sites)	13
3.4 Nationally Significant Infrastructure Projects (NSIPs) and the Development Consent Order (DCO) Process	14
3.5 How to apply for an SBD Solar Farm Award	14
4 Proportionate Security and Zoning	14
4.1 Principle	14
4.2 Site Risk Classification	14
4.3 Layered Approach	15
4.4 Compensatory Measures	15
4.5 Alignment with Safety Legislation	15
4.6 Review and Adjustment	15

PART 2

16

5 Construction Phase Security	17
6 Layer 1 – Outer Environment	17
6.1 Principle	17
6.2 Vehicle Parking and Access	17
6.3 Public Rights of Way (PROWs)	18

6.4	Hostile Vehicle Mitigation (HVM)	18
6.5	Exclusion Zones and Buffer Land	19
6.6	Security Signage	19
6.7	Lighting (Outer Environment)	19
7	Layer 2 – Perimeter Security	19
7.1	Principle	19
7.2	Boundary Treatments	19
7.3	Lighting	22
7.4	Operational Requirement (OR) for Electronic Security Systems	23
7.5	Video Surveillance Systems (VSS)	23
7.6	Perimeter Intrusion Detection Systems (PIDS)	24
7.7	Audio Challenge Systems	24
7.8	Electronic Access Control Systems (EACS)	25
8	Layer 3 – Internal Compounds and Building Security	26
8.1	Principle	26
8.2	Doorsets and Windows	26
8.3	Intruder and Hold-Up Alarm Systems (I&HAS)	26
8.4	Secure Storage Units (Modular Units, Temporary Buildings and Steel Containers)	27
8.5	Photovoltaic (PV) Panels and Cabling	28
8.6	Property Marking and Tracking	29
8.7	Arson and Fire Protection	30
8.8	Battery Energy Storage Systems (BESS)	30
9	Layer 4 – Operational Security	31
9.1	Principle	31
9.2	On-Site Guarding	31
9.3	Security Management and Maintenance	32
9.4	Community Engagement	33
9.5	Secure Connected Device (SCD) Accreditation Scheme	34
9.6	Accurate Site Location Identification	34
9.7	Incident Response and Reporting	34
9.8	First Responder Co-ordination	35
9.9	Security Review and Continuous Improvement	35
Appendix A		36
A.1	National Infrastructure Crime Reduction Partnership (NICRP)	36
A.2	Police Crime Prevention Initiatives (Police CPI)	36
A.3	Abbreviations	36
A.4	Contacts and Further Information	37
A.5	Review and Updates	37
Appendix B		38
1.4	Proportionate Security	38
3	SBD Award Routes	38
5	Construction Phase Security	39

6	Layer 1 – Outer Environment	39
6.4	Hostile Vehicle Mitigation (HVM)	39
7	Layer 2 – Perimeter Security	40
7.3	Lighting	40
7.4	Operational Requirement (OR) for Electronic Security Systems	40
7.5	Video Surveillance Systems (VSS)	41
7.6	Perimeter Intrusion Detection Systems (PIDS)	41
7.8	Electronic Access Control Systems (EACS)	41
8.3	Intruder and Hold Up Alarm Systems (I&HAS)	42
8.2	Doorsets and Windows	42
8.4	Secure Storage Units	42
8.5	Photovoltaic (PV) Panels and Cabling	42
8.6	Property Marking and Tracking	43
8.8	Battery Energy Storage Systems (BESS)	43
9	Layer 4 – Operational Security	43

PART 1



1 Introduction

1.1 Purpose

This guide defines the security measures required to obtain the SBD Solar Farm Award. It establishes a risk-based process for designing out crime and sets the technical standards that must be achieved for certification.

1.2 Scope

The guidance applies to ground-mounted solar farms, including associated battery storage, substations, and control buildings. It covers security from planning through construction, to operation. It does not apply to rooftop or building-integrated photovoltaic installations.

Solar farms vary in size, purpose and location, and these differences directly influence the level of security required. Some small-scale or ancillary developments may benefit from permitted development rights, while most commercial-scale solar farms will require full planning permission. The design principles in this guide apply in both cases, with measures selected to be proportionate to the assessed risk and planning context.

This guide is intended for use across the United Kingdom. However, planning systems, terminology, consenting routes and statutory thresholds differ between England, Scotland, Wales and Northern Ireland. Users must ensure that references to planning processes, capacity thresholds and statutory consultees are interpreted in line with the planning system applicable to the site location.

1.3 Context

Solar farms have become high-value targets for organised crime, with theft and vandalism focused on photovoltaic (PV) panels, inverters, batteries and cabling.

Between January 2022 and September 2024, domestic organised crime groups (OCGs) have increasingly targeted solar farms across the UK, with a particular focus on the theft of copper cable. According to the National Crime Agency, domestic organised crime groups continue to target solar farms, primarily for earthing cable, which accounted for 43% of all solar farm thefts between January 2022 and September 2024.¹ The primary motivation for offenders is believed to be the scrap metal value of copper and other conductive materials used in these cables.

The financial impact of these thefts has been significant, with an estimated £7.1 million in total losses recorded across the sector. Importantly, these figures only account for direct losses (replacement costs and stolen materials). The true cost is likely to be considerably higher when factoring in operational disruption, damage to infrastructure during thefts, and the costs of security upgrades or insurance premiums.

Copper cables are a prime target for criminals because they are extensive and relatively exposed on many solar farm sites. In particular, two forms are especially vulnerable: copper DC string cables and copper earthing cables. Theft of copper DC string cables can result in an immediate loss of generation and significant labour costs associated with locating faults, replacing cabling, and recommissioning the affected PV arrays. Removal of copper earthing cables, meanwhile, compromises electrical safety systems, increasing the risk of equipment damage, electrical faults, and potential fire hazards.

The pattern of thefts suggests a degree of planning and organisation. OCGs often use vehicles equipped for bulk removal, operate during low-visibility periods, and may exploit knowledge of solar farm layouts to target vulnerable sections of the site.

This ongoing threat highlights the importance of layered security strategies for solar farms, including:

- Perimeter protection (fencing, access controls, intrusion detection)
- Surveillance systems (CCTV, thermal cameras, drones for remote sites)
- Target-hardening (burying or concealing cabling, anti-theft fixings)
- Situational awareness (staff training, local intelligence sharing, law enforcement liaison)
- Community engagement (working with rural watch schemes and nearby landowners)

1. National Crime Agency – National Strategic Assessment 2025 <https://www.nationalcrimeagency.gov.uk/threats-2025/nsa-oac-2025>

1.4 Proportionate Security

While respecting ecological and planning constraints, security measures must deter, detect, and delay unauthorised activity and where applicable, enable a response, human and/or electronic, before the attacker is successful.

Given the sustained nature of the threat and the high value of solar farms as long-term national energy assets, theft prevention should be considered a critical part of operational risk management. A failure to address these vulnerabilities not only results in financial losses but also undermines the resilience of the UK's renewable energy infrastructure.

Security must correspond to assessed risk. A documented crime-risk analysis (CRA), prepared with either the DOCO, SBD Licensed Consultant, other security specialist who works on such schemes, determines whether baseline or enhanced measures are required. The analysis considers site size and type, local crime history, asset value, response capability, and any planning or environmental constraints. The format of the CRA is not prescribed, but must be documented, proportionate and capable of audit.

Not all measures in this guide are mandatory for an award. Some represent minimum requirements, while others are best practice enhancements to be adopted where proportionate. Successful SBD solutions are developed within the planning framework and aligned with relevant policies. Ecological conditions, dark sky policies, or landscape sensitivities may limit options such as lighting or fencing. In such cases alternative measures must be explored with DOCO support.

Use of language within this guide

Must – mandatory requirement for SBD compliance.

Should – strong recommendation representing recognised best practice; departures require written agreement from the DOCO.

May – optional or context- dependent measure that can be applied where proportionate to risk.

The use of *must*, *should* and *may* reflects the security outcome required, not a presumption that every physical measure will be feasible on every site. There may be legitimate constraints that prevent the implementation of a specific measure, including but not limited to planning conditions, ecological restrictions, heritage considerations, land ownership, constructability, operational safety or disproportionate cost.

Where a *must* requirement cannot be delivered as described, this does not automatically preclude SBD certification. In such cases, the requirement must be addressed through the crime-risk analysis process, with alternative or compensatory measures agreed and documented with the DOCO to achieve an equivalent level of protection.

A consolidated summary of *must*, *should* and *may* requirements in this guide is provided in **Appendix B**.

Standards referenced in this guide

References to standards (BS, PAS, LPS, STS, Sold Secure, etc.) relate to the current published editions unless otherwise stated.

Early engagement with the DOCO, ideally before a planning application is submitted, helps ensure that the security strategy is proportionate, achievable, and compliant, and that it does not conflict with planning or environmental requirements advocated within the Security Overlay to the RIBA Plan of Work (see [2.3](#)).

1.5 Counter-Terrorism Co-ordination

Where terrorism, sabotage, or state-level threat is identified, the DOCO will act as the liaison with a Counter Terrorism Security Advisor (CTSA). The CTSA is responsible for assessing the terrorism-related threat and specifying any Hostile Vehicle Mitigation or other CT measures. The DOCO will not advise on, design, or sign off CT-related measures, but will help ensure that CTSA advice is understood and integrated with the wider site-security design and SBD requirements.

1.6 Data Protection and Privacy

Security systems that capture or process personal data must comply with UK data-protection law. Operators must follow Information Commissioner's Office (ICO) guidance on Closed Circuit Television (CCTV) and Video Surveillance Systems (VSS), Automatic Number Plate Recognition (ANPR), and audio recording, including lawful basis, transparency, retention, subject-access, and signage requirements. ICO resources. Further information is available at: <https://ico.org.uk/for-organisations>

Note: VSS is the broader, modern term for video surveillance; CCTV is the legacy term for analogue closed-circuit systems. Digital VSS now covers advanced technologies beyond traditional cameras, such as AI, drones, body-worn video, and ANPR. For the purposes of this guide, we will use the term VSS.

1.7 Sustainability and Carbon Considerations

Security-led design should also minimise whole-life carbon. Preventing crime reduces repeat manufacture, replacement, site visits, waste, and grid interruption. Where options offer equal security, the lower-carbon solution should be the preferred solution.

2 Designing Out Crime Process

2.1 Purpose

By embedding security from the concept stage, designing out crime delivers effective, cost-efficient mitigation.

2.2 Planning Context

Planning and consenting routes for solar farm developments vary across the UK due to differences in devolved planning systems. Capacity thresholds generally determine which authority is responsible for determining an application.

In England, solar farm developments are determined by capacity. Schemes below 100 MW are determined by the local planning authority. Schemes of 100 MW or greater are classified as Nationally Significant Infrastructure Projects (NSIPs) and require consent through a Development Consent Order (DCO).

In Wales, energy generation projects between 10 MW and 350 MW are generally classified as Developments of National Significance (DNS) and are determined on behalf of the Welsh Ministers. Schemes above 350 MW are treated as Nationally Significant Infrastructure Projects (NSIPs) and require a Development Consent Order (DCO).

In Scotland, solar farm developments up to and including 50 MW are typically determined by the local planning authority. Schemes above 50 MW are determined by Scottish Ministers through the national energy consent process.

In Northern Ireland, schemes below 30 MW are generally determined by the local planning authority (district council). Schemes of 30 MW or greater are classified as regionally significant developments and are determined by the Department for Infrastructure.

Planning policy and thresholds may evolve over time. Applicants should confirm the applicable consenting route with the relevant authority during early project development.

Security requirements for large-scale solar developments should be addressed early in the design process and clearly set out within planning documentation where required.

2.3 Security Overlay to the Royal Institute of British Architects (RIBA) Plan of Work

The National Protective Security Authority (NPSA) in collaboration with the RIBA and Police CPI, have created the Security Overlay to the RIBA Plan of Work which is for everyone involved in the safe and secure design, construction, and operation of any building. This process will support better long-term security outcomes for everyone involved in the lifecycle of a building. The following link provides access to the document: <https://www.riba.org/work/insights-and-resources/security-overlay-to-riba-plan-of-work>

2.4 Planning Policy and Design Quality

Security is a design quality and must be integrated from the earliest stages, not added later. Embedding security within the site layout, access strategy, and landscape design supports planning approval, community acceptance, operational resilience, and investor confidence.

Crime is a material planning consideration. Solar farm proposals must therefore demonstrate that security and planning requirements have been addressed together, rather than competing with one another. Schemes that follow SBD principles typically show lower rates of crime and reduced disruption throughout the life of the development.

Proposals that successfully accord with SBD will be supported by Design and Access Statements and Planning Statements that consistently demonstrate how planning compliance, heritage requirements, ecology constraints, landscape objectives, and effective security have been achieved simultaneously.

Where designated or non-designated heritage assets fall within the red line boundary, early engagement with the Local Planning Authority's conservation and archaeology officers is essential, and Historic England must be consulted where relevant. A proportionate Heritage Impact Assessment is required. Where heritage constraints limit standard physical measures, the most robust certified alternatives must be used, supported by enhanced electronic monitoring and management.

All security measures described in this guide are subject to the outcome of the relevant planning or Development Consent Order (DCO) process. Where a planning authority, Examining Authority or Secretary of State requires amendments that affect agreed security measures, the security strategy must be reviewed and, where necessary, revised in consultation with the DCO.

SBD certification is based on the security solution that is ultimately consented and delivered. Where originally proposed measures are not approved through the planning process, alternative or compensatory measures must be identified to maintain proportionate protection consistent with the assessed risk.

2.5 Example Planning Condition

"The solar farm hereby approved shall be carried out in accordance with the physical security standards set out in the latest version of the Secured by Design (SBD) Solar Farm Guide. A Security Design Statement, prepared in consultation with a police Designing Out Crime Officer, shall be submitted to and approved in writing by the Local Planning Authority prior to first operation of the solar farm. The approved security measures shall be implemented prior to the first operation of the solar farm and thereafter retained and maintained for the lifetime of the development."

2.6 Design and Access Statements (DAS)

DAS form part of the public planning record. Although solar farms are not always formally classed as Critical National Infrastructure, they contribute to national energy security, and it may not be appropriate for detailed security information to enter the public domain.

Where necessary, Local Planning Authorities may accept a redacted DAS or a two-part submission. A public-facing DAS will address design, layout, access, and landscape principles, while a separate confidential security annex will contain sensitive detail that is withheld from publication. This approach ensures planning transparency while protecting information that could compromise site security.

2.7 Role of the Designing Out Crime Officer (DOCO)

The DOCO provides professional advice on crime prevention through environmental design and protective security. They will:

- Review design using a documented crime-risk analysis
- Advise on proportionate measures and relevant standards
- Confirm compliance for the SBD Solar Farm Award

Where risk includes terrorism or sabotage, the DOCO must liaise with a CTSA.

2.8 Crime-Risk Analysis (CRA)

The CRA should be completed by someone with appropriate expertise in crime prevention and security design, typically:

- A DOCO, or
- A security professional experienced in site risk assessment and protective security measures, ideally in consultation with the design team and client

In practice, the best approach is collaborative: the DOCO or security specialist leads the assessment, while designers, planners, and site managers contribute contextual and operational information. The format of the CRA is not prescribed, but must be documented, proportionate and capable of audit.

The analysis must:

- Identify credible threats and crime types
- Evaluate vulnerabilities and potential impacts
- Consider response capability and environmental constraints
- Agreed measures, including compensatory provisions, must be recorded

Local community tensions, including protest, trespass, damage and sabotage, must also form part of the CRA. Large-scale solar developments can attract organised opposition and increased public interest, even where most activity remains lawful. The security strategy must therefore consider the potential for disruption from protest groups, activists and opportunistic offenders, and reflect any elevated risk in the design of perimeter treatments, access control, surveillance and management procedures.

2.9 Integration with Other Disciplines

Security design must align with planning, environmental, safety, and operational objectives. Early co-ordination prevents conflict and ensures balanced outcomes.

2.10 Documentation

Developers must retain evidence that security has been addressed, including:

- DOCO consultation notes
- The crime-risk analysis
- Drawings and specifications identifying security features
- Confirmation of compensatory measures

These documents support both planning submissions and later SBD verification.

3 SBD Award Routes

3.1 Overview

The SBD Solar Farm Award confirms that a site meets police-approved security standards proportionate to

its assessed risk. It provides assurance to developers, operators, and insurers that protective measures have been verified by a qualified DOCO.

Two routes to SBD accreditation are available:

1. SBD Solar Farm Award (Traditional Route)

For new developments. The developer engages the DOCO at pre-planning, a crime-risk analysis is completed, proportionate measures are agreed, and compliance is checked during construction and at completion. Certification is issued after final verification.

2. SBD Vulnerability Survey Route

For existing or operational sites where full design-stage compliance is not feasible. The DOCO undertakes a risk-based survey of the as-built site and issues a written report identifying required measures and any recommended enhancements. The developer must confirm an implementation plan and timescales. Certification is issued only after the DOCO verifies completion of the required measures. This route also leads to an SBD Solar Farm Award.

Important: The SBD Vulnerability Survey is a risk-based audit. The DOCO's role is advisory and independent. The SBD Solar Farm Award is only issued when the DOCO verifies that the recommended security measures have been implemented.

Continued compliance depends on maintaining all approved measures. Re-inspection may be required if significant operational changes occur.

3.2 SBD Solar Farm Award (New Developments)

Stage 1 – Early Engagement

Developers should consult the DOCO at pre-planning stage to identify risks and integrate proportionate security measures into the design.

Stage 2 – Design Review and Agreement

A review based on the crime-risk analysis confirms security measures required for certification.

Stage 3 – Planning and Construction

Security requirements are incorporated in planning submissions and the Construction Management Plan. The DOCO will visit the site to verify implementation.

Stage 4 – Post-Completion Verification

When all agreed measures are in place, the DOCO conducts a final inspection. If compliance is confirmed, an SBD Solar Farm Award is issued.

3.3 SBD Vulnerability Survey (Existing Sites)

This applies to operational or retrofit sites where design-stage engagement was not possible.

Stage 1 – Site Assessment

The DOCO undertakes a SBD Vulnerability Survey assessing layout, boundary security, surveillance coverage, and management controls.

Stage 2 – Recommendations

A written report outlines required improvements and optional enhancements. The operator must confirm in writing how each will be addressed.

Stage 3 – Verification and Award

Once agreed actions are completed and verified, the DOCO issues the SBD Solar Farm Award. Failure to implement required actions will delay or prevent certification.

3.4 Nationally Significant Infrastructure Projects (NSIPs) and the Development Consent Order (DCO) Process

Large solar farms that qualify as NSIPs require a DCO under the Planning Act 2008. Security must be addressed at pre-application stage, as changes become more difficult once the DCO process is underway.

Applicants should consult the DOCO during pre-application so that SBD requirements are built into the scheme submitted to the Planning Inspectorate. Security measures should be reflected consistently across the planning application documents and the Security Management Plan. If post-consent design changes affect security, the applicant must re-engage the DOCO to confirm continued SBD compliance.

Where the DCO process results in changes to layout, access or landscape proposals that affect security, continued SBD compliance will require re-engagement with the DOCO to confirm that equivalent protection is maintained.

Fire considerations

Fire safety within NSIP/DCO schemes is dealt with under separate fire-safety legislation and guidance. The DOCO does not assess or approve fire engineering. Applicants must consult the Fire and Rescue Service and competent fire engineers on access, water supplies, Battery Energy Storage Systems (BESS) fire strategy, and related issues.

Where fire requirements influence security features, such as emergency access points or separation distances, the DOCO will advise only on the crime-prevention implications of those features. Responsibility for fire safety remains with the appropriate fire authorities and fire professionals.

3.5 How to apply for an SBD Solar Farm Award

Applicants should make themselves familiar with the relevant parts of this guide and are strongly advised to consult the DOCO for site specific information at the earliest opportunity, ideally at the pre-planning stage, and submit an SBD Solar Farm Award application as part of the process. Doing so will ensure that SBD measures are effective, proportionate and visually appropriate to the landscape.

The development will be measured against the requirements of the SBD Solar Farm Award scheme current at the time the application was made. Developments that have not started construction on site within 3 years of the original SBD application will be subject to a new application, including developments where only a phase of construction begins more than 3 years from the original application date.

Developers wishing to apply for Secured by Design approval should contact their local Designing Out Crime Officer at: <https://www.securedbydesign.com/contact-us>

4 Proportionate Security and Zoning

4.1 Principle

Protective security must be proportionate to assessed risk. Not all solar farms require the same degree of protection. Security design should be informed by a crime-risk analysis prepared in consultation with the DOCO and reviewed throughout the project lifecycle.

4.2 Site Risk Classification

Risk classification should consider:

- Location and accessibility
- Crime history and local policing intelligence
- Asset value and operational criticality
- Response capability and site supervision

The outcome determines whether the site requires Baseline or Enhanced protective measures.

Baseline Security

The minimum level of protective measures required for all solar farms to achieve Secured by Design certification. Baseline security addresses common, predictable risks such as theft, vandalism, and unauthorised access. It establishes a consistent standard of deterrence, delay, and detection suitable for typical rural or semi-rural sites with low to moderate crime risk.

Enhanced Security

A higher level of protective measures applied where the crime-risk analysis identifies elevated or site-specific threats, such as repeated offences, proximity to populated areas, protest activity, or critical infrastructure designation. Enhanced security builds upon the baseline by increasing the strength, certification level, or extent of protective measures to achieve a greater level of resistance and resilience.

4.3 Layered Approach

Solar farms should be divided into functional layers so that resources are directed effectively:

- **Layer 1 – Outer Environment:** approach routes, parking areas, signage, and vehicle mitigation.
- **Layer 2 – Perimeter Security:** boundary fencing, gates, lighting, surveillance, and access control.
- **Layer 3 – Internal Compounds and Building Security:** compounds, PV equipment, cable drums and string cabling, storage, and fire protection.
- **Layer 4 – Operational Security:** management, maintenance, connected systems, and incident response.

Each layer strengthens the previous one, creating integrated defence in depth. Measures appearing in multiple layers are described once and cross-referenced elsewhere.

4.4 Compensatory Measures

Where planning, ecological, or heritage restrictions prevent standard features (for example, certified fencing or lighting), compensatory measures must be agreed with the DOCO. These may include:

- Enhanced surveillance or intrusion detection
- Reinforced access controls
- Defensive planting or landscaping
- Increased inspection or response procedures

Compensatory measures must provide an equivalent level of protection to the standard requirement. Defensive planting may form part of such design, provided it avoids concealment or fire risk and can be maintained within the site's management plan.

4.5 Alignment with Safety Legislation

Security measures must complement statutory obligations under:

- Electricity at Work Regulations 1989
- Health and Safety at Work Act 1974
- Management of Health and Safety at Work Regulations 1999
- Network and Information Systems Regulations 2018

4.6 Review and Adjustment

Security performance should be reviewed after incidents or operational changes. Adjustments to agreed security levels must be documented and approved by the DOCO.

PART 2



5 Construction Phase Security

Solar farms are particularly vulnerable during construction because high-value equipment, cabling, materials, fuel, and temporary security systems are present before permanent measures are complete. Security must be planned from the outset and maintained until commissioning.

Deliveries and storage

Manage deliveries so that items are not left on site longer than necessary.

- Where storage is unavoidable, keep equipment in lockable containers within secure compounds that meet the fencing standards in 7.2, with lighting in 7.3 and VSS in 7.5
- Cable drums and string cabling held in coils or bulk must be stored inside secure compounds with lighting and VSS. Deliveries should be timed as close as practicable to installation. Maintain forensic marking and accurate inventory records

Temporary protective measures

Provide monitored VSS, a monitored intruder alarm, secure perimeter fencing, controlled access points, and suitable lighting. Where lighting is restricted by ecology or planning, use motion-activated or centrally operated lighting and compensatory measures as set out in 7.3.

Mobile VSS towers may be deployed to achieve full temporary coverage.

Display clear security signage with emergency contact details, in accordance with 6.6 and ICO requirements in 1.6.

Guarding

Consider on-site security guards during storage of high-value assets, critical installation stages, or periods of increased local risk. Guarding must follow 9.2.

Consultation

The Construction Management Plan and associated security measures should be prepared following consultation with the DOCO.

Where boundaries adjoin railways or tube lines, consult the British Transport Police DOCO.

Further advice on construction site security is available from Secured by Design:

https://www.securedbydesign.com/images/CONSTRUCTION_SITE_SECURITY_GUIDE_A4_8pp.pdf

6 Layer 1 – Outer Environment

6.1 Principle

The outer environment defines the relationship between the site and its surroundings. Design at this layer should reduce unauthorised approach, support natural surveillance, and clarify the distinction between public and private land.

Where site scale, landscape character, or planning conditions permit, a defined outer boundary such as fencing or dense, defensive planting may be used to reinforce territorial definition and control access.

Planting must be selected and maintained so that it does not create concealment or fire risk.

6.2 Vehicle Parking and Access

Entrances must be limited to the minimum necessary for safe operation.

Where visitor or contractor parking is provided, it should normally be located within the secure perimeter, recognising that access will be required in any event. Where this is not practicable, parking outside the perimeter must be supported by proportionate surveillance and management controls.

Access routes must allow safe operation of authorised vehicles and prevent accidental encroachment on restricted areas.

Where grazing or land management continues within the solar farm, regular presence of authorised persons provides a guardianship benefit. Those visitors must receive basic training on security awareness, access control, and incident reporting. These duties must be detailed in the Security Management Plan (see 9.3).

6.3 Public Rights of Way (PROWs)

PROWs, including public footpaths and bridleways, near or across a solar farm must be considered from the outset. Routes must remain open and unobstructed, but measures may be needed to prevent unauthorised access into the site. Where PROWs run close to the perimeter, use clear signage, suitable boundary treatments, and, where necessary, additional detection such as Perimeter Intrusion Detection Systems (PIDS) or VSS coverage. Existing landscape features can help provide natural separation. Any changes affecting PROWs must be agreed with the local authority, and the DOCO should be consulted early so that security and public access are balanced appropriately.

6.4 Hostile Vehicle Mitigation (HVM)

CTSAs are responsible for advising on HVM where a counter-terrorism risk has been identified. Where HVM is required to prevent unlawful vehicle access or vehicle-related sabotage in a crime-prevention context, the DOCO will advise. The DOCO will not sign off or approve any counter-terrorism related measures, which remain the responsibility of the CTSA.

Vehicle access points must be designed to resist deliberate ramming or unauthorised entry.

Typical measures include:

- Layout that prevents direct approach to vulnerable equipment
- Natural barriers such as earth bunds, ditches, watercourses, sunken barriers (ha-ha walls), and/or dense defensive planting

Vehicle security barriers certified to one of the following standards:

- ISO 22343-1 (*Note 6.4*), or
- PAS 170-1

These are recognised international and national standards for vehicle security barriers. They set out how barriers must be tested, including the size and speed of impacting vehicles, the measurement of penetration distance and the performance required to stop or slow an attacking vehicle. Products certified to these standards provide assurance that they have been independently tested and can deliver reliable protection when correctly selected and installed.

Ha-ha walls are suitable where permanent vehicle exclusion is required with low visual impact. They must be designed to local ground conditions and maintained to prevent informal crossing points. Existing landscape features such as banks, ditches, and mature planting should be used where possible to support these measures and reduce additional construction. Early engagement with the DOCO, landscape architect, and planning authority is essential when developing landscape proposals that form part of the security strategy.

Where open farmland or buffer land enables vehicle approach, concrete poacher blocks may be used to prevent non-agricultural vehicle access while allowing tractors or authorised maintenance traffic. Blocks must be anchored securely, spaced appropriately, marked for night visibility, and positioned in consultation with the landowner and the landscape designer so that they integrate with existing features and agreed landscape proposals.

Note 6.4: ISO 22343-2 provides guidance on the appropriate selection, installation and use of such bollards and should be referenced in the first instance.

6.5 Exclusion Zones and Buffer Land

Biodiversity buffers and farm margins outside the fence can enable vehicle movement or offender reconnaissance. VSS design should assume potential approach within these strips, with overlapping perimeter views, analytics along likely tracks, and attention to out-of-sight corners.

Engage landowners early to understand historic access routes and agree proportionate controls that retain their cooperation.

6.6 Security Signage

Signage must clearly state that the site is private property under surveillance and that unauthorised access is prohibited.

Signs should be placed at all entrances and regular intervals along boundaries to create psychological deterrence.

Signage must comply with UK data protection law and ICO guidance, including stating that monitoring is in use, the purpose of monitoring, and contact details for the data controller (see 1.6).

6.7 Lighting (Outer Environment)

Lighting at approach roads and parking areas must comply with BS 5489-1.

Illumination must not spill beyond the site boundary or conflict with ecological or planning conditions.

Where lighting is restricted or prohibited, compensatory measures such as infrared VSS or PIDS should be used.

For full lighting requirements, see 7.3.

7 Layer 2 – Perimeter Security

7.1 Principle

The perimeter forms the first physical line of defence. It should clearly define the site boundary, restrict unauthorised access, and enable detection and delay of intrusion.

Where constraints or local policy prevent standard physical measures, compensatory electronic or procedural systems must provide equivalent protection (see 4.4).

7.2 Boundary Treatments

Where feasible, perimeter fencing should be at least 2.0 metres high and be certified to one of the following minimum standards, or above:

- LPS 1175 Issue 8 Security Rating B3
- STS 202 Issue 12 BR2
- Sold Secure SS323 Silver
- LPS 1673 Issue 1 AR.B180

These are recognised security standards for fencing, gates and enclosure systems. They set the test and performance requirements for resistance to forced entry using a range of tools and attack methods within defined time periods. Products certified to these standards have been independently tested and provide assurance that the fence line can deliver reliable delay and intrusion resistance when correctly specified and installed.

Where planning, ecological, or financial constraints prevent installation of certified fencing across the full perimeter, particularly on large rural sites, alternative solutions must be agreed with the DOCO. Acceptable alternatives may include:

- Partial certified fencing around compounds or critical assets
- Deer or livestock fencing to define site ownership and manage livestock or vehicle movement, with compensatory measures such as VSS, PIDS, audio challenge and clear security signage, as this type of fencing is not security certified
- Dense, defensive planting combined with natural or engineered barriers such as earth bunds, ditches, watercourses and/or sunken barriers (ha-ha walls)
- Compensatory detection measures such as VSS, PIDS and Audio Challenge Systems provide an equivalent overall level of protection

Fencing, barriers and defensive planting must be not obstruct drainage infrastructure or routine maintenance. Where defensive planting forms part of the perimeter, suitable gated access points must be provided to enable authorised emergency and operational access.

Where lighting or fencing is prohibited by planning or ecological restrictions, alternative deterrence and detection systems must be agreed with the DOCO to maintain equivalent protection.

Buffer zone

A clear buffer zone should be maintained between the perimeter fence and the PV panel array so that cable and/or panels must be moved a meaningful distance before removal from the site, reducing the risk of theft.

This buffer zone also facilitates maintenance access, can act as a firebreak, and improves visibility for Video Surveillance Systems (VSS), assisting in the detection of intruders.

Where practicable, the buffer zone should align with the minimum access width required for fire responders, typically 4.5–5 metres, unless alternative arrangements are agreed with the Fire and Rescue Service and the DOCO.

Gates

Where certified security fencing is provided, gates must offer equivalent resistance to the adjoining fence line. Even where planning, ecological or financial constraints prevent the use of certified security fencing, the primary vehicle and pedestrian gates must still be certified to one of the following minimum standards, or above:

- LPS 1175 Issue 8 Security Rating B3
- STS 202 Issue 12 BR2
- Sold Secure SS323 Silver
- LPS 1673 Issue 1 AR.B180
- Gates must be secured using robust locking systems suitable for the gate type and intended environment. Where padlocks are used, they should be certified to one of the following minimum standards, or above:
 - BS EN 12320:2012 Grade 5 (*Note 7.2*)
 - LPS 1654 Issue 1 Security Rating 3 (*Note 7.2*)
 - Sold Secure SS303 Diamond (*Note 7.2*).

‘Tayhope’-style multi-user latches may be used where multiple authorised parties require access, and all padlocks, including those used with ‘Tayhope’-style latches, must be protected by welded or bolted shrouds to prevent cutting or levering. Padlock housings, hasps and fittings must be designed to resist tampering and environmental degradation. Where a gate has been certificated to a recognised security standard, any locking system, padlock or associated hardware fitted to the gate must be compatible with the certified design and must not compromise the gate’s ability to achieve the security performance to which it has been tested and certified.

Gate hardware such as shrouds, hinges, ground bolts and associated fittings must provide resistance equivalent to the adjoining fence line and prevent lift-off, levering or forced opening. The adjoining fence should also provide resistance equivalent to the gate to avoid creating a weaker attack point adjacent to emergency escape hardware.

For short-term or heightened-risk periods, temporary internal obstacles (for example removable blocks or weighted barriers) may be used on the secure side to provide additional delay. Any temporary measure must not impede emergency access or site operations.

Automated gates are unlikely to be required on most solar farms, but if they are installed an emergency release must be provided for fire and safety purposes. The release must be positioned on the secure side of the boundary and designed so that it cannot be reached, tampered with or operated through any gap in the gate or fence. The device must be shielded or recessed to prevent manipulation from the public side.

Where emergency exits or secondary escape routes are required, their design must follow relevant health and safety legislation and electrical industry safety policies, ensuring that emergency egress does not compromise perimeter security.

Gates must be designed to prevent collapse in the event of component failure. A gate must not fall due to the failure of a single hinge. Each gate must have at least three hinges or a suitable tether of adequate strength. Where an inverted, non-load-bearing hinge is used to prevent lift-off, two tethers must be fitted, one at the top and one at the bottom.

Controls and intercoms for automated gates must be positioned so they can be used safely without entering the gate's moving zone or being exposed to the moving leaf or track. Intercoms intended for visitors or authorised arrivals should be located on the public (non-secure) side of the entrance. Operational controls and emergency release mechanisms should be protected against unauthorised use and positioned on the secure side where appropriate. Visual and audible warning devices must operate before and throughout gate movement.

To prevent entrapment, all gaps greater than 100 mm must be eliminated wherever practicable. The under-gate gap must be less than 100 mm. Gap reduction must not exceed 20% of the original opening and must not reduce below 25 mm. The run-back zone of sliding gates must be fenced, and designs that create tapering gaps avoided.

Sliding gates must include robust end stops in both directions. Limit-switch actuators must be securely fixed, and drive racking must terminate just beyond the limit to prevent overrun if the limit fails. Long leaves must be supported by twin posts or goal-post frames so that a single roller failure cannot cause collapse.

Automated gates must comply with all relevant statutory safety standards and be either UKCA-marked or CE-marked:

- UKCA marking confirms products meet applicable UK safety, health and environmental requirements
- CE marking indicates conformity with safety, health and environmental protection standards within the EEA

Specifiers must confirm that powered gate installers are appropriately qualified, trained and follow recognised industry codes of practice.

Duty holders must maintain a written inspection and maintenance plan. Gates must be inspected at least every six months. Commissioning records, user manuals and maintenance logs must be retained. Authorised staff must be trained in safe operation and manual release, with a manual-release key safe provided where appropriate.



The following organisations provide recognised guidance and training for powered gate safety and maintenance:

- Gate-Safe: <https://www.gate-safe.org>
- Door & Hardware Federation (DHF), publisher of DHF TS 011 Code of Practice for powered gate safety. Installations to this code are subject to National Security Inspectorate inspection

Note 7.2: BS EN 12320:2012, LPS 1654 and the Sold Secure are recognised standards for padlock performance. They set test and classification requirements for resistance to forced attack, including cutting, pulling and manipulation, and for durability in outdoor conditions. Padlocks certified to these levels provide assurance that they have been independently tested and offer a robust level of security when correctly selected and fitted.

7.3 Lighting

Lighting plays a key role in site security by improving visibility and supporting surveillance.

On rural solar farm sites, motion-activated lighting is often unsuitable due to frequent activation by wildlife and livestock. In addition, poorly timed lighting can inadvertently assist offenders during the interval between alarm activation and response. Lighting that is switched on when required, under monitored control, is generally more appropriate.

In some locations, lighting may be restricted or prohibited for ecological or heritage reasons. In such cases, compensatory measures such as infrared or thermal VSS, PIDS, and/or Audio Challenge Systems will be required to provide an equivalent level of detection and response. On some sites, planning and ecological constraints mean that only motion-activated lighting under central monitoring and control will be acceptable.

Where lighting is permitted, it must be designed in accordance with BS EN 12464-2 (*Note 7.3a*) for outdoor workplaces and, where it is used on access roads or vehicle routes, BS 5489-1 (*Note 7.3b*).

Key design requirements include:

- Columns and fittings should resist tampering and be positioned to minimise glare or spill beyond the boundary
- Lighting may be concentrated on the most vulnerable areas, for example control buildings, battery storage compounds, gates, and storage yards, rather than providing uniform illumination across the entire site
- Layout must be co-ordinated with VSS so that cameras benefit from the lighting and are not compromised by glare or shadow

To demonstrate compliance, the DOCO must be provided with written confirmation from a competent lighting design professional. Additionally, a Construction (Design and Management) Regulations (CDM) risk assessment must be completed.

To be deemed competent to design under CDM regulations, the lighting design professional must:

- Provide written evidence that they are either IEng or CEng qualified, and that they are either a Member or Fellow of the Institution of Lighting Professionals (MILP or FILP), a Member or Fellow of the Society of Light and Lighting (MSLL or FSLL), or a full member of the International Association of Lighting Designers
- Have lighting design experience within the field they are delivering
- Anyone who is not qualified to that level with that specific experience should have their designs checked and signed off by someone within their organisation who is of the required level and whose qualifications and experience are supplied with the submission. A design from a lighting manufacturer will not be acceptable as they do not supply CDM compliance and the required risk assessments

Note 7.3a: BS EN 12464-2 sets the requirements for illuminance, uniformity, glare control, and colour rendition needed for safe operation in external work areas.

Note 7.3b: BS 5489-1 covers the design of road and amenity lighting. Together these standards ensure that lighting supports safe working conditions while also improving visibility, surveillance performance, and identification across the site.

7.4 Operational Requirement (OR) for Electronic Security Systems

All electronic security systems within this guide, including VSS, PIDS, Audio Challenge, Automated Access Control, and the Intruder and Hold-Up Alarm must be designed in accordance with a documented Operational Requirement (OR).

The OR must be developed with the DOCO and the site operator and must define what the system needs to detect, monitor, identify, or report, the environmental or planning constraints that apply, and the response actions required by the Alarm Receiving Centre (ARC). All system designs must align with the OR so that detection, verification, and response procedures work together as a unified security strategy.

7.5 Video Surveillance Systems (VSS)

VSS forms part of the wider electronic security system by providing continuous visual monitoring and enabling verification of alarms generated by PIDS, access control systems, and other security measures.

VSS must comply with BS EN 62676 (*Note 7.5*).

Where VSS is used as a remotely monitored detector-activated system, including systems incorporating Audio Challenge and ARC response, it should also comply with BS 8418 – Remotely monitored detector-activated CCTV systems.

Pending formal amendment of BS 8418:2021, systems installed from 1 April 2026 should align with the provisions of Industry Agreement IA 2401:2026, which provides an interim update intended for future incorporation into BS 8418.

Systems must be installed and maintained by a company certificated by the NSI or the SSAIB under a United Kingdom Accreditation Service (UKAS)-accredited VSS scheme. Further information is available at:

<https://www.nsi.org.uk>

<https://www.ssaib.org>

Key design requirements include:

- Cameras must be positioned to cover likely approach routes, including across adjoining farmland, along the fence line and at known or potential breach points
- Perimeter coverage should provide continuous observation of the fence line with no significant gaps, supplemented by internal cameras where required to track movement within the site
- VSS design must consider buffer strips and biodiversity margins outside the fence, as these can enable reconnaissance or unauthorised approach. Camera placement must maintain continuous coverage of approach routes, corners, and out-of-sight areas
- Cameras and housings must resist tampering and environmental degradation
- Recorded images must be retained for a period agreed with the DOCO and the site operator, normally not less than 31 days

All VSS must be monitored. The security strategy must identify the monitoring station, the response arrangement following activation, and the location from which that response is deployed.

A block plan should be provided showing camera locations, fields of view, arcs of coverage, and whether cameras are static or Pan-Tilt-Zoom (PTZ).

Advances in AI-enabled security systems continue to improve the performance of VSS and related measures. Modern analytics can support reliable detection of intruders, vehicles, and unusual behaviour while reducing false alarms caused by wildlife or weather. AI-assisted tracking, automatic threat classification, and intelligent event filtering can help operators and ARC respond more effectively.

These technologies must enhance, not replace, certified physical security measures, and any AI-enabled VSS must comply with UK data protection law and ICO CCTV guidance, including a clear lawful basis, proportionate coverage, appropriate retention periods, subject-access arrangements, transparency, and appropriate human oversight. (see 1.6).

Note 7.5: BS EN 62676 is the British and European Standard for video surveillance systems. It sets the requirements for design, installation and maintenance so that VSS delivers reliable image quality, appropriate detection and identification levels, and consistent performance in a range of environmental and operational conditions.

7.6 Perimeter Intrusion Detection Systems (PIDS)

PIDS forms part of the wider Intruder and Hold-Up Alarm System (I&HAS) by providing real-time detection at the boundary and passing alarms to the system control and monitoring equipment.

PIDS must comply with BS EN 50131-1 (*Note 7.6a*) and PD CLC/TS 50661-1 (*Note 7.6b*).

Systems must be installed and maintained by a company certificated by the NSI or the SSAIB under a UKAS-accredited PIDS scheme.

Key design and integration requirements include:

- Sensors must be positioned or buried so they cannot be bypassed or damaged without activation, and system design must reflect local environmental conditions such as wildlife movement, vegetation growth, and weather exposure
- All alarms must integrate with VSS to support visual verification at the Alarm Receiving Centre (ARC)
- PIDS must integrate with the I&HAS so that detections are logged, alarmed and managed in a co-ordinated way
- For larger installations, zonal mapping should be used so that breaches are accurately located and responders can be directed to the correct area

Where fencing is not possible on large, remote, or ecologically sensitive sites, alternative detection technologies must be deployed to provide equivalent protection. Options include buried sensors, thermal imaging, virtual tripwires, or fibre optic vibration detection. Fibre optic sensing can be particularly effective on long perimeters because a single cable can detect climbing, cutting, footsteps, digging, or vehicle movement while identifying the location of activity to within a few metres. Fibre-based systems are passive, resistant to environmental interference, and suited to sites where traditional fencing is impractical.

PIDS technologies may also include microphonic or accelerometer cable sensors, taut-wire systems, infrared or microwave detectors, or video analytics configured with perimeter rules. All of these systems must be fully integrated with VSS so that alarms can be verified remotely, preventing false alarms from overwhelming operators.

Modern PIDS may incorporate AI-assisted filtering to reduce false alarms caused by wildlife or weather. Where used, these functions must complement certified performance and comply with UK data protection requirements.

Innovative sensing technologies may include resident or deployable sentry drones for alarm verification and live audio challenge. Any deployment must comply with Civil Aviation Authority regulations and use geofenced flight paths, line-of-sight patrols, and secure data handling consistent with ICO guidance (see [1.6](#)).

Note 7.6a: BS EN 50131-1 is the British and European Standard for I&HAS. It sets the general requirements for grading, design, installation, signalling and maintenance so that detection performance, signalling integrity and alarm verification are reliable under expected operating conditions.

Note 7.6b: PD CLC/TS 50661-1 is the British and European technical specification for external perimeter security systems. It sets the system and performance requirements for perimeter intrusion detection systems so that intrusion detection, signalling and alarm management are reliable under expected operating conditions.

7.7 Audio Challenge Systems

There is no dedicated British Standard for security audio challenge systems. Equipment must therefore be selected and installed in line with industry best practice, manufacturer performance specifications, and the integration requirements of the wider security system. Loudspeakers must be suitable for outdoor installation, provide consistent audio clarity across the monitored area, and be mounted to resist tampering.

Audio challenge provides an immediate verbal warning to intruders detected by PIDS or VSS. Systems must integrate with VSS for event-based activation and deliver clear, intelligible messages that are audible throughout the monitored zone. They must operate without causing nuisance to nearby receptors and support remote activation by the Alarm Receiving Centre (ARC) or on-site guards.

Key design and integration requirements include:

- Integration with VSS analytics so that audio challenge is triggered by verified events rather than continuous operation
- Loudspeakers positioned and configured to achieve intelligible sound across the monitored area without causing nuisance to neighbours or distraction to road users
- Support for remote activation and acknowledgement by the ARC and, where present, on-site guards

Event-based deterrence systems combining high-visibility strobe beacons with authoritative voice warnings can strengthen deterrence when configured to mirror emergency-service cues. These must integrate with VSS analytics for alarm-based activation, avoid distraction to road users, and include tamper detection, remote health monitoring, and audit logging. They supplement, but do not replace, certified physical and electronic security measures.

Where audio recording is enabled, operators must follow ICO guidance on audio capture, retention, and transparency (see 1.6).

7.8 Electronic Access Control Systems (EACS)

Electronic Access Control Systems (EACS) form part of the wider electronic security system by ensuring that only authorised persons or vehicles can enter the secure area and by providing auditable control over all access events.

EACS must comply with BS EN 60839-11-1 (*Note 7.8*).

Systems must be installed and maintained by a company certificated by the NSI or the SSAIB under a UKAS-accredited EACS scheme.

Key design and operational requirements include:

- Gates, turnstiles and barriers must integrate with the certified access control system
- Electronic access devices such as cards, fobs or PINs must be managed through a controlled database with individual audit trails
- Remote or automatic operation must be fail safe so that security is maintained if power or communication is lost
- Where vehicle control is required, ANPR may form part of the EACS. ANPR capture must meet BS EN 62676 performance expectations (see *Note 7.5*) and comply with ICO guidance and UK GDPR (see 1.6)

Site-controller managed access

Many solar-farm operators use a site-controller model rather than full EACS, in which technicians contact the controller on arrival. The controller then verifies the work orders, the number of entrants, the Risk Assessment and Method Statement (RAMS) and induction details before remotely disarming the site for a set period. At the end of the work, the controller confirms completion by phone and re-arms the system.

This approach must achieve the same security outcomes as EACS, including accurate audit trails, controlled disarming and verification of authorised personnel.

Multi-field sites

Whether using EACS or a site-controller process, multi-field layouts must support partitioned control so that only the active field is disarmed and all other fields remain protected. System configuration must provide clear audit logs and integrate with VSS for verification.

Note 7.8: BS EN 60839-11-1 is the British and European Standard for electronic access control systems. It sets the requirements for system components, integrity, data management and event logging so that access control systems perform reliably and record access attempts in a consistent, auditable way.

8 Layer 3 – Internal Compounds and Building Security

8.1 Principle

This layer covers compounds, buildings, and all electrical and operational infrastructure within the secure perimeter. Measures must prevent unauthorised access, detect intrusion promptly, and enable timely response. Where requirements duplicate those set out in earlier sections, refer to the relevant clause rather than repeat content.

8.2 Doorsets and Windows

Where doorsets and windows are present (including on substations, BESS enclosures, modular units and site offices), they must comply with the police preferred specification in the latest Secured by Design Non-Residential (Commercial) Guide, using third-party certified products to the stated standards and installed by competent contractors. Further information is available at: <https://www.securedbydesign.com/guidance/design-guides>

8.3 Intruder and Hold-Up Alarm Systems (I&HAS)

I&HAS form part of the wider electronic security system by providing early detection of intrusion, supporting staff safety and enabling timely response to incidents.

I&HAS must comply with BS EN 50131-1 (*Note 8.3a*), BS EN 50136 (*Note 8.3b*) and PD 6662 (*Note 8.3c*).

Systems must be installed and maintained by a company certificated by the NSI or the SSAIB under a UKAS-accredited intruder-alarm scheme.

Key design requirements include:

- Intruder alarms must protect all secure compounds as a minimum
- On larger or higher-risk sites, systems should provide wider zoned coverage so that intrusion points can be identified quickly and accurately
- Zoning must allow only the active field or compound to be disarmed, with all other areas remaining armed. Clear procedures and signage must support safe operation
- Detectors and control equipment must be positioned to reflect local risk, site layout, approach routes and likely intrusion paths
- Alarm signalling must meet the performance required for the risk level, with dual-path signalling used where increased resilience is needed
- Where staff or contractors work on site, hold-up alarm devices must be provided to support personal safety and enable rapid escalation to the ARC
- PIDS alarms must be integrated with the intruder and hold-up alarm system so that all detections are logged, signalled to the ARC and linked with VSS for visual verification
- Alarm systems must integrate with VSS more broadly to support visual verification and reduce false alarms caused by wildlife or environmental conditions
- Responder arrangements must be defined through contracted local responders with clear SLAs, short travel times and site familiarity. Responder packs must include access protocols, contact details, maps and muster points

- Systems must be subject to routine maintenance and periodic testing in line with manufacturer guidance and the site's wider security-management plan

Where an immediate police response is required, installers must comply with the NPCC policy document – Guidelines on Police Requirements & Response to Security Systems, available at: <https://www.policesecuritysystems.com/national-police-chiefs-council-security-systems-policy>.

Specifiers should also note the Secured by Design Alarm Standard, developed with the national alarm inspectorate bodies and trade organisations. While not mandatory, this standard improves system performance and increases detection rates. Further information is available at: <https://www.policesecuritysystems.com/secured-by-design-alarm-standard/sbd-technical-guide>.

Note 8.3a: BS EN 50131-1 is the British and European Standard for I&HAS. It sets the general requirements for grading, design, installation, signalling and maintenance so that detection performance, signalling integrity and alarm verification are reliable under expected operating conditions.

Note 8.3b: BS EN 50136 is the British and European Standard for alarm transmission systems. It sets the requirements for communication paths, resilience and the performance of equipment that carries alarm signals to the Alarm Receiving Centre (ARC).

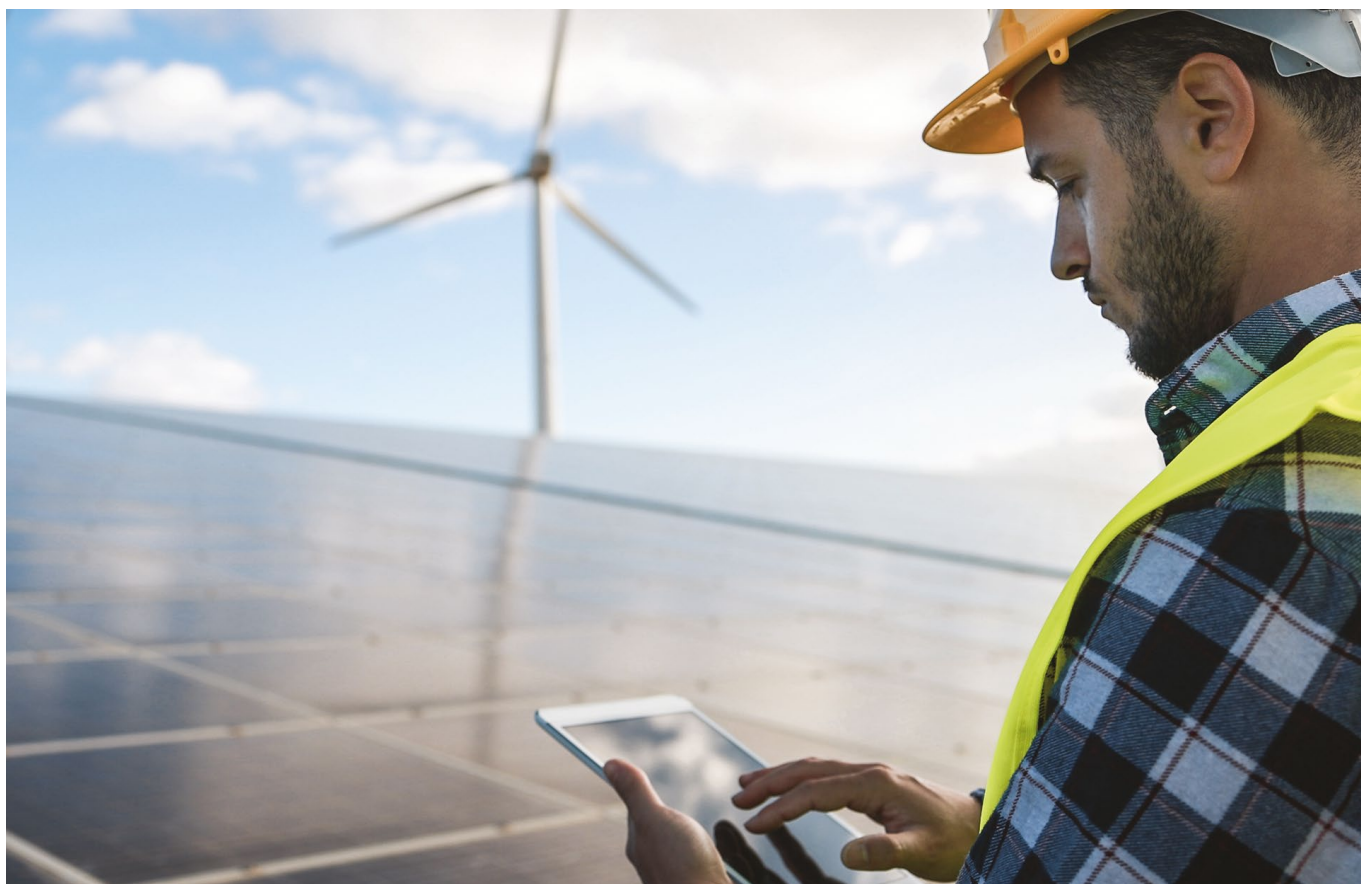
Note 8.3c: PD 6662 is the UK scheme for the application of European Standards for Intruder and Hold-Up Alarm Systems. Compliance with PD 6662 is required to obtain and maintain a Unique Reference Number (URN) for police response.

8.4 Secure Storage Units (Modular Units, Temporary Buildings and Steel Containers)

Temporary and modular storage must provide resistance to forced entry equivalent to permanent buildings on site.

Performance requirements

- Secure storage units must be certified to LPS 1175 Issue 8 Security Rating B3 or higher, or be purpose-built to provide equivalent resistance



Installation and siting

- Secure storage units should not be incorporated into the site's boundary treatment, as this could create a weaker point in the boundary and increase their vulnerability to attack from outside the site. Instead, they should be located within a secure compound that meets the requirements of Section 7.2 and be covered by lighting that meets Section 7.3 and VSS that meets Section 7.5. This ensures they benefit from the site's layered security measures, reducing the risk of unauthorised access and attack
- Units must be anchored or otherwise secured to prevent removal by vehicle or lifting equipment
- Doors should be positioned to maximise visibility from the site's VSS and minimise opportunities for concealment during unauthorised access

Operational controls

- Access must be restricted to authorised personnel, with key or code management recorded in the Security Management Plan (9.3)
- High value items should be secured to internal anchor points or secondary locked cages within the unit
- Inventory checks must be carried out regularly and any discrepancies identified during those checks must be reported

8.5 Photovoltaic (PV) Panels and Cabling

PV panel arrays, inverters and associated cabling are high-value components. Industry reporting and incident data indicate that theft on utility-scale sites most often targets exposed string cabling, with earthing conductors and other copper cabling also affected. These elements therefore require particular attention within the overall security strategy, as repeated losses can result in increased insurance premiums and higher excesses on future policies.

Tamper-resistant fixings

Tamper-resistant fixings are suitable for selected components such as frame-mounted inverters, weather stations, combiner boxes and similar equipment. They are generally not appropriate for PV module clamps.

Key design guidance includes:

- Use anti-tamper or non-standard fasteners that require specialist tooling, such as shear nuts or clutch-head screws, only where supported by the manufacturer
- Apply these measures to ancillary components, for example frame-mounted inverters, weather stations and combiner boxes, rather than to modules
- Module clamps typically require torque marking and verification and must satisfy wind-loading and certification requirements, particularly on high-wind sites, including those within approximately 100 miles of the UK's western coastline. Security fasteners are unlikely to be compatible with these requirements and many module-clamp manufacturers do not supply approved security fasteners
- Do not specify non-standard fasteners for module clamps unless explicitly approved by both the manufacturer and the design engineer

All selections must follow OEM instructions and preserve warranties and certification. Where PV panel theft risk remains, rely on surveillance and procedural controls.

Cabling and earthing

Cabling routes should, where practicable, be enclosed within protective systems and buried to reduce accessibility and accidental damage. Earthing conductors require particular attention because of their copper value and exposure at terminations.

Key design guidance includes:

- Enclose cabling routes within protective systems such as galvanised steel trunking, metal-armoured trays or concrete-encased ducts where practicable

- Bury cabling and earthing where feasible, with sufficient trench depth and backfill to deter excavation and reduce accidental damage
- Give particular attention to earthing conductors by preferring buried or concealed routes, minimising exposed vertical runs and protecting terminations within secure cabinets or kiosks
- Secure terminations, combiner boxes and entry points with tamper-resistant fixings and provide VSS coverage and, where appropriate, PIDS
- Minimise exposed runs and avoid unnecessary external joints. Use lockable cabinets or kiosks for switchgear and terminations

Layouts of cabling and earthing must be shown on Single Line Diagrams (SLDs) for use by Senior Authorised Persons (SAPs) when planning and carrying out works, in accordance with the Electricity at Work Regulations 1989.

Concealment or irregular routing must not take precedence over compliant design and accurate documentation.

String cabling

String cabling should be routed and managed to minimise theft opportunity while supporting safe operation and maintenance.

Key design guidance includes:

- Route string cabling to minimise exposed spans and unnecessary external joints, recognising that accessible string runs are the primary theft risk on many sites. Use enclosed trays or conduits where practicable along walkways, between table ends and towards combiner boxes
- Fix cables at regular intervals using robust clips or ties and remove surplus coils once commissioning is complete
- Configure monitoring so that the loss of a string or block raises an alarm to the ARC and calls a VSS preset to the affected area for verification
- Apply forensic-marking signage at key terminations and cabinets rather than along entire cable runs
- Where burial is feasible for array-to-collector routes, provide sufficient trench depth and backfill to deter excavation

SIM-Connected Devices

Many SIM-connected inverter platforms record unique device serial numbers within the monitoring system. If a stolen inverter is installed on another site, its serial number will appear in the new operator's monitoring account. Where supported, approximate location can be inferred from the monitoring platform, for example the registered site address or network information. This capability applies to utility-scale solar farms.

8.6 Property Marking and Tracking

Forensic marking or traceable identification can assist recovery and act as a deterrent when applied strategically.

- Forensic marking of every individual component is not required and should not be recommended. The deterrent value lies primarily in visible signage rather than in the volume of marked assets
- Visible deterrent signage should be implemented approximately every 50 metres along the boundary fence, on every gate, inverter, combiner box, MV skid (a pre-assembled unit containing transformer and switchgear) or standalone transformer, power tool, and on the doors of site storage containers and other building units
- Where forensic marking is applied, it must follow manufacturer recommendations to ensure durability, compatibility, and traceability
- The marking product used must be recognised by SBD. The forensic code, serial number and other relevant identification details for each item must be recorded, and the item registered on an SBD-recognised asset registration system, such as one certified to LPS 1224

- Signage must clearly indicate that forensic marking is in use, in accordance with 6.6 Security Signage, and be maintained in legible condition
- The site operator must retain secure records linking forensic codes to specific assets and locations

The marking product and signage strategy must be approved by the DOCO as part of the SBD Solar Farm Award process.

8.7 Arson and Fire Protection

Electrical and vegetation fires create safety and continuity risks.

- A site-specific Fire Risk Assessment (FRA) must be completed by a competent person to define separation, compartmentation and suppression requirements. Where this expertise is not available in-house, appoint a competent Fire Risk Assessment consultant
- Maintain vegetation and combustible materials within the separation distances specified in the FRA
- Use non-combustible fencing and materials adjacent to high-risk areas identified in the FRA
- Defensive planting must be selected and maintained so that it does not contribute to fire spread (see 4.4)

Where arson threat is assessed as elevated by the FRA, the DOCO or the Fire and Rescue Service, refer also to 9.3 for management procedures.

8.8 Battery Energy Storage Systems (BESS)

Battery Energy Storage Systems are an established part of renewable infrastructure. On solar farms, larger BESS compounds sit within the inner layers of protection and must be secured to the same standard as substations, inverters and other critical compounds. Smaller stand-alone units in residential or mixed-use areas have a different risk profile and require context-specific security and fire measures.

National fire-safety guidance for BESS continues to evolve, and operators should ensure they are working to the most current advice issued by the National Fire Chiefs' Council and the Fire and Rescue Service.

Small stand-alone BESS in residential or mixed-use areas

Compact stand-alone BESS typically occupy no more than two parking spaces and connect to the local distribution network to balance supply and demand. They are usually sited within about 50 metres of an existing substation or three-phase low-voltage cable, often close to homes or public spaces. Security, fire and access arrangements for these installations must be proportionate to their setting and agreed with the local planning authority, Fire and Rescue Service and, where appropriate, the DOCO.

Large-scale BESS within solar farms

BESS compounds within solar farms are high-value Layer 3 assets and must achieve protection equivalent to, or higher than, other internal compounds.

Enclosure and access

- Enclose BESS compounds using boundary treatments that meet the requirements in 7.2, selecting certified fencing or an agreed compensatory solution proportionate to risk
- Gates must follow the provisions in 7.2 (Gates), including equivalent certification, locking standards and safety requirements
- Maintain an inspection strip on both sides of the enclosure so that VSS, patrols and maintenance staff have clear visibility
- Where Hostile Vehicle Mitigation is justified, apply the measures in 6.4

Access points

- Doorsets, hatches and service cabinets must follow 8.2

- Windows, if present, must provide equivalent resistance
- Apply intruder and hold-up alarm coverage in line with 8.3 and integrate with VSS as set out in 7.5

Detection and monitoring

- Provide monitored VSS covering gates, access aisles and container façades
- Deploy PIDS where fencing is non-certified or approach routes create vulnerabilities (see 7.6)
- Audio challenge may be used where proportionate (see 7.7)

Fire and emergency co-ordination

- Treat arson as a specific risk (see 8.7)
- A competent Fire Risk Assessment consultant must define separation, compartmentation and suppression requirements
- Record accurate entrance and compound locations (for example GPS or What3Words) and share them with the ARC and the Fire and Rescue Service

Access control and key management

- Apply EACS in accordance with 7.8; where vehicle access is required, ANPR may be used, subject to ICO compliance (see 1.6)
- Maintain robust key and permit-to-work controls within the Security Management Plan (see 9.3)

Cabling and interfaces

- Protect cabling and control wiring in line with 8.5, using underground routing where feasible and minimising exposed runs

Sustainability and privacy

- Select solutions consistent with the carbon considerations in 1.7
- Ensure any recording, telemetry or monitoring complies with ICO requirements (see 1.6)

9 Layer 4 – Operational Security

9.1 Principle

Operational security ensures that physical and electronic measures remain effective throughout the solar farm's life. Procedures must sustain performance, define responsibilities, and enable timely response to incidents. Where previous layers rely on management or technological controls, they must be supported here through documented systems and contracts.

9.2 On-Site Guarding

On-site guarding provides a visible deterrent and an immediate response capability. Deployment must be risk-based and may be permanent or used temporarily during heightened threat periods, construction, or when power, alarms or other systems are offline.

Guarding providers must be licensed by the Security Industry Authority (SIA) and must operate to BS 7499:2020 (*Note 9.2*).

A written guarding plan, forming part of the contract with the guarding company and referenced in the Security Management Plan (see 9.3), must:

- define patrol routes, check points and shift patterns
- set out incident reporting and escalation procedures

- specify guarding requirements for power outages, alarm outages and any other circumstances where ad hoc guarding is required as a temporary measure
- confirm how guards will communicate with the ARC and emergency services

Guard equipment

To operate effectively, guards must be properly equipped. Equipment should include:

- handheld thermal imaging devices for intruder detection at night or in poor visibility
- weather-resistant high-powered torches suitable for extended outdoor use
- loud hailers or public address devices for issuing verbal warnings
- reliable communications equipment, such as handheld radios supported by any base stations or repeaters needed for full site coverage
- high-visibility strobe beacons on security vehicles, site buildings or guard booths to reinforce deterrence and aid identification at night

Remote monitoring

Where remote monitoring replaces or supplements on-site guarding, the system must meet the VSS (see 7.5) and PIDS (see 7.6) requirements so that detection, verification and response capability remain equivalent.

Note 9.2: BS 7499:2020 is the British Standard for static site guarding and mobile patrol services. It sets the operational, training and management requirements that guarding companies must follow so that patrols, supervision, incident handling and record-keeping are delivered consistently and safely.

9.3 Security Management and Maintenance

The long-term effectiveness of solar farm security depends on consistent management and maintenance. All protective measures must be supported by a formal Security Management Plan.

Security Management Plan

The Security Management Plan must:

- Identify a named person responsible for security management, inspections, record-keeping and compliance



- Set out inspection and maintenance regimes for physical and electronic systems, including fencing, gates, VSS, lighting, PIDS, access control and intruder alarms
- Record incidents, inspections and maintenance activities so that trends and recurring faults can be identified
- Provide a schedule for periodic security reviews so that measures remain proportionate to risk and reflect changes in technology or local crime patterns
- Confirm that equipment continues to meet the certification standards specified at design stage. Where standards evolve, the plan must define how upgrades or replacement will maintain compliance with current SBD requirements

Servicing and contracts

The Security Management Plan must define how servicing and fault response will be managed, including:

- Planned preventive maintenance for all security systems in line with manufacturer and installer recommendations
- Corrective maintenance with clear response times so that faults are rectified promptly and system performance is maintained
- Formal service agreements for VSS and other monitored systems, with Service Level Agreements (SLAs) that reflect the site's risk profile
- Where detailed servicing requirements are specified in other sections (for example VSS, PIDS or EACS), the plan should reference those clauses rather than repeat them

Access control and alarm management

Operational procedures must support the technical measures described in Layer 2 and Layer 3.

The Security Management Plan must:

- Describe the site-access workflow, including pre-arrival verification of work orders, RAMS, inductions and headcount, and the use of timed disarm windows and re-arm confirmation (see 7.8)
- For multi-field sites, maintain partitioned alarm areas so that only the active field is disarmed and all other fields remain protected. Arm and disarm events must be logged with time, operator, field and reason

Data protection and records

Policies for VSS and ANPR must:

- Follow ICO guidance and UK data-protection law, including lawful basis, retention, access control and subject-access requests (see 1.6)
- Be reflected in operational procedures, staff training and contracts with any third-party monitoring providers

Sustainability and service life

The Security Management Plan should:

- Record incident-related carbon impacts, such as repairs, replacements and call-outs, and use this information to prioritise preventive measures and lower-carbon options (see 1.7)
- Specify maintenance regimes that extend service life and avoid premature replacement where equipment remains fit for purpose and compliant with current standards

9.4 Community Engagement

Solar farms are often located on agricultural land as part of farm diversification, and landowners have a direct interest in the success of the renewable project. Regular activity by farmers, land managers or gamekeepers provides natural guardianship and can strengthen early detection of suspicious behaviour.

Developers and operators should consider formal local engagement as part of the security strategy. This may include:

- Commercially engaging the landowner, farmer or gamekeeper to undertake daily or periodic checks of approach routes, the external perimeter and, when safe, internal compounds and buildings
- Reporting any unusual vehicles, persons or site conditions to the Site Operations Centre or the police
- Including hedge, grass and land maintenance within the landowner's contracted duties, linked to biodiversity or countryside stewardship schemes where appropriate
- Encouraging the operator or security partner to participate in local neighbourhood or farm watch schemes and relevant community alert groups to maintain situational awareness
- These measures help integrate the solar farm within its rural context, improve routine oversight and support early intervention

9.5 Secure Connected Device (SCD) Accreditation Scheme

SCD is the Secured by Design scheme for connected security products. It covers devices, hubs, apps and cloud services and aligns with UK Product Security and Telecommunications Infrastructure (PSTI) requirements and ETSI EN 303 645, the European Standard for cyber security of consumer IoT devices.

Where security or monitoring relies on connected devices, SCD accredited equipment should be specified wherever suitable options exist. This includes VSS cameras and analytics, ANPR, access control, intruder alarm components, sensors and IoT gateways.

Specifications should require SCD accreditation for the exact make and model. Suppliers must provide evidence and highlight any non-accredited items with agreed mitigation. Where no SCD option is available, suppliers must confirm compliance with PSTI and ETSI EN 303 645 and set out how SCD products will be adopted when practicable.

Operators must receive SCD documentation at handover and keep records of accredited devices and firmware so that security updates and replacement are controlled.

9.6 Accurate Site Location Identification

Accurate site location information must be available to the ARC, emergency services, and maintenance contractors.

Each site entrance, building, and compound must have a unique GPS or What3Words reference, recorded within operational documentation and signage where appropriate.

Location data must also be included within the emergency response plan.

9.7 Incident Response and Reporting

Incident response must be proportionate to the risk and clearly documented within the management plan.

- The ARC or site controller must maintain contact lists for escalation to keyholders, contractors, and emergency services
- Response timelines, reporting methods, and post-incident review procedures must be defined and tested periodically
- Incident records must capture time, date, alarm type, verification result, and outcome, and be retained in accordance with ICO guidance (see [1.6](#))

9.8 First Responder Co-ordination

The local Fire and Rescue Service (FRS), Police, and Ambulance Service must be provided with up-to-date site layout plans and contact details.

Plans must show access points, isolation switches, hydrants, and high-voltage or battery storage areas.

The operator should invite first responders to visit the site at least once before operation to familiarise themselves with the layout and hazards.

Where significant changes occur (such as additional PV panel arrays or new storage systems), responders must be informed and new plans issued.

All emergency responders must have 24-hour contact details for the ARC or site control.

9.9 Security Review and Continuous Improvement

Operators must review security performance at least annually, incorporating incident data, maintenance records, and technological developments.

Any changes to layout, equipment, or management that could affect security must be reviewed with the DOCO.

Where deficiencies or new threats are identified, improvements must be implemented and recorded.

A.1 National Infrastructure Crime Reduction Partnership (NICRP)

The National Infrastructure Crime Reduction Partnership (NICRP) provides a co-ordinated platform for police forces, government and industry to share intelligence, analyse crime trends and develop common approaches to reducing crime affecting the UK's infrastructure. The partnership supports the energy, transport, water and communications sectors by helping ensure that relevant intelligence reaches operators, Designing Out Crime Officers (DOCOs) and security professionals. NICRP does not replace local policing or site-level security design; it strengthens them by promoting consistent, evidence-based protective measures across national infrastructure.

Further information is available at: <https://www.nicrp.org>

A.2 Police Crime Prevention Initiatives (Police CPI)

Police Crime Prevention Initiatives (Police CPI) is a police-owned, non-profit organisation that delivers crime-prevention services on behalf of the UK Police Service. It owns and manages Secured by Design (SBD), the official police security initiative, and works with industry, government and standards bodies to improve the security of residential and non-residential developments. Police CPI partners with manufacturers, designers and operators to embed effective security and reduce crime through nationally recognised standards, certification and evidence-based security recommendations informed by crime risk and crime trends.

Further information is available at: <https://www.policecpi.com>

A.3 Abbreviations

ARC	Alarm Receiving Centre
BESS	Battery Energy Storage System
BS EN	British Standard
CDM	Construction (Design and Management) Regulations
CTSA	Counter-Terrorism Security Advisor
DOCO	Designing Out Crime Officer
EACS	Electronic Access Control System
HVM	Hostile Vehicle Mitigation
ICO	Information Commissioner's Office
MILP / FILP	Member / Fellow, Institution of Lighting Professionals
MSLL / FSLL	Member / Fellow, Society of Lighting and Lighting
NPCC	National Police Chiefs' Council
NPSA	National Protective Security Authority
NSI	National Security Inspectorate
NSIP	Nationally Significant Infrastructure Project
OR	Operational Requirement
PAS	Publicly Available Specification
PIDS	Perimeter Intrusion Detection System
PROW	Public Right of Way

PSTI	Product Security and Telecommunications Infrastructure
PV	Photovoltaic
RAMS	Risk Assessment and Method Statement
SBD	Secured by Design
SIA	Security Industry Authority
SSAIB	Security Systems and Alarms Inspections Board
UKAS	United Kingdom Accreditation Service
VSS	Video Surveillance System

A.4 Contacts and Further Information

For further information or to begin the application process for the SBD Solar Farm Award, contact your local DOCO at:

<https://www.securedbydesign.com/contact-us>

A.5 Review and Updates

This guide will be reviewed periodically by Secured by Design in consultation with policing, industry, and government partners.

Users should ensure they are working from the latest version of this document.

Appendix B

This appendix summarises the requirements in this guide and groups them by topic. It shows, for each subject, what is mandatory for SBD compliance, what is strongly recommended, and what is optional or context dependent.

Definitions

Must – mandatory requirement for SBD compliance.

Should – strong recommendation representing recognised best practice. Any departure should be discussed with, and recorded by, the Designing Out Crime Officer (DOCO).

May – optional or context dependent measure that can be applied where proportionate to risk.

The following summary sets out security requirements by topic. Where site-specific constraints prevent a stated requirement from being met in its prescribed form, equivalent protection may be achieved through alternative or compensatory measures agreed with the DOCO and recorded within the crime-risk analysis.

1.4 Proportionate Security

Must

- Security measures must correspond to the assessed risk and a documented crime risk analysis
- Where lighting or fencing is restricted, alternative measures must be explored with DOCO support
- References to standards must relate to the current published edition
- Where relevant, counter-terrorism measures must be specified by the CTSA
- Security documentation must be retained for Secured by Design verification

Should

- Crime risk analysis should be collaborative, involving the DOCO and project team
- Early engagement with conservation and archaeology officers should take place where heritage assets are affected

May

- None stated

3 SBD Award Routes

Must

- For the Vulnerability Survey route, the operator must confirm in writing how required measures will be implemented
- The applicant must re-engage the DOCO to confirm continued SBD compliance if post-consent design changes affect security

Should

- Developers should consult the DOCO at pre-planning stage for new developments

May

- None stated

5 Construction Phase Security

Must

- Cable drums and coils must be stored inside secure compounds with lighting and VSS where practicable
- Temporary protective measures must include monitored VSS, a monitored intruder alarm, secure fencing, controlled access points and suitable lighting
- Security signage must comply with ICO requirements

Should

- On-site guarding should be used during high-risk periods or when vulnerable components are present

May

- None stated

6 Layer 1 – Outer Environment

Must

- Signage must clearly identify private property, surveillance and prohibited access
- Signage must comply with ICO requirements

Should

- Entrances should be limited to what is operationally necessary
- Parking, where provided, should be located outside the secure perimeter where practicable
- Public Rights of Way close to boundaries should include clear signage and suitable boundary treatments

May

- Grazing or land management may continue where compatible with security
- Additional detection such as PIDS or VSS may be used along Public Rights of Way where risk requires it

6.4 Hostile Vehicle Mitigation (HVM)

Must

- Where a counter-terrorism risk is identified, HVM measures must follow CTSA advice

Should

- None stated

May

- Natural or engineered features such as ha ha walls, earth bunds, ditches, watercourses or defensive planting may contribute to HVM
- Concrete poacher blocks may be used to prevent unauthorised vehicle access

7 Layer 2 – Perimeter Security

Must

- Fencing must be at least 2.0 metres high and certified to the standards listed in Section 6.2 where feasible
- Where certified fencing cannot be applied to all boundaries, alternative solutions must be agreed with the DOCO
- Gates must provide resistance equivalent to the fencing
- Padlocks must be certified and protected by shrouds
- Gate hardware must prevent lifting, levering or forced opening
- Automated gates must have secure side emergency release and comply with UKCA or CE marking
- Gaps over 100 mm must be eliminated wherever practicable
- Duty holders must maintain a written inspection and maintenance plan

Should

- Emergency egress arrangements should not compromise perimeter security

May

- Multi-user latch systems may be used where several parties require access
- Temporary internal obstacles may be used during heightened risk periods

7.3 Lighting

Must

- Where lighting is provided, it must comply with BS EN 12464 2 and BS 5489 1 where applicable
- The DOCO must be provided with written confirmation from a competent lighting designer
- Lighting designers must hold the competencies listed in Section 6.3 or be supervised by someone who does

Should

- Lighting should focus on vulnerable areas rather than providing uniform lighting
- Lighting should avoid unnecessary glare and should support VSS effectiveness

May

- Motion activated or controlled lighting may be used where ecological or planning constraints limit uniform lighting

7.4 Operational Requirement (OR) for Electronic Security Systems

Must

- All electronic systems must be designed against a documented Operational Requirement

Should

- None stated

May

- None stated

7.5 Video Surveillance Systems (VSS)

Must
■ VSS must comply with BS EN 62676 ■ Systems must be installed and maintained by a company certificated by the NSI or the SSAIB ■ Cameras must cover entry points and external approaches ■ Recorded images must be retained for an agreed period, normally at least 31 days ■ All VSS operation must comply with ICO requirements and UK GDPR
Should
■ AI analytics should be used to support detection and reduce false alarms
May
■ None stated

7.6 Perimeter Intrusion Detection Systems (PIDS)

Must
■ PIDS must comply with BS EN 50131 1 and BS EN 50131 2 7 1 ■ Systems must be installed and maintained by a company certificated by the NSI or the SSAIB ■ PIDS alarms must integrate with VSS for verification ■ Where fencing is not possible, alternative detection must be deployed ■ Where PIDS signals are transmitted to an ARC, the handling of personal data must comply with ICO requirements
Should
■ Larger sites should use zonal mapping for accurate incident location
May
■ Drone verification may be used if CAA compliant

7.8 Electronic Access Control Systems (EACS)

Must
■ Access control must comply with BS EN 60839 11 1 ■ Systems must be installed and maintained by a company certificated by the NSI or the SSAIB ■ Any processing of personal data, including ANPR image capture or credential logs, must comply with ICO requirements and UK GDPR
Should
■ ANPR capture should meet BS EN 62676 expectations
May
■ ANPR may support vehicle access control

8.3 Intruder and Hold-Up Alarm Systems (I&HAS)

Must

- I&HAS must comply with BS EN 50131 1, BS EN 50136 and PD 6662
- Systems must be installed and maintained by a company certificated by the NSI or the SSAIB
- Alarms must protect secure compounds

Should

- Wider zoned coverage should be used on larger or higher risk sites

May

- None stated

8.2 Doorsets and Windows

Must

- Products must comply with the SBD Non-Residential (Commercial) Guide

Should

- None stated

May

- None stated

8.4 Secure Storage Units

Must

- Storage containers must meet LPS 1175 B3 or equivalent
- Padlocks must be certified and shrouded
- Units must not be used as part of the perimeter

Should

- Windows should be avoided
- Doors should face inward where practicable

May

- None stated

8.5 Photovoltaic (PV) Panels and Cabling

Must

- Cabling and earthing layouts must be shown on Single Line Diagrams and comply with Electricity at Work Regulations

Should

- Cabling should be enclosed or buried where practicable
- Exposed spans should be minimised

May

- Forensic marking may be used where proportionate

8.6 Property Marking and Tracking

Must

- Where forensic marking is used, the product must be SBD recognised and properly recorded

Should

- Visible deterrent signage should be spaced appropriately

May

- None stated

8.8 Battery Energy Storage Systems (BESS)

Must

- Boundary treatments must meet Section 6.2 or an agreed compensatory solution
- Accurate entrance and compound locations must be recorded and shared with responders

Should

- Inspection strips should be maintained

May

- Audio challenge may be used where proportionate

9 Layer 4 – Operational Security

Must

- Guarding providers must be SIA licensed and comply with BS 7499
- A Security Management Plan must name responsible persons, inspection regimes and incident reporting
- Service arrangements must include suitable SLAs
- Access control and alarm procedures must support technical security measures
- VSS and ANPR policies must comply with ICO guidance and UK GDPR
- Each site entrance or compound must have a unique location reference

Should

- Guarding equipment should include appropriate tools for patrol
- Incident response should be tested periodically
- Security should be reviewed after incidents or operational changes

May

- Landowners or gamekeepers may support routine checks
- Operators may participate in local watch schemes



Secured by Design

**2nd Floor, 50 Broadway, St James's Park
Westminster, London, SW1H 0BL**

Tel: 0203 8623 999

Email: enquiries@police-cpi.co.uk

Web: www.securedbydesign.com