energynetworks association

Department for Business, Energy & Industrial Strategy

# Distributed Energy Resources – Cyber Security Connection Guidance

# Foreword

Cyber threats to the energy sector pose economic and national security risks, threatening a key Department for Business, Energy and Industrial Strategy (BEIS) objective to ensure consumers have a reliable, low cost and clean energy system. Our energy system is amongst our most Critical National Infrastructure (CNI), underpinning many of our essential services.

Achieving the Net Zero target by 2050 will require rapid digitalisation and decentralisation of the energy system. New cyber security risks will emerge as the energy system becomes more connected and driven by data and technology. BEIS recognises that effective cyber security will need to underpin our policy and actions to facilitate a smarter, digitalised and decarbonised energy system.

Improving cyber security will help ensure that we have a secure and resilient energy system, able to avoid disruption through a cyber attack that could have a severe impact on the country's national security. There have been concerning cases of disruptive and destructive cyber activity against international energy CNI targets in recent years which have demonstrated the capability of attackers who continually refine their methodology, and the level of threat that the UK energy sector could be subject to.

The Network and Information Systems (NIS) Directive came into force 10 May 2018, placing an additional legislative requirement on organisations deemed operators of essential services (OES), to protect against and respond to cyber attacks and wider incidents affecting energy delivery systems.

Whilst not currently meeting the 'essential service' criteria laid out in the NIS regulations, the growth of Distributed Energy Resource (DER) usage, is such that they are now becoming increasingly important to the UK's energy supply. The potential impact to the grid stability from a cyber compromise of multiple smaller DER assets could be significant. For example, on the 9 August 2019 there was widespread power disruption, caused, in part by the loss of DER assets. To date, there is no tailored cyber security guidance and standards to ensure connected assets are securely installed, connected and managed.

Working closely with the NCSC, Energy Emergencies Executive Cyber Security Task Group (E3CC) and the Energy Networks Association (ENA), BEIS has identified the need to address cyber security controls across the increasing amount of DER connected to distribution networks.

This guidance is a result of collaboration between BEIS, the ENA, Distributed Network Operators (DNOs) and DER operators who have provided industry insight, shared challenges and made suggestions to improve DER cyber security connections across the industry.

The guidelines have been aligned to the four objectives and fourteen principles from the NCSC Cyber Assessment Framework (CAF), which is itself intended for use by organisations responsible for services and activities that are of vital importance such as those designated CNI.

Adoption of these cyber security connection guidelines, developed from the CAF, will support delivery of end-to-end cyber security for DER, at an industry-accepted level that will help manage the risk of a cyber attack. It will also enable DNOs and operators to effectively and consistently implement an industry baseline for cyber security when connecting new DER assets to the distribution networks.

# Contents

# Figures and tables

## Figures



## Tables

## About the ENA

Energy Networks Association (ENA) is the “voice” of the network operators, representing the electricity and gas transmission and distribution network operators in the UK and Ireland. Users of this guidance are diverse, from major international companies to independent network operators.

ENA is actively engaged with government, regulators and the EU Commission as well as producing a wide range of industry standards.

The impact of regulation, the increasing influence of European legislation, the challenge of new technologies and the importance of securing our energy future, all against the background of the UK’s Net Zero targets, are just some of the issues that the ENA helps users of this guidance to address.

***DISCLAIMER***

- This guidance provides a list of outcome based guidelines tailored for DERs. ENA takes no responsibility for its application within organisations; Any legislative requirements supersede statements in this guidance, including, but not limited to, energy sector regulation or legislation under the NIS Regulations, the UK Data Protection Act and EU General Data Protection Regulation, and HSE or other safety regulations
- This guidance will provide a foundation for a secure system, and does not claim to meet the full requirements of any specific standard
- The DER provider is accountable to provide cyber security governance such that policies and procedures are established to ensure that security of the DER are appropriate and proportionate to any identified DER cyber security risk, and that security measures for the DER are operated and maintained throughout the DER lifecycle

# Acknowledgements

BEIS together with ENA and Actica Consulting wish to thank the following organisations for their contribution to the development of this guidance:

- UK Power Networks
- Electricity North West
- Western Power Distribution
- Scottish Power Energy Networks
- Scottish and Southern Electricity Networks
- Northern Powergrid
- NCSC
- National Grid UK
- National Grid ESO
- Orsted
- BSR
- Natural Power
- Uniper
- Passiv Systems
- Infinis
- EDF Energy
- Energy UK
- Association of Distributed Energy
- Renewable Energy Association
- BEAMA
- Solar Trade Association
- Scottish Renewables
- Sustainable Energy Association
- Viridis Power
- Schneider Electric

# 1 Introduction to the guidance

This document, Distributed Energy Resources (DER) - Cyber Security Connection Guidance (CSCG), will support users in the design, development, deployment, connection and maintenance of new and existing DERs to the distribution networks. This guidance contains a suite of outcome-based guidelines that may be used as part of a risk based approach to improving the cyber security posture for DER and demonstrate a known security baseline that can be readily understood and recognised by generators, aggregators, network operators and other service providers.

The outcomes from this guidance are based on the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) Indicators of Good Practice (IGP). Alignment with the CAF provides a consistent approach to the NIS regulations and across the electricity sector as a whole.

The guidance should ideally be followed prior to connection, however it can also be retroactively applied afterwards for legacy connections.

## 1.1 Objective

The objectives of this guidance are to:

- Promote cyber security throughout the design, development, deployment, connection and maintenance of new DER projects.
- Provide a consistent approach to cyber security for DER connections.
- Provide a baseline level of cyber security for new DER connections
- Assist the Deparment for Businees Energy and Industrial Startegy (BEIS), NCSC and the Energy Networks Association (ENA) to identify short-term and long-term threats and promote standardisation
- Provide cyber security guidelines that are flexible, regardless of size, maturity or location
- Influence technology providers to improve security for their devices out of the box.

## 1.2 Scope

The primary focus of this guidance is the connection of non-domestic DER to the electricity distribution networks. Its scope includes:

- All DER technology types (wind, solar, gas, hydro, battery storage, etc.)
- Suggests requirements to adhere to the NIS regulations
- The use of aggregators, control centres and third-party organisations
- DER controlled through the National Grid ESO

This guidance can be used by those who have a responsibility for cyber security throughout the DER lifecycle as a reference during design, build, connection and running of DER.

The specific requirements for each DER asset or site will vary depending on the situation, but this guidance provides flexibility to select the appropriate guidelines.

### 1.2.1 Out of scope

The scope for this guidance does not include:

- Transmission network connected DER
- Domestic applications

- Non Domestic Electric Vehicles (EVs)

However, this guidance is still largely useful to other applications.

## 1.3 Who should use this guidance

The CSCG is primarily aimed at:

- Generators using solar, wind, gas, hydro and other technologies to generate electricity
- Organisations using storage technologies such as batteries to provide frequency response or flexibility services for the distribution networks
- Aggregators who act as an intermediary for multiple generators to provide management and flexibility services
- DNOs into whom the DER will feed electricity (or provide load)
- Installers of DER infrastructure
- Vendors, service providers and other third-parties who support and maintain DER resources.

## 1.4 Consultation

Interim guidelines outlined in this document will be subject to periodic review in the view of converting these guidelines to Connection Codes. The first review of the document will take place in 6 - 9 months.

Details of the consultation will be published on; www.energynetworks.org/operating-the-networks/managing-cyber-security

Aditionally, you can submit in any initial feedback/commnets you have by sending an email to CyberSecurity@energynetworks.org.

We welcome your input to the development of an enduring connection codes for DER. This approach will, over time, improve security and lower the risks associated with DER in the UK.

# 2 Distributed Energy Resources

DER, as referred to in this guidance, are a group of technologies that have, over the years, had a number of names and definitions. One of the common terms used for small scale electricity generation has been '*Distributed Generation (DG)*' : A technology connected to the distribution network that produces electricity.

As electricity storage technologies improved, this term has been replaced with a more inclusive term: *Distributed Energy Resources (DER)*: DER is defined as a resource on the distribution network that produces or stores electricity.

DER are typically in the range of 3kW to 50MW in size, located within the distribution network at or near the end user. They may also include:

- Behind The Meter Generation (BTMG): A generating unit or multiple generating units at a single location, on the customer's side of the retail meter that serve all or part of the customer's retail load with electric energy (out of scope for this work).
- Energy Storage Facility (ES): An energy storage device or multiple devices at a single location, on either the utility (DNO or Supplier) side or the customer's side of the retail meter (out of scope for this work).

- DER aggregation (DERA): A virtual resource formed by aggregating multiple DG, BTMG, or ES devices at different points of interconnection on the distribution system.

Micro-grid (MG): An aggregation of multiple DER types behind the customer meter at a single point of interconnection that has the capability to island. It may range in size and complexity from a single "smart" building to a larger system such as a university campus or industrial/commercial park.

# 3 Cyber security and resilience for DER

Cyber threats to the energy sector pose economic and national security risks. Addressing these threats is critical for our economy, national security and household budgets. Improving cyber security across the energy sector will help ensure that consumers have a reliable, low cost and clean energy system. Energy underpins all our essential services and its disruption could severely affect public safety and public health.

The UK Government recognises cyber attacks as a tier-one risk to UK interests[1], and the energy sector is included in the UK Cyber Security Strategy. The UK Government advises that the threat from cyber attacks is increasing. Cyber incidents have affected energy and utility networks, such as the Ukraine hack in 2015 which resulted in the loss of electricity supply to 250,000 customers. It is widely recognised that the energy sector is a likely target for cyber attack due to the essential services it provides to the UK.

Cyber security incidents can arise from a targeted cyber attack, but they can also be untargeted, collateral damage or even accidental. Cyber security incidents can adversely affect DER availability, reliability, investment return or ability to fulfil its intended function.

The increase in DER and renewable energy, combined with the ongoing adoption of digital technology in the energy sector means DER are increasingly reliant on IT and telecommunications. Digitalisation brings huge advantages to the customer and provides significant operational benefits. Widespread use of digital communications and interconnectivity between organisations and systems carries a significant risk from cyber attack. This risk will increase as the reliance on DER and flexibility contracts increases, which will result in an increased attack surface.

This section considers cyber security trends, cyber considerations, determination of the security groups and the application of cyber security controls. It contains the target profile or security groups that will be used to develop the CSCG statements.

[1] National Security strategy and Strategic Defence and Security

## 3.1 Current cyber security trends that affect DER

There are a number of cyber security trends that affect DER as outlined in Table 1.

**Table 1 Cyber security trends affecting DER connections**

| Key challenge | Description |
|---|---|
| **Keeping pace with technology** | Energy organisations and other CNI sectors are heavily reliant on Operational Technology (OT) systems for their core operations and face ongoing challenges with keeping such technology up to date as it typically has 15 years or longer lifespan.<br>Managing the transition from DNO to Distribution System Operator (DSO)[2] and the implementation of the Smart Systems and Flexibility Plan (SSFP). |
| **Convergence of OT and IT** | Traditionally OT systems were bespoke and not connected to enterprise data networks. However, OT has increasingly moved to using standard IT technologies, such as Windows and Linux Operating Systems, Ethernet, Transmission Control Protocol and Internet Protocol (TCP/IP), web applications and wireless technologies. In parallel these once separate domains are becoming increasingly connected and using new technologies to drive efficiency and improve operational performance, having the following implications:<br>• Increasing the size of the accessible attack surface<br>• Creating interdependencies and interfaces<br>• Putting pressure on industry cyber security capability and resourcing |
| **Range of standards** | A high number of cyber security standards exist for the energy sector. IT standards are not necessarily appropriate to the operational environment. There are evolving Industrial Control Systems (ICS) standards and guidance being adopted on an ad-hoc basis by UK industry, with no current consensus on which to use. |
| **Legislation** | Complying with the NIS Regulations that apply to transmission connected generation with a capacity ≥ 2GW and General Data Protection Regulation (GDPR). |
| **Skills and resources within the sector** | The cyber security skills gap in the engineering domain is still prevalent. This is widening with IT/OT convergence.<br>DER is also increasingly being owned and operated by entities not from a traditional energy or technology background. |
| **Technology trends** | DER are leveraging modern IT technologies to meet the change in demands of the business, such as:<br>• Use of low cost commodity hardware<br>• Use of mobile technology in DER environment e.g. tablets and thin clients<br>• Shift to centralised software management and security solutions e.g. patching and antivirus updates<br>• Increased digitisation in DER, including in substations and monitoring systems<br>• Smart grid infrastructure and management<br>– Interconnectivity throughout information system layers |

[2] Open Networks Project, Energy Networks Association

| | |
|---|---|
| | – DER data crossing system and organisational boundaries<br>– Increased reliance on technology and real-time operational information.<br>Many of these trends and technology advances bring improvement but also increase the cyber security risk to DER. |
| **Third parties** | Third parties are increasingly being targeted to gain access to facilities through their "trusted" status. Third parties are being targeted through:<br>• Compromising updates files such as with the Havex malware attack<br>• Using remote connections to access control systems from third parties<br>• Compromised embedded components being used in hardware |

## 3.2 DER Security Considerations

For any given DER type or size, requirements should meet the security attributes to support the desired level of security for that site (based on regulations, guidelines, contractual requirements and industry good practice). This means that the assets, systems and services within the DER site need to be examined and key features identified.

Areas to consider when evaluating the cyber security requirements for a DER asset, site or connection include, but are not limited to:

- Identifying who would be responsible for ensuring an effective response to a DER failure or outage (the person responsible should be the risk owner)
- Varying maturity levels and approaches to cyber security risk management
- Location of the assets, systems or services
- Size and generation capacity of the DER assets and sites
- Identification of all interfaces to the asset, system or service
- Users, including where and how they access the asset, system or service
- User authentication and authorisation, and how they are implemented
- Physical security of the DER site
- Low cost, commodity hardware with limited security controls built in
- Understanding any control or data connections required by the Network Operator
- Understanding the organisations architecture relevant to the asset, system or service, such as communications within the DER site and external to the DER site
- The use of flexibility contracts and the mechanisms employed to implement these
- The use of third party organisations for management or support
- Key dependencies with other sites or systems
- Core functionality of the assets, and impact of a system failure or outage of the asset or site
- Use of a consistent time for logging and event investigation
- Recovery mechanisms, such as spares holding configuration status, requirements to rebuild from scratch
- Where alarm and event data are processed
- Which system triggers a cyber security incident

To ensure requirements are appropriately identified, it is also necessary for DER organisations to understand the interactions that assets, systems or services may have with other equipment or information systems both internally or external to the organisation. DER have a number of potential interfaces that may have cyber security risks to be managed throughout the system's lifecycle.

## 3.3 Determining the CSCG security group

Having understood the security considerations, it is necessary to understand the overall impact of a compromise to the relevant DER or site. An impact assessment will evaluate DER to identify any immediate, delayed or cascading effects from cyber security incidents considered in the assessment.

Understanding the risk profile for the DER and where it is located is important to determining the appropriate and proportionate management for the cyber security risk. One of the key elements to assessing the risk is understanding the potential impact that a cyber security incident may have, as this allows an appropriate CSCG security group to be defined.

Cyber security incidents present in various ways, with different effects on the DER and electricity networks. Examples include:

- Loss of control or visibility to one or more DER asset
- Loss or disruption to services that the systems rely on, such as telecommunication networks
- Loss or disruption to the generation of electricity
- Widespread, co-ordinated incident affecting multiple DER sites simultaneously

The impact of these effects could be:

- Loss of supply
- Excess supply
- Frequency instability on the distribution or transmission networks
- Inability to use the DER for frequency response when required
- Inability to use the DER for active or reactive power when required
- Disconnection of the one or more DER asset from the distribution network
- Reputational damage

As the CSCG will need to be applicable across a very wide range of DER, from just above domestic level right up to around 2GW (single site/accumulated capacity), there is a need to divide the DER into logical groups to allow the selection of the most appropriate guidance statements to apply. There is not likely to be a 'one size fits all' approach, so for this reason four groups have been defined as set out in Table 2 below.

**Table 2 DER Groupings**

| Group | Description |
|---|---|
| Baseline | • Typically a single site<br>• Installed capacity < 5MW<br>• Single inverter or turbine |
| Small | • Typically a single site<br>• Installed capacity < 20MW<br>• Multiple inverters or turbines |
| Medium | • Multiple sites<br>• Collective installed capacity < 200MW<br>• Could be a combination of DER types |
| Large | • Multiple sites<br>• Collective installed capacity < 2GW<br>• Could be a combination of DER types |

Whilst not an exact science, the sizings for these groups have been defined to allow a reasonable spread of the DER across the groups, was based on the current landscape of DER and are proportionate to the likely capabilities of an organisation. It is important that any guidelines ensure that DER connectivity remains accessible and viable for operators as well as secure.

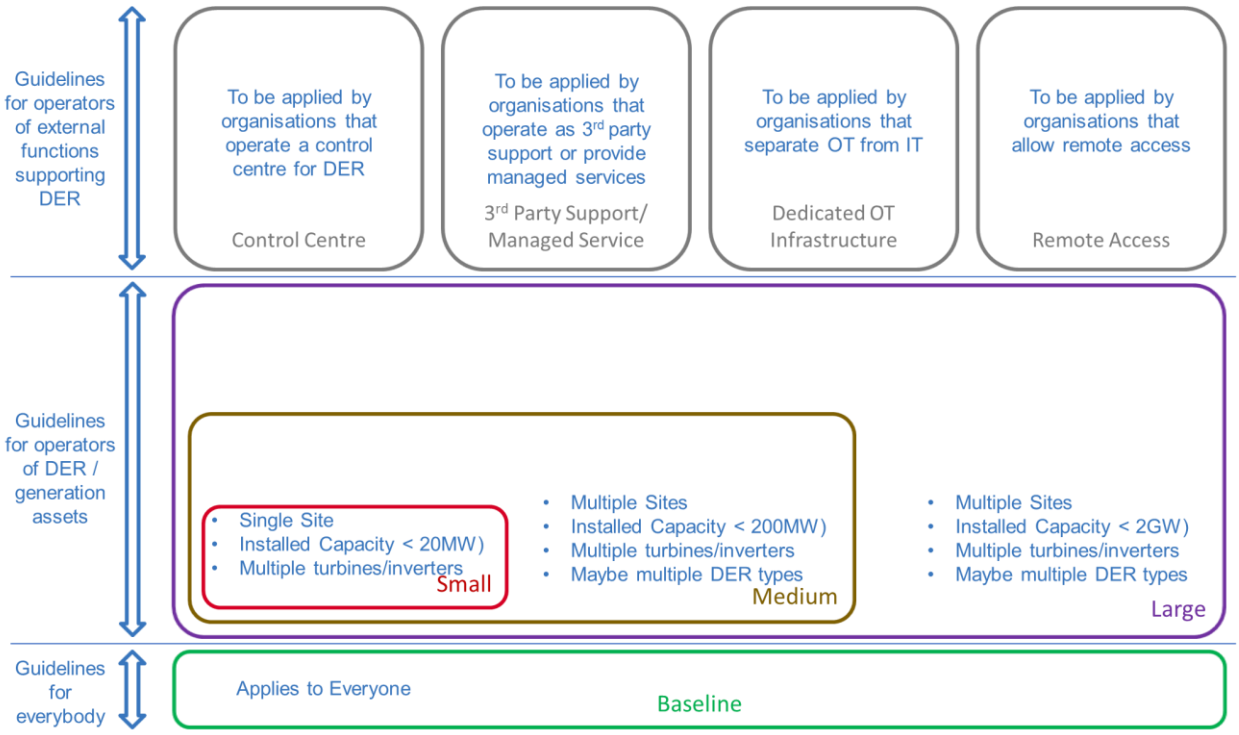
All sizings will remain under review and will likely be updated as either the landscape or the maturity of the technology/operators changes. For example, the largest inverters currently available to purchase are around 5MW, so this was used for the baseline group.

As well as the basic groups defined above, it is also useful to represent some of the additional entities that may apply across the groups:

- Control Centre – The set of guidelines and controls that are specific to organisations with their own control centres. This may apply to DERs that maintain their own control centres, or may be the set applied to a third-party that provides a control centre as a managed service. A control centre in this context applies to a central location (physical or virtual), typically running a Supervisory Control and Data Acquisition (SCADA) or Distributed Control System (DCS) system that has control, monitoring and management responsibility for a number of DER assets.
- Third party support or Managed Service – The set of guidelines and controls that apply to external suppliers that provide either remote support for DER assets, or a managed service (Other than control centre) providing day to day operational services to a DER. This group would include vendors and manufacturers providing full access warranty cover for equipment. This group would apply to 3rd parties offering their services, or for contracted third parties where the end client has included in their contractual obligations.
- Dedicated OT – The set of guidelines and controls for entities that operate their OT separate to the main corporate IT infrastructure. Typically the DER entities that have a SCADA or DCS system.
- Remote Access – The set of guidelines and controls that should be applied wherever there is remote access to the DER assets or connections.

Figure 1 shows the CSCG grouping structured in a graphical way.

**Figure 1 CSCG Security Groupings**




All DERs should apply the baseline and the group most relevant for their size. They will then also apply any or all of the additional groups based on their configuration. The application of guidelines for the groups is cumulative in nature (i.e. Medium includes all of the Small guidelines, plus the Medium guidelines).

## 3.4 Mapping of the NCSC CAF principles

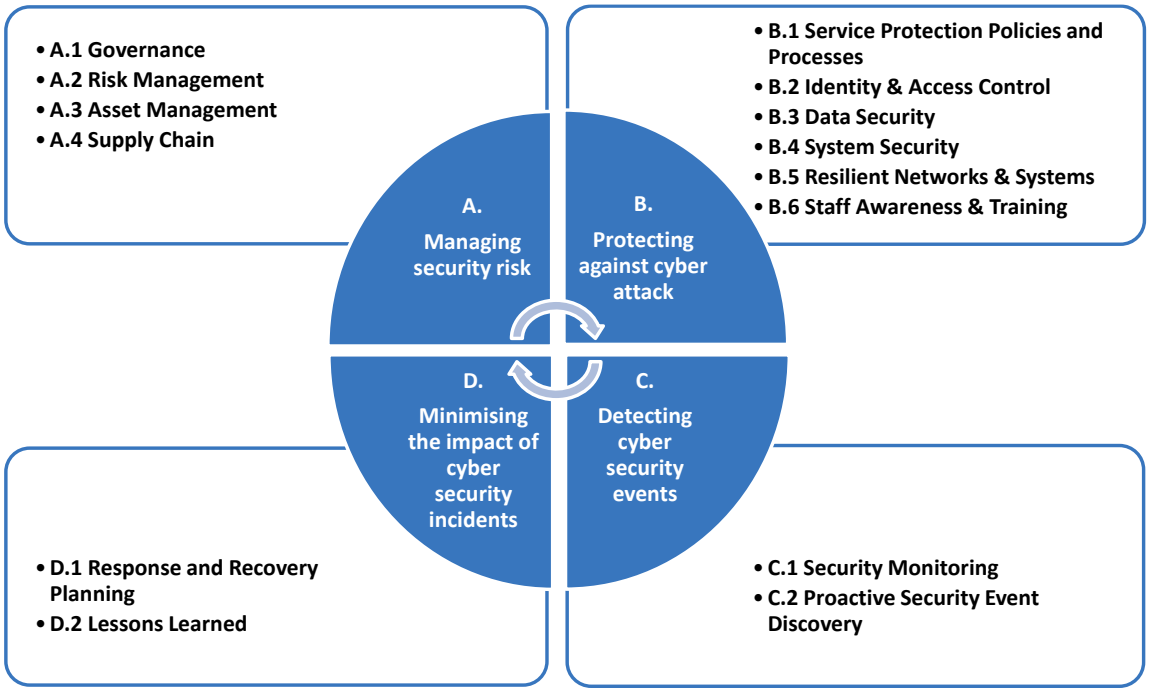
Now that the groupings have been defined, the guidelines and controls for each can be defined. In order to remain consistent with the CAF, the CSCG have been designed to work in cooperation with the 14 principles contained in the NCSC's CAF.

The CAF collection consists of a set of 14 cyber security and resilience principles, together with guidance on using and applying the principles, and the CAF itself. It is aimed at helping an organisation achieve and demonstrate an appropriate level of cyber resilience in relation to certain specified essential functions performed by that organisation.

The four key security objectives and supporting principles to deliver the objectives are shown in

Figure 2.

**Figure 2 NCSC Cyber Assessment Framework (CAF) Summary**




A more detailed breakdown of the CAF objectives and principles can be found in Appendix A. Full details can be found on the NCSC website.

It is important to note that the CSCG are not the NCSC CAF, but rather they provide an interpretation of the CAF, its contributing outcomes and its Indicators of Good Practice (IGP), that can be applied to the diverse spectrum of DER resources. The CAF is written primarily in terms of outcomes to be achieved, rather than a compliance checklist. The CSCG aims to add some DER-specific guidelines and measures which could be used to facilitate delivery of CAF outcomes.

To allow flexibility and to recognise the diverse scale of DER organisations, the CSCG has adapted the CAFs contributing outcomes and IGP approach, into three tiers: Foundational, Light and Full:

- 'Foundational' guidelines are the suggested minimum level recommended to help the organisation implement a core level of the CAF 'partially achieved' IGP for that contributing outcome and principle.
- 'Light' guidelines help the organisation 'partially achieve' the CAF IGP for that contributing outcome and principle but may include some of the 'achieved' IGP as well.
- 'Full' guidelines help the organisation 'achieve' the contributing outcomes of the CAF Principle.

Table 3 below gives a high level view of how the foundational, light and full tiers could be applied to the CAF principles. The third column contains a brief indication of the measures that could be in place for each tier. Full details of the guidelines applicable for each tier is found in section 6.

**Table 3 CAF Principle breakdown**

| Objective A Managing Security Risk | Contributing Outcomes | CSCG Tiers | |
|---|---|---|---|
| A.1 Governance | A.1a Board Direction | Foundational | Existence of a security policy defining the lines of responsibility and accountability for the security of DER assets. |
| | | Light | Clear governance structures in place, clearly articulated risk appetite and risk management policy and processes. |
| | | Full | Appropriate management policies and processes in place to govern the approach to security. Often as part of an industry recognised security management system. |
| | A.1b Roles and Responsibilities | Foundational | Necessary roles and responsibilities have been identified and are regularly reviewed. |
| | | Light | Appropriately capable and knowledgeable staff fill the identified roles and have the resources and authority to carry them out. |
| | | Full | Roles are filled and there is clarity on who has overall accountability for cyber security. |
| | A.1c Decision Making | Foundational | Decision makers understand their responsibilities in the context of the risk appetite – as set by senior management |
| | | Light | Senior management have visibility of key decisions and they are periodically reviewed |
| | | Full | Risk management decision making is delegated and escalated across the organisation to the people who have the skills, knowledge, tools and authority they need |
| A.2 Risk Management | A.2a Risk Management Process | Foundational | Existence of a risk management policy and a process for identifying, assessing and understanding risks to DER assets. |
| | | Light | Following the NCSC Risk Management Guidance to choose a risk management approach that considers the threats, vulnerabilities and impacts relevant to DER. Regular risk assessments carried out. |
| | | Full | Risk assessments are dynamic and updated in light of relevant changes. Threat analysis carried out to understand the implications for the organisation |
| | A.2b Assurance | Foundational | Security measures are understood and validated regularly to ensure they remain effective. |
| | | Light | Security deficiencies uncovered during assurance activities are assessed, prioritised and remedied where necessary. |
| | | Full | The organisation takes appropriate steps to identify, assess and understand security risks to the operation of essential functions. |
| A.3 Asset Management | A.3a Asset Management | Foundational | Existence of an asset list including the location and owner for each asset. |
| | | Light | Existence of an asset management policy and process along with a central asset repository that includes all DER assets, their owners and the dependencies between them. |
| | | Full | Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential |

| | | | |
|---|---|---|---|
| | | | functions is determined and understood. This includes data, people and systems as well as any supporting infrastructure |
| A.4 Supply Chain | A.4a Supply Chain | Foundational | Awareness of external suppliers and ensuring network connections and data sharing does not compromise the DER. |
| | | Light | Effective specification of security properties for the provision of DER equipment or services from a third party and ensure the protection of data shared with the third party. |
| | | Full | The organisation understands and manages security risks to networks and information systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used. |
| **Objective B Protecting against cyber attack** | **Contributing Outcomes** | **CSCG Tiers** | |
| B.1 Service Protection Policies and Processes | B.1a Policy and process development | Foundational | Basic policies and processes in place related to the securing of DER assets and information. |
| | | Light | Policies and processes are updated in response to major cyber security incidents. |
| | | Full | Policies and processes are reviewed and updated at regular intervals to ensure they remain relevant. Systems are designed so that they remain secure even when security policies and processes are not always followed. |
| | B.1b Policy and process implementation | Foundational | Basic policies and processes in place related to the securing of DER assets and information. |
| | | Light | Policies and processes actively maintained throughout their lives. Adherence to the policies is checked. Breaches are tracked and assessed to determine actions. |
| | | Full | The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support operation of essential functions. |
| B.2 Identity and Access Control | B.2a Identity verification, authentication and authorisation | Foundational | All DER assets are protected with a username and secure password. |
| | | Light | Users are individually authenticated and authorised for remote access. The list of authorised users is regularly reviewed. |
| | | Full | 2 factor authentication or hardware backed certificates are used to individually authenticate and authorise access to systems. |
| | B.2b Device management | Foundational | Assets are physically secure in a locked enclosure. |
| | | Light | All privileged access occurs from dedicated management devices. It is possible to detect and investigate unknown devices connecting to the network |
| | | Full | Independent assurance is gained for the security of third party devices or networks before the connect to DER assets. Regular scans are performed to detect unknown devices. |
| | B.2c Privileged user management | Foundational | Separation of operator and administrative access. Periodic review of user and their rights. |

| | | | |
|---|---|---|---|
| | | Light | Principle of least privilege implemented. |
| | | Full | The organisation understands, documents and manages access to networks and information systems supporting the operation of essential functions. |
| | B.2d Identity and access management (IdAM) | Foundational | User follow a robust procedure to be verified prior to being granted the minimum access rights required |
| | | Light | All user access is logged and monitoring. Permissions and users are regularly reviewed and revoked when no longer required |
| | | Full | Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised. Attempts by unauthorised users is alerted and promptly investigated |
| B.3 Data Security | B.3a Understanding data | Foundational | All important DER data is identified and catalogued together with who has access to that data. |
| | | Light | The location, transmission, quantity and quality of data is periodically reviewed. The impact of a data breach is understood and documented. |
| | | Full | All mobile devices and media that may hold key data are identified and steps are taken to remove or minimise unnecessary or historic copies. |
| | B.3b Data in transit | Foundational | Data in transit is transmitted over encrypted channels where available[3] (TLS/IPSec for internet traffic). |
| | | Light | All data links that carry DER data have been identified and secured by appropriate means, such as cryptography |
| | | Full | Data transmitted electronically is protected from actions such as unauthorised access, modification, or deletion. Such protection extends to the means by which authorised users, devices and systems access critical data. It also covers information that would assist and attacker. |
| | B.3c Stored data | Foundational | Data at rest is protected from unauthorised access, modification or deletion. |
| | | Light | Data removal from the system is controlled and data backups are suitable and secured. |
| | | Full | Data stored electronically is protected from actions such as unauthorised access, modification, or deletion. Such protection extends to the means by which authorised users, devices and systems access critical data. It also covers information that would assist and attacker. |
| | B.3d Mobile data | Foundational | Mobile devices that hold DER data are identified |
| | | Light | DER data is only stored or processed on mobile devices secured to a similar standard to the rest of the organisation |
| | | Full | Organisation can remote wipe data help on mobile devices. Data is automatically removed after a specified time |
| | | Foundational | All data is removed from device storage prior to disposal |

[3] Where there are industrial protocols such as DNP3 that are difficult to secure, this would not be expected at foundational level.

| | | | |
|---|---|---|---|
| | B.3e Media/equipment sanitisation | Light | All data is securely removed from device storage before the media is destroyed. |
| | | Full | Organisation can remote wipe data help on mobile devices. Data is automatically removed after a specified time |
| B.4 System Security | B.4a Secure by design | Foundational | Appropriate expertise is used to design and implement DER systems. Firewalls separating DER from untrusted networks. |
| | | Light | DER systems separated from normal IT systems. Data flows and system recovery mechanisms are simple |
| | | Full | An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures. |
| | B.4b Secure configuration | Foundational | User access control enabled for all assets. Secure platform and device builds are used. Software is verified before installation. |
| | | Light | Boundaries protected and messages content checked. Simple and consistent configurations used across device types |
| | | Full | Network and information systems and technology critical for the operation of essential functions are protected from cyber attack. Only permitted software can be installed |
| | B.4c Secure management | Foundational | Malware and unauthorised software is prevented and detected. |
| | | Light | Monitoring of essential systems in place. Systems are administered and maintain by authorised privileged users |
| | | Full | Dedicated management devices are used to maintain the DER systems. Technical knowledge and documentation regularly reviewed and securely stored |
| | B.4d Vulnerability management | Foundational | Software updated and patched regularly. Anti-malware measures in place. |
| | | Light | Announced vulnerabilities for DER related systems are tracked and mitigated promptly. Regular testing takes place. |
| | | Full | Regular third party testing is carried out. Only supported software and firmware is allowed in the system |
| B.5 Resilient Networks and Systems | B.5a Resilience preparation | Foundational | Understanding of the technologies and inter dependencies to aid restore of DER if needed |
| | | Light | Documented procedures for restoring the DER system in the event of a failure |
| | | Full | The organisation builds resilience against cyber-attack and systems failure into the design, implementation, operation and management of systems that support the operation of DER. |
| | B.5b Design for resilience | Foundational | capacity of the system managed. |
| | | Light | Segregation between the DER systems and the rest of the organisations IT |
| | | Full | The organisation builds resilience against cyber-attack and systems failure into the design, implementation, operation and management of systems that support the operation of DER. |
| | B.5c Backups | Foundational | Regular backups taken and securely stored |
| | | Light | Automated backups are taken and regularly tested |

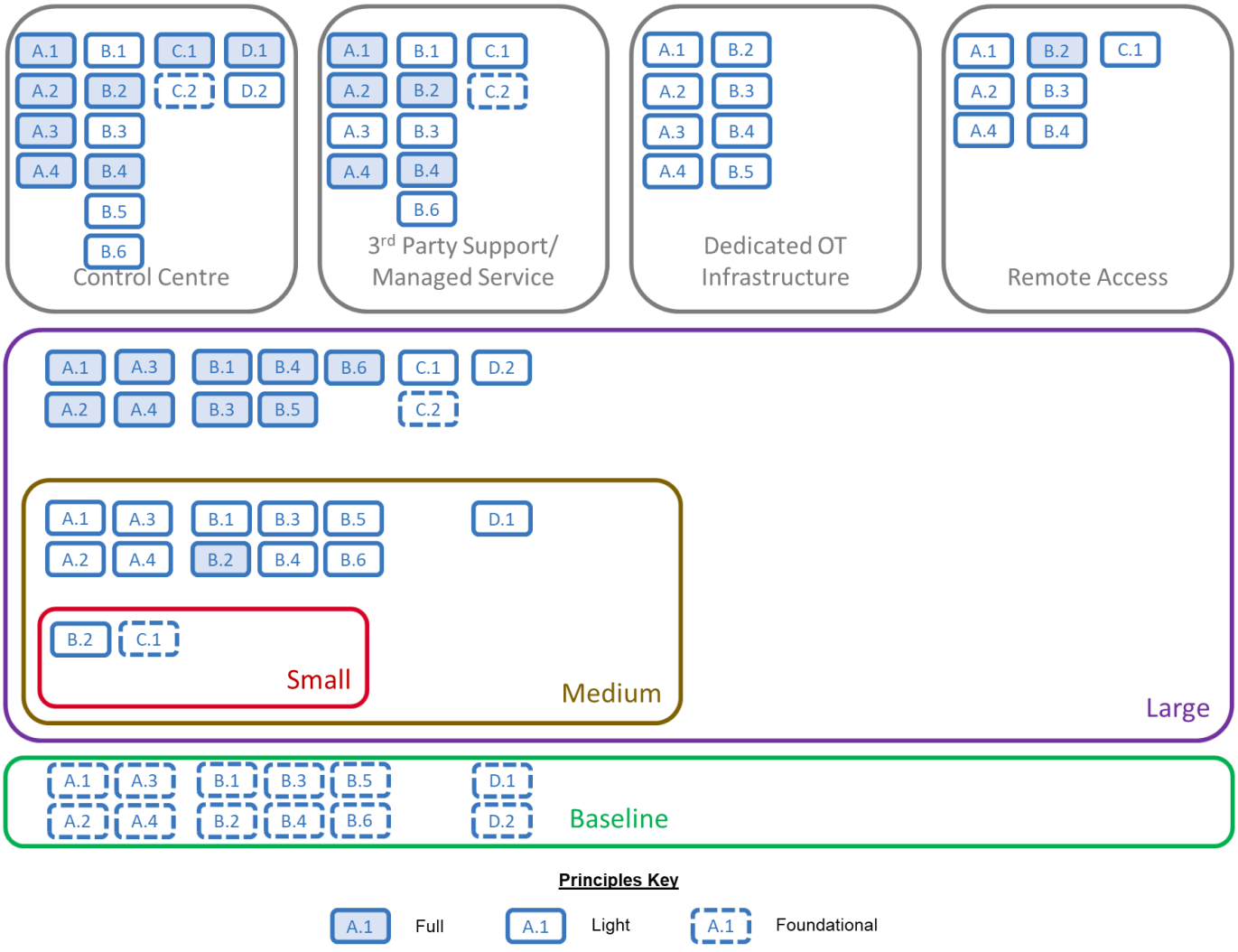
| | | | |
|---|---|---|---|
| | | Full | Backups and restore procedures routinely tested. Backups held off site. People and roles are also duplicated. |
| B.6 Staff Awareness and Training | B.6a Cyber security culture | Foundational | All staff understand their roles and responsibilities with respect to the DER. |
| | | Light | Clear security communications and announcements. Staff understand how to raise a security issue |
| | | Full | Staff have appropriate awareness and knowledge to carry out their organisational roles effectively in relation to the security of the DER. Issues are routinely reported with any concerns being taken seriously |
| | B.6b Cyber security training | Foundational | Cyber security information is easily available |
| | | Light | Training is defined using a range of techniques. Regular refresher training for staff. |
| | | Full | Staff have appropriate knowledge and skills to carry out their organisational roles effectively in relation to the security of the DER. Training is easily accessible and tracked. |
| **Objective C Detecting cyber security events** | **Contributing Outcomes** | **CSCG Tiers** | |
| C.1 Security Monitoring | C.1a Monitoring coverage | Foundational | Basic monitoring of DER functionality and availability. |
| | | Light | Full monitoring of DER functionality and availability.<br>Basic logging and auditing of user actions. |
| | | Full | The organisation monitors the security status of the DER in order to detect potential security problems and to track the ongoing effectiveness of protective security measures. |
| | C.1b Securing logs | Foundational | Only authorised staff have access to the logging information |
| | | Light | Access to logging information is monitored |
| | | Full | The integrity of logging data is protected such that information cannot be modified or deleted. |
| | C.1c Generating alerts | Foundational | Alerts from third party security software are investigated. The resolution of alerts is performed regularly |
| | | Light | Logs are monitored with alerts raised where specific entry types are present |
| | | Full | Logs and systems are monitored continuously. Alerts are tested to ensure they are genuinely reliable and not false alarms. |
| | C.1d Identifying security incidents | Foundational | Regular checks with related threat intelligence sources. Regular updates for Anti-virus tools |
| | | Light | Automatic updates for AV and IDS technologies are applied in a timely way. |
| | | Full | Monitoring and threat intelligence updates are kept up to date and their effectiveness tracked. |

| | | | |
|---|---|---|---|
| | C.1e Monitoring tools and skills | Foundational | Monitoring staff are capable of following most of the required workflows and the tools can make use of some logging information |
| | | Light | Monitoring tools can capture most unsophisticated and untargeted attacks. |
| | | Full | Monitoring staff are empowered to look beyond the alerts and investigate non-standard threats. |
| C.2 Proactive Security Event Discovery | C.2a System abnormalities for attack discovery | Foundational | Monitoring for activity that deviates from normal. |
| | | Light | System abnormality descriptions from past attacks are used to monitor for malicious activity |
| | | Full | The system abnormalities searched for consider the nature of attacks likely to impact on DER operation |
| | C.2b Proactive attack discovery | Foundational | Routine checking for system abnormality that may indicate malicious activity |
| | | Light | Designing of custom 'trip-wires' for the DER assets. |
| | | Full | The organisation detects malicious activity affecting, or with the potential to affect, the operation of DER even when the activity evades standard signature based security prevent/detect solutions. |
| **Objective D Minimising the impact of cyber security incidents** | **Contributing Outcomes** | **CSCG Tiers** | |
| D.1 Response and Recovery Planning | D.1a Response plan | Foundational | Existence of a documented incident response and recovery plan. |
| | | Light | Use of the NCSC '10 Steps: Incident Management' guidance. |
| | | Full | The response plan is comprehensive and covers likely impacts of both known and unknown tacks. The plan is communicated throughout the business |
| | D.1b Response and recovery capability | Foundational | Resources required to undertake response activities are identified. |
| | | Light | Use of the NCSC '10 Steps: Incident Management' guidance. |
| | | Full | There are well-defined and tested incident management processes in place to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place. |
| | D.1c Testing and exercising | Foundational | Exercise scenarios are documented, regularly reviewed and validated |
| | | Light | Exercises are based on incidents experienced by varying organisations or from threat intelligence |
| | | Full | There are well-defined and tested incident management processes in place, to ensure continuity of DER functions in the event of system or service failure. |

| | | | |
|---|---|---|---|
| D.2 Lessons Learned | D.2a Incident root cause analysis | Foundational | Root cause analysis is conducted routinely as a key part of lessons learned activities |
| | | Light | Root cause analysis is comprehensive and covers both technical and process. |
| | | Full | All relevant incident data is made available to the analysis team for root cause analysis |
| | D.2b Using incidents to drive improvements | Foundational | There is a documented incident review process to identify lessons learned |
| | | Light | Lessons learned are used to improve security measures |
| | | Full | Analysis is fed back to senior management and included in risk management and continuous improvement |

Figure 3 shows how the CAF Principles and CSCG tiers should be applied to each of the CSCG security groups.

**Figure 3 Mapping the CAF and CSCG tiers to CSCG Security Groups**



This mapping is suggested as a minimum level of cyber security protection and is aimed at helping organisation manage the cyber security risk. It will not, on its own, eliminate that risk. Moving up through the foundational, light and full levels indicates a growing cyber security maturity and should be aspired to by all organisations, whatever their size, as this will reduce their overall cyber security risk level.

# 4 Guidance

It is important that the CSCG guidelines are applied as part of a risk-based approach to cyber security. The CSCG set of guidelines are outcome based and enable users to implement the most appropriate controls for them in order to arrive at the outcome. The outcomes from this guidance are based on the NCSC CAF Indicators of Good Practice (IGP). Alignment with the CAF provides a consistent approach with the NIS regulations and across the electricity sector as a whole.

This section provides details of the applicability of the guidelines and key terms used within them.

## 4.1 Application of the CSCG guidelines

All DER assets in should be installed and operated with a suggested minimum standard of appropriate cyber security resilience. The CSCG guidelines have been produced to reflect the level of cyber security resilience that is recommended of any new DER connecting to the distribution networks today.

It is recommended that the CSCG guidelines should be implemented for all DER connections and with consulation between the DER operator, DNO and any third party service providers.

The cyber security connection guidelines are written as outcomes so that they are flexible enough to be applied to any DER related infrastructure or organisation. They will allow the users to effectively manage the risks associated with the most common and likely threats.

It is recommended that organisations review the outcomes given in the guidelines and tailor their cyber security controls to the most proportionate and appropriate for their environment. The tailoring of the guidelines and controls should be carried out by people with an understanding of cyber security and its application for power and industrial control systems.

## 4.2 Key terms used within the CSCG guidelines

The following provides a description of key terms used within the CSCG guidelines which are described to aid understanding of the language.

**Table 4 Terms used within the CSCG guidelines**

| Term | Description |
|---|---|
| Where available | Refers to a configuration setting or control that is available as part of the standard technology or process that needs to be configured and turned on. |
| Where feasible | Refers to either a customisation or additional work to provide a configuration or control where one does not exist as standard. |
| Should | Signifies a strong recommendation to do something. |

# 5 Using the CSCG guidelines

This section explains the process for selecting the applicable security groups and applying the appropriate guidelines.

## 5.1 Identify the CSCG security groups

The first stage of applying this guidance is to identify the groups that your organisation falls under. This section should be read in conjunction with section 3.3 (Determining the CSCG security group) of this guidance, but the key points to note when doing this are as follows:

- All organisations using this guidance will fall into the baseline group. This is seen as a suggested minimum level of cyber security activity and applies regardless of your organisation size or function.
- If your organisation is in direct ownership or control of DER assets, you should select the most appropriate group based on the cumulative size of the DER assets within your organisation (not on a site by site basis).
- If your organisation operates a control centre for DER assets, whether all owned by you or you offer a control centre service to others, you should apply the guidelines contained in the "Control Centre" group.
- If your organisation provides a managed service, maintenance or support for DER assets, you should apply the guidelines contained in the "3rd Party Support/Managed Service" group.
- If your organisation has its OT separate from its corporate IT, you should apply the guidelines contained in the "Dedicated OT Infrastructure" group.
- If your organisation uses remote access to manage, control or support your DER assets, you should apply the guidelines contained in the "Remote Access" group.

As you work through these groups, the guidelines you should aim to apply are cumulative in nature (A Medium DER applies both the Baseline, Small and Medium guidelines) although there will be some overlap and commonality between the groups.

## 5.2 Select guidelines

Once the CSCG security groups have been identified, the individual guidelines can be obtained from the appropriate tables in Section 6 of this guidance.

These guidelines should be seen as a suggested minimum level of control that should be applied to DER assets within your organisation, and it is encouraged to look at ways of improving your cyber security maturity by also looking at adopting some or all of the guidelines from the higher groups.

## 5.3 Worked Example

To aid in the understanding of the group selection, this worked example aims to walk through the process.

**Organisation**: single site DER operating solar arrays and 2 x SMA MV power station units for a total maximum capacity of 10MW. Control and monitoring is outsourced to a service provider.

**DER Groups**: The following CSCG groups would be applicable for this organisation.

- Baseline: All organisations have the baseline group as a minimum.
- Small DER: At 10MW and single site, this puts the organisation in the "Small" DER Group

- Additional Groups: As all the day to day control and monitoring is outsourced, the DER organisation will only require the “Remote Access” additional group on their part.

Whilst the DER group is not responsible for the managed service provider and their cyber security controls, it would be highly recommended that when appointing a service provider, checks are made regarding the controls in place – these guidelines can be used to inform those checks.

**DER Guidelines**: Based on the DER groups, the following guideline tables would apply

- Baseline: Table 5 Baseline guidelines
- Small DER: Table 6 Small DER guidelines
- Additional Groups: Table 12 Remote access guidelines

**Service Provider Groups**: The following CSCG groups would be applicable for the service provider.

- Baseline: All organisations have the baseline group as a minimum.
- Additional Groups: As the primary function of the service provider is control and monitoring, the “Control Centre” additional group would apply here. Potentially the “Remote access” and “Dedicated OT Infrastructure” may also apply depending on their setup.

The Managed Service Provider would be responsible for following the guidelines for their systems.

**Service Provider Guidelines**: Based on the Service Provider groups, the following guideline tables would apply (Brackets denote the ‘potential’ groups depending on their setup).

- Baseline: Table 5 Baseline guidelines
- Additional Groups: Table 9 Control centre guidelines, (Table 11 Dedicated OT guidelines), (Table 12 Remote access guidelines)

## 5.4 Implementation

Due to the wide range of technologies and architectures that exist for DER, this guidance does not aim to provide step by step instructions on how to implement a particular guideline. Each operator is empowered to enact the guidelines using the most proportionate and appropriate controls for their environment.

## 5.5 Assurance

Following this guidance will not guarantee that an organisation is 100% safe from a cyber attack. Correctly implemented guidelines will lower the risk of compromise, however, the residual risk levels for each organisation will vary.

In order to better understand your residual risk after the guidelines have been implemented, the controls should be appropriately tested to ensure there are operating correctly. Testing options range from internal testing of specific controls through to penetration testing by independent security consultants.

Assurance activities should be carried out as a regular exercise and not just as part of the initial build and connection.

Certification against named standards, for example, ISO 27001 or IEC 62443, is possible and may help with ongoing assurance, but this document does not require this to be implemented.

# 6 Cyber security connection guidelines

This section contains the CSCG guidelines which have been grouped in accordance with the CSCG Security Groups described earlier in this guidance.

These guidelines are based on an interpretation of the NCSC CAF with the aim of suggesting ways for DER organisations to achieve the outcomes specified in the CAF and IGP. The guidelines for each principle are grouped such that all of the CAFs contributing outcomes are included.

The information in this section can be augmented with details of common technical controls given in Appendix B of this document.

## 6.1 Baseline guidance

The following guidelines form the baseline guidance that all DER owners/operators should be aiming to implement. They are aimed at enabling a suggested minimum level of cyber security and resilience, whilst remaining cost effective and achieveable.

**Table 5 Baseline guidelines**

| Baseline DER | |
|---|---|
| Managing security risk (CAF Objective A) | The foundational layers for managing security risk (CAF principles A.1 to A.4) focus around the following guidelines:<br>– A security policy should be created, to cover the DER assets, that is owned by senior management and defines elements such as:<br>o Lines of responsibility<br>o Accountability for security<br>– A risk management policy and process should be created to aid in the identification, assessment, prioritisation and management of security risks<br>– Regular assessments of risks to the DER assets should be carried out<br>– Security measures should be regularly checked to ensure that they remain effective<br>– A list of DER assets such as inverters, controllers, firewalls and networking, should be created, regularly maintained and held securely that contains:<br>o Asset name<br>o Asset type<br>o Model number<br>o Serial number<br>o Location<br>o Owner<br>o Support arrangements<br>– Dependencies between assets should be known and recorded.<br>– Selection of equipment from trusted sources<br>– There should be awareness of each third-party supplier necessary for the operation of the DER, such as:<br>o Equipment manufacturers<br>o Equiment support providers<br>o Software vendors<br>o Outsourced functions and services<br>o Anyone with remote access to the DER or its associated systems |

| | |
|---|---|
| Protecting against cyber attack (CAF Objective B) | The foundational layers for protecting against cyber attack (CAF principles B.1 to B.6) focus around the following guidelines:<br>– The security policy along with the risk management policy and process should be documented (as covered under 'Managing Security Risk' above). It should be practical, appropriate and achievable.<br>– Policies and process should be routinely reviewed and updated to ensure that they remain relevant<br>– All staff should be aware of their responsibilities under all of the policies in place and be aware of any consequences of non-compliance<br>– All DER assets should be protected with a username and secure password<br>– All default passwords should be changed<br>– All remote access users should be individually authenticated<br>– Where feasible, all DER assets should be located in a secured cabinet or building to prevent easy physical access by unauthorised people<br>– Locks should be appropriate to the security level of the asset being protected<br>– Administration accounts should not be used for directly browsing the web or accessing email<br>– Only authorised devices should be able to connect to any network associated with the DER assets<br>– All data important to the function of the DER should be located and recorded<br>– All entities that have access to important DER data should have been identified and recorded<br>– All data being transmitted over a network should be done using a secure protocol or through an encrypted tunnel (e.g. HTTPS, TLS or IPsec)<br>– Modern cryptographic tools and ciphers should be used<br>– Secure communications should be terminated on modern, patched devices/software<br>– All data at rest should be protected from unauthorised access, modification or deletion<br>– Data held on mobile devices should be recorded and appropriately protected from unauthorised access, modification or deletion<br>– DER assets should be protected from unsecured networks using an appropriate firewall<br>– Untrusted remote connections to the DER should be limited<br>– Connections between co-located devices and remote management systems should be secured<br>– DER assets that require careful configuration to maintain their security should be identified and recorded<br>– All DER assets should be protected from forms of malware using appropriate anti-malware software and boundary protection such as content inspection firewalls<br>– Management interfaces should not be exposed to untrusted networks<br>– All software related to the DER should be regularly patched and updated<br>– Firmware patches and updates should be managed appropriately to the risk levels they hold<br>– Regular backups should be taken for all DER assets<br>– The recovery procedure following an incident should be documented and maintained |

| | |
|---|---|
| Minimising the impact of cyber security incidents (CAF Objective D) | The foundational layers for minimising the impact of cyber security incidents (CAF principles D.1 and D.2) focus around the following guidelines:<br>– The incident response and recovery plan should be documented and maintained and should cover all essential DER functions<br>– Details of suspected incidents, including remedial actions taken, should be routinely collected and recording to allow for basic root cause analysis to take place |

## 6.2 Small DER guidance

The following guidelines describe the additional steps a Small DER organisation should aim to implement over and above those descibed as being part of the baseline.

**Table 6 Small DER guidelines**

| Small DER | |
|---|---|
| Protecting against cyber attack (CAF Objective B) | The guidelines for detecting cyber security events (CAF principle B.2) is increased to the 'Light' level for Small DER and now focuses around the following additional guidelines:<br>– All users should have individual user IDs<br>– Where possible, operators should have separate accounts from administrative users<br>– Users should be granted the minimum level of access required by their job responsibilities<br>– Users and permissions should be routinely validated to ensure they are still required and correct<br>– Where available, 2-factor authentication should be applied to user accounts<br>– Unauthorised devices connected to the DER networks should be detected and investigated<br>– Only permitted software should be allowed to be installed in the DER environment<br>– Unused physical ports should be disabled and unused software removed.<br>– There should be a separation of duties between different administration zones, e.g. systems, networks, etc.<br>– Privileged user access should require additional validation<br>– All user access should be logged and monitored |
| Detecting cyber security events (CAF Objective C) | The foundational layers for detecting cyber security events (CAF principle C.1) focus around the following guidelines:<br>– Monitoring for DER functionality and availability should be carried out to identify when things are not operating correctly<br>– Traffic crossing the network boundary should be monitored (IP addresses and connections)<br>– Alerts from monitoring tools should be investigated and action taken<br>– Operations staff dealing with the monitoring should be suitably skilled in the steps to carry out for detected incidents<br>– Threat intelligence services should be regularly checked (even if manually) to identify potential vulnerabilities |

## 6.3 Medium DER guidance

The following guidelines describe the additional steps a Medium DER organisation should aim to implement over and above those descibed as being part of the baseline and Small DER guidelines.

**Table 7 Medium DER guidelines**

| Medium DER | |
|---|---|
| Managing security risk (CAF Objective A) | The guidelines for managing security risk (CAF principles A.1 to A.4) are increased to the 'Light' level for Medium DER and now focuses around the following additional guidelines:<br>– The security policy and risk management policy should be managed at the senior management level, with clear governance structures and communicated to all staff<br>– Security related job roles and responsibilities should be identified and periodically reviewed<br>– There should be clarity on who in the organisation is responsible for security and risk management<br>– Risk management decisions should be periodically reviewed to ensure they stay relevant<br>– The NCSC Risk Management Guidance should be consulted to help choose an approach that is right for the organisation<br>– The risk management approach should consider the threats, vulnerabilities and impacts to the DER assets<br>– Risk assessments should be informed by an understanding of the vulnerabilities with technology supporting the DER<br>– Threat analysis should be carried out so that generic threats to the DER can be understood<br>– There should be an understanding of the assurance methods available and how to use them to gain confidence in the security of the DER<br>– There should be an understanding of the general risks suppliers may pose to the DER<br>– Suppliers should be engaged with regarding security, including the communication of security requirements in contracts<br>– Using a single supplier for all DER equipment should be avoided<br>– There should be confidence that information shared with suppliers to support the DER is properly protected from well known attacks and vulnerabilities |
| Protecting against cyber attack (CAF Objective B) | The guidelines for protecting against cyber attack (CAF principles B.1, B.3 to B.6) are increased to the 'Light' level for Medium DER and now focuses around the following additional guidelines:<br>– Policies and processes should be updated in response to major cyber security incidents<br>– The application of policies and processes should be monitored<br>– Secure backup should be taken regularly to enable continued operation should something happen to the live data<br>– All devices that contain important DER data should be catalogues and tracked<br>– The DER systems and networks should be designed by someone with training and experience of designing DER systems<br>– Data flows between systems should be designed to be simple to enable effective security monitoring<br>– All inputs to the DER systems should be checked and validated at the network boundary where possible |

| | |
|---|---|
| | – Secure platform and device builds should be used where available<br>– Device configurations across the same types of evironment should be consistant, secure and minimal<br>– Software and firmware should be verified prior to installation<br>– Details about publicly-known vulnerabilities for any of the DER equipment of systems should be routinely tracked, prioritised and mitigated<br>– Regular vulnerability testing should be carried out to understand the risk to the DER<br>– Operational technology and systems related to the DER should be logically separated from the business IT systems (e.g. by the use of firewalls, Demilitarised Zones (DMZs), etc.)<br>– Resource limitations such as network bandwidth and single network paths should be identified<br>– Backups should be routinely tested to ensure they are usable<br>– All staff should receive appropriate security training for their role, which includes knowing who to contact in the case of a suspected incident<br><br>The guidelines for protecting against cyber attack (CAF principle B.2) is increased to the 'Full' level for Medium DER and now focuses around the following additional guidelines:<br>– The list of users with access to the DER should be reviewed on a regular basis, at a minimum every 6 months<br>– There should be dedicated devices used for privileged actions (such as administration). Such device should not be used for directly browsing the web or accessing email<br>– There should be independent and professional assurance of the security of third-party devices before they connect to the DER<br>– Where feasible, there should be certificate based device identity management in place and only known devices are allowed to connect<br>– Access control systems should be compatible with time-bound, single use passwords<br>– Privileged user activity should be routinely reviewed, validated and recorded for offline analysis<br>– Where appropriate, staff with privileged access should be vetted |
| Minimising the impact of cyber security incidents (CAF Objective D) | The guidelines for minimising the impact of cyber security incidents (CAF principle D.1) is increased to the 'Light' level for Medium DER and now focuses around the following additional guidelines:<br>– The NCSC guidance: "10 Steps: Incident Management" should be used to improve and refine the incident response plan<br>– The incident response plan should include the likely impacts of well known and well understood attacks<br>– The incident response plan should be shared with, and understood by, all relevent staff<br>– Backup mechanisms should be available and readily activated to allow continued operation of the DER<br>– The incident response plan should be regularly reviewed, and tests should be run to verify the scenarios. Findings should be documented and used to refine the plan |

## 6.4 Large DER guidance

The following guidelines describe the additional steps a 'Large' DER organisation should aim to implement over and above those descibed as being part of the baseline, 'Small' and 'Medium' DER guidelines.

**Table 8 Large DER guidelines**

| Large DER | |
|---|---|
| Managing security risk (CAF Objective A) | The guidelines for managing security risk (CAF principles A.1 to A.4) are increased to the 'Full' level for Large DER and now focuses around the following additional guidelines. Often this is covered as part of an industry recognised security management system:<br>– Staff should be given the time, authority and resources to be able to carry out their duties effectively<br>– The approach to risk should be based on the possibility of adverse impact to the DER, leading to a detailed understanding of how such impact might arise as a consequence of a possible attacker and the security properties of the DER networks and information systems<br>– Risk assessments should be based on a clear understanding of threat assumptions and security threats towards the DER<br>– The ouptut of the risk management process should be a clear set of security requirements to address the risks identified<br>– Risk assessments should be conducted whenever significant events potentially affect the DER<br>– Detailed threat analysis should be carried out to understand the risks faced in the context of DER and the wider electricity sector<br>– Security measures should be regularly tested to ensure that they remain effective<br>– Security deficiencies identified during testing should be assessed, prioritised and remedied where necessary in a timely and effective way<br>– DER assets should be managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal |
| Protecting against cyber attack (CAF Objective B) | The guidelines for protecting against cyber attack (CAF principles B.1, B.3 to B.6) are increased to the 'Full' level for Large DER and now focuses around the following additional guidelines:<br>– Policies and processes should be reviewed and updated at regular intervals to ensure they remain relevant. This is in addition to reviews carried out following a cyber security incident<br>– Any changes to the DER function or the threat it faces should trigger a review of policies and processes<br>– Systems should be designed such that they remain secure even when user security policies and processes are not always followed<br>– Appropriate action is taken to address breaches of policies and processes that have the potential to adversely affect the DER<br>– There should be understanding and documentation of the impact on the DER of all relevent scenarios, including unauthorised data access, modification or deletion, or when authorised users should be able to appropriately access this data<br>– Impact statements should be validated regularly<br>– All data links that carry important DER data should have been identified and protected (effectively and proportionately)<br>– Any necessary historic or archived data should be secured in storage |

| | |
|---|---|
| | – Mobile devices that may hold important DER data should be secured according to good practice for the platform with appropriate technical and procedures in place<br>– All data important to the DER should be sanitised from all devices and media before disposal<br>– Networks and information systems related to the DER should be designed to be easy to recover<br>– Changes to the DER environment should be effectively managed and assured<br>– The configuration and security settings of DER assets should be regularly checked and verified |
| Detecting cyber security events (CAF Objective C) | The foundational layers for detecting cyber security events (CAF principle C.2) focus around the following guidelines:<br>– System abnormality descriptions from past attacks and threat intelligence should be used to configure monitoring to identify malicious activity.<br>The guidelines for detecting cyber security events (CAF principle C.1) is increased to the 'Light' level for Large DER and now focuses around the following additional guidelines:<br>– To detect the presence of indicators of compromise should be part of standard practice and should look for known malicious command and control signatures<br>– Basic user monitoring should be carried out<br>– CCTV should be used to deter and monitor physical access<br>– Only authorised privileged users should be able to access and analyse logging data<br>– Security alerts from key DER systems are received and prioritised for remedial action<br>– Logs should be reviewed regularly to look for indicators of compromise<br>– Threat intelligence agencies are used to provide data and threat signatures to monitoring tools |
| Minimising the impact of cyber security incidents (CAF Objective D) | The guidelines for minimising the impact of cyber security incidents (CAF principle D.2) is increased to the 'Light' level for Large DER and now focuses around the following additional guidelines:<br>– Root cause analysis should be conducted following each incident<br>– The results of the root cause analysis should be used to improve security measures and monitoring as well as be fed into the risk management process |

## 6.5 Control centre guidance

The following guidelines describe the additional steps an organisation running their own control centre for DER should aim to implement over and above those described as being part of the baseline, 'Small' and 'Medium' DER guidelines. For organisations without any of their own generation/storage assets (such as managed control centres or aggregators) these guidelines will apply.

**Table 9 Control centre guidelines**

| Control Centre | |
|---|---|
| Managing security risk (CAF Objective A) | The guidelines for managing security risk (CAF principles A.1 to A.4) are increased to the 'Full' level for control centres and now focuses around the following additional guidelines. Often this is covered as part of an industry recognised security management system:<br>– Staff in the identified necessary roles should be given the time, authority and resources to be able to carry out their duties<br>– The approach to risk should be based on the possibility of adverse impact to the DER, leading to a detailed understanding of how such impact might arise as a consequence of a possible attacker and the security properties of the DER networks and information systems<br>– Risk assessments should be based on a clear understanding of threat assumptions and security threats towards DER<br>– The output of the risk management process should be a clear set of security requirements to address the risks identified<br>– Risk assessments should be conducted whenever significant events potentially affect the DER<br>– Detailed threat analysis should be carried out to understand the risks faced in the context of DER and the wider electricity sector<br>– Security measures should be regularly tested to ensure that they remain effective<br>– Security deficiencies identified during testing should be assessed, prioritised and remedied where necessary in a timely and effective way<br>DER assets should be managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal |
| Protecting against cyber attack (CAF Objective B) | The guidelines for protecting against cyber attack (CAF principles B.2 and B.4) are increased to the 'Full' level for control centres and now focuses around the following additional guidelines:<br>– The list of users with access to the DER should be reviewed on a regular basis, at a minimum every 6 months<br>– There should be dedicated devices used for privileged actions (such as administration). Such device should not be used for directly browsing the web or accessing email<br>– There should be independent and proffessional assurance of the security of third-party devices before they connect to the DER<br>– Where feasible, there should be certificate based device identity management in place and only known devices are allowed to connect<br>– Access control systems should be compatible with time-bound, single use passwords<br>– Privileged user activity should be routinely reviewed, validated and recorded for offline analysis. Networks and information systems related to the DER should be designed to be easy to recover<br>– Changes to the DER environment should be effectively managed and assured |

| | |
|---|---|
| | – The configuration and security settings of DER assets should be regularly checked and verified<br><br>The guidelines for protecting against cyber attack (CAF principles B.1, B.3, B.5 and B.6) are increased to the 'Light' level for control centres and now focuses around the following additional guidelines:<br>– Policies and processes should be updated in response to major cyber security incidents<br>– The application of policies and processes should be monitored<br>– Secure backup should be taken regularly to enable continued operation should something happen to the live data<br>– All devices that contain important DER data should be catalogued and tracked<br>– The DER systems and networks should be designed by someone with appropriate expertise<br>– Data flows between systems should be designed to be simple to enable effective security monitoring<br>– All inputs to the DER systems should be checked and validated at the network boundary where possible<br>– Secure platform and device builds should be used where available<br>– Device configurations across the same types of evironment should be consistant, secure and minimal<br>– Software and firmware should be verified prior to installation<br>– OT and systems related to the DER should be logically separated from the business IT systems (e.g. by the use of firewalls, DMZs, etc.)<br>– Resource limitations such as network bandwidth and single network paths should be identified<br>– Backups should be routinely tested to ensure they are usable<br>– All staff should recieve appropriate security training for their role, which includes knowing who to contact in the case of a suspected incident. |
| Detecting cyber security events (CAF Objective C) | The foundational layers for detecting cyber security events (CAF principle C.2) focus around the following guidelines:<br>– System abnormality descriptions from past attacks and threat intelligence should be used to configure monitoring to identify malicious activity.<br><br>The guidelines for detecting cyber security events (CAF principles C.1) is increased to the 'Full' level for control centres and now focuses around the following additional guidelines:<br>– Monitoring data should provide enough detail to reliably detect security incidents that could affect the operation of the DER<br>– Monitoring coverage should include both host based monitoring and network gateways<br>– The integrity of logs is protected, log modifications are detected and attributed<br>– Logging systems should be synchronised to an accurate, common time source<br>– Threat intelligence feeds should be automated, where feasible, or installed into the monitoring tools within a reasonable (risk-based) time of receiving them<br>– Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats |

| | |
|---|---|
| Minimising the impact of cyber security incidents (CAF Objective D) | The guidelines for minimising the impact of cyber security incidents (CAF principle D.1) is increased to the 'Full' level for organisations running control centres and now focuses around the following additional guidelines:<br>– The incident response plan should be based on a clear understanding of the security risks to the DER<br>– The resources required to carry out any response activities should be understood and arrangements should be in place to make these resources available<br><br>The guidelines for minimising the impact of cyber security incidents (CAF principle D.2) is increased to the 'Full' level for organisations running control centres and now focuses around the following additional guidelines:<br>– Security improvements identified as a result of lessons learned ae prioritised, with the highest priority items comleted quickly<br>– Root cause analysisis comprehensive, covering organisational process issues, as well as vulnerabilities in your networks, systems or software |

## 6.6 Third-party guidance

The following guidelines describe the additional steps an organisation operating as a managed service, support/warranty provider or maintenance provider for DER should aim to implement over and above those descibed as being part of the baseline, 'Small' and 'Medium' DER guidelines. For organisations without any of their own generation/storage assets (such as equipment manufacturers or managed services) these guidelines will apply.

**Table 10 Third-party guidelines**

| Third-Party | |
|---|---|
| Managing security risk (CAF Objective A) | The guidelines for managing security risk (CAF principles A.1, A.2 and A.4) are increased to the 'Full' level for large DER and now focuses around the following additional guidelines. Often this is covered as part of an industry recognised security management system:<br>– Staff in the identified necessary roles should be given the time, authority and resources to be able to carry out their duties<br>– The approach to risk should be based on the possibility of adverse impact to the DER, leading to a detailed understanding of how such impact might arise as a consequence of a possible attacker and the security properties of the DER networks and information systems<br>– Risk assessments should be based on a clear understanding of threat assumptions and security threats towards DER<br>– The output of the risk management process should be a clear set of security requirements to address the risks identified<br>– Risk assessments should be conducted whenever significant events potentially affect the DER<br>– Detailed threat analysis should be carried out to understand the risks faced in the context of DER and the wider electricity sector<br>– Security measures should be regularly tested to ensure that they remain effective<br>– Security deficiencies identified during testing should be assessed, prioritised and remedied where necessary in a timely and effective way<br><br>The guidelines for managing security risk (CAF principle A.3) is increased to the 'Light' level for organisations with third-parties or managed services and now focuses around the following additional guidelines: |

| | |
|---|---|
| | – There should be an understanding of the general risks suppliers may pose to the DER |
| Protecting against cyber attack (CAF Objective B) | The guidelines for protecting against cyber attack (CAF principles B.2 and B.4) are increased to the 'Full' level for organisations with third-parties or managed services and now focuses around the following additional guidelines:<br>– The list of users with access to the DER should be reviewed on a regular basis, at a minimum every 6 months<br>– There should be dedicated devices used for privileged actions (such as administration). Such device should not be used for directly browsing the web or accessing email<br>– There should be independent and proffessional assurance of the security of third-party devices before they connect to the DER<br>– Where feasible, there should be certificate based device identity management in place and only known devices are allowed to connect<br>– Access control systems should be compatible with time-bound, single use passwords<br>– Privileged user activity should be routinely reviewed, validated and recorded for offline analysis. Networks and information systems related to the DER should be designed to be easy to recover<br>– Changes to the DER environment should be effectively managed and assured<br>– The configuration and security settings of DER assets should be regularly checked and verified<br><br>The guidelines for protecting against cyber attack (CAF principles B.1, B.3 and B.6) are increased to the 'Light' level for organisations with third-parties or managed services and now focuses around the following additional guidelines:<br>– Policies and processes should be updated in response to major cyber security incidents<br>– The application of policies and processes should be monitored<br>– Secure backup should be taken regularly to enable continued operation should something happen to the live data<br>– All devices that contain important DER data should be catalogued and tracked<br>– The DER systems and networks should be designed by someone with appropriate expertise<br>– Data flows between systems should be designed to be simple to enable effective security monitoring<br>– All inputs to the DER systems should be checked and validated at the network boundary where possible<br>– Secure platform and device builds should be used where available<br>– Device configurations across the same types of evironment should be consistant, secure and minimal<br>– Software and firmware should be verified prior to installation<br>– All staff should recieve appropriate security training for their role, which includes knowing who to contact in the case of a suspected incident |
| Detecting cyber security events (CAF Objective C) | The foundational layers for detecting cyber security events (CAF principle C.2) focus around the following guidelines:<br>– System abnormality descriptions from past attacks and threat intelligence should be used to configure monitoring to identify malicious activity. |

| | |
|---|---|
| | The guidelines for detecting cyber security events (CAF principle C.1) is increased to the 'Light' level for organisations with third-parties or managed services and now focuses around the following additional guidelines:<br>– To detect the presence of indicators of compromise should be part of standard practice and should look for known malicious command and control signatures<br>– Basic user monitoring should be carried out<br>– Only authorised privileged users should be able to access and analyse logging data<br>– Security alerts from key DER systems are received and prioritised for remedial action<br>– Logs should be reviewed regularly to look for indicators of compromise<br>– Threat intelligence agencies are used to provide data and threat signatures to monitoring tools |

## 6.7 Dedicated OT guidance

The following guidelines describe the additional steps an organisation operating their OT isolated from the rest of their IT or corporate network should apply.

**Table 11 Dedicated OT guidelines**

| Dedicated OT | |
|---|---|
| Managing security risk<br>(CAF Objective A) | The guidelines for managing security risk (CAF principles A.1 to A.4) are increased to the 'Light' level for organisations with dedicated Operational Technology and now focuses around the following additional guidelines:<br>– The security policy and risk management policy should be managed at the senior management level, with clear governance structures and communicated to all staff<br>– Security related job roles and responsibilities should be identified and periodically reviewed<br>– There should be clarity on who in the organisation is responsible for security and risk management<br>– Risk management decisions should be periodically reviewed to ensure they stay relevant<br>– The NCSC Risk Management Guidance should have been consulted to help choose an approach that is right for the organisation<br>– The risk management approach should consider the threats, vulnerabilities and impacts to the DER assets<br>– Risk assessments should be informed by an understanding of the vulnerabilities with technology supporting the DER<br>– Threat analysis should be carried out so that generic threats to the DER can be understood<br>– There should be an understanding of the assurance methods available and how to use them to gain confidence in the security of the DER<br>– There should be an understanding of the general risks suppliers may pose to the DER<br>– Suppliers should be engaged with regarding security, including the communication of security requirements in contracts<br>– There should be confidence that information shared with suppliers to support the DER is properly protected from well known attacks and vulnerabilities |

| | |
|---|---|
| Protecting against cyber attack (CAF Objective B) | The guidelines for protecting against cyber attack (CAF principles B.2 to B.5) are increased to the 'Light' level for environments with dedicated OT and now focuses around the following additional guidelines:<br>– All users should have individual user IDs<br>– Where possible, normal users should have separate accounts from administrative users<br>– Users should be granted the minimum level of access required by their job responsibilities<br>– Users and permissions should be routinely validated to ensure they are still required and correct<br>– Where feasible, 2-factor authentication should be applied to user accounts<br>– Unauthorised devices connected to the DER networks should be detected and investigated<br>– Only permitted software should be allowed to be installed in the DER environment<br>– Unused physical ports should be disabled and unused software removed<br>– Privileged user access should require additional validation<br>– All user access should be logged and monitored.<br>– Secure backup should be taken regularly to enable continued operation should something happen to the live data<br>– All devices that contain important DER data should be catalogued and tracked<br>– The DER systems and networks should be designed by someone with appropriate expertise<br>– Data flows between systems should be designed to be simple to enable effective security monitoring<br>– All inputs to the DER systems should be checked and validated at the network boundary where possible<br>– Secure platform and device builds should be used where available<br>– Device configurations across the same types of evironment should be consistant, secure and minimal<br>– Software and firmware should be verified prior to installation<br>– Details about publicly know vulnerabilities for any of the DER equipment of systems should be routinely tracked, prioritised and mitigated<br>– Regular vulnerability testing should be carried out to understand the risk to the DER<br>– Operational technology and systems related to the DER should be logically separated from the business IT systems (e.g. by the use of firewalls, DMZs, etc.)<br>– Resource limitations such as network bandwidth and single network paths should be identified<br>– Backups should be routinely tested to ensure they are usable |

## 6.8 Remote access guidance

The following guidelines describe the additional steps an organisation that allows remote access to their DER should aim to implement over and above those descibed as being part of the baseline, 'Small' and 'Medium' DER guidelines.

**Table 12 Remote access guidelines**

| Remote Access | |
|---|---|
| Managing security risk (CAF Objective A) | The guidelines for managing security risk (CAF principles A.1 to A.4) are increased to the 'Light' level for organisations with remote access and now focuses around the following additional guidelines:<br>– The security policy and risk management policy should be managed at the senior management level, with clear governance structures and communicated to all staff<br>– Security related job roles and responsibilities should be identified and periodically reviewed<br>– There should be clarity on who in the organisation is responsible for security and risk management<br>– Risk management decisions should be periodically review to ensure they stay relevant<br>– The NCSC Risk Management Guidance should have been consulted to help choose an approach that is right for the organisation<br>– The risk management approach should consider the threats, vulnerabilities and impacts to the DER assets<br>– Risk assessments should be informed by an understanding of the vulnerabilities with technology supporting the DER<br>– Threat analysis should be carried out so that generic threats to the DER can be understood<br>– There should be an understanding of the assurance methods available and how to use them to gain confidence in the security of the DER<br>– There should be an understanding of the general risks suppliers may pose to the DER<br>– Suppliers should be engaged with regarding security, including the communication of security requirements in contracts<br>– There should be confidence that information shared with suppliers to support the DER is properly protected from well known attacks and vulnerabilities |
| Protecting against cyber attack (CAF Objective B) | The guidelines for protecting against cyber attack (CAF principles B.3 to B.4) are increased to the 'Light' level for environments with remote access and now focuses around the following additional guidelines:<br>– Secure backups should be taken regularly to enable continued operation should something happen to the live data<br>– All devices that contain important DER data should be catalogued and tracked<br>– The DER systems and networks should be designed by someone with appropriate expertise<br>– Data flows between systems should be designed to be simple to enable effective security monitoring<br>– All inputs to the DER systems should be checked and validated at the network boundary where possible<br>– Secure platform and device builds should be used where available<br>– Device configurations across the same types of evironment should be consistant, secure and minimal |

| | |
|---|---|
| | – Software and firmware should be verified prior to installation<br>– Details about publicly know vulnerabilities for any of the DER equipment of systems should be routinely tracked, prioritised and mitigated<br>– Regular vulnerability testing should be carried out to understand the risk to the DER<br><br>The guidelines for protecting against cyber attack (CAF principle B.2) is increased to the 'Full' level for organisations with remote access and now focuses around the following additional guidelines:<br>– The list of users with access to the DER should be reviewed on a regular basis, at a minimum every 6 months<br>– There should be dedicated devices used for privileged actions (such as administration). Such devices should not be used for directly browsing the web or accessing email<br>– There should be independent and professional assurance of the security of third-party devices before they connect to the DER<br>– Where feasible, there should be certificate based device identity management in place and only known devices are allowed to connect<br>– Access control systems should be compatible with time-bound, single use passwords<br>– Privileged user activity should be routinely reviewed, validated and recorded for offline analysis |
| Detecting cyber security events (CAF Objective C) | The guidelines for detecting cyber security events (CAF principle C.1) is increased to the 'Light' level for organisations with remote access and now focuses around the following additional guidelines:<br>– To detect the presence of indicators of compromise should be part of stadard practice and should look for known malicious command and control signatures<br>– Basic user monitoring should be carried out<br>– Only authorised privileged users should be able to access and analyse logging data<br>– Security alerts from key DER systems are received and prioritised for remedial action<br>– Logs should be reviewed regularly to look for indicators of compromise<br>– Threat intelligence agencies are used to provide data and threat signatures to monitoring tools |

# References

| No. | Source | Document |
|---|---|---|
| 1 | NCSC | NIS Introduction |
| 2 | NCSC | Cyber Assessment Framework |
| 3 | IEC 62443 | Part 2.4: Requirements for an IACS security management system |
| 4 | IEC 62443 | Part 3.3: System security requirements and security levels |
| 5 | IEC 62351 | Security for information exchange in power systems |
| 6 | National Institute of Standards and Technology (NIST) | SP800-82 – Guide to ICS Security |
| 7 | NIST | SP800-53 – Security and Privacy Controls for information systems and organisations |
| 8 | NIST | Framework for improving critical infrastructure |
| 9 | ANSSI | Cyber security for industrial control systems |
| 10 | Health and Safety Executive (HSE) | OG0086 – Supplimentary guidance in addition to the CAF |
| 11 | IEEE 1547 – Family of standards for interconecting DERs to distribution Grids | G98 and G99 for the UK connection codes |
| 12 | National Renewable Energy Laboratory (NREL) | DER Cyber Security Standards |
| 13 | NREL | An overview of DER interconnection: Current practices and emerging solutions |
| 14 | Sandia National Laboratories | Cyber security primer for DER vendors, aggregators and grid operators |
| 15 | International Standards Organisation (ISO) | ISO 27019 – ISO 27002 applied to process control systems in the energy industry |

# Glossary

| Acronym | Definition |
|---|---|
| BEIS | Department for Business, Energy and Industrial Strategy |
| CAF | Cyber Assessment Framework |
| CCTV | Closed Circuit Television |
| CNI | Critical National Infrastructure |
| CPNI | Centre for the Protection of National Infrastructure |
| CREST | International accreditation and certification body for technical information security |
| DCS | Distributed Control System |
| DER | Distributed Energy Resources |
| CSCG | Cyber Security Connection Guidance |
| DG | Distributed Generation |
| DMZ | De-Militarised Zone |
| DNO | Distributed Network Operator |
| DNP3 | Distributed Network Protocol v3 |
| DSO | Distribution Service Owner / Distribution System Operator |
| E3CC | Energy Emergencies Executive Cyber Security Task Group |
| ENA | Energy Networks Association |
| ESO | Electricity Systems Operator |
| GDPR | General Data Protection Regulations |
| GW | Gigawatts |
| HSE | Health and Safety Executive |
| HTTPs | HyperText Transfer Protocol |
| ICS | Industrial Control Systems |
| IGP | Indicators of Good Practice |
| IPSec | Internet Protocol Security |
| IT | Information Technology |
| MW | Megawatts |
| NCSC | National Cyber Security Centre |
| NIS | Network and Information Systems |
| NIST | National Institute of Standards and Technology |
| OES | Operators of Essential Services |
| OT | Operational Technology |
| PV | Photovoltaic |
| SCADA | Supervisory Control and Data Acquisition |
| SOC | Security Operations Centre |
| SSFP | Smart Systems and Flexibility Plan |
| SSH | Secure Shell |
| TCP/IP | Transmission Control Protocol / Internet Protocol |
| TLS | Transport Layer Security |
| UK | United Kingdom |
| UPS | Uninterruptible Power Supply |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |

# Appendices

# A. NCSC CAF Principles

A high-level summary of details of the NCSC Cyber Assessment Framework (CAF) objectives and principles is provided in Table 13.

This table contains a high level summary of the CAF guidance for each principle. For more comprehensive information on any part of the CAF, please see the NCSC website: https://www.ncsc.gov.uk/collection/caf

**Table 13 CAF Objectives and Principles**

| | |
|---|---|
| **Objective A: Managing Security Risk** | **Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services** |
| **A.1 Governance:** | The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.<br>Key security considerations and references relevant to third party:<br>– Approach to managing cyber security<br>– Reference to ISO/IEC 27001:2013, IEC 62443-2-1:2010 |
| **A.2 Risk Management:** | The organisation takes appropriate steps to identify, assess and understand security risks to network and information systems supporting the delivery of essential services. This includes an overall organisational approach to risk management.<br>Key security considerations and references relevant to third party:<br>– Approach to managing cyber security risk<br>– References to NCSC Risk Management Guidance, Risk methods and frameworks, NCSC Penetration Testing guidance and Cloud Security Collection. |
| **A.3 Asset Management:** | Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).<br>Key security considerations and references relevant to third party:<br>– Inventory<br>– System interfaces and dependencies<br>– Reference to ISO/IEC 27001:2013, IEC 62443-2-1:2010, ISO 55001:2014, ITIL |
| **A.4 Supply Chain:** | • The organisation understands and manages security risks to the network and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.<br>• Key security considerations and references relevant to third party:<br>– Reference to NCSC Supply Chain Security, Cloud service security, Principle B.3 |

| **Objective B: Protecting against cyber attack** | **Proportionate security measures are in place to protect essential services and systems from cyber attack** |
|---|---|
| B.1 Service Protection Policies and Processes: | • The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that supports delivery of essential services.<br>• Key security considerations and references relevant to third party:<br>– Communication of policy and procedures<br>– Personnel security<br>– Reference to CPNI Personnel and people security and BS ISO/IEC 27002:2013 Section 5&7, SANS material, IEC/TS 62443-1-1 Section 5.8, BS IEC 62443-2-2:2011 Section 4.3.2.6. |
| B.2 Identity & Access Control: | • The organisation understands, documents and manages access to systems and functions supporting the delivery of essential services. Users (or automated functions) that can access data or services are appropriately verified, authenticated and authorised.<br>• Key security considerations and references relevant to third party:<br>– User, system and device access<br>– Reference to NCSC Introduction to identity and access management, CPNI Physical Security guidance, BS ISO/IEC 27002:2013 section 9, BS IEC 62443-2-1:2011, NIST Identity and Access Management publications, e.g. SP 800-63 suite "Digital Identity Guidelines" |
| B.3 Data Security: | • Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause disruption to essential services. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the delivery of essential services. It also covers information that would assist an attacker, such as design details of networks and information systems.<br>• Key security considerations and references relevant to third party:<br>– Design to protect data<br>– Protecting data in transit<br>– Protect data at rest<br>– Protecting data on mobile devices<br>– Secure disposal<br>– Reference to NCSC 10 Steps: Home and Mobile Working, NCSC End User Device Security Collection, NCSC VPN guidance, NCSC TLS guidance, NCSC cloud security principle 2 on asset protection and resilience, BS ISO/IEC 27002:2013 section 8, BS IEC 62443-2-1:2011 section 4.3.4.4, ENISA Big Data Security (2016) |
| B.4 System Security: | • Network and information systems and technology critical for the delivery of essential services are protected from cyber attack. An organisational understanding of risk to essential services informs the use of robust and reliable protective |

| | |
|---|---|
| | security measures to effectively limit opportunities for attackers to compromise networks and systems.<br>• Key security considerations and references relevant to third party:<br>– System design<br>– Configuration<br>– System management<br>– Vulnerability management<br>– Reference to NCSC Common Cyber Attacks: Reducing the Impact, NCSC Secure by default platforms, NCSC Penetration testing, NCSC Obsolete platforms security guidance, IEC/TS 62443-1-1:2009, BS ISO/IEC 27002:2013 |
| B.5 Resilient Networks & Systems: | • The organisation builds resilience against cyber attack and system failure into the design, implementation, operation and management of systems that support the delivery of essential services.<br>• Key security considerations and references relevant to third party:<br>– Prepare to respond to disruption<br>– Maintenance and repair<br>– Segregation<br>– Capacity<br>– Diversity and dependencies<br>– Working backups<br>– Reference to IEC 62443 |
| B.6 Staff Awareness & Training: | • Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the delivery of essential services.<br>• Key security considerations and references relevant to third party:<br>– Security culture<br>– Communications<br>– Reference to NCSC 10 Steps: User Education and Awareness, CPNI's guidance on developing a security culture, GCHQ certified training scheme |
| **Objective C: Detecting cyber security events** | **Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services** |
| C.1 Security Monitoring: | • The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.<br>• Key security considerations and references relevant to third party:<br>– Detecting incidents or activity<br>– Log collection and aggregation<br>– Analysis and threat intelligence<br>– Protection of personal data and general network performance and service quality<br>– Reference to 10 Steps: Monitoring, NCSC - SOC Buyer's Guide, CREST - Protective Monitoring Guidance, NIST - Continuous Security Monitoring, NIST |

| | |
|---|---|
| | Guide to Intrusion Detection and Intrusion Prevention Systems, ISO 27002 / 27019, IEC 62443 |
| C.2 Proactive Security Event Discovery: | • The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployed).<br>• Key security considerations and references relevant to third party:<br>– Detection capability |
| **Objective D: Minimising the impact of cyber security incidents** | **Capabilities to minimise the impact of a cyber security incident on the delivery of essential services including the restoration of those services where necessary** |
| D.1 Response and Recovery Planning: | • There are well-defined and tested incident management processes in place that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.<br>• Key security considerations and references relevant to third party:<br>– Preparation for an incident<br>– Reference to **10 Steps: Incident Management,** NIST Computer Security Incident Handling Guide, CREST Cyber Security Incident Response Guide, Prepare section of ISO 27035, CIR scheme |
| D.2 Lessons Learned: | • When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.<br>• Key security considerations and references relevant to third party:<br>– Reference to NCSC 10 Steps: Incident Management, Chapter 8 of ENISA Good Practice Incident Management Guide, Section 3 NIST Computer Security Incident Handling Guide, Part 6 CREST Cyber Security Incident Response Guide |

# B. Suggested Cyber Security Controls

This section gives a number of technical security controls that can be applied to DER to assist with the implementation of this guidance. These controls do not form part of the NCSC CAF, but are more prescriptive, technical controls that can directly improve security and lower the cyber security risks associated with DER.

## B.1. VPN remote access

### Description

In order to protect connections made over untrusted networks, operators should use Virtual Private Networks (VPNs) or similar technologies[4] to provision secure cryptographically protected tunnels.

VPN protocols[5] are well supported by most computer operating systems and firewall devices and are generally relatively straightforward to configure for a wide range of system/network sizes. Some firewall devices may be limited in their support for modern VPN protocols and cryptographic cyphers so care should be taken to ensure a selected product supports a suitably secure solution.

Cryptographic authentication is strongly recommended for any VPN or other tunnel over the internet. If password authentication is used, long randomly generated strong passwords and two factor authentication should be used where available. Password generation and storage for complex passwords could be handled using one of the mainstream password safe tools.

### CAF

Use of an appropriately configured VPN can contribute towards meeting the following CAF principles:

- B3.b
- B4.a
- B4.b

### Architectures

The use of a VPN or equivalent protection is recommended for all DER systems where any level of remote access is required to a remote site. Smaller operators may use a simpler solution with pre-shared keys to establish connections. Operators with larger systems may consider more complex solutions with key management/public key infrastructure in order to simplify administration as the number of end points scales.

## B.2. Boundary firewall/VPN endpoint

### Description

The system should be connected to external networks via a boundary firewall. This serves the function of protecting the network from unauthorised connections to interfaces that should not be externally exposed.

[4] Such as SSH tunneling or TLS with mutual certificate authentication.
[5] E.g. IPSEC, OpenVPN and WireGuard

The firewall should only permit inbound traffic from the external network for the VPN or other cryptographic tunnel. This connection may terminate on the firewall itself or a separate endpoint device inside the network protected by the firewall.

Operators should consider the requirement for outbound access from the DER system to the internet/external network and disable/restrict access that is not required. Larger operators should consider web proxies/content scanners on any required access.

### CAF

Use of an appropriately configured firewall may contribute towards achieving the following CAF principles:

- B2.d
- B4.a
- B4.d

### Architectures

Usage of boundary firewalls is strongly recommended for all DER systems with any connections to external networks. Smaller operators may find 'professional grade' gear suitably inexpensive while providing an adequate range of features and support without the cost and difficulty of using 'enterprise grade' equipment which larger organisations may prefer for more feature rich software and more scalable remote management solutions.

## B.3. Internal networks

### Description

While external network connections should be protected using firewalls and VPNs, internal networks may also need consideration, depending on the installation.

With small installations a 'flat' network with all devices sharing a communication domain may be the most appropriate network solution, but as a site increases in scale such as a large wind farm, it may be more suitable to include additional segmentation such as VPN endpoints/firewalls for each individual tower.

Where an operator has multiple different network connected systems operating on the same site such as DER systems, IT devices, OT Devices and CCTV cameras, consideration should be put into isolating different systems onto different network segments[6].

### CAF

Appropriately configuring and securing internal networks may contribute towards achieving the following CAF principles:

- B3.b
- B4.a

[6] This could be achieved through separate physical network connections or through VLAN assigned ports using managed switches.

### Architectures

Of particular concern should be larger installations where an attacker could gain physical access to a network connection controlling a large number of devices.

## B.4. Wireless network security

### Description

Wireless networks allow an attacker to gain access without physical access to the equipment so should always be subject to protection with appropriate cryptographic controls. Built in wireless security standards[7] evolve slowly and are difficult to patch when security vulnerabilities are discovered due to limitations of existing wireless hardware. It is not recommended to rely solely upon such standards for communication security over wireless networks and you should also use software cryptography with the capability for upgrade where feasible.

Where wireless access needs to be provided for local access by technicians with laptop/tablet devices, it will often be more suitable to provide separate wireless internet access and leverage existing remote access capability (eg a VPN) rather than attempting to provide secure wireless access to the operational network infrastructure.

### CAF

Appropriately configuring and securing internal networks may contribute towards achieving the following CAF principles:

- B3.b

### Architectures

Wherever wireless networks are used, appropriate security controls should be put around them to prevent a malicious attacker gaining remote access to the internal network of the DER system.

## B.5. Dedicated secure management system

### Description

The management system used to control the DER system will normally have full privileged access over all the managed DER sites. It will have the ability to remotely connect, authenticate to devices and send critical instructions that could disrupt energy supply. For this reason, the management system is a significant single point of compromise and a large attack target for the total system.

Corporate IT systems typically support several business functions that expose a significant attack surface to 3rd party systems. These include web browsing, email and exchange of documents. Segregating a management system from corporate IT allows a reduction in the size of attack surface and the likelihood of compromise by a remote attacker.

Just like conventional IT systems, using up to date, patched software and systems is vital to ensure secure operation and this should typically be handled automatically to ensure prompt consistent

[7] E.g. WEP and WPA/WPA2

protection. Anti-malware protection systems can be useful to prevent the ingestion of malicious code from external sources into the system.

In certain cases, it may be necessary to run outdated software on management systems to interact with legacy devices and systems. While this should be avoided where possible, outdated systems can be run inside a virtualised environment. This enables running legacy software on modern hardware and operating systems that may not normally be supported by the software. By removing all remote connections to the legacy system and forcing access through the secured virtualisation platform, greater protection can be achieved.

### CAF

An appropriately designed secure management system may contribute towards achieving the following CAF principles:

- B2.b
- B4.c
- B4.d

## Architectures

All DER systems should be managed from a secure dedicated management system. The complexity of this system can vary between:

- A stand-alone laptop used for local configuration of systems that have no remote management
- Remotely connected laptops for small remotely managed systems
- Dedicated operational technology platforms with standalone server infrastructure, networking, monitoring systems and control room

The nature of the security systems in place will vary depending on the scale and design of the management system in question. Larger systems should look towards the NCSC CAF guidance for appropriate measures to secure OT/IT systems.

# C. Existing DER security standards and guidance

Unlike traditional IT security standards, DER standards are still in their infancy and there is not one standard to apply. There are, however, a number of countries and organisations working towards securing DER and have some published guidance available to work with.

This section provides an overview of the various standards and guidance that have been used to develop the guidelines. Whilst creating the CSCG, the approach is to be more outcome focussed and flexible so as not to cause any compatibility issues with other international approaches.

There are a variety of standards and guidance available that are loosely relevant for DER with no particular source being used significantly more than another, or specifically for DER related risks. These are summarised in Table 14.

**Table 14 Summary of relevant standards and guidance**

| Source | Ref. | Document | Observations |
|---|---|---|---|
| IEC 62443 | 3,4 | Industrial Automation and Control Systems Security | • Leading standard for ICS security and network architecture. Sections include system design guidance and requirements. Not all sections are published.<br>• The Health and Safety Executive (HSE) inspectorate guidance is based on this and vendors widely adopting.<br>• Part 2-1 Includes mapping to ISO 27001.<br>• Whilst not DER specific, this is useful for the industrial control components of DER. |
| IEC 62531 | 5 | Security for information exchange in power systems | • Aimed at covering gaps in IEC 62443.<br>• Covers low level technical controls useful for power systems. |
| NIST SP800-82 | 6 | Guide to ICS Security | • Contains a holistic review of relevant components for cyber security.<br>• Whilst not DER specific, serves as a good baseline for the ICS components of DER implementations. |
| NIST SP800-53 | 7 | Security and Privacy Controls for Information Systems and Organisations | • Exhaustive list of security controls for Information Systems.<br>• Whilst not DER specific, serves as a good base for a checklist of security principles and controls. |
| NIST | 8 | NIST Framework for Improving Critical Infrastructure | • Covers risk management and high level organisational processes.<br>• More relevant for DNOs and National Grid for organisational and policy structures. |

| | | | |
|---|---|---|---|
| ANSSI | 9 | ANSSI Cyber Security for Industrial Control Systems | • Focus is on Industrial Control Systems.<br>• Useful as an overview of how to assess the level of risk associated with a control system and the appropriate measures needed to secure them. |
| NCSC[8] | 1,2 | • UK NCSC – NIS regulations Guidance to Industry (January 2018)<br>• Security of Network and Information Systems Government response<br>• CAF (May 2018) | • EU Network and Information Systems Directive from May 2018 to ensure cyber security risks managed for UK CNI or equivalent.<br>• This is supplemented by the CAF. |
| ISO 27019 | 15 | ISO 27002 applied to Process Control Systems in the energy industry | • Summarises IT controls to deliver cyber security and how they may be extended for process control environment for energy delivery systems.<br>• Mainly of use to the network operators. |
| UK HSE - OG 0086 | 10 | HSE supplementary guidance in addition to the NCSC CAF | • Not directly relevant for DER connections.<br>• Could be used as an example of where organisations have added extra fields to supplement the CAF. |
| IEEE 1547 | 11 | Family of standards for interconnecting DERs to distribution grids | • In the UK, these are in the form of the G98 and G99 connection codes.<br>• Only covers electrical connection and does not contain cyber security guidelines. |
| NREL | 12 | DER Cyber Security Standards | • Copy of a presentation introducing the creation of DER cyber security standards.<br>• Still in development and currently limited to basic controls. This is expected to change. |
| NREL | 13 | An overview of DER interconnection: Current practices and emerging solution | • Summarise the considerations, practices and emerging solutions.<br>• Does not aim to recommend or dictate practices.<br>• Contains generic cyber security guidelines. |
| Sandia National Laboratories | 14 | Cyber security primer for DER vendors, Aggregators and Grid Operators | • Contains many general cyber security principles and background information. |

[8] The documents listed here are just a small subset of the valuable resources available through the NCSC. Please refer to the NCSC website for the full set of resources.

Energy Networks Association
4 More, London Riverside
London SE1 2AU

Tel +44 (0)20 7706 5100
Fax +44 (0)20 7706 5101
www.energynetworks.org