energynetworks association

Department for Business, Energy & Industrial Strategy

Energy Delivery Systems – Cyber Security Procurement Guidance

Foreword

Cyber threats to the energy sector pose economic and national security risks, threatening a key Department of Business, Energy and Industrial Strategy (BEIS) objective to ensure consumers have secure, affordable and clean energy. The UK Energy System is amongst our most Critical National Infrastructure (CNI), underpinning many of our essential services. Improving cyber security will help ensure that the UK has a secure and resilient energy system, avoiding disruption through cyber-attack that could have a severe impact on the country's national security. This impact could have a bearing on the lives of UK citizens, the stability and strength of the UK economy, and/or the UK's international standing and reputation.

The Network and Information Systems Directive (NIS Directive) came into force 10th 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 (EDS).

Since the launch of the Energy Cyber Security Programme in 2013, the BEIS Energy Cyber Security Team and the National Cyber Security Centre (NCSC) have focused efforts on collaboration with CNI Operators to ensure that they have appropriate technical advice and guidance to manage the cyber risks that they are exposed to.

Weaknesses in supply chain and procurement processes are a means by which malicious code, compromised equipment and support services can affect EDS. It is therefore necessary to address vulnerabilities across the supply chain, specifically the products, vendors and integrators of operational technology (OT) and network and information systems that underpin the operation of EDS.

Improving cyber security in the supply chain of EDS in the UK has been challenging as;

- There are no UK-centric procurement language/reference documents available
- Cybersecurity requirements vary in approach and degree of technical content
- There is no common approach to cybersecurity procurement in the UK resulting in vendors struggling to develop product roadmaps that will meet the industry's requirements
- A one size fits all solution will not work.

This guidance is a result of collaboration between BEIS, the Energy Networks Association (ENA), vendors and operators who have provided industry insight, shared challenges and made suggestions to improve procurement processes and requirements across the industry.

In order to develop the baseline for our industry, key cyber security elements required alignment to ensure a common level of understanding. This involved:

- Defining and mapping of asset and technology areas for EDS
- Developing of a cyber security reference model for the asset and technology areas or zones
- Reviewing existing procurement language references, good practice and international standards for cyber security that may be relevant to EDS
- Determining cyber security requirements to deliver target cyber security levels which can be aligned to the reference model
- Developing cyber security procurement guidance statements (CSPG) that will enable procured products and services to meet the cyber security requirements identified.

The statements have been aligned to the fourteen NCSC principles for OES and grouped into reference areas. The reference areas are:

- General – containing a high-level set of requirements to deliver key EDS cyber security measures in general terms
- Supply chain and external zone – outlining the requirements that the third party organisation should meet to ensure cyber security risk is managed in the delivery processes for the procured product (assets, systems or services for EDS). These primarily address the NCSC principles associated with management of cyber security of the EDS supply chain
- EDS reference security zones – outlining sets of security requirements that the third party should meet in the delivery of assets, systems or service to the EDS environment, as applicable to the primary implementation zone for the procured product. These aim to ensure that good practice cyber security is delivered, and the purchasers operating environment is appropriately considered. The reference security zones are:
- Process control zone
- Operational management zone
- Enterprise zone.

Supporting guidance for the application of these statements has also been included. Adoption of these target baseline EDS CSPG statements will support delivery of end to end security for our systems, at an industry accepted level. It will also enable our users to effectively and consistently articulate an industry baseline for cyber security in the software, hardware and services they purchase across the supply chain.

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 2020 renewable energy targets, are just some of the issues that the ENA helps our users of this guidance to address.

Disclaimer

This guidance is provided for guidance only, ENA takes no responsibility for its application within organisations.

- Any legislative requirements supersede statements in this guidance, including energy sector regulation or legislation under the NIS Directive, 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 purchaser is accountable to provide cyber security governance such that policies and procedures are established to ensure that security of the procured product is appropriate and proportionate to the identified EDS cyber security risk, and that security measures for the procured product are operated and maintained throughout the EDS lifecycle.

Acknowledgements

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

- UK Power Networks
- Electricity North West
- Northern Ireland Electricity Networks
- National Grid UK
- Western Power Distribution
- Scottish Power Energy Networks
- NCSC
- Northern Powergrid
- ABB
- Siemens
- Rockwell Automation
- GE
- Schneider Electric.

1 Introduction to the guidance

The EDS – CSPG will support users in delivering an effective approach to procurement by industry. This guidance contains a suite of procurement statements that can be incorporated into procurement related documentation. This will enable users to effectively and consistently articulate and implement an industry baseline level of cyber security for the products and services used within their EDS.

1.1 Objective

The objectives of this guidance are to provide:

- A consistent approach to EDS procurement in managing their cyber security risk from the supply chain[1]
- A baseline level of security that is required for EDS products and services
- Cyber security procurement statements that support the cyber security risk management of third party supplier risk to EDS by providing relevant procurement statements for the purchase of associated products and services
- Guidance to assist third parties in the EDS supply chain in providing appropriate security within their products and/or services.

It is envisaged that the CSPG is implemented as part of a wider risk-based approach to managing EDS security, based on best practice and international standards to lower the risk of cyber incidents in the energy sector.

1.2 Scope

This guidance covers the operational asset/technology areas and capabilities common to gas and electricity distribution and transmission network operators.

The primary focus of this guidance are EDS, these are predominantly comprised of what are widely referred to as Industrial Automation and Control Systems (IACS). The specific requirements for each asset, system or service will be different depending on the business requirements for the organisation.

This guidance applies to all EDS where the Purchaser has operational accountability and should be used as part of procurement processes which cover all installed IACS, upgrades, new systems and projects, and by all employees, contractors and third parties involved in the procurement process. This guidance can also be used by those who have a responsibility for cyber security throughout the lifecycle of EDS as a reference during design development, build, test, management and operation of these systems. This may include systems that reside in the traditional IT environment but are used to support operational EDS.

The Purchaser refers to the organisation acquiring or buying the asset, system or service. This may be through new, or renewal of, support contracts, tender documents for new systems or purchasing

[1] The supply chain refers to the providers of software, hardware and services to the operators of EDS. It also includes the vendors that supply products and the systems integrators that bring together subsystems. The supply chain for EDS tends to be very complex, employing bespoke solutions and often involving hundreds of different companies.

requisitions for individual components for use in EDS. Security requirements vary depending on the asset, system or services, operational function and the asset or technology area where it is deployed.

1.2.1 Out of scope

This guidance is not targeted at the electricity generation, gas storage and gas supply/terminals sectors. However, the CSPG statements could be adapted where similar industrial systems and technologies are used.

The CSPG excludes customer metering at point of delivery and other retail aspects of the business.

Organisations may have an internal standard or reference international standards for the specification of equipment for EDS which have historically not addressed cyber security. These statements in this guidance do not cover the engineering design principles for EDS including, but not limited to, function, operation, interoperability, safety or environment.

1.3 Who should use this guidance

The CSPG is primarily aimed at those within the EDS business that have a relationship to the supply chain of EDS related assets, systems or services, such as:

- Procurement teams
- Project managers or their team responsible for leading projects that include the acquisition of EDS, components, or modifications to them
- Those developing technical specifications for reference by procurement contracts
- Innovation or product development/acceptance teams assessing new technology or components that may be introduced to EDS or require modifications to them
- Those purchasing maintenance, support, system diagnostics or analysis of EDS or their components from third parties in the supply chain (such as system integrators, vendors, suppliers and other service providers)
- System integrators, vendors, suppliers, service providers and other third parties in the supply chain interested in the understanding the direction for EDS cyber security and to aid in understanding the original intent of the CSPG.

2 Energy delivery systems

EDS, as referred to in this guidance and that the cyber security procurement statements can be applied to, are the systems and networks for monitoring and controlling the transmission and distribution of electricity and gas. This includes, but is not limited to, the equipment and technology comprising the IACS including communications and tele-control applications and Safety instrumented systems (SIS), and the computer-based systems and networks that analyse and store their data, or support their development, operation, maintenance and security. This section provides a more details of the typical types of systems in an EDS.

2.1 Definition of IACS

If a system interacts with the physical world then it should be considered as an IACS. The following, more detailed IACS definition is based on the international standard, IEC62443-1-1. IACS covers systems that can affect or influence the safe, secure, and reliable operation of any industrial or cyber-physical process. They include, but are not limited to:

- IACS and their associated communications networks, including Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), intelligent electronic devices, Supervisory Control and Data Acquisition systems (SCADA), networked electronic sensing and control, metering and custody transfer systems, and monitoring and diagnostic systems. In this context, IACS include basic process control system and safety-instrumented system functions, whether they are physically separate or integrated.
- Associated systems that support IACS and are classed as IACS. Examples include advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, quality monitors, pipeline leak detection systems, work management, outage management, energy management systems and systems that provide services (e.g. file transfer, anti-virus updates, and communications network management) to IACS.
- Associated internal, human, data network, software, machine or device interfaces used to provide control, safety, manufacturing, or remote operations functionality to continuous, batch, discrete, and other processes.

Where systems meet the requirements of any of the above bullets then they should be considered IACS. This includes those referred to as the Internet of Things (IoT) or Industrial Internet of Things (IIoT) but may also include, for example, building management systems.

Associated systems which are integrated or essential to operation of IACS may also be classified as IACS in some circumstances, for example, physical access control systems and physical monitoring.

Typical IACS include but are not limited to:

- Electrical, Control & Instrumentation Systems (E,C&I)
- Emergency Shutdown Systems (ESD)
- Fire and Gas Systems (F&G)
- Industrial Control Systems (ICS)
- Operational Technology (OT)
- Distributed Control Systems (DCS)
- Process Automation Systems (PAS)
- Programmable Electrical Control Systems
- Programmable Logic Controllers (PLC)
- Remote Terminal Units (RTU)

- Intelligent electronic devices (IEDs), including smart instrumentation
- Supervisory Control and Data Acquisition systems (SCADA)
- ICS configuration systems (e.g. engineering workstations and/or laptops)
- Load management or shedding systems
- Safety instrumented systems (SIS), which may range from simple logic systems to complex programmable PLC type systems
- Plant Information Systems (e.g. management historians and data servers)
- Network and telecommunications infrastructure to provide connectivity to the above
- Connectivity to systems outside the IACS (e.g. the corporate networks etc.).

2.2 Typical components of EDS

EDS compromises many elements and not all will be used by each Operator. The following provides high-level descriptions of the typical devices that make up EDS. These are split into five areas:

- EDS E,C&I
- EDS monitoring and control
- Operations management system
- Enterprise system
- External system

Table 1 EDS E,C&I

Layer	Communications	EDS Asset / Technology Areas
0 - Physical process: Electronic instrumentation that directly interacts with the physical world	Electrical field wiring from local or remote termination or wireless field communications	• Output devices, e.g. valves, actuators, relays, audio and visual alerts, indicators • Input transmitters, sensors and detectors, e.g. level, pressure, temperature, doors, motion, perimeter, cameras
1 - Local process control / protection systems: Local electronic controllers using functional programs to automatically interact with field devices, based on field, pre-set or operator inputs.	Direct serial or electrical field wiring, fieldbus, industrial Ethernet networks or wireless field communications e.g. Modbus, Profibus, DeviceNet	• Protection relay • Transducer • Capacitor bank controller • Auto-reclose relay • Transformer tap changer controller • Programmable Logic Controller (PLC) • Distributed Controller • Voltage regulator controller • Primary and secondary substation RTUs • Lone worker device • Remote I/O module • Safety instrumented systems (SIS) • Communications Network Devices (Switches, Routers, Media converters, Terminal servers)

Table 2 EDS monitoring and control

Layer	Communications	EDS Asset / Technology Areas
2 - EDS monitoring / Site supervisory control and local display: Plant operator/human interface local to the process, interacting with controllers	Direct serial, fieldbus or Industrial Ethernet, telemetry and TCP/IP networks	• Digital Fault Recorder (DFR) • Transformer monitoring device • Circuit breaker monitoring device • Power quality monitor (PQM) • HAM & LAM Metering (Balancing & Settlements and Protection) • Fault indication / alarms • CCTV • Site worker management systems • Remote Terminal Units (RTU) • Programmable Logic Controller (PLC) • Distributed Control System (DCS) • DNO Substation gateway (Grid, primary and secondary) • Human Machine Interface (HMI): Operating system and applications • Communications Network Devices (Switches, Firewalls (e.g. inline/industrial), Media converters/Communications servers, Terminal servers)

Table 3 Operations management system

Layer	Communications	EDS Asset / Technology Areas
3 - Operations management / remote supervisory control: Systems to manage plant operations outside, or remote to, the local process Enclaves to support security services to EDS e.g. DMZ(s)	Wide area and local area telemetry and TCP/IP networks e.g. DNP3, DNP3 Secure, Modbus TCP or Modbus over IP	• Communications Network Devices (Switches, Routers, Firewalls, Media converters, Servers, Data Diode) • SCADA servers and remote operator workstations: Operating systems and Application software (Application, Historian Databases, Logging, Communications, Domain Controllers, Monitoring) • Energy Management Systems / Energy Distribution Systems (EDS) / Network Management systems (NMS) / Distribution Management Systems (DMS): Servers (Operating system and Application software) • Third party interfaces (independent network providers) • Distributed Generation Control (FPP) • Security services and devices (as above)

Table 4 Enterprise systems

Layer	Communications	EDS Asset / Technology Areas
4 - EDS business planning and logistics: Business systems for managing network and plant operations, e.g. maintenance, access, scheduling, inventory.	Wide area and local area TCP/IP networks	• Maintenance laptops: Operating systems and Application software • EDS Test kits • Field force enablement (tablets - work instructions, switching instructions, isolations, online mapping, real-time network status information (read only from NMS/SCADA)
4 - Enterprise / Corporate: Core business systems not directly related to the EDS but providing support to operational service Enclaves to support security services to EDS e.g. DMZ(s)	Wide area and local area TCP/IP networks, and public/private cloud services	• HR, finance and business management • Data hosting and analytics (e.g. logs, reports, time and sequence, condition monitoring • Firewalls, data diodes • Intrusion Detection Systems (IDS) • Authentication and Authorisation • Remote access system/gateway • Security services and devices: Operating system and applications (Patch Management, Malware Protection/AV, SIEM, IDS/FIM, Configuration Management, Virtualisation Management)

Table 5 External systems

Layer	Communications	EDS Asset / Technology Areas
5 - External Systems: Internet and other systems owned and operated by third parties that the enterprise or operational plant depends on (vendors, suppliers, integrators, contractors, business partners, joint ventures, value chain, etc.)	Wide area, local area and TCP/IP networks and public/private cloud services	• Balancing settlements code (Elexon) • Vendor Data analytics services • Cloud data hosting (e.g. logs, reports) • Cloud data Analytics (e.g. time and sequence)

3 Cyber security for the energy sector

The adoption of digital technology in the energy sector is ongoing and EDS are increasingly reliant on IT and telecommunications. Digitisation brings huge advances 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 energy sector moves towards Smart Grids and Distribution system operators (DSO), which will result in an increased attack surface.

3.1 Cyber security and EDS

The UK Government recognises cyber-attack as a tier-one risk to UK interests, 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.

A cyber-attack can directly or indirectly lead to a cyber security incident affecting the EDS and in turn disrupting energy supplies. Cyber security incidents can arise from a targeted cyber-attack, but they can also be non-targeted or even accidental. Cyber security incidents can adversely affect the EDS availability, reliability or ability to fulfil its intended function.

EDS are a potential target for cyber-attack and this could result in one or more of the following impacts if EDS are affected:

- Health, safety or environmental events resulting in harm to people, property or the environment
- Disruption to energy services
- Financial loss to the UK operator or the wider UK economy
- Loss of commercial or sensitive information
- Reputational damage
- Criminal damage
- Regulatory fines.

Cyber security is delivered through a set of technical, procedural and managerial security measures to ensure that confidentiality, integrity and availability of systems and information are not compromised. Cyber security also requires the consideration of physical and personnel risks which are included in the CSPG statements where they pertain to the protection of the EDS but not the wider organisation.

Owners and Operators of EDS are responsible for the cyber security and resilience of their systems.

3.2 Current cyber security trends that affect EDS procurement

There are a number of cyber security trends that affect procurement of IACS in EDS and associated support contracts as outlined in Table 6.

Table 6 Cyber security trends affecting EDS procurement

Key challenge	Description
Keeping pace with technology	Energy organisations and other CNI sectors are heavily reliant on OT systems for their core operations and maintaining "state of the art". The transition from DNO to DSO and the implementation of the Smart Systems and Flexibility Plan (SSFP)
Convergence of OT and IT	Traditionally IACS systems were bespoke and not connected to the enterprise data networks. However, IACS 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: • Adds complexity to EDS networks and their security • Creates interdependencies and interfaces • Puts 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. Evolving ICS standards and guidance being adopted on ad-hoc basis by UK industry. No current consensus on which to use.
Incoming legislation	Network and Information Systems Directive (NIS Directive) and General Data Protection Regulation (GDPR).
Skills and resources within the sector	Cyber security skills gap in engineering domain still prevalent. This is widening with IT/OT convergence for both environments. Also extends to business functions e.g. procurement, contracts management, project management, sales, innovation teams
Technology trends	EDS are leveraging modern IT technologies to meet the change in demands of the business, such as: • Cloud computing and outsourcing for IACS data storage, data analytics and associated cost savings (e.g. monitoring of switching, sequence of event reporting and condition monitoring) • Access controls using Radio Frequency Identification (RFID) and biometric solutions in IACS leading to data privacy considerations • Software defined networks and virtualisation technology converging with historically IT systems • Use of mobile technology in IACS environment e.g. tablets and thin clients • Use of Voice over IP (VoIP) communications to support operational environments • Shift to centralised software management and security solutions e.g. patching and antivirus updates • Increased digitisation in EDS, including in IACS and monitoring systems • Smart grid infrastructure and management – Interconnectivity throughout information system layers

	– EDS data crossing system and organisational boundaries – Increased reliance on technology and real-time operational information. Many of these trends and technology advances bring improvement but also increase the cyber security risk to EDS.
Third parties	Third parties are increasingly being targeted to gain access to IACS through their "trusted" status. Third parties are being targeted through: • Compromising updates files such as with the Havex malware attack, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A • Using remote connections to access IACS from third parties • Compromised embedded components being used in hardware.

3.3 Challenges of cyber security in EDS procurement

Operators have varying maturity levels and approaches to cyber security risk management and procurement. Individually, operators as a single customer have limited leverage to drive improvement or drive consistent management of this risk across the industry.

Vendors have varying approaches to the cyber security of the products and services that they provide. There is a risk that an impact to the EDS can be brought about by compromising products, vendors or integrators that are procured and used by operators.

4 IACS security standards and guidance

Unlike traditional IT security standards IACS security standards are relatively immature and there is not one definitive standard to apply. There is, however, a large amount of guidance available on securing IACS that can be utilised by operators to secure their systems.

A recent development from the UK Government is the NIS Directive which came into force on May 10th, 2018.

This section provides an overview of the various standards and guidance that have been used to develop the statements and a high-level overview of the NIS Directive.

4.1 Industry standards and guidance

There are a variety of IACS security standards with no one standard being used significantly ahead of others. In addition to the standards, there is a wide range of guidance available and a number of procurement language documents have also been developed. These are summarised in Table 7.

Table 7 Summary of relevant standards and guidance

Source	Document	Year	Observations
IEC62443	Industrial Automation and Control Systems Security • Part 2.1 Requirements for an IACS security management system • Part 3.1 Security technologies for IACS • Part 3.3 System security requirements and security levels • Part 2.4 Security program requirements for IACS service providers	2011 2009 2013 2015	• Leading standard for ICS security and network architecture. Sections include system and security program requirements. Not all sections are published. • HSE inspectorate guidance is based on this and vendors widely adopting. • Part 2-1 Includes mapping to ISO27001 • Part 2-4 Formerly WIB Process Control Domain–Security Requirements for Vendors
US DHS	Cyber Security Procurement Language for Control Systems (CSPLCS)	2009	Considered far too comprehensive to be readily absorbed and adopted by many.
EPRI	US Electricity Power Research Institute - Cyber Security Procurement Methodology (CSPM)	2012	Provides an approach for managing cyber-security risk in the supply chain and delivering procurement clauses in contracts, refers to CSPLCS
US DOE	Cyber Security Language for Energy Delivery Systems (CSLEDS)	2014	Created due to complexity in DHS and to fulfil a requirement to simplify and modernise for EDS
BDEW	White Paper - Requirements for Secure Control and Telecommunication Systems	2014	EU supported document provides basic requirements for utilities, with reference to controls from ISO27002 and 27019 (for those countries using ISO27001 ISMS for energy companies)

NCSC	UK National Cyber Security Centre – NIS Directive Guidance to Industry (January 2018), Security of Network and Information Systems Government response and future Cyber Assessment Framework (CAF) (May 2018)	2018	EU Network and Information Systems Directive incoming in May 2018 to ensure cyber security risks managed for UK CNI or equivalent. This will be supplemented by CAF.
ISO27019	ISO 27002 applied to Process Control Systems (ICS/IACS) in EDS	2017	Summarises IT controls to deliver cyber security and how they may be extended for process control environment for energy delivery systems
CENELEC	Smart Grid Information Security and Reference Architecture	2011	Security standard for smart grid to apply consistency across the networks

4.2 Outline of the Network and Information Systems Directive (NIS Directive) as relevant to EDS

The UK Government transposed the EU NIS Directive into UK law on the 9th May 2018 and the regulation came into force effective 10th May 2018. Penalties for non-compliance are set to a maximum limit of £17 million.

A large number of operators of EDS are designated as OES and will need to comply with the requirements of the NIS Directive.

It is important for OES to understand that these services can be dependent on others, some of which may be internal or external third-party products and services. The OES will be held responsible for the security and resilience of its suppliers and the supply chain.

4.2.1 High-level NIS Directive Requirements

Under the NIS Directive OES are required to:

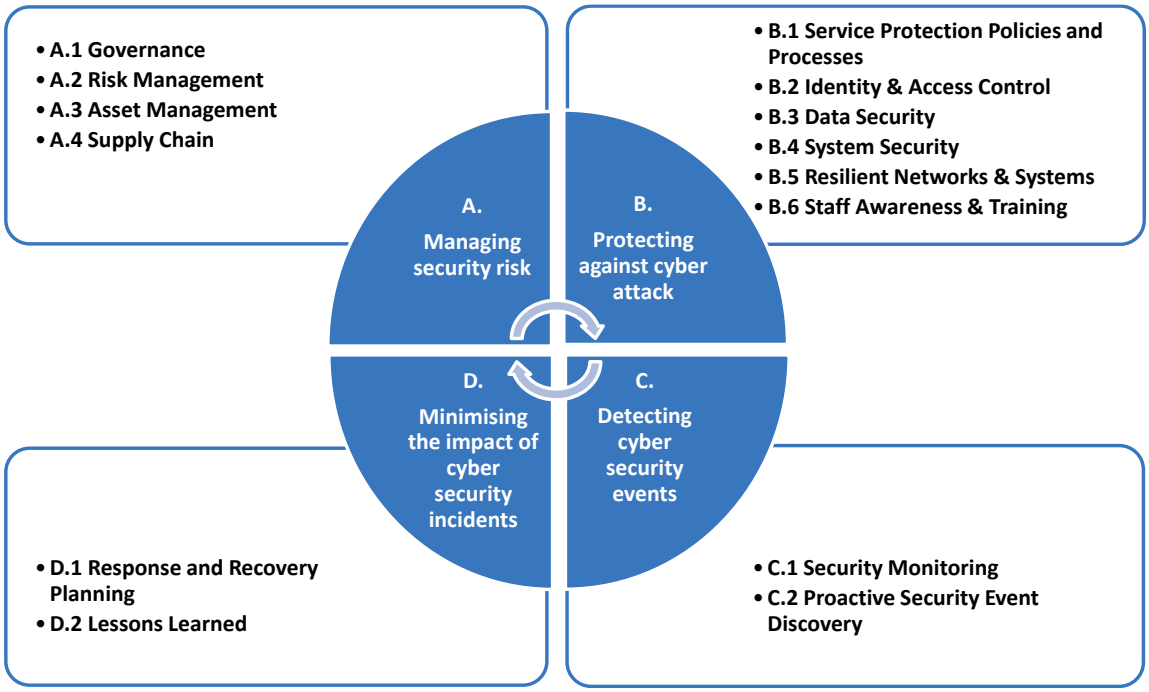
- Implement risk management practices, to 'take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in their operations'
- Establish effective incident response and reporting capabilities, which includes reporting 'significant' cyber security incidents to the 'Competent Authority'.

The NIS Directive encourages the use of European or internationally accepted standards and/or specifications relevant to the security of networks and information systems, to develop a culture of security across sectors.

4.2.2 NCSC Principles

The NCSC published the guidance that supports the UK Government's implementation of the NIS Directive in January 2018 which applies to OES. The four key security objectives and supporting principles to deliver the objectives are shown in Figure 1 and details can be found in Appendix C.

Figure 1 NIS Directive Summary



5 EDS asset and technology areas

Assets, systems or services being applied into the EDS environment will have a different cyber security risk management approach depending on where and how it is used in the operational environment. This section provides details on the target security model that has been developed, from which the procurement statements will be developed.

5.1 Determining a target model for procurement

Establishing a set of baseline security requirements for EDS procurement will help drive cyber security improvements across the supply chain.

Various minimum baseline requirements are described in a variety of procurement standards to reduce the risk from third parties and to ensure that industrial systems are secure by design. However, the level of detail and the target level of security is not always appropriate for the operational environment intended for the product.

To provide a baseline or target level for cyber security there are many frameworks that could be followed, with nuances in each. Cyber security target levels can take the form of target operating models, OT or IACS cyber security standards or reference architectures. Direct adherence to international standards is not always possible as cyber security controls or security measures are applied as appropriate to manage the identified risk.

In order to meet the industry's requirements, and in consultation with key stakeholders, the following approach has been adopted in the development of the industry baseline:

- The EDS Asset and Technology Areas will align with the IEC62443 reference levels
- The architecture 'Zone concept' from IEC62443 will be adopted, and aligned with the Smart Grid Reference Architecture for ease of reference. This will provide consistency between the procurement guidance and other widely adopted standards
- The target profile for cyber security will deliver to a baseline set of requirements for EDS in order to achieve an appropriate level of security.
- The CSPG statements will achieve a target profile of an appropriate level, to provide an industry baseline for our members
- The CSPG statements will include cyber security elements that may be present to ensure that an organisation can select and adapt to meet their specific needs.

5.2 EDS Cyber Security Reference Model

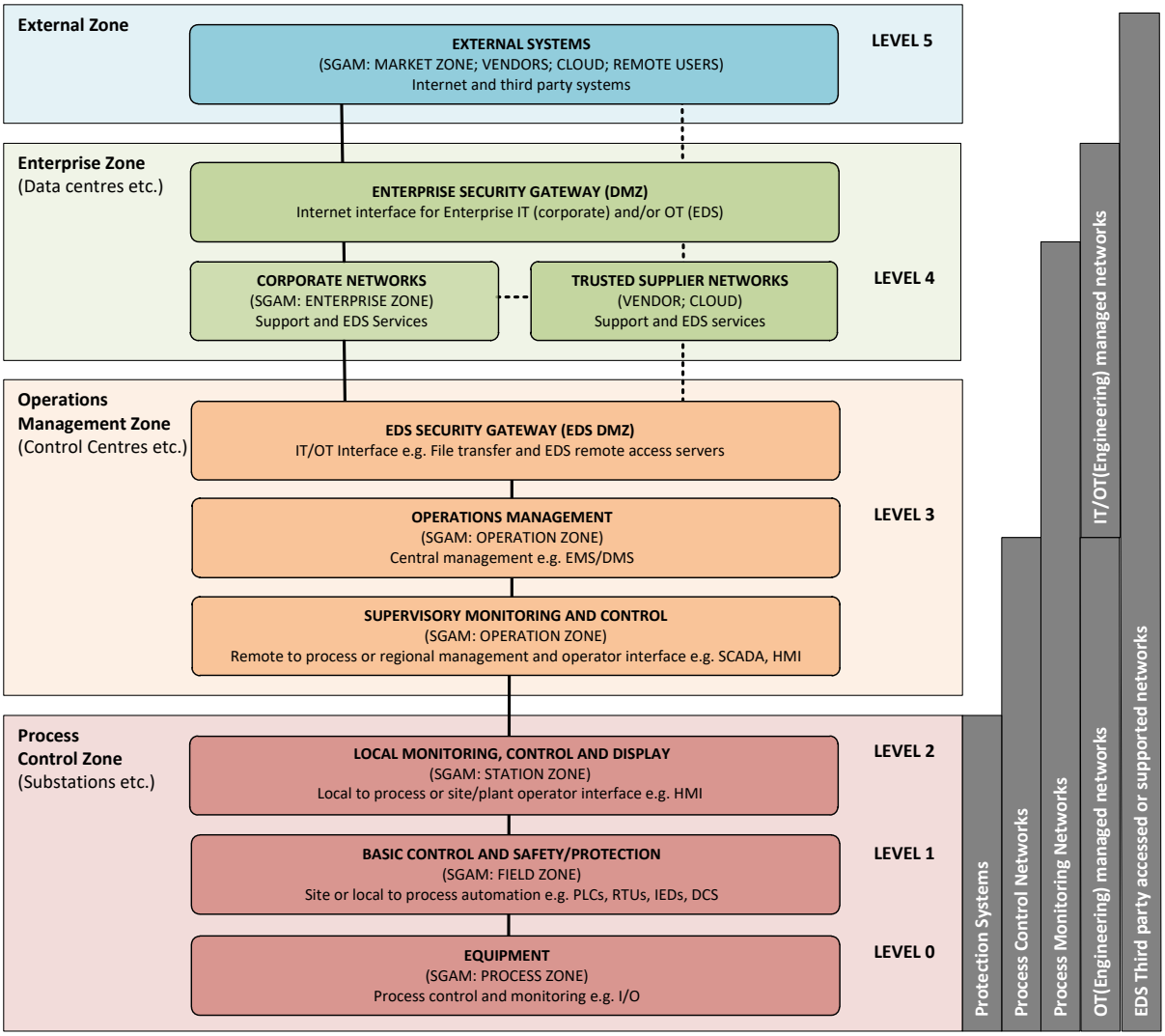
Good practice for cyber security recommends that a defence in depth strategy is applied to protect IACS. Organisations have a number of data networks that host systems and provide the communications, to support the core business services. To facilitate common understanding between our members, reference EDS security zones have been defined which considers typical OT, networks and functions relevant to EDS today.

An EDS IACS Cyber Security Reference Model (EDS-CSRM) has been developed to support application of the CSPG and define the reference EDS security zones. Data networks and typical EDS asset and technology areas within each zone can be mapped to this model for reference in applying the CSPG. This will support those involved with procurement in understanding the function of, and the security requirements for, the procured products for implementation in the EDS environment.

The EDS-CSRM shown in Figure 2, is an adapted Purdue Model, as defined in IEC 62443. It shows IEC62443 reference levels and reference security zones as applicable to EDS. It also includes reference to the Smart Grid Architecture Model (SGAM) Operational Zones increasingly adopted by the energy sector.

Note: The reference network level, LEVEL 0, is the physical process or electrical plant of the EDS.

Figure 2 EDS Cyber Security Reference Model (EDS-CSRM)



5.3 EDS Reference Security Zones

For reference, common EDS assets, systems and services have been mapped to the EDS reference security zone and Purdue level where they would typically be located, to support users of this guidance in selecting the reference zone for the asset, system or service being acquired. Supporting systems, communications and typical security solutions deployed to support EDS have also been included.

5.3.1 Process Control Zone

PROCESS CONTROL ZONE
The Process Control Zone consists of assets, systems and services local to the physical process or operational plant. This operational environment contains the local E,C&I and process control that provide the core function of the EDS, such as at electrical substations and local control rooms. These typically include the data networks supporting the IACS as outlined in Table 8, and contain typical EDS assets as outlined in Table 9. Security considerations at this level are typically focused on protecting the asset or system's functionality or supporting service, such as local area networks (LANs). Cyber security risk management extends to the components and their individual security capability and the impact they could have, individually or with consideration to exposure on a wider scale.

Table 8 Process Control Zone – Typical Data Networks

Typical Data Network	Description
Process Control Networks (PCNs)	These data networks consist of the plant or field-based systems that are safety/protection or operation critical and/or allow interaction with the controllers and field instrumentation to change parameters such as set-points, open or close breakers, valves, and start or stop pumps. These data networks typically host SCADA, RTUs, DCS, PLCs, safety systems, Human Machine Interfaces (HMIs) and servers, engineering workstations, local historians and process alarm servers. Alongside the PCNs controlling the process in this zone, there are typically two subsets of networks, which are functionally different, those supporting protection systems and asset or system monitoring.
Protection Systems	These data networks consist of Protection Systems, SIS's and ESD's which systems used to bring the plant to a safe condition and are typically independent from the control or SCADA systems. Vendors increasingly offer integrated control and safety systems (ICSS) which can diminish the distinction between control and protection networks. These systems often have additional requirements and functional safety standards used e.g. IEC61508 or IEC61511. Safety management and associated risk assessments should include cyber security implications related to these systems to be able to deliver their intended functions and to consider whether the protection elements of an ICSS require additional security controls.
Process Monitoring Networks (PMNs)	These networks consist of systems that only monitor processes and have no capability to make changes to the process. These data networks typically consist of systems such as quality monitoring, condition monitoring systems, voltage monitoring, CCTV and environmental monitoring systems.
Local / Wide Area Networks (LANs/WANs)	Communications networks at this level include data networks or LANs to support connectivity of the above systems but also includes EDS area communications such as public or private telecommunications networks or WANs for control, protection or monitoring purposes. These increasingly use Multi-Protocol Layer Switching (MPLS) and virtual private network technologies to provide dedicated communications links *Typical data communications at the boundary of the process control zone include, but are not limited to:* *SCADA connections to operations management zone, e.g. RTUs/PLCs and IEDs via telemetry or telecommunications networks* *Operations networks, e.g. remote HMI workstation client to central servers*

	Interface to other energy process control zones e.g. transmission or other substation zones, e.g. RTUs/PLCs/IEDs via tele control or tele protection networks *Interfaces for security updates, network management, and time synchronisation.*

Table 9 Process Control Zone – Typical EDS Assets

Level	Typical EDS Asset and Technology Areas
0	**Equipment –** *Electronic instrumentation that directly interacts with the physical process* • Output devices, e.g. valves, actuators, relays, audio and visual alerts, indicators • Input transmitters, sensors and detectors, e.g. level, pressure, temperature, flow doors, motion, perimeter, cameras • External connections to field equipment such as for maintenance, diagnostics or support. • Conduits and data communications at this level typically include: Electrical field wiring from local or remote termination or wireless field communications
1	**Basic Control and Safety / Protection –** *Local electronic controllers using functional programs to automatically interact with field devices, based on field, pre-set or operator inputs.* • Field equipment for monitoring, control or protection, e.g. intelligent field devices and infrastructure, these may include: – Safety instrumented systems (SIS) – Primary and secondary substation Intelligent electro unit – Protection relay – Transducer – Capacitor bank controller – Auto-reclose relay – Transformer tap changer controller – Distributed controller – Voltage regulator controller – Intelligent Electronic Devices (IED) – Digital fault recorder (DFR) – Transformer or phase monitoring device – Circuit breaker monitoring device – Power quality monitor (PQM) – HAM & LAM metering (Balancing & Settlements and Protection) – Emergency shutdown systems (ESD) – Programmable logic controller (PLC) – Electrical, Control & Instrumentation (E,C&I) systems, e.g. flow controllers, isolation, pilot systems – Pressure regulator/reduction controllers – Gas mixing controller – Compressor controller – Separator controller – Remote I/O module – Valve monitoring (e.g. cycles, differential pressure, calibration, travel) – Gas quality monitor (GQM) – Compressor monitoring – Gas Metering (Revenue & Process management) • Connections enabling data transfer between control, monitoring and protective systems within the EDS process control zone, such as industrial communications or network devices and infrastructure. These may include: – Switch – Router – Media converter – Protocol convertors – Communications / Terminal server • External connections to basic control and safety / protection systems and data networks e.g. field connectivity, links to generation systems, and any remote access for maintenance, diagnostics, support or other service provisions.

	• All wireless technology directly associated with the IACS, and including associated wireless supporting and configuring devices Conduits and data communications at this level typically include: Direct serial or electrical field wiring, fieldbus, industrial Ethernet networks or wireless field communications (e.g. Modbus, Profibus, DeviceNet.) and Telephony networks (e.g. PTSN, FO, MPLS, Cellular, satellite, microwave)
2	**Local monitoring control and display -** *Plant operator/human interface local to the process, interacting with monitors and controllers* • Monitoring systems (hardware, firmware and software), and monitoring applications and software that are implemented on control or monitoring systems, protective systems or data networks. Dedicated monitoring systems may include: – Fault indication / alarms – CCTV – Site worker management systems, e.g. lone worker device, gas detection • Control systems (hardware, firmware and software), and control applications and software that are implemented on control systems: including: – RTU – PLC – Distributed control system (DCS) – Substation (grid, primary and secondary) – Pressure reduction station, Governor, national transmission system – Human machine interface (HMI): Panel view or operating system and applications • Protective systems (hardware, firmware and software) – Protection systems – HMI • Connections enabling data transfer between control, monitoring and protective systems within the EDS operations zone, and with the operations management zone, enterprise zone or external zone, such as industrial communications or network devices and infrastructure. These may include: – Switch – Router – Firewall e.g. inline/industrial – Media converter – Communications / Terminal server – External connections to local monitoring, control and display systems and data networks e.g. field connectivity, and any remote access for maintenance, diagnostics, support or other service provisions. • Any other applications (e.g. business applications) and associated software that are implemented on control and monitoring systems or data networks • Ongoing support and maintenance provisions for whole-of-life EDS performance monitoring and security management, which may include systems, system elements or network nodes to support services as outlined in the Operations Management Zone. • Conduits and data communications at this level typically include: Direct serial or electrical field wiring, fieldbus, industrial Ethernet networks or wireless field communications (e.g. Modbus, Profibus, DeviceNet, Modbus TCP or Modbus over IP) and Telephony networks (e.g. PTSN, FO, MPLS, Cellular)

5.3.2 Operations Management Zone

OPERATIONS MANAGEMENT ZONE

The Operations Management Zone consists of assets, systems and services local, or remote to, the process control zone. This environment typically contains the operations or control room interface, local or remote to the process control zone to manage the EDS, and central control and energy management systems. These typically include the data networks supporting the IACS as outlined in Table 10, and contain typical EDS assets as outlined in Table 11.

Security considerations at this level are typically focused on protecting the EDS's functionality or delivery of the supporting service, such as wide area networks (WANs) or remote access. Cyber security risk management extends to the technology and its security capability and the impact it could have, individually or with consideration to exposure on a wider scale.

Any connections with the EDS environment for business benefits or to facilitate security for the EDS should not tangibly increase the risk to the EDS operational environment or to the organisations enterprise infrastructure or systems.

Table 10 Operations Management Zone – Data Networks

Typical Data Network	Description
Process Control Networks (PCNs)	These networks consist of control systems that interact with the plant or field-based PCNs that are local to the operations as outlined above. At this level the control systems, SCADA or HMI may be local to the plant operation, cover multiple plants or a region in a centralised control centre arrangement. This level also includes systems interacting with the control systems for additional operations management such as energy or distribution management systems (EMS/DMS). Alongside the PCNs controlling the process in this zone, there may be two subsets of networks, which are functionally different, those supporting protection systems and asset or system monitoring.
Process Monitoring Networks (PMNs)	These networks consist of monitoring systems that interact with the plant or field based PMNs outlined above, such as to consolidate information, or those that monitor the local PCNs and operations management systems or environment at this level.
EDS Security Gateway and Process Demilitarised Zone (DMZ) Networks	These data networks are used to provide an additional layer of separation between both the process control systems and the enterprise environment. They allow a tighter control of access to the IACS data networks. Systems at this level may include historians, data collectors and advanced alarm servers for providing information to the enterprise systems, file transfer servers, local antivirus repository and servers to facilitate remote access to the IACS.
Local / Wide Area Networks (LANs/WANs)	Communications networks at this level include data networks or LANs to support connectivity of the above systems but also includes EDS area communications such as dedicated telecommunications networks or WANs for SCADA/EMS and to support geographically dispersed control centres. These increasingly use MPLS and virtual private network technologies to provide dedicated communications links. *Typical data communications at the boundary of the operations management zone include, but are not limited to:* • *SCADA connections to process control zone, e.g. RTUs/PLCs and IEDs via telemetry or telecommunications networks* • *Operations networks, e.g. remote HMI workstation client to central servers* • *Interface to Enterprise zone for database replication or historical alarm and event data or security services* • *Interfaces for security updates, network management, and time synchronisation.*

Table 11 Operations Management Zone – Typical EDS Assets

Level	EDS Asset and Technology Areas
3	**Operations management / Supervisory monitoring and control and EDS Gateways and DMZ(s) –** *Systems to manage plant operations outside, or remote to, the local process, and enclaves to support security of the EDS.* • Computer-based EDS management systems, including network devices, infrastructure and system management services, including – SCADA servers and operator workstations / HMI: containing operating systems and application software (application, historian databases, logging, communications, domain controllers, monitoring) – Energy Management Systems (EMS) / Energy Distribution Systems (EDS) / Network Management systems (NMS) / Distribution Management Systems (DMS): containing operating systems and application software (as above) – Third party interfaces (independent network providers) – Distributed generation control (FPP) • Connections enabling data transfer between systems within the EDS operations management zone, and with the enterprise or external zone, such as network devices and infrastructure. These may include: – Switch – Router – Firewall – Media converter – Communications / Terminal server. – External connections to operations management / supervisory monitoring and control systems and data networks e.g. local connectivity, and any remote access for maintenance, diagnostics, support or other service provisions. • Gateways to support defence in depth architecture – Firewalls – Data diodes – Authentication and authorisation servers, e.g. remote access • Monitoring and management systems (hardware, firmware and software), and monitoring applications and software that are implemented on supervisory monitoring and control systems and operations management systems or data networks • Non-production control or monitoring systems, data networks and applications used to support EDS control and monitoring systems such as test, development, hot spare, training systems • Any other applications (e.g. business applications) and associated software that are implemented supervisory monitoring and control systems and operations management systems or data networks • Any maintenance computers or laptops used to configure EDS devices, whether the connection is temporary or permanent, and whether the device is company-owned or 3rd party-owned, or other maintenance tools with operating systems and application software • Interfaces with physical security systems • Ongoing support and maintenance provisions for whole-of-life EDS performance monitoring and security management, which may include systems, system elements or network nodes (hardware, firmware and software), for: – Central and field device health status – IDS/IPS and other security applications/devices for system or network performance monitoring and management e.g. Security information and event management (SIEM) – Compliance or security status reporting solutions, such as FIM, patch management and AV status (configuration management)

	– Incident response tools or management interfaces, e.g., Security operations centre (SOC) systems – Disaster recovery tools e.g. back-ups, and other service provisions – EDS integrated asset management solutions – EDS application configuration management tools – Vendor security products for EDS management – Antivirus and patch management solutions – Virtualisation management or other system or security services. Conduits and data communications at this level typically include: Wide area and local area telemetry and TCP/IP networks (e.g. DNP3, DNP3 Secure, Modbus TCP or Modbus over IP), and Telephony networks (e.g. PTSN, FO, MPLS, Cellular)

5.3.3 Enterprise Zone

ENTERPRISE ZONE
The Enterprise Zone typically contains the core business data networks for the EDS organisation. These systems are generally provisioned and managed by the corporate IT function within an organisation. In the context of the IACS it consists of assets, systems and services local, or remote to, the process control zone that provide supporting functions such as maintenance, scheduling and systems used for design and procurement. These typically include the data networks supporting the IACS as outlined in Table 12, and contain typical EDS assets as outlined in Table 13. Security considerations at this level are typically focused on protecting the EDS's information and providing access controls to the IACS. This environment is considered untrusted to the IACS, and often the enterprise considers the IACS untrusted due to the types of communications and security concerns from legacy systems and infrastructure. This environment is increasingly connected with the EDS to facilitate business benefits, such as remote access and data analytics for process optimisation and asset management. The enterprise level should be used to provide an additional level of protection between the open external environment and the EDS services delivered by the IACS. Any connections with the EDS environment for business benefits or to facilitate security for the EDS should not tangibly increase the risk to the EDS operational environment or to the organisations enterprise infrastructure or systems.

Table 12 Enterprise Zone – Data Networks

Typical Data Network	Description
Corporate Networks	This is the core business data network and supports systems such as email, file servers, HR systems, finance systems and customer management systems for the EDS organisation. In the context of IACS, these networks may contain file transfer servers, central antivirus and update servers and EDS business planning and logistics systems, such as maintenance, scheduling and asset inventories.
Trusted Supplier Networks	These networks consist of trusted supplier networks where the enterprise has a contract regarding the data connections and management of the environment, this may include enterprise services hosted as a cloud service on behalf of the EDS organisation which may be considered part of the corporate network, or trusted arrangements with third parties providing support or services to the ESD, such as remote access or data analysis.

Enterprise Security Gateway and Demilitarised Zone (DMZ) Networks	These data networks are used to provide a layer of separation between the enterprise and the external environments to protect the corporate networks from the Internet. They allow a tighter control of access to the enterprise data networks. Systems at this level may include security gateways, web servers for customer services and servers for providing information to third parties, and authentication servers to facilitate remote access to the enterprise or the IACS.
Local / Wide Area Networks (LANs/WANs)	Communications networks at this level include data networks or LANs to support connectivity of the above systems but also includes enterprise wide communications such as wide-area networks to support geographically dispersed offices and data centres. Virtual private networks may be established with trusted supplier networks.

Table 13 Enterprise Zone – Typical EDS Assets

Level	EDS Asset and Technology Areas
4	**Corporate Networks and Enterprise Gateways / DMZs and Trusted Supplier Networks –** *Business systems for supporting EDS planning and logistics, and enclaves to support security of EDS and systems containing information about, or essential to the EDS operations, such as:* • EDS Test kits • Field force enablement (tablets - work instructions, switching instructions, isolations, online mapping, real-time network status information (typically read only from NMS/SCADA) • Business management directly supporting EDS e.g. supply chain dependencies, revenue systems and other data connections and remote access • Data hosting and analytic systems such as storage and processing for logs, reports, event time and sequence consolidation, condition monitoring • Ongoing support and maintenance provisions for whole-of-life EDS performance monitoring and security management, which may include systems, system elements or network nodes to support services as outlined in operations management above • Communications network devices, e.g. as outlined in operations management zone above • Gateways to support defence in depth architecture, e.g. as outlined in operations management zone above • Conduits and data communications at this level typically include: Wide area and local area TCP/IP networks and VPNs • Infrastructure often hosted by enterprise, including virtualised servers.

5.3.4 External Zone

EXTERNAL ZONE

The External Zone is the public data networks of the Internet and systems connected via it. Internet-based systems or those connecting via it are considered hostile in the context of the EDS. In the context of the IACS it may consist of systems or users remote to the enterprise that require connections to provide business benefit for the EDS, such as third-parties for remote access. These typically include the data networks supporting the IACS as outlined in Table 14, and contain typical EDS assets as outlined in Table 15.

Security considerations at this level are the overall protection for the EDS organisation, including the actual EDS. All connections facing the external zone should be identified and appropriately managed as part of cyber security risk management practices for the organisation to reduce exposure to risk. This area contains the highest threat sources to the EDS and IACS are increasingly targeted.

Table 14 External Zone – Data Networks

Typical Data Network	Description
Cloud networks	Cloud networks of other organisations or the energy sector reside in this area. Public or private cloud environments are increasingly used by EDS for information sharing and data analytics.
Third Party Networks	These data networks are owned and managed by third parties and are not connected directly to the EDS organisations data network. These data networks may be owned and operated by a joint venture party or a control system vendor. Where third party networks require connection for IACS, they should be connected securely such as through the use of a third-party DMZ (forming part of trusted supplier networks).
Internet	Public internet where customers or others in the energy sector may access data via enterprise web services.

Table 15 External Zone – Typical EDS Assets

Level	EDS Asset and Technology Areas
5	**External Systems –** *Internet and other systems owned and operated by third parties that the enterprise or operational plant depends on (vendors, suppliers, integrators, contractors, business partners, joint ventures, value chain, etc.)* • Balancing settlements code (Elexon) • Vendor data analytics services (e.g. process and condition monitoring services) • Cloud data hosting (e.g. logs, reports) • Cloud data analytics (e.g. time and sequence) • Third party networks, systems and users, including external connections to EDS zones, e.g. as outlined in EDS zones above, including maintenance laptops to remote access connections • Conduits and data communications at this level typically include: Wide area, local area and TCP/IP networks, VPNs and public/private cloud services

6 Determining EDA security requirements

This section covers cyber security considerations, determination of the security levels and baseline cyber security requirements. It contains the target profile or security level that will be used to develop the reference CSPG statements.

6.1 EDS cyber security considerations

For any given security zone, requirements should meet the desired security attributes to support the desired level of security for that zone. This means that the assets, systems and services within the zone need to be examined and key features identified.

Areas to consider when evaluating cyber security requirements for an EDS asset, system or service include, but are not limited to:

- Core functionality of the system, and impact to the business of a system failure or outage of the asset, system or service
- Key dependencies with other systems
- Use of a consistent time for logging and event investigation
- Identification of interfaces to the asset, system or service, with documented user and system data flows
- Understanding of the organisations architecture relevant to the asset, system or service, such as communications within the zone and external to the zone
- Users, including where and how they access the asset, system or service
- Location of the assets, systems or services
- Types of information about the asset, system or service, and how much important information or sensitive data is contained in related documentation or configuration files
- Storage locations of system related data, such as monitoring data in the cloud or back up discs
- Recovery mechanisms, such as spares holding configuration status, requirements to rebuild from disc or out of the box re-configuration and programming
- Where alarm and event data are processed
- Which system triggers a cyber security incident
- Identify who would be responsible for ensuring an effective response to a system failure or outage (the person responsible should be the risk owner.

To ensure requirements are appropriately identified, it is also necessary for our members to understand the interaction assets, systems or services may have with other equipment or information systems both internally or external to the organisation. EDS have a number of potential interfaces that may have cyber security risks to be managed throughout the system life.

6.2 Determining security levels

Having understood the security considerations, it is necessary to understand the business impact of a compromise to the relevant systems or their information. A business impact assessment will evaluate EDS to identify any immediate, delayed or cascading effects from cyber security incidents considered in the assessment.

Understanding the risk profile for the EDS and where the procured product will be implemented 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 security level to be defined.

Cyber security incidents present in various ways, with different effects on the EDS, examples include:

- A loss of control or visibility to one or more systems
- Loss or disruption to services that the systems rely on, such as telecommunications networks
- Inaccurate information or a loss of confidence in data affecting operation or maintenance of EDS
- Partial of full system outage

The impact of these effects could be:

- Loss of supply
- Health, safety or environmental incident (e.g. explosion at a site)
- Direct or indirect impact on economy and threat to public life
- Lost revenue and/or increased costs to the business
- Reputational damage
- Failure to comply with legislation resulting in fines or even loss of a licence to operate.

A number of reference materials exist for determining energy sector security impact levels, such as the Smart Grid Information Security Level (SGIS-SL). These may be tailored for each organisation and, in some cases, will be associated with the safety risk assessment process that is used within an organisation.

For the purposes of developing the CSPG, Figure 3 shows the reference cyber security impact levels for EDS, this has been adapted from SGIS-SL. Further, more detailed criticality assessments may be undertaken for EDS assets, systems or services as required.

Figure 3 EDS Reference Security Levels

Security Level	Security Level Name	EDS cyber security impact
5	Highly Critical	• CNI highly critical to UK • Health, safety or environmental incident - catastrophic harm • Business damage - loss of license to operate
4	Critical	• CNI critical to UK • Health, safety or environmental incident - very high harm • Business damage (e.g. reputation, financial) ~very high (££££)
3	High	• Health, safety or environmental incident - high harm • Business damage (e.g. reputation, financial) - high (£££) • Operational impact - high % EDS customers affected (e.g. CNI or SGIS-SL or NIS Directive 'essential services')
2	Medium	• Health, safety or environmental incident - medium harm • Business damage (e.g. reputation, financial) - medium (££) • Operational impact - medium % EDS customers affected
1	Low	• Health, safety or environmental incident - low harm • Business damage (e.g. reputation, financial) - low (£) • Operational impact - low % EDS customers affected

6.3 Baseline Requirements for EDS-CSPG

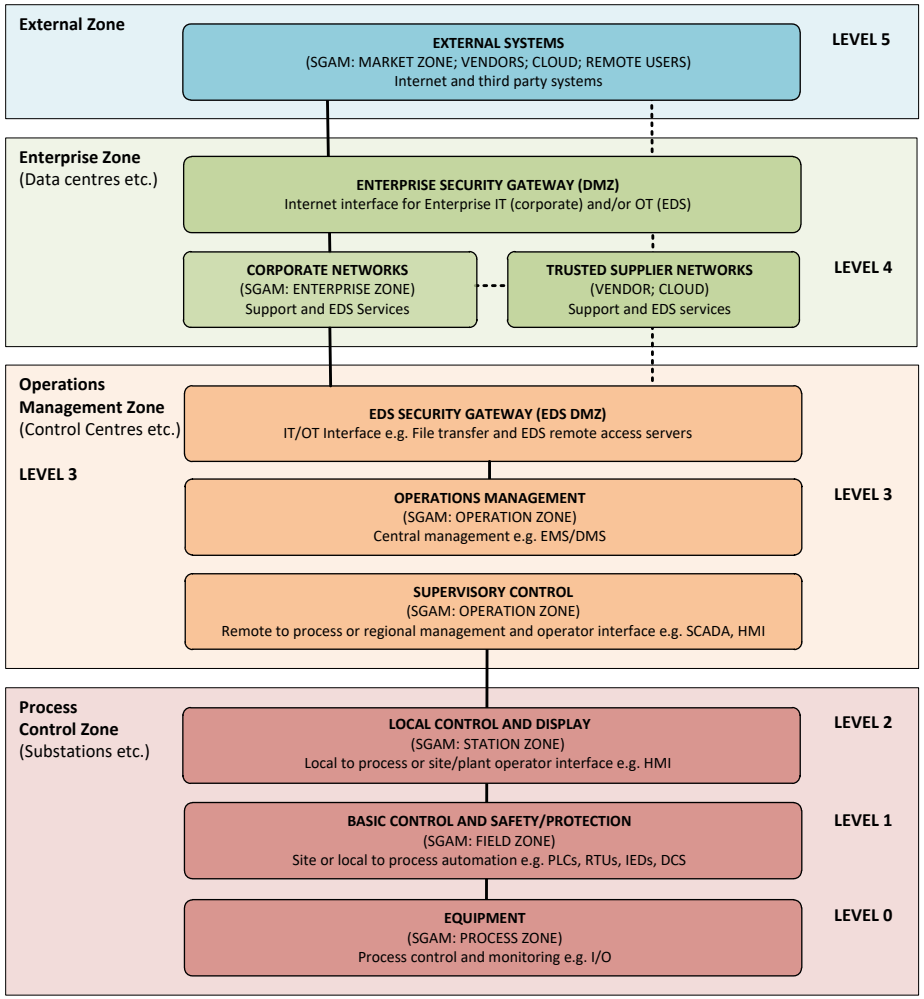
The objective of the EDS-CSPG is to provide tangible risk reduction to the EDS.

Procurement statements have been produced to reflect an industry baseline target state for cyber security across asset and technology areas and throughout the EDS lifecycle. For each security zone reference security levels have been defined to provide a point of reference for the application of the CSPG statements, these are shown in Figure 4.

The scale for the target security level is considered differently in each zone to ensure the baseline security level for our members is appropriate to the requirements for EDS and the reference level can be easily adapted to suit the requirements of the purchaser. As such for operations management the EDS reference security levels have been used as these systems vary in application and criticality, whereas for the process control zone, system functions have been used as these typically share security attributes.

The CSPG statements have been developed to deliver cyber security requirements aligned to a medium security level. These can be enhanced to deliver a higher level or reduced to deliver a lower level where it is determined to be proportionate and appropriate for the EDS, see section 8.4 for a high-level approach to tailoring the statements.

Figure 4 Reference security levels applied to the adapted EDS-CSRM



One reference security level for EDS in this zone **(Target Security Profile for CSPG)** covering: third party requirements for design and development and systems connecting to or processing EDS information.

One reference security level for EDS in this zone **(Target Security Profile for CSPG)** covering:

- Third party adherence to IT/EDS policies as appropriate.
- Implementation in accordance with EDS organisations architecture.
- Consideration to EDS support requirements for access controls, logging, and SLAs.

Three reference security levels for EDS in this zone:

- LOW e.g. Monitoring systems or EMS/SCADA where EDS cyber incident impact could be rated as ~low security level
- **MEDIUM (Target Security Profile for CSPG)** e.g. EMS/SCADA where EDS cyber incident impact ~medium security level
- HIGH e.g. EMS/SCADA where EDS cyber incident impact is ~≥ high security level, NISD Critical or CNI

Covering adherence to EDS policies, architecture, and operational requirements.

Three reference security levels for EDS in this zone:

- LOW e.g. Monitoring systems
- **MEDIUM (Target Security Profile for CSPG)** e.g. Industrial automation and control systems (IACS) and local HMI
- HIGH e.g. Essential services, CNI or SIS

Covering adherence to EDS policies, architecture, and operational requirements, including HSE guidance. Technical standards may include cyber security requirements.

7 Guidance

It is important that the CSPG statements are applied as part of a risk-based approach to cyber security. The CSPG set of statements allows users to improve their supply chain security alongside supporting a consistent application across both the organisation and the wider energy sector.

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

It is recommended that organisations have the following established to manage the security of EDS and provide the appropriate support to the procurement process:

- Governance for cyber security within the EDS organisation
- Organisational policy and standards for cyber security of EDS/OT/IACS
- Cyber security risk assessment and management for the organisation's EDS.

7.1 Application of the CSPG statements

All contracts for new or modified EDS assets, systems or services should contain appropriate cyber security procurement clauses, and any referenced technical specifications should contain further detail relevant to the environment that the technology is being applied in. The reference CSPG statements have been produced to reflect security requirements for EDS across the operational environment and throughout the lifecycle of manufacturing, delivery, installation, testing, and support phases.

Working relationships should be established with third parties involved in delivery of EDS, including projects, operations and the support of these systems. This will enable those in the supply chain to develop appropriate product and service security roadmaps to meet the energy sectors security and product requirements.

It is recommended that the CSPG statements should be implemented in consultation with appropriate personnel to ensure their applicability to each EDS environment. The CSPG does not provide an exclusive set of statements; internal organisational standards, international standards and other procurement guidance can be used to supplement this set of statements as appropriate to the organisation and its approach to managing EDS cyber security risk.

The cyber security statements are written so that they can be integrated into an organisations procurement processes, ensuring that procured products, delivered by third parties in the supply chain include the specified level of cyber security.

It is recommended that organisations review and tailor the CSPG Statements where necessary to suit their own situation, before legal checks and inclusion into procurement contracts. The tailoring of the statements from the suite of clauses should be carried out by people with an understanding of cyber security and its application in the EDS assets, systems or services that are being procured.

The person accountable for EDS cyber security should nominate a responsible person for ensuring that cyber security procurement clauses are included in the contracts for new or upgraded EDS assets, system or services.

Exact procurement clauses will need to be validated against the purchaser's risk assessment to ensure an appropriate and proportionate selection of statement for the product.

7.2 Key terms used within the CSPG statements

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

Term	Description	
'Procured product'	Refers generally to the scope of supply of the procurement contract or purchase agreement and includes all assets, systems or services (see below) being procured for the EDS, and all hardware, software and firmware they are comprised of.	
	• Asset(s)	Includes devices, products, components or pieces of equipment for use in the EDS environment individually or part of a system or service supporting EDS.
	• System(s)	Includes an EDS, a group of sub-systems delivering functionality as part of, or to the EDS, or one individual sub-system delivering functionality as part of, or to the EDS or a standalone system operating within the EDS environment. It may include those systems and sub-systems that support the EDS such as a monitoring or integrated security system(s).
	• Services	Includes the supporting infrastructure and support or maintenance services that the system relies on to operate or maintain its operational capability and security level. Services may include telecommunications, links to transmission networks, or other utilities key to EDS operations and cloud, enterprise IT and security solutions that the EDS relies of for operation or maintenance.
'Purchaser'	Refers to the organisation purchasing, acquiring, or procuring, the contracted product, such as our members or EDS operators.	
'Third Party'	Refers to the supply chain organisation that is contractually obligated to deliver procured products to the EDS organisation. • Third parties include, but are not limited to, suppliers, vendors, system integrators, contractors, support organisations and service providers, including any sub-contractors and product or service delivery partners contracted to provide services on behalf of the contracted third party, such as outsourced IT services (e.g. cloud, data centres, and security management) or contracted personnel. • [Third party] can be changed to vendor, supplier, organisation name etc. as preferable to the organisation	

8 Using the CSPG statements

The sections below provide guidance in using this guidance to select and tailor the reference statements to be fit for use by the purchaser.

8.1 Identify the reference security zone for the procured product

Align the procured product to the cyber security reference model (EDS-CSRM, Section 5.1) to establish the CSPG statements that are appropriate to the contract. This can be done using the asset and technology areas (tables provided in Section 5.3) as necessary.

This guidance is designed to provide guidance for a wide range of EDS procurement, covering:

- Individual EDS components (e.g. field or network device or controller)
- Individual EDS sub-systems (e.g. substation automation, SCADA or DCS)
- Wider or networked EDS (e.g. energy management systems for a number of connected electrical substations or gas transmission stations).
- Services and service provisions to operate, support and maintain the above

As such the procured product may include assets, systems or services that will be implemented in more than one reference security level.

8.2 Understand the security level

Confirm that the required security level is appropriate for the specific EDS environment in relation to the reference baseline target states used in the development of the CSPG statements (see Section 6). The cyber security risk assessment for the organisation's EDS and associated criticality or business impact assessment will provide further details to support this determination.

This will allow the purchaser to evaluate whether the reference 'medium' target state is correct for the environment of the procured product. These reference statements can be enhanced to deliver a higher level, or reduced to deliver a lower level where it is determined to be proportionate and appropriate for the EDS.

8.3 Select reference statements

Select the reference statements relevant to the asset, system technology or service being procured. The statements have been grouped into reference areas as outlined in Table 16, CSPG statements are provided in Section 9.

Table 16 EDS-CSPG statement groupings

Reference statement group	Description
General	Contains a high-level set of requirements to deliver key EDS cyber security measures in general terms.
Supply chain and EDS reference security zone: • External zone	Outlines the requirements that the third-party organisation should meet to ensure cyber security risk is managed in the delivery processes for the procured product (assets, systems or services for EDS). These primarily address the NCSC principles associated with management of cyber security of the EDS supply chain.
EDS reference security zones: • Process control zone	Outlines sets of security requirements that the third party should meet in the delivery of assets, systems or service to the EDS

• Operational management zone • Enterprise zone.	environment, as applicable to the primary implementation zone for the procured product. These aim to ensure that good practice cyber security is delivered and the purchasers operating environment is appropriately considered.

The CSPG statements have been designed to be complementary such that all groups can be used as applicable to the purchaser's procurement processes. For example:

- Use of the 'General' and 'Supply Chain' groups will cover a minimum level of cyber security for any 'procured product' for EDS which may be used to meet an urgent need however; it is recommended that further statements are included based on the reference security zone
- The 'General' group can be included in top level procurement contracts or tender clauses
- The 'Supply Chain' group can be included in or as the basis for an organisation's EDS security specification
- The reference security zone groups can be included within relevant asset or system technical specifications or service agreement, or an organisation's EDS security specification as is most suitable to the purchaser's organisation.

8.4 Tailor for use in procurement processes

Modify the reference statements so they become cyber security procurement clauses appropriate for the specific needs of the purchaser. The exact procurement clauses should be aligned to the actual security level for the EDS environment that the procured product will be implemented in, with appropriate security measures and functionality to meet the business need.

The statements can be tailored to align with the organisations technical specifications and EDS/OT/IACS cyber security standard by changing the statement or providing further information. Reference statements should be strengthened, weakened or left at the baseline level as required. A number of identifiable methods are available within the statements, as outlined in Table 17.

Table 17 Terms for tailoring statements

Term	Method of adapting the statement
[has]	The [has] can be changed to 'shall have' or 'should have' statements as preferable to the organisation and its requirements.
[agreed]	Used in a statement to highlight where the associated elements from the statement should be identified, documented and agreed between the purchaser and the third party as part of the contract or scope of works. Many areas are unique to each organisation or its operational environment and these have been left generic. The agreed statement can draw attention to areas where it is recommended that further detail be specified in supporting documentation, such as technical specification, referenced standards or organisation policy, or agreed with the third party, such as to leverage their expertise in a given area or allow submission of detailed system designs as part of the tender processes.
E.g.'s and notes	Commentary is included with some statements to provide additional guidance to the purchaser for the areas that may be covered by the statement in the form of examples or notes. These can be kept with the statement or removed to maintain the baseline level or changed to sub-clauses or modified for inclusion in technical specifications as desired to strengthen the cyber security measures included for the procured product.

[Third party] and [purchaser]	These terms may be changed from third party and purchaser as desired to personalise or make more appropriate for the contracting parties.

- *E.g. Taking CSPG statement "The procured product has met current good practice or agreed standards for cyber security of EDS at the time of delivery." This statement can be strengthened to a mandatory statement by using [shall have], or weakened to a desirable feature by using [should have]*
- *The [or agreed standards] can be changed to a specific standard that the purchaser wants the procured product to have the design or security controls assured against.*
- *As such the exact statement may be: "The procured product shall have met current good practice and standard IEC62443-2-4 for cyber security of EDS at the time of delivery."*

Additional considerations for tailoring the statements:

- Where additional security requirements are required, the purchaser should use industry accepted reference materials as appropriate for cyber security provisions in industrial systems (such as those in Table 7).
- The purchaser to use statements in conjunction with the organisation's technical standards as relevant, as in addition to the statements included in this guidance, procured products should meet the requirements of applicable IT standards and OT standards for EDS.
- The purchaser to ensure any referenced policies and procedures exist and can be supplied as necessary.

8.5 Provide relevant information to the third party

In addition to the procurement statements the purchaser may have to provide additional information or liaise with the third party to agree security measures and implementation arrangements for the procured product.

- Where CSPG statements reference specifications, policies or procedures then these should be provided to the third party at the time of contract, or an agreed time as recorded in the contract or scope of works.
- Key delivery stages to be agreed as part of the contract or scope of works. The CSPG statements are based on the engineering phases:
  - design and development,
  - product acceptance
    - providing verification and validation of the asset,
    - system or service, including factory acceptance testing (FAT) and site acceptance testing (SAT)
  - operational handover
    - a proof of concept
    - live operation period.

8.6 Assurance

Purchasers will need to verify and validate the delivery of products and services. This includes product assurance, FAT/SAT and other testing processes. As part of this process, security requirements that have been specified will need to undergo equivalent testing.

For any CSPG or contractual security clause, the purchaser should understand how they intend to assess that the product, service or asset is meeting the requirement(s). The purchaser should include testing of cyber security functionality in the FAT, SAT and other product acceptance procedures and documentation. This should cover that the inclusion of the specified security

measures does not adversely affect connectivity, latency, bandwidth, response time and throughput for the EDS during operation, maintenance or emergency conditions. Full lifecycle considerations should be considered in the testing phases.

Users of this guidance should ensure they have the relevant skills and capability to assess that the appropriate security requirements have been included in the procured product. They should also be cognisant that physical and personnel controls may influence the overall security position for the EDS and therefore they should be considered and verified alongside software-based security controls, as relevant to the procured product.

8.6.1 Security Penetration testing

In addition to the above the purchaser may consider use of independent security consultants to perform penetration testing on EDS during procurement stages. Penetration testing should incorporate and refer to the NCSC guidelines for commercially available penetration testing. The security consultant and scope of the testing should be mutually agreed by both the purchaser and the third party. A penetration test report should be submitted to the purchaser and the third party simultaneously and should not be modified from original form.

Any test report produced should be considered as sensitive and should not be disclosed to any third party outside of the agreed EDS security representatives, which may include governmental, regulatory or NCSC groups.

At security boundaries for new EDS, security penetration testing should be carried out in both directions e.g. from the operations management zone to the enterprise / external / process control zones as appropriate and from the enterprise zone to the operations management zone.

9 Cyber security procurement guidance statements

This section contains the CSPG statements which have been grouped into sets that can be adopted for use relevant to the assets, their function, each specific organisation or to any services being supplied to the EDS.

These have been developed with reference to the EDS-CSRM (Figure 2), the reference security levels (Figure 4), and a reference EDS (comprised of energy management, central control system, telecommunications networks and remote sites - See Appendix A). Adoption of these cyber security statements will support delivery of end to end security for EDS.

The statements have been grouped into four reference areas:

- **General** – this section outlines a high-level set of statements to deliver key EDS cyber security measures in general terms. These may be adapted for use in high-level procurement contracts.
- **Supply Chain and external zone** – this section outlines requirements that the third-party organisation should meet to ensure cyber security risk is managed in the delivery processes for the procured product[2]. The statements primarily address the NCSC principles associated with management of cyber security of the EDS supply chain and set expectations that a third party committed to improving cyber security in the procured product should endeavour to meet.
- **EDS reference security zones –** this section outlines sets of baseline security requirements that the third party should meet in the delivery of assets, systems or service to the EDS environment, as applicable to the primary implementation zone for the procured product. These Reference Security Zones aim to ensure that good practice cyber security is delivered and the purchasers operating environment is appropriately considered. The reference security zones (as outlined in section 5.3) are:
  - Process control zone
  - Operational management zone
  - Enterprise zone.

[2] Assets, systems or services as outlined in Section 6

9.1 General procurement statements

GENERAL

Generic cyber security statements that may be used in an overarching procurement contract are provided in this section.

- The procured product is aligned to current good practice for cyber security of industrial systems
- The procured product meets the specified security requirements at the time of delivery, and has the capability to meet the specified security requirements during operation and maintenance, in accordance with agreed support levels
- The third party has responsibility to ensure the agreed design requirements for the EDS are not adversely affected by the addition of the procured product
  - *E.g. functional, operational, performance, safety, environmental and security requirements.*
- The procured product has appropriate security measures to manage recognised and foreseeable cyber security risks and protect the confidentiality, integrity and availability of the Purchaser's information and services and any connections to the Purchaser's environment:
  - The procured product has physical and cyber security features including, but not limited to, identification, authentication, authorisation and accountability mechanisms, e.g. encryption (as appropriate), access control, event and communication logging, monitoring, and alarming, to protect any system devices and configuration from unauthorised modification or use and monitor access.
- The third party has responsibility to include appropriate security measures to protect agreed EDS data within the procured product in accordance with agreed security specifications. The security measures included for the procured product makes use of the latest available proven security technology or functionality.
- The security measures for the procured product includes appropriate software and service updates or agreed measures to manage vulnerabilities associated with the procured product and to maintain the agreed level of system security.
- The third party to notify the purchaser of potential security incidents or relevant risk, such as breaches affecting agreed data connections, personnel issues or compromise of information (physical or electronic) in their organisation and identified vulnerabilities that may affect the purchaser's systems whether considered a cyber security risk by the third party or not.
- The third party has the responsibility to comply with the purchaser's security policies and procedures relating to the information or connections to the purchaser's systems.
- Agreed system security measures included for the procured product, or where modifications to existing security configurations are required, will require testing before being implemented in the agreed operational environment.
- Product acceptance criteria will include assurance that cyber security requirements have been met at agreed contract stages for the procured product, aligning with appropriate system development stages in the EDS lifecycle.
  - *E.g. verification and validation activities to be included in project stage gates or FAT/SAT.*
- The third party is responsible for providing valid licences for security related software and operating systems included with the procured product.

9.2 Supply chain statements and external zone

SUPPLY CHAIN AND EXTERNAL ZONE

Cyber security statements in this section cover cyber security requirements for the third-party organisation providing procured products for implementation for the EDS environment or operating in the external zone of the EDS.

In this zone there are no statements for Identity & Access Control, Data Security, Security Monitoring, Proactive Security Event Discovery, Response and Recovery Planning and Lessons Learned as these are not applicable for this zone.

9.2.1 Governance

- The third party has an Information Security Management System (ISMS) or IACS Cyber Security Management System (CSMS) that covers the procured product.
- The third party has a named individual(s) who is accountable for security of the procured product.
- The third party has appropriate cyber security management policies and processes in place to cover the procured product.
- The third party has appropriate management policies and processes in place to govern its approach to the security of network and information systems relevant to the purchaser's EDS.
- The procured product has the capability to have personally identifiable information identified and managed in accordance with any data protection legislation.
  - The third party has configured the procured product to protect agreed information.

9.2.2 Risk Management

- The third party has a method or framework for managing cyber security risk appropriate to the procured product.

  E.g. during design and development, build, implementation and testing.
- The third party has a security-based risk assessment for the procured product, where appropriate and has implemented security measures to mitigate agreed risks identified in the risk assessment.
  - The risk assessment has included threats appropriate to the agreed EDS environment.
  - The risk assessment has taken into account the purchaser's reference security levels.
- The third party has responsibility to manage any identified vulnerabilities prior to delivery of any procured product and inform the purchaser of any remaining in the procured product at the time of delivery.
- The third party has responsibility to provide product vulnerability notifications related to any procured products during their life in accordance with agreed support contracts.
- The third party must meet any agreed product assurance, monitoring, vulnerability testing, audits or other supply chain security requirements appropriate to the procured product.

  Note: security assurance measures for the procured product may include penetration testing against non-operational environments or testing of individual components in a test environment.

9.2.3 Asset Management

- The third party has responsibility to provide an inventory of all assets included in the delivery of procured products. The inventory contains appropriate information for asset management and identifies critical or operationally important assets where possible.
- The third party has identified and documented system interfaces and dependencies for the procured product.

9.2.4 Supply Chain

- The third party has policies and processes to manage data protection, classification and information handling as appropriate to the procured product.
- The third party has responsibility to treat any user information identifying personal or important EDS information in accordance with agreed information security and data handling policies.

  E.g. the following may be considered as the equivalent of sensitive or confidential: user movements and other Personal Identifiable Information (PII), network topology, EDS designs or procured product configuration, IP addresses of networked devices, security logs, firewall rules and access configurations
- The third party can demonstrate role base access controls, or equivalent measures, for third party personnel with access to information about the purchaser's EDS.

  E.g. project teams during design and development, support staff during operations.

- The third party to apply role-based access controls during development of the procured product in accordance with the purchaser's requirements and data protection policies.
- The third party has accountability for the cyber security of their supply chain, this includes but is not limited to sub-contractors or sub-suppliers contracted in the supply of the procured product to the purchaser.
  - Where equipment is included in the scope of the procured product, these devices are subject to the same security requirements as the third-party delivery.

    E.g. those manufactured with common computer software, such as those including web, ftp or telnet services for maintenance support.
- The third party has responsibility to inform the purchaser of any identified security concerns within the technical specifications as appropriate for the procured product.

  Note: references should be made to international standards for technical specifications and cyber security requirements as appropriate.
- Connections between the third party and the purchaser to only be implemented though agreed methods and using agreed security controls.

  E.g. agreed connections to be documented and security controls identified, such as for interconnected systems, remote access connections, or third-party devices used in the purchaser's organisation.
- The third party and the purchaser are responsible for notifying agreed cyber security events affecting identified and agreed interconnected systems with the other party within agreed timeframes.

  Note: agreed systems and cyber security events to be documented, this may also include threat information and security breaches by personnel. Notification or reporting procedures to be arranged.
- *Confidentiality or non-disclosure agreements covering the purchaser's EDS information will be agreed between the third party and the purchaser.*
- The third party has a policy for personnel management that covers cyber security breaches and personnel changes as appropriate for the procured product.

  E.g. joiners, leavers and movers process covering personnel with access to, or access to information about, the procured product.
- The third party has appropriate management processes to inform the purchaser who has access to the procured product, and access to information about them.

9.2.5 Service Protection Policies and Processes

- The procured product has met the identified requirements to support the purchaser's compliance to agreed security standards and regulations.
- The third party has responsibility to comply with the purchaser's service protection policies and processes appropriate to the procured product and in accordance with agreed support contracts.
- The third party has responsibility to ensure appropriate security checks are performed for their personnel[3] with access to the procured product.

9.2.6 System Security

- The third party has responsibility to include security measures in accordance with good practice for procured products using cloud technology or cloud-based implementation.

  E.g. following NCSC Cloud security principles.

9.2.7 Resilient Networks & Systems

- The third party has responsibility to include security measures in accordance with good practice for procured products providing services that are agreed to be the equivalent of critical or essential to the EDS.

9.2.8 Staff Awareness & Training

- The third party has responsibility to ensure their personnel[3] have awareness of cyber security risk, and capability as appropriate to their role and can provide records of their training.

[3] Personnel includes employees and any sub-contractors or contractors of the third party

- Third party personnel are to agree and adhere to the purchaser's information security or EDS/OT/IACS cyber security policy and supporting guidance when using or connected to the purchaser's systems.

  E.g. sign the purchasers acceptable use policies or equivalent; adhere to defence in depth architecture requirements for access; or to provide appropriate details of any personnel that require access to the purchaser's operational systems, such as for on-site maintenance or remote access.

9.3 Process control zone

PROCESS CONTROL ZONE

Cyber security statements in this section cover cyber security requirements for the third-party organisation providing assets, systems or services for implementation in the EDS process control zone.
In this zone there are no statements for Supply Chain, Proactive Security Event Discovery, Response and Recovery Planning and Lessons Learned as these are not applicable for this zone.

9.3.1 Governance

- The third-party has responsibility to comply with EDS/OT/IACS cyber security standards, technical specifications including EDS security or existing security measures as appropriate to the lifecycle stage of the procured product or the EDS.

9.3.2 Risk Management

- The third-party has a vulnerability assessment for the procured product at the time of delivery.

  Note: This may evaluate the hardware, software, firmware/operating systems, agreed network connections and access mechanisms.

9.3.3 Asset Management

- The third party has responsibility to ensure any changes to the EDS are updated in inventory or a record is provided to the purchaser.

9.3.4 Service Protection Policies and Processes

- The security measures included for the procured product adopt a secure system architecture whilst allowing the EDS to meet agreed specified design requirements, such as functional, operational, performance, safety, and environmental requirements.
  - The third party has responsibility to ensure that any security measures do not adversely impact EDS design requirements.
- The procured product has met current good practice or agreed standards for cyber security of EDS at the time of delivery.
- The procured product has appropriate security, network and segregation provisions to support and enable a 'defence-in-depth' approach to the wider EDS security.
- The procured product has the capability to allow for forensic analysis to be performed as appropriate for it or its connection to the EDS to gather information in accordance with legislative requirements. This includes, but is not limited to, historical event and action logs storage and retention, covering EDS operation and network activity.
- The third party has the responsibility to provide appropriate documentation to support operation, maintenance, restoration or modification of security measures included in the procured product. This may include, but is not limited to:
  - Back up, restore and recovery procedures
  - Processes for installation of application and product software updates, e.g. vendor patches or firmware
  - Details for security management of user and system accounts password or authentication policy management and other access controls

- Configured security settings or operating system permissions required for operation and maintenance
- Operation and maintenance procedures for procured product security configuration
- Appropriate architecture information, contacts and procedures for accessing agreed procured product data or systems from within the EDS boundary and external to it, e.g. enterprise zone
- Appropriate architecture information, contacts and procedures for accessing agreed asset, system or service data or systems hosted external to it, e.g. enterprise or external zone
- Details of any hardening undertaken on the procured products, e.g. software components that have been removed and/or disabled from default configuration, and details of all disabled or removed ports
- Details of the agreed protocols for use by the procured product required for operation and maintenance (including emergency conditions or to support remote access) and the purpose of these data connections, to support secure configuration for data communications.
- Details to enable appropriate personnel to re-configure or re-build a replacement asset, system or service to the same security level as relevant to the procured product

  E.g. Details of applications, administrative utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems included with the procured product.
- Details of device or equipment connectivity included with the procured product, such as network diagrams.
- Details for how to change security parameters from third party configured or product default parameters
- Details for how to apply patches, security files or firmware updates to the procured product with consideration to the agreed operational environment.
- *Details for configuration of security event detection, e.g. information of baseline asset, system or service configuration, such as static file names, dynamic file name patterns, system and user accounts permissions, baseline procured product operational parameters to support detection of unauthorised code execution on the host, abnormal host utilisation or permissions*

9.3.5 Identity & Access Control

- The procured product has the capability to only allow authorised users to connect to the Layer 1 controllers (e.g. IED, PLC, RTU, etc.), both locally and remotely, whilst maintaining security of the EDS such that is not accessible by unauthorised users.
- The procured product has protection via passwords as a minimum to level 1 controller configuration.

Where the procured product includes servers, workstations or wide-area networking equipment these should meet the following:

- The procured product has capability to implement access controls for users and system connections.
  - The procured product has appropriate access controls applied to protect against unauthorised access.
  - The procured product has appropriate configuration such that only software accounts required for operation and maintenance are active, and others have been disabled, removed or modified from default settings.
  - The procured product has the capability to configure user account-based lockouts and system connection timeouts.
  - The procured product has the capability to incorporate password protection for core systems or administrative functions such as computer Basic Input Output System (BIOS) and system accounts.
- The procured product has capability to implement access permissions based on user's role, e.g. privileged user management.
- The third party to apply defence in depth architecture as appropriate for the procured product.

- The procured product has the capability to authenticate and authorise user and system connections as appropriate. This may use passwords, two-factor authentication, biometric or proximity devices, or hardware-backed certificate authentication as appropriate.
- The procured product has the capability to configure restrictions or requirements for passwords used on the procured product as appropriate
  - *E.g. Passwords may have expiration and user notification requirements, users may not be able to repeat passwords for a period of passwords, and passwords may have complexity requirements such as length, character, and symbol or number usage.*
- The third party has appropriate configuration such that generic user accounts are not used for the procured product, e.g. administrator or engineer.
- The procured product has capability of event logging agreed actions and protecting logs against tampering throughout the agreed retention period.
  - Procured product has the capability to log authorised access and unauthorised access attempts as appropriate
  - The third party supplied system being supplied has appropriate configuration to log unauthorised access attempts.
  - The procured product includes access logging mechanisms to record when a user or device connects to them
  - Procured product has the capability to log account activity and to audit activity, such as management, application of policy, and user account activity as appropriate.
- The procured product has capability of having physical security controls applied
  - The procured product has appropriate physical security controls applied to protect it as appropriate.
  - *E.g. port locks, facility door controls or alarms, cabinets with lockable doors, device or equipment locks, consideration for equipment categories within enclosures, and intrusion detection systems*
  - *E.g. the procured product includes lockable or locking enclosures for important control system components, such as critical servers and networking hardware.*
  - The procured product has appropriate port and key management or other physical access control processes provided as agreed.
  - The procured product has appropriate security measures and configuration to meet agreed identity and access specifications.

9.3.6 Data Security

- The procured product has capability to support data protection requirements, such as to transfer EDS data securely with minimal risk of data loss, corruption or unauthorised access.
  - *E.g. Secure data transfer through communications connections*
  - *E.g. Secure data transfer through all SGAM interoperability or SGIS interoperability layers*
  - *E.g. Secure data transfer to systems outside the EDS operations management zone, e.g. moving data for back up or log retention and data analytics*
- The third party has the responsibility to ensure that user or system authentication credentials for the procured product are not transmitted in clear text.
- The procured product has the capability to have protocols in use within the EDS monitored and controlled.
  - All protocols being used within the operations management zone or for connecting with it are to be agreed to ensure any security devices or system management permits authorised traffic without delay or rejection during operation and maintenance (including emergency conditions).
  - The procured product has capability to notify, log and alarm any unauthorised protocols detected at agreed EDS locations to protect the operations management zone as appropriate to the technology.
- The procured product has capability to preserve data confidentiality in accordance with legislative requirements. This may include time stamping, encrypting (if required), and controlling access to audit trails and log files containing PII.

- The procured product has capability to enable network segregation and intermediary network connections to isolate security zones, as appropriate to the technology.
- For procured products delivering security at the EDS operations management zone boundary:
  - The procured product has the capability of authenticating agreed user or service access independently of the enterprise environment where appropriate and without relying on services provided by the enterprise.
  - The third party has responsibility to evaluate if data encryption is required for the purchaser's security level and as appropriate for the application of the procured product.
  - If data encryption is required, an appropriate encryption method and implementation is agreed with the purchaser proportionate to the technology and any data communication considerations for the EDS such as response time constraints and information handling.
  - The procured product has the capability to limit access to any networked devices from specific locations or network zones as appropriate.
  - The third party has responsibility to restrict access to networked devices from agreed locations or network zones in accordance with agreed security policy or procedures, and provide appropriate configuration documentation.
- The procured product has capability to support data protection requirements, such as to store EDS data securely with minimal risk of data loss, corruption or unauthorised access.
  - *E.g. Secure storage of backup and recovery files or configuration data, and agreed logs*
  - *E.g. Lifecycle management of agreed EDS data to offline storage to meet data retention requirements*
  - *E.g. Storage of information required to comply with legislation.*
- The procured product has the capability to have system hardening implemented such that only the services, applications, and ports required to deliver the agreed functionality are enabled at the time of delivery in accordance with good practice guidance or agreed industry benchmarks
  - The procured product includes appropriately hardened servers, workstations and equipment; locked down to meet agreed security using appropriate physical protection and software security measures. This includes, but is not limited to, ports, services and applications.
  - *E.g. Centre for Internet Security (CIS) benchmarks*
  - The third party has the responsibility to demonstrate agreed ports and interfaces can be enabled and disabled as required.
  - The equipment, or supporting systems, have the capability to allow authorised maintenance personnel access to the maintenance ports in accordance with agreed security policy and procedures. The third party is responsible for ensuring only authorised personnel have the capability to modify agreed configurations at the time of delivery.
- The procured product has appropriate security measures and configuration to meet agreed data security specifications.

9.3.7 System Security

- The procured product has a clearly identified security boundary.
- The procured product has all connection points identified and security measures documented.
- The procured product has the capability to have access permitted only through the agreed EDS architecture and security policy.
- The procured product has appropriate security measures and configuration to restrict access to agreed mechanisms.
- The procured product has security measures included to meet current good practice for EDS security, agreed cyber security standards and relevant legislation.

  E.g. IEC62443, sections completed at the time of contract award or as agreed
  E.g. IEC61508 revision 2, has risk assessment requirements for cyber security for safety related systems
  E.g. IEC 62351, includes requirements to protect integrity and availability in EDS data communications from threats to data in transit.
  E.g. IEC 61850, includes requirements to protect integrity and availability in substation communications

Note: where standards or guidance is agreed the purchaser to provide appropriate information for the third party to be able to meet the requirements.
Note: where standards or approaches are agreed the requirements from these are to be included in verification and validation of the procured product.

- The procured product has the capability of using IPv4 and IPv6 as appropriate, where equipment is not compliant to both protocol standards these are identified such that EDS networks can be managed appropriately at the time of delivery or in the future.
- The procured product has appropriate security measures between network zones to manage agreed network traffic and configuration information is protected and handled in accordance with security policies

  E.g. firewall with corresponding rule sets or equivalent measures and configuration documentation between process control zone(s) and operations management zone
  E.g. data diodes between process control zone and enterprise zone or external zone for monitoring or read only data
  E.g. outbound initiated VPN tunnel from process control zones to operations management zones to protect WAN traffic
  E.g. firewalls deployed to protect operations management or process control zones certified by the latest version of the ICSA Labs Modular Firewall Certification Criteria or by the Common Criteria Recognition Agreement or by a similar recognised certification body.
  E.g. device authentication for authorised network nodes.
- The third party has identified all appropriate software and hardware configuration parameters for the procured product.

  E.g. Details for applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including, but not limited to software revisions, operating system and application patch levels and firmware versions
- The third party has responsibility to incorporate appropriate software and service updates to mitigate identified vulnerabilities associated with the product prior to delivery and to maintain the agreed security level in accordance with agreed support contracts.

  E.g. operating system, application patches, security file and firmware updates, protocol upgrades, agreed work arounds
- The procured product has the capability to have software patches or firmware updates applied.
  - The third party to include documentation, operational and maintenance guidelines for all product and functional/application software included in the procured product.
- Where the procured product includes servers, workstations or networking equipment to be implemented in the process control zone that are connected to and managed by operations management systems (e.g. EMS/SCADA), these should meet the highest security requirements, such as those for the centralised system (e.g. operational management zone) or specific requirements at this level.

  E.g. local control room HMI accessing to central SCADA servers
- The procured product has appropriate capability to support network protection measures and system monitoring to support the agreed security level for the EDS, including but not limited to
  - Patch management
  - Malware detection
  - Vulnerability management
  - Network and/or host-based intrusion detection/prevention system(s) (IDS/IPS) tailored to the IACS environment;
  - Gateway solutions, tailored to the IACS environment, including monitoring and response
  - Digitally signed update files to support the above.
  - Processes and procedures to support implementation of the above in the IACS environment.

  E.g. Recommended Practice: Updating Antivirus in an Industrial Control System (NCCIC, January 2018)
- The procured product has appropriate security measures and configuration to deliver malware prevention, removable media controls and configuration to the agreed security level and specifications for equipment implemented in the process control zone.

9.3.8 Resilient Networks & Systems

- The procured product is compatible with any agreed EDS security or system management and monitoring systems.

  E.g. SIEM, IP address management, network management (traffic, vulnerability scans) AV or equivalent enterprise arrangements, configuration and file integrity management.
- The procured product has the capability for controlled management for EDS in the event of a cyber incident in another security zones.

  E.g. the procured product has identifiable network disconnection points
  E.g. process control zone to maintain local operational capability when disconnected from operations management systems (e.g. EMS/SCADA).
- The procured product has appropriate security measures and configuration to deliver network security and secure configuration to the agreed security level and specifications for equipment implemented in the process control zone.

9.3.9 Staff Awareness & Training

- The third party has the responsibility to provide appropriate training and documentation for security software and hardware included within the procured product, and as required for the maintenance of the procured product where it provides EDS security. Training requirements include, but are not limited to:
  - All security devices
  - Access points onto the procured product or EDS as relevant (e.g. where the access points are)
  - System security management for the procured product (this includes system administrator training)
  - Procedures for upgrades and patching the procured product
  - Appropriate penetration testing methods
  - Disaster recovery for after a security event occurs, as agreed and is appropriate to the procured product.

9.3.10 Security Monitoring

- The procured product has capability to be monitored by agreed EDS security operations or management systems.

  Note: these may be in the process control zone or other EDS security zones.
- The procured product to notify or generate an alarm for agreed security events. This capability includes, but is not limited to:
  - Access logging and generation of a security event alarm when the level 1 devices are connected to either remotely or locally.
  - Configuration logging and generation of a security event alarm when controller configurations are changed.
  - Where equipment has the capability of producing multiple alarms, the third party has the responsibility to ensure alarms are amalgamated into agreed common alarm(s) for identified security events in the EDS management system.

    Note: security events, may also include indicators of compromise, such as unauthorised access attempts, server, workstation or controller system performance or network performance outside of operational baseline parameters, and other unusual system or operator connections or behaviour.
- The procured product has appropriate security measures and configuration to deliver agreed monitoring specifications and incident response capability for equipment implemented in the process control zone.

9.4 Operations management zone

OPERATIONS MANAGEMENT ZONE

Cyber security statements in this section cover cyber security requirements for the third-party organisation providing assets, systems or services for implementation in the EDS operations management zone.
Communications conduits to any other EDS security zones are covered within this section, e.g. network communications to process control zones, enterprise or external zone.
In this zone there are no statements for Supply Chain, Response and Recovery Planning and Lessons Learned as these are not applicable for this zone.

9.4.1 Governance

- The third party has responsibility to comply with EDS/OT/IACS cyber security standards, technical specifications including EDS security or existing security measures as appropriate to the lifecycle stage of the procured product or the EDS.

9.4.2 Risk Management

- The third party has a vulnerability assessment for the procured product at the time of delivery.
  Note: This may evaluate the hardware, software, firmware/operating systems, agreed network connections and access mechanisms.

9.4.3 Asset Management

- The third party has responsibility to ensure any changes are updated in inventory or a record is provided to the purchaser.

9.4.4 Service Protection Policies and Processes

- The security measures included for the procured product adopt a secure system architecture whilst allowing the EDS to meet agreed specified design requirements, such as functional, operational, performance, safety, and environmental requirements.
  - The third party has responsibility to ensure that any security measures do not adversely impact EDS design requirements.
- The procured product has met current good practice or agreed standards for cyber security of EDS at the time of delivery.
- The procured product has appropriate security, network and segregation provisions to support and enable a ‘defence-in-depth’ approach to the wider EDS security.
- The procured product has the capability to allow for forensic analysis to be performed as appropriate for it or its connection to the EDS to gather information in accordance with legislative requirements. This includes, but is not limited to, historical event and action logs storage and retention, covering EDS operation and network activity.
- The third party has the responsibility to provide appropriate documentation to support operation, maintenance, restoration or modification of security measures included in the procured product. This may include, but is not limited to:
  - Back up, restore and recovery procedures
  - Processes for installation of application and product software updates, e.g. vendor patches or firmware
  - Details for security management of user and system accounts password or authentication policy management and other access controls
  - Configured security settings or operating system permissions required for operation and maintenance
  - Operation and maintenance procedures for procured product security configuration
  - Appropriate architecture information, contacts and procedures for accessing agreed procured product data or systems from within the EDS boundary and external to it, e.g. enterprise zone
  - Appropriate architecture information, contacts and procedures for accessing agreed asset, system or service data or systems hosted external to it, e.g. enterprise or external zone

- Details of any hardening undertaken on the procured products, e.g. software components that have been removed and/or disabled from default configuration, and details of all disabled or removed ports
- Details of the agreed protocols for use by the procured product required for operation and maintenance (including emergency conditions or to support remote access) and the purpose of these data connections, to support secure configuration for data communications.
- Details to enable appropriate personnel to re-configure or re-build a replacement asset, system or service to the same security level as relevant to the procured product

  E.g. Details of applications, administrative utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems included with the procured product.
- Details of device or equipment connectivity included with the procured product, such as network diagrams.
- Details for how to change security parameters from third party configured or product default parameters
- Details for how to apply patches, security files or firmware updates to the procured product with consideration to the agreed operational environment.
- *Details for configuration of security event detection, e.g. information of baseline asset, system or service configuration, such as static file names, dynamic file name patterns, system and user accounts permissions, baseline procured product operational parameters to support detection of unauthorised code execution on the host, abnormal host utilisation or permissions*

9.4.5 Identity & Access Control

- The procured product has capability to implement access controls for users and system connections.
  - The procured product has appropriate access controls applied to protect against unauthorised access.
  - The procured product has appropriate configuration such that only software accounts required for operation and maintenance are active, and others have been disabled, removed or modified from default settings.
  - The procured product has the capability to configure user account-based lockouts and system connection timeouts.
  - The procured product has the capability to incorporate password protection for core systems or administrative functions such as computer Basic Input Output System (BIOS) and system accounts.
- The procured product has capability to implement access permissions based on user's role, e.g. privileged user management.
- The third party to apply defence in depth architecture as appropriate for the procured product.
- The procured product has the capability to authenticate and authorise user and system connections as appropriate. This may use passwords, two-factor authentication, biometric or proximity devices, or hardware-backed certificate authentication as appropriate.
- The procured product has the capability to configure restrictions or requirements for passwords used on the procured product as appropriate

  E.g. Passwords may have expiration and user notification requirements, users may not be able to repeat passwords for a period of passwords, and passwords may have complexity requirements such as length, character, and symbol or number usage.
- The third party has appropriate configuration such that generic user accounts are not used for the procured product, e.g. administrator or engineer.
- The procured product has capability of event logging agreed actions and protecting logs against tampering throughout the agreed retention period.
  - Procured product has the capability to log authorised access and unauthorised access attempts as appropriate
  - The third party supplied system being supplied has appropriate configuration to log unauthorised access attempts.

  - The procured product includes access logging mechanisms to record when a user or device connects to them
  - Procured product has the capability to log account activity and to audit activity, such as management, application of policy, and user account activity as appropriate.
- The procured product has capability of having physical security controls applied
  - The procured product has appropriate physical security controls applied to protect it as appropriate.

    E.g. port locks, facility door controls or alarms, cabinets with lockable doors, device or equipment locks, consideration for equipment categories within enclosures, and intrusion detection systems
    E.g. the procured product includes lockable or locking enclosures for important control system components, such as critical servers and networking hardware.
  - The procured product has appropriate port and key management or other physical access control processes provided as agreed.
- The procured product has appropriate security measures and configuration to meet agreed identity and access specifications.

9.4.6 Data Security

- The procured product has capability to support data protection requirements, such as to transfer EDS data securely with minimal risk of data loss, corruption or unauthorised access.

  E.g. Secure data transfer through communications connections
  E.g. Secure data transfer through all SGAM interoperability or SGIS interoperability layers
  E.g. Secure data transfer to systems outside the EDS operations management zone, e.g. moving data for back up or log retention and data analytics
- The third party has the responsibility to ensure that user or system authentication credentials for the procured product are not transmitted in clear text.
- The procured product has the capability to have protocols in use within the EDS monitored and controlled.
  - All protocols being used within the operations management zone or for connecting with it are to be agreed to ensure any security devices or system management permits authorised traffic without delay or rejection during operation and maintenance (including emergency conditions).
  - The procured product has capability to notify, log and alarm any unauthorised protocols detected at agreed EDS locations to protect the operations management zone as appropriate to the technology.
- The procured product has capability to preserve data confidentiality in accordance with legislative requirements. This may include time stamping, encrypting (if required), and controlling access to audit trails and log files containing PII.
- The procured product has capability to enable network segregation and intermediary network connections to isolate security zones, as appropriate to the technology.
- For procured products delivering security at the EDS operations management zone boundary:
  - The procured product has the capability of authenticating agreed user or service access independently of the enterprise environment where appropriate and without relying on services provided by the enterprise.
  - The third party has responsibility to evaluate if data encryption is required for the purchaser's security level and as appropriate for the application of the procured product.
  - If data encryption is required, an appropriate encryption method and implementation is agreed with the purchaser proportionate to the technology and any data communication considerations for the EDS such as response time constraints and information handling.
  - The procured product has the capability to limit access to any networked devices from specific locations or network zones as appropriate.
  - The third party has responsibility to restrict access to networked devices from agreed locations or network zones in accordance with agreed security policy or procedures, and provide appropriate configuration documentation.
- The procured product has capability to support data protection requirements, such as to store EDS data securely with minimal risk of data loss, corruption or unauthorised access.

E.g. Secure storage of backup and recovery files or configuration data, and agreed logs
E.g. Lifecycle management of agreed EDS data to offline storage to meet data retention requirements
E.g. Storage of information required to comply with legislation.

- The procured product has the capability to have system hardening implemented such that only the services, applications, and ports required to deliver the agreed functionality are enabled at the time of delivery in accordance with good practice guidance or agreed industry benchmarks
  - The procured product includes appropriately hardened servers, workstations and equipment; locked down to meet agreed security using appropriate physical protection and software security measures. This includes, but is not limited to, ports, services and applications.
    E.g. Centre for Internet Security (CIS) benchmarks
  - The third party has the responsibility to demonstrate agreed ports and interfaces can be enabled and disabled as required.
  - The equipment, or supporting systems, have the capability to allow authorised maintenance personnel access to the maintenance ports in accordance with agreed security policy and procedures. The third party is responsible for ensuring only authorised personnel have the capability to modify agreed configurations at the time of delivery.
- The procured product has appropriate security measures and configuration to meet agreed data security specifications.

9.4.7 System Security

- The procured product has a clearly identified security boundary.
- The procured product has all connection points identified and security measures documented.
- The procured product has the capability to have access permitted only through the agreed EDS architecture and security policy.
- The procured product has security measures included to meet current good practice for EDS security, agreed cyber security standards and relevant legislation.
  E.g. NCSC guidance, recommendations for industrial systems to be applied as appropriate to cover all lifecycle stages
  E.g. IEC62443, sections completed at the time of contract award or as agreed
  E.g. ISO27019, addressing differences between ISO27002:2005 and 2013.
  E.g. IEC 62351, includes requirements to protect integrity and availability in EDS data communications from threats to data in transit.
  E.g. NERC CIP includes comprehensive compliance driven requirements for EDS.
  E.g. NIST 800-53 includes cyber security controls appropriate for EDS.
  Note: where standards or guidance is agreed the purchaser to provide appropriate information for the third party to be able to meet the requirements.
  Note: where standards or approaches are agreed the requirements from these are to be included in verification and validation of the procured product.
- The procured product has the capability of using IPv4 and IPv6 as appropriate, where equipment is not compliant to both protocol standards these are identified such that EDS networks can be managed appropriately at the time of delivery or in the future.
- The procured product has appropriate security measures between network zones to manage agreed network traffic and configuration information is protected and handled in accordance with security policies
  E.g. firewall with corresponding rule sets or equivalent measures and configuration documentation between operations management zone and enterprise zone
  E.g. data diodes between operations management zone and enterprise zone or process control zone for monitoring or read only data
  E.g. outbound initiated VPN tunnel from process control zones to operations management zones to protect WAN traffic
  E.g. firewalls deployed to protect operations management or process control zones certified by the latest version of the ICSA Labs Modular Firewall Certification Criteria or by the Common Criteria Recognition Agreement or by a similar recognised certification body.
  E.g. Device authentication for authorised network nodes.
- The third party has identified all appropriate software and hardware configuration parameters for the procured product

E.g. Details for applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including, but not limited to software revisions, operating system and application patch levels and firmware versions

- The third party has responsibility to incorporate appropriate software and service updates to mitigate identified vulnerabilities associated with the product prior to delivery and to maintain the agreed security level

  E.g. operating system, application patches, security file and firmware updates, protocol upgrades, agreed work arounds
- The procured product has the capability to have software patches or firmware updates applied.
  - The third party to include documentation, operational and maintenance guidelines for all product and application software included in the procured product.
- The procured product has appropriate security measures and configuration to deliver malware prevention, removable media controls and configuration to the agreed security level and specifications for equipment implemented in the operations management zone.

9.4.8 Resilient Networks & Systems

- The procured product is compatible with any agreed EDS security or system management and monitoring systems.

  E.g. SIEM, IP address management, network management (traffic, vulnerability scans) AV or equivalent enterprise arrangements, configuration and file integrity management.
- The procured product has the capability for controlled management for EDS in the event of a cyber incident in another security zone.

  E.g. the procured product has identifiable network disconnection points
  E.g. EDS to maintain local operational capability when disconnected from operations management systems (e.g. EMS/SCADA).
  E.g. Shutdown process for EMS/SCADA if loss of control or visibility occurs due to cyber security event. The procured product should fail in a safe manner on agreed incident trigger.
- The procured product has the capability for controlling security related configuration changes such that only authorised personnel are allowed to make changes or modifications to the procured product, and any included equipment affecting EDS security.
  - The procured product is compatible with agreed integrated change control management functionality for the EDS, to support system version management, restoration/roll-back, reporting, and configuration access controls.
  - The third party has responsibility to document processes to support change management for security
  - Configuration changes affecting EDS system security require appropriate design acceptance and testing before being implemented in the EDS environment.
- The third party has the responsibility to inform the purchaser where configuration changes for the procured product may affect interfaces or dependencies to other asset, systems or services within the agreed EDS or enterprise environments.
- The procured product is compatible with any agreed EDS / central security management system for the purpose of monitoring security status of systems or files, and allowing installation of security configuration changes, updates, patches or other agreed administrative functions to the assets or devices included in agreed security management zone(s), such as centralised EDS user management, access controls, or network/device port management.
- The third party has responsibility to include appropriate security measures to protect agreed EDS data within the procured product in accordance with agreed security specifications.
  - The third party has responsibility to ensure that included security measures do not adversely affect connectivity, latency, bandwidth, response time, and throughput of agreed EDS data at acceptance testing and when connected to existing equipment (e.g. at SAT or delivery).
  - The third party has responsibility to adopt a secure software development life cycle (SDLC) process in accordance with agreed standards (see section 9.4.7) to minimise risk of common vulnerabilities or malicious code in applications during development of EDS.

    E.g. identify software development process standards, requirements for code reviews and independent software code reviews as appropriate.

  - The third party is responsible for informing the purchaser of the plan to manage software development in the procured product for the EDS.
- The third party has the responsibility to ensure that data connections for monitoring or to provide viewing capability from other level security zones are implemented in a secure way such that data transfer arrangements protect the asset, system and service from unauthorised access, and data flow is restricted to preserve monitoring or read-only status as appropriate.

  E.g. read only connections protected with gateways, not only system configuration.
  E.g. outbound initiated traffic from high security level to lower security level
  E.g. historical data transferred out of EDS environment via data diodes
- The third party has the responsibility to ensure that data connections for remote access, file transfer into the operational environment or other agreed capability from other level security zones are implemented in a secure way and in accordance with the purchasers operational procedures, such that data transfer arrangements and access controls protect the procured product from unauthorised access, and data flow is restricted to agreed data connections or access roles, and to preserve agreed security levels.

  E.g. remote access authorisation and configuration controls through agreed security gateways
  E.g. data connections established from highest security level to lowest as appropriate (typically low Purdue level to high Purdue level)
  E.g. data connections for this purpose to block unauthorised access, e.g. users or system access requests denied if not agreed.
  E.g. arrangements and processes to be established to ensure authorised user or system access is not restricted.
  E.g. data connections from process control zone to operations management zone to view live EMS/SCADA system information in real-time, such as maintenance access to historical logs or creation of specific diagnostic reports.
  E.g. access arrangements during installation and testing phases and their removal upon procured product delivery.
- The procured product has appropriate security measures and configuration to deliver network security and configuration to the agreed security level and specifications for equipment implemented in the operations management zone.

9.4.9 Response and Recovery Planning

- The procured product has the capability to have its configuration saved in accordance with agreed EDS backup and recovery mechanisms for all software, hardware, networks and communications components, and their configuration

  E.g., the procured product is compatibility with wider EDS back up and restoration technologies.

9.4.10 Staff Awareness & Training

- The third party has the responsibility to provide appropriate training and documentation for security software and hardware included within the procured product, and as required for the maintenance of the procured product where it provides EDS security. Training requirements include, but are not limited to:
  - All security devices
  - Access points onto the procured product or EDS as relevant (e.g. where the access points are)
  - System security management for the procured product (this includes system administrator training)
  - Procedures for upgrades and patching the procured product
  - Appropriate penetration testing methods
  - Disaster recovery for after a security event occurs, as agreed and is appropriate to the procured product.

9.4.11 Security Monitoring

- The procured product has capability to be monitored by agreed EDS security operations or management systems.

Note: these may be in the operations management zone or other EDS security zones.

- The procured product to notify or generate an alarm for agreed security events. This capability includes, but is not limited to:
  - Access logging and generation of a security event alarm when *important EDS system* are accessed either remotely or locally, e.g. critical EMS/SCADA servers.
  - Configuration logging and generation of a security event alarm when *important EDS system* configurations are changed, e.g. critical EMS/SCADA applications.

    Note: security events, may include indicators of compromise, such as unauthorised access attempts, server and workstation system performance or network performance outside of operational baseline parameters, and other unusual system or operator connections or behaviour.
  - Where equipment has the capability of producing multiple alarms, the third party has the responsibility to ensure alarms are amalgamated into agreed common alarm(s) for identified security events in the EDS management system.
- The procured product has appropriate security measures and configuration to deliver agreed monitoring specifications and incident response capability for equipment implemented in the operations management zone.

9.4.12 Proactive Security Event Discovery

- The procured product has the capability to detect intrusion at the equipment where appropriate to the technology.

  E.g. the third party has configured Host Intrusion Detection System (HIDS) for servers, workstations and networking equipment included in the procured product.
- The procured product has the capability to generate an event log each time a port on any device within the agreed zone has changed state, e.g. is enabled/activated or disabled/deactivated, such as when a maintenance port is connected to.

  E.g. network ports, USB ports or any other port that can be used to access the agreed EDS zone.
- The procured product has the capability to detect intrusion in the network.

  E.g. the third party has provided Intrusion Detection System (IDS) for the procured product, or information to configure the purchaser's EDS IDS, such as baseline traffic profiles within agreed communications paths or network traffic across agreed boundaries.

9.5 Enterprise Zone

ENTERPRISE ZONE

Cyber security statements in this section cover cyber security requirements for the third-party organisation providing assets, systems or services for implementation in the EDS organisations enterprise zone.

The following sections provide statements for procured products that provide key services to the EDS environment. The purchaser is responsible for ensuring that any additional cyber security requirements appropriate to the implementation of the procured product in the enterprise zone are also met.

In this zone there are no statements for Supply Chain, Proactive Security Event Discovery, Response and Recovery Planning and Lessons Learned as these topics are not applicable for this zone.

9.5.1 Governance

- The third party has responsibility to comply with the EDS organisation's enterprise information or cyber security standards, and relevant technical specifications or existing security measures as appropriate for the procured product and its implementation for the EDS.

  Note: where the procured product connects to EDS within the operations management zone, it is the purchaser's responsibility to address any conflicts between enterprise policies and standards and any requirements for the procured product (such as the purchasers

EDS/OT/IACS cyber security standards, technical specifications including EDS security or other EDS security measures)

9.5.2 Risk Management

- The third party has a vulnerability assessment for the procured product at the time of delivery.

  Note: This may evaluate the hardware, software, firmware/operating systems, agreed network connections and access mechanisms.

9.5.3 Asset Management

- The third party has responsibility to ensure any changes are updated in inventory or a record is provided to the purchaser.

9.5.4 Service Protection Policies and Processes

- The security measures included for the procured product adopt a secure system architecture whilst allowing the EDS to meet agreed specified design requirements, such as functional, operational, performance, safety, and environmental requirements.
  - The third party has responsibility to ensure that any security measures do not adversely impact EDS design requirements.
- The procured product has met current good practice or agreed standards for cyber security of EDS at the time of delivery.
- The procured product has appropriate security, network and segregation provisions to support and enable a 'defence-in-depth' approach to the wider EDS security.
- The procured product has the capability to allow for forensic analysis to be performed as appropriate for it or its connection to the EDS to gather information in accordance with legislative requirements. This includes, but is not limited to, historical event and action logs storage and retention, covering EDS operation and network activity.
- The third party has the responsibility to provide appropriate documentation to support operation, maintenance, restoration or modification of security measures included in the procured product. This may include, but is not limited to:
  - Back up, restore and recovery procedures
  - Processes for installation of application and product software updates, e.g. vendor patches or firmware
  - Details for security management of user and system accounts password or authentication policy management and other access controls
  - Configured security settings or operating system permissions required for operation and maintenance
  - Operation and maintenance procedures for procured product security configuration
  - Appropriate architecture information, contacts and procedures for accessing agreed procured product data or systems from within the EDS boundary and external to it, e.g. enterprise zone
  - Appropriate architecture information, contacts and procedures for accessing agreed asset, system or service data or systems hosted external to it, e.g. enterprise or external zone
  - Details of any hardening undertaken on the procured products, e.g. software components that have been removed and/or disabled from default configuration, and details of all disabled or removed ports
  - Details of the agreed protocols for use by the procured product required for operation and maintenance (including emergency conditions or to support remote access) and the purpose of these data connections, to support secure configuration for data communications.
  - Details to enable appropriate personnel to re-configure or re-build a replacement asset, system or service to the same security level as relevant to the procured product

    E.g. Details of applications, administrative utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems included with the procured product.
  - Details of device or equipment connectivity included with the procured product, such as network diagrams.

  - Details for how to change security parameters from third party configured or product default parameters
  - Details for how to apply patches, security files or firmware updates to the procured product with consideration to the agreed operational environment.
- Details for configuration of security event detection, e.g. information of baseline asset, system or service configuration, such as static file names, dynamic file name patterns, system and user accounts permissions, baseline procured product operational parameters to support detection of unauthorised code execution on the host, abnormal host utilisation or permissions.
- The third party has responsibility to ensure that any security measures do not adversely impact enterprise zone design requirements.

9.5.5 Identity & Access Control

Where the procured product includes servers, workstations or wide-area networking equipment these should:

- The procured product has capability to implement access controls for users and system connections.
  - The procured product has appropriate access controls applied to protect against unauthorised access.
  - The procured product has appropriate configuration such that only software accounts required for operation and maintenance are active, and others have been disabled, removed or modified from default settings.
  - The procured product has the capability to configure user account-based lockouts and system connection timeouts.
  - The procured product has the capability to incorporate password protection for core systems or administrative functions such as computer Basic Input Output System (BIOS) and system accounts.
- The procured product has capability to implement access permissions based on user's role, e.g. privileged user management.
- The third party to apply defence in depth architecture as appropriate for the procured product.
- The procured product has the capability to authenticate and authorise user and system connections as appropriate. This may use passwords, two-factor authentication, biometric or proximity devices, or hardware-backed certificate authentication as appropriate.
- The procured product has the capability to configure restrictions or requirements for passwords used on the procured product as appropriate
  - *E.g. Passwords may have expiration and user notification requirements, users may not be able to repeat passwords for a period of passwords, and passwords may have complexity requirements such as length, character, and symbol or number usage.*
- The third party has appropriate configuration such that generic user accounts are not used for the procured product, e.g. administrator or engineer.
- The procured product has capability of event logging agreed actions and protecting logs against tampering throughout the agreed retention period.
  - Procured product has the capability to log authorised access and unauthorised access attempts as appropriate
  - The third party supplied system being supplied has appropriate configuration to log unauthorised access attempts.
  - The procured product includes access logging mechanisms to record when a user or device connects to them
  - Procured product has the capability to log account activity and to audit activity, such as management, application of policy, and user account activity as appropriate.
- The procured product has capability of having physical security controls applied
  - The procured product has appropriate physical security controls applied to protect it as appropriate.
  - *E.g. port locks, facility door controls or alarms, cabinets with lockable doors, device or equipment locks, consideration for equipment categories within enclosures, and intrusion detection systems*

- *E.g. the procured product includes lockable or locking enclosures for important control system components, such as critical servers and networking hardware.*
- The procured product has appropriate port and key management or other physical access control processes provided as agreed.

- The procured product has appropriate security measures and configuration to meet agreed identity and access specifications.
- The third party is responsible that procured products located in the enterprise zone can be managed in accordance with EDS/OT/IACS and enterprise IT security policies and procedures as appropriate.

  E.g. access control configuration, security logging and reporting, service provisions and security policies such as patch management and configuration management authorised by EDS representatives or deployed by EDS functions.

9.5.6 Data Security

Where the procured product includes servers, workstations or wide-area networking equipment these should:

- The procured product has capability to support data protection requirements, such as to transfer EDS data securely with minimal risk of data loss, corruption or unauthorised access.
  - *E.g. Secure data transfer through communications connections*
  - *E.g. Secure data transfer through all SGAM interoperability or SGIS interoperability layers*
  - *E.g. Secure data transfer to systems outside the EDS operations management zone, e.g. moving data for back up or log retention and data analytics*
- The third party has the responsibility to ensure that user or system authentication credentials for the procured product are not transmitted in clear text.
- The procured product has the capability to have protocols in use within the EDS monitored and controlled.
  - All protocols being used within the operations management zone or for connecting with it are to be agreed to ensure any security devices or system management permits authorised traffic without delay or rejection during operation and maintenance (including emergency conditions).
  - The procured product has capability to notify, log and alarm any unauthorised protocols detected at agreed EDS locations to protect the operations management zone as appropriate to the technology.
- The procured product has capability to preserve data confidentiality in accordance with legislative requirements. This may include time stamping, encrypting (if required), and controlling access to audit trails and log files containing PII.
- The procured product has capability to enable network segregation and intermediary network connections to isolate security zones, as appropriate to the technology.
- For procured products delivering security at the EDS operations management zone boundary:
  - The procured product has the capability of authenticating agreed user or service access independently of the enterprise environment where appropriate and without relying on services provided by the enterprise.
  - The third party has responsibility to evaluate if data encryption is required for the purchaser's security level and as appropriate for the application of the procured product.
  - If data encryption is required, an appropriate encryption method and implementation is agreed with the purchaser proportionate to the technology and any data communication considerations for the EDS such as response time constraints and information handling.
  - The procured product has the capability to limit access to any networked devices from specific locations or network zones as appropriate.
  - The third party has responsibility to restrict access to networked devices from agreed locations or network zones in accordance with agreed security policy or procedures, and provide appropriate configuration documentation.
- The procured product has capability to support data protection requirements, such as to store EDS data securely with minimal risk of data loss, corruption or unauthorised access.
  - *E.g. Secure storage of backup and recovery files or configuration data, and agreed logs*

- *E.g. Lifecycle management of agreed EDS data to offline storage to meet data retention requirements*
- *E.g. Storage of information required to comply with legislation.*

- The procured product has the capability to have system hardening implemented such that only the services, applications, and ports required to deliver the agreed functionality are enabled at the time of delivery in accordance with good practice guidance or agreed industry benchmarks
  - The procured product includes appropriately hardened servers, workstations and equipment; locked down to meet agreed security using appropriate physical protection and software security measures. This includes, but is not limited to, ports, services and applications.
  - *E.g. Centre for Internet Security (CIS) benchmarks*
  - The third party has the responsibility to demonstrate agreed ports and interfaces can be enabled and disabled as required.
  - The equipment, or supporting systems, have the capability to allow authorised maintenance personnel access to the maintenance ports in accordance with agreed security policy and procedures. The third party is responsible for ensuring only authorised personnel have the capability to modify agreed configurations at the time of delivery.
- The procured product has appropriate security measures and configuration to meet agreed data security specifications.
- The third party is responsible for ensuring that EDS data is classified, handled and stored in accordance with EDS/OT/IACS and enterprise IT security policies and procedures as appropriate.
- The purchaser is responsible for ensuring that procured products located in the enterprise zone have their cyber security risk managed in accordance with EDS/OT/IACS and enterprise IT security policies and procedures as appropriate.

  E.g. trusted supplier or energy sector cloud service provisions affecting EDS are appropriately managed within the enterprise zone.
  E.g. service level agreements for procured products and maintenance arrangements align with EDS requirements

9.5.7 System Security

- The third party is responsible for ensuring that the procured product is implemented in accordance with EDS requirements.

Where the procured product includes servers, workstations or wide-area networking equipment these should:

- The procured product has a clearly identified security boundary.
- The procured product has all connection points identified and security measures documented.
- The procured product has the capability to have access permitted only through the agreed EDS architecture and security policy.
- The procured product has security measures included to meet current good practice for EDS security, agreed cyber security standards and relevant legislation.
  - *E.g. NCSC guidance, recommendations for industrial systems to be applied as appropriate to cover all lifecycle stages*
  - *E.g. IEC62443, sections completed at the time of contract award or as agreed*
  - *E.g. ISO27019, addressing differences between ISO27002:2005 and 2013.*
  - *E.g. IEC 62351, includes requirements to protect integrity and availability in EDS data communications from threats to data in transit.*
  - *E.g. NERC CIP includes comprehensive compliance driven requirements for EDS.*
  - *E.g. NIST 800-53 includes cyber security controls appropriate for EDS.*
  - *Note: where standards or guidance is agreed the purchaser to provide appropriate information for the third party to be able to meet the requirements.*
  - *Note: where standards or approaches are agreed the requirements from these are to be included in verification and validation of the procured product.*
- The procured product has the capability of using IPv4 and IPv6 as appropriate, where equipment is not compliant to both protocol standards these are identified such that EDS networks can be managed appropriately at the time of delivery or in the future.

- The procured product has appropriate security measures between network zones to manage agreed network traffic and configuration information is protected and handled in accordance with security policies
  - *E.g. firewall with corresponding rule sets or equivalent measures and configuration documentation between operations management zone and enterprise zone*
  - *E.g. data diodes between operations management zone and enterprise zone or process control zone for monitoring or read only data*
  - *E.g. outbound initiated VPN tunnel from process control zones to operations management zones to protect WAN traffic*
  - *E.g. firewalls deployed to protect operations management or process control zones certified by the latest version of the ICSA Labs Modular Firewall Certification Criteria or by the Common Criteria Recognition Agreement or by a similar recognised certification body.*
  - *E.g. Device authentication for authorised network nodes.*
- The third party has identified all appropriate software and hardware configuration parameters for the procured product
  - *E.g. Details for applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including, but not limited to software revisions, operating system and application patch levels and firmware versions*
- The third party has responsibility to incorporate appropriate software and service updates to mitigate identified vulnerabilities associated with the product prior to delivery and to maintain the agreed security level
  - *E.g. operating system, application patches, security file and firmware updates, protocol upgrades, agreed work arounds*
- The procured product has the capability to have software patches or firmware updates applied.
  - The third party to include documentation, operational and maintenance guidelines for all product and application software included in the procured product.
- The procured product has appropriate security measures and configuration to deliver malware prevention, removable media controls and configuration to the agreed security level and specifications for equipment implemented in the operations management zone.

9.5.8 Resilient Networks & Systems

Where the procured product includes servers, workstations or wide-area networking equipment these should:

- The procured product is compatible with any agreed EDS security or system management and monitoring systems.
  - *E.g. SIEM, IP address management, network management (traffic, vulnerability scans) AV or equivalent enterprise arrangements, configuration and file integrity management.*
- The procured product has the capability for controlled management for EDS in the event of a cyber incident in another security zone.
  - *E.g. the procured product has identifiable network disconnection points*
  - *E.g. EDS to maintain local operational capability when disconnected from operations management systems (e.g. EMS/SCADA).*
  - *E.g. Shutdown process for EMS/SCADA if loss of control or visibility occurs due to cyber security event. The procured product should fail in a safe manner on agreed incident trigger.*
- The procured product has the capability for controlling security related configuration changes such that only authorised personnel are allowed to make changes or modifications to the procured product, and any included equipment affecting EDS security.
  - The procured product is compatible with agreed integrated change control management functionality for the EDS, to support system version management, restoration/roll-back, reporting, and configuration access controls.
  - The third party has responsibility to document processes to support change management for security
  - Configuration changes affecting EDS system security require appropriate design acceptance and testing before being implemented in the EDS environment.

- The third party has the responsibility to inform the purchaser where configuration changes for the procured product may affect interfaces or dependencies to other asset, systems or services within the agreed EDS or enterprise environments.
- The procured product is compatible with any agreed EDS / central security management system for monitoring security status of systems or files, and allowing installation of security configuration changes, updates, patches or other agreed administrative functions to the assets or devices included in agreed security management zone(s), such as centralised EDS user management, access controls, or network/device port management.
- The third party has responsibility to include appropriate security measures to protect agreed EDS data within the procured product in accordance with agreed security specifications.
  - The third party has responsibility to ensure that included security measures do not adversely affect connectivity, latency, bandwidth, response time, and throughput of agreed EDS data at acceptance testing and when connected to existing equipment (e.g. at SAT or delivery).
  - The third party has responsibility to adopt a secure software development life cycle (SDLC) process in accordance with agreed standards (see section 9.4.7) to minimise risk of common vulnerabilities or malicious code in applications during development of EDS.
  - *E.g. identify software development process standards, requirements for code reviews and independent software code reviews as appropriate.*
  - The third party is responsible for informing the purchaser of the plan to manage software development in the procured product for the EDS.
- The third party has the responsibility to ensure that data connections for monitoring or to provide viewing capability from other level security zones are implemented in a secure way such that data transfer arrangements protect the asset, system and service from unauthorised access, and data flow is restricted to preserve monitoring or read-only status as appropriate.
  - *E.g. read only connections protected with gateways, not only system configuration.*
  - *E.g. outbound initiated traffic from high security level to lower security level*
  - *E.g. historical data transferred out of EDS environment via data diodes*
- The third party has the responsibility to ensure that data connections for remote access, file transfer into the operational environment or other agreed capability from other level security zones are implemented in a secure way and in accordance with the purchasers operational procedures, such that data transfer arrangements and access controls protect the procured product from unauthorised access, and data flow is restricted to agreed data connections or access roles, and to preserve agreed security levels.
  - *E.g. remote access authorisation and configuration controls through agreed security gateways*
  - *E.g. data connections established from highest security level to lowest as appropriate (typically low Purdue level to high Purdue level)*
  - *E.g. data connections for this purpose to block unauthorised access, e.g. users or system access requests denied if not agreed.*
  - *E.g. arrangements and processes to be established to ensure authorised user or system access is not restricted.*
  - *E.g. data connections from process control zone to operations management zone to view live EMS/SCADA system information in real-time, such as maintenance access to historical logs or creation of specific diagnostic reports.*
  - *E.g. access arrangements during installation and testing phases and their removal upon procured product delivery.*
- The procured product has appropriate security measures and configuration to deliver network security and configuration to the agreed security level and specifications for equipment implemented in the operations management zone.

9.5.9 Staff Awareness & Training

- The third party has the responsibility to provide appropriate training and documentation for security software and hardware included within the procured product, and as required for the maintenance of the procured product where it provides EDS security. Training requirements include, but are not limited to:
  - All security devices

  - Access points onto the procured product or EDS as relevant (e.g. where the access points are)
  - System security management for the procured product (this includes system administrator training)
  - Procedures for upgrades and patching the procured product
  - Appropriate penetration testing methods
- Disaster recovery for after a security event occurs, as agreed and is appropriate to the procured product.

9.5.10 Security Monitoring

- The procured product should meet the 'Security Monitoring' requirements as outlined in operations management zone (Section 9.4.11) and as appropriate for implementation in the enterprise zone.
- The purchaser is responsible for ensuring that any enterprise monitoring requirements appropriate to the implementation of the procured product are also met.
- The procured product has appropriate security measures and configuration to deliver agreed monitoring specifications and incident response capability for EDS equipment implemented in the enterprise zone.

9.5.11 Proactive Security Event Discovery

- The procured product has capability to be monitored by agreed EDS security operations or management systems.
  - *Note: these may be in the operations management zone or other EDS security zones.*
- The procured product to notify or generate an alarm for agreed security events. This capability includes, but is not limited to:
  - Access logging and generation of a security event alarm when *important EDS system* are accessed either remotely or locally, e.g. critical EMS/SCADA servers.
  - Configuration logging and generation of a security event alarm when *important EDS system* configurations are changed, e.g. critical EMS/SCADA applications.
  - *Note: security events, may include indicators of compromise, such as unauthorised access attempts, server and workstation system performance or network performance outside of operational baseline parameters, and other unusual system or operator connections or behaviour.*
  - Where equipment has the capability of producing multiple alarms, the third party has the responsibility to ensure alarms are amalgamated into agreed common alarm(s) for identified security events in the EDS management system.
- The procured product has appropriate security measures and configuration to deliver agreed monitoring specifications and incident response capability for equipment implemented in the operations management zone.
- The purchaser is responsible for ensuring that any enterprise monitoring requirements appropriate to the implementation of the procured product are also met.

References

- NCSC – UK National Cyber Security Centre Website
- DHS – Cyber Security Procurement Language for Control Systems (CSPLCS)
- IEC62443 – Industrial Automation and Control Systems Security
    - Part 2.1 Requirements for an IACS security management system;
    - Part 3.3 System security requirements and security levels; and others)
- NIST – National Institute of Standards and Technology – Cyber Security Framework (CSF)
- EPRI – US Electricity Power Research Institute - Cyber Security Procurement Methodology (CSPM)
- US DOE Cyber Security Language for Energy Delivery Systems (CSLEDS)
- BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.(German Department for Energy and Water) White Paper -Requirements for Secure Control and Telecommunication Systems
- CEN-CENELEC-ETSI Smart Grid Coordination Group – Smart Grid Information Security (SGIS) (Including Security Levels – SL)
- CEN-CENELEC-ETSI Smart Grid Coordination Group – Smart Grid Reference Architecture (including Architecture Model - SGAM)

Definitions and acronyms

Key acronyms relevant to this guidance

Key definitions are included below, only commonly used terms are included below.

AV	Anti-virus and equivalent anti-malware applications
BEIS	UK Government – Department of Business, Energy and Industrial Strategy
CAF	Cyber Assessment Framework
CCTV	Closed Circuit Television
CNI	Critical National Infrastructure
CSPG	Cyber Security Procurement Guidance (this guidance)
DCS	Distributed Control Systems
DFR	Dynamic Frequency Response
DHS CSPLCS	Department of Homeland Security – Cyber Security Procurement Language for Control Systems
DOE CSLEDS	US Department of Energy – Cyber Security Language for Energy Delivery Systems
DMS	Distributed Management System
DMZ	Demilitarised Zone
DNO	Distributed Network Operator
DSO	Distributed Systems Operator
E,C&I	Electrical, Control & Instrumentation
EDS	Energy Delivery System
EDS CSRM	Energy Delivery System – Cyber Security Reference Model
EMS	Energy Management Systems
ENA	Energy Network Association
EPRI	Electric Power Research institute
ESD	Emergency Shutdown Systems
FAT	Factory Acceptance Test
F&G	Fire and Gas System
FIM	Fibre Interface Module
FO	Fibre Optic
FPP	Flexible Plug and Play
GDPR	EU General Data Protection Regulation.
HMI	Human Machine Interface
HIDS	Host Intrusion Detection System
HR	Human Resources

HSE	UK Health and Safety Executive (responsible for health, safety and environmental effects of process industries and in the health and safety in the workplace)
IACS	Industrial Automation and Control Systems
ICS	Industrial Control Systems
ICSS	Integrated Control and Safety System
IDS/IPS	Intrusion Detection System / Intrusion Protection System
ISMS	Information Security Management System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IIoT	Industrial Internet of Things
IoT	Internet of Things
IPS	Intrusion Protection System
ISO	International Organisation for Standards
IT	Information Technology
LAN	Local Area Network
MPLS	Multi-Protocol Layer Switching
NCSC	UK National Cyber Security Centre
NIS Directive	EU Network and Information Systems Directive or NIS Directive
NMS	Network Management System
OT	Operational Technology
PAS	Process Automation Systems
PCN	Process Control Network
PLC	Programmable Logic Controllers
PMN	Process Monitoring Network
PTSN	Public switched telephone network
RFID	Radio Frequency Identification
RTU	Remote Terminal Units
SAT	Site Acceptance Testing
SCADA	Supervisory Control and Data Acquisition Systems
SDLC	Software Development Lifecycle
SGAM	Smart Grid Architecture Model
SGIS-SL	Smart Grid Information Security – Security Levels
SIEM	Security information and event management
SIS	Safety Instrumented Systems
SOC	Security Operations Centre
TCP/IP	Transmission Control Protocol and Internet Protocol

VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WBED	Bundesverband der Energie- und Wasserwirtschaft e.V.(German Department for Energy and Water)
UK	United Kingdom

Key definitions relevant to this guidance

Key definitions are included below, additional definitions can be found in the guidance included in Table 7 that may be used as a source in further understanding this guidance.

Concept	Definition
Security Zone	An area of protection, a grouping of electronic assets that share common security requirements
Conduit	The security groupings for the communications of information into, out of and within the security zones
Security Level	A definition for the desired level of security for a zone
Countermeasures	The security (counter)measures or controls that are put in place to prevent the security of the zone or conduit being compromised
Demilitarised Zone (DMZ)	A security zone that is provides a network layer to support the transfer of information between security zones of different security levels
Security Perimeter	The boundary that the physical and logical countermeasures protect the assets within, for the business and its respective security zones

Appendices

A. Development of this guidance

A collaborative approach was used to develop the CSPG utilising expertise from EDS operators, BEIS and vendors.

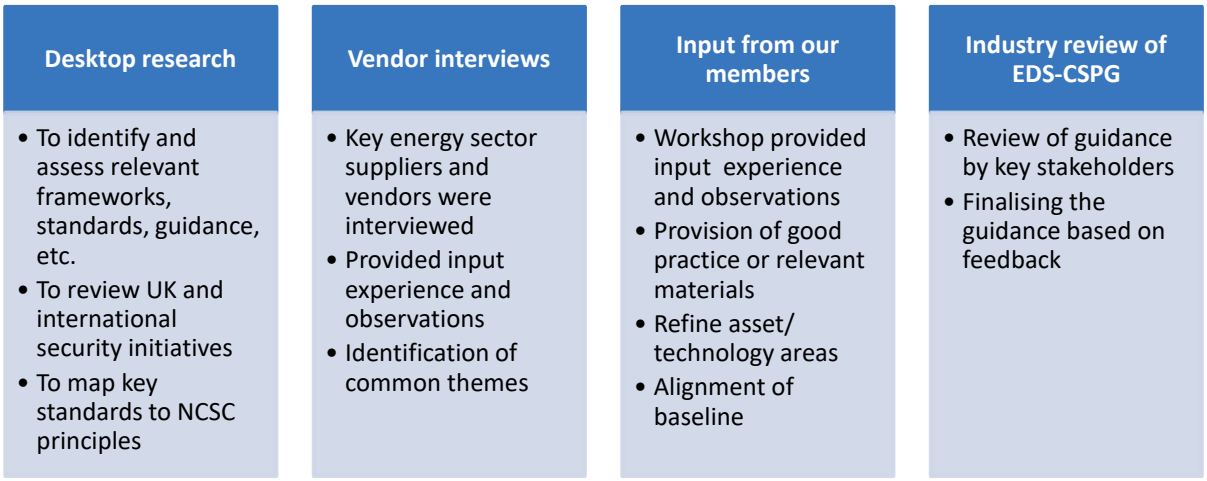
A.1. Approach

We have worked to ensure the correct balance has been achieved in producing procurement guidance that non-cyber security procurement staff can understand, whilst clearly defining the assets/technology areas, such that the EDS-CSPG statements can be meaningfully implemented and assessed.

This guidance is aligned to the 14 High-Level Principles (see https://www.ncsc.gov.uk/guidance/table-view-principles-and-related-guidance/) required by the NIS Directive. The document then provides specific security statements, developed from government guidance, published standards and recognised industry good practice.

In order to ensure this document is useable and pragmatic, while also meeting the cyber security needs of the industry, this guidance has been developed following a structured and collaborative approach as outlined in Figure 5 .

Figure 5 Approach outline



A.2. Outline of the NCSC 10 Steps to Cyber Security

NCSC recommend organisations apply their 10 Steps to Cyber Security (see https://www.ncsc.gov.uk/guidance/10-steps-cyber-security) to provide an effective means to help protect an organisation from attack, as shown in Figure 6. This principle has been further developed to provide guidance relating to key areas considered most at risk because they are commonly used in cyber-attacks.

The key areas relevant to industrial systems that will be used to develop the CSPG statements are:

- Network security
- Malware prevention
- Removable media controls
- Secure configuration
- Managing user privileges

- Monitoring
- Incident management.

To support our members and to ensure an acceptable, adaptable and appropriate industry baseline for EDS in the absence of specific industry guidelines, the UK Government's 10 Steps to Cyber Security will be conceptually adopted and enhanced with requirements from the most relevant international standards. As such where cyber security capability is identified to deliver security in the above key areas, the EDS-CSPG statements include additional statements to reflect that the above security measures should be configured appropriately in procured products[4] for implementation in the EDS environment.

Figure 6 NCSC's 10 Steps to cyber security

[4] Assets, systems or services as outlined in Section 7 Guidance

B. NIS Directive applicability

The published thresholds under the NIS Directive for operators of essential services are shown in Table 18.

Table 18 EDS Operators of Essential Services

Essential Service	UK Identification Thresholds
Electricity transmission	In England, Scotland and Wales: Network operators with the potential to disrupt supply to greater than 250,000 consumers. International interconnectors and Direct Current converter station with a capacity greater than or equal to 1 Gigawatts (GW). In Northern Ireland: The holder of a transmission licence under Article 8(1)(b) of the Electricity (NI) Order 1992.
Electricity distribution	In England, Scotland and Wales: Network operators with the potential to disrupt supply to greater than 250,000 consumers. In Northern Ireland: The holder of a distribution licence under Article 8(1)(bb) of the Electricity (NI) Order 1992.
Gas transmission (downstream)	In England, Scotland and Wales: Network operators with the potential to disrupt supply to greater than 250,000 consumers. Operators of gas interconnectors with technical capacity greater than 20mcm/d In Northern Ireland: The holder of a licence under Article 8(1)(a) of the Gas (NI) Order 1996.
Gas distribution	In England, Scotland and Wales: Network operators with the potential to disrupt supply to greater than 250,000 consumers. For Northern Ireland: The holder of a licence under Article 8(1)(a) of the Gas (NI) Order 1996.

C. NCSC principles

A high-level summary of details of the NIS Directive objectives and principles is provided in Table 19.

Table 19 NIS Directive 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. • Key security considerations and references relevant to third party: – Approach to managing cyber security – 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. • Key security considerations and references relevant to third party: – Approach to managing cyber security risk – 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). • Key security considerations and references relevant to third party: – Inventory – System interfaces and dependencies – 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. • Key security considerations and references relevant to third party: – 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 support delivery of essential services.

	• Key security considerations and references relevant to third party: – Communication of policy and procedures – Personnel Security: – 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. • Key security considerations and references relevant to third party: – User, system and device access – 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. • Key security considerations and references relevant to third party: – Design to protect data – Protecting data in transit – Protect data at rest – Protecting data on mobile devices – Secure disposal – 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. • Key security considerations and references relevant to third party: – System design – Configuration – System management – Vulnerability management – 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. • Key security considerations and references relevant to third party: – Prepare to respond to disruption – Maintenance and repair – Segregation – Capacity – Diversity and dependencies – Working backups – 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. • Key security considerations and references relevant to third party: – Security culture – Communications – 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. • Key security considerations and references relevant to third party: – Detecting incidents or activity – Log collection and aggregation – Analysis and threat intelligence – Protection of personal data and general network performance and service quality – 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). • Key security considerations and references relevant to third party: – 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.

	• Key security considerations and references relevant to third party: – **Preparation for an incident** – 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. • Key security considerations and references relevant to third party: – 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

D. Alignment with key procurement language sources

NCSC Ref	Source: Section No	Procurement Language Source: Section Heading	Procurement Language Source: Section Title
A.1 Governance			
		N/A	None identified
A.2 Risk Management			
		N/A	None identified
A.3 Asset Management			
		N/A	None identified
A.4 Supply Chain			
	DHS CSPLCS 6.1	FLAW REMEDIATION	Notification and Documentation from Vendor
	DHS CSPLCS 6.2	FLAW REMEDIATION	Problem Reporting
	DOE CPLEDS 3.2	THE SUPPLIER'S LIFE CYCLE SECURITY PROGRAM	Documentation and Tracking of Vulnerabilities
	DOE CPLEDS 3.3	THE SUPPLIER'S LIFE CYCLE SECURITY PROGRAM	Problem Reporting
	DOE CPLEDS 3.5	THE SUPPLIER'S LIFE CYCLE SECURITY PROGRAM	Supplier Personnel Management
	DOE CPLEDS 3.6	THE SUPPLIER'S LIFE CYCLE SECURITY PROGRAM	Secure Hardware and Software Delivery
B.1 Service Protection Policies and Processes			
	DHS CSPLCS 4.7	ACCOUNT MANAGEMENT	Separation Agreement
	DOE CPLEDS 3.1	THE SUPPLIER'S LIFE CYCLE SECURITY PROGRAM	Secure Development Practices
B.2 Identity & Access Control			
	DHS CSPLCS 2.3	SYSTEM HARDENING	Changes to File System and Operating Systems Permissions
	DHS CSPLCS 4.1	ACCOUNT MANAGEMENT	Disabling, Modifying or Removing Well Known or Guest Accounts
	DHS CSPLCS 4.2	ACCOUNT MANAGEMENT	Session Management
	DHS CSPLCS 4.3	ACCOUNT MANAGEMENT	Password / Authentication Policy and Management
	DHS CSPLCS 4.4	ACCOUNT MANAGEMENT	Account Auditing and Logging
	DHS CSPLCS 4.5	ACCOUNT MANAGEMENT	Role Based Access Control for Control Systems Applications
	DHS CSPLCS 4.6	ACCOUNT MANAGEMENT	Single Sign On
	DOE CPLEDS 2.2	GENERAL CYBERSECURITY PROCUREMENT LANGUAGE	Access Control
	DOE CPLEDS 2.3	GENERAL CYBERSECURITY PROCUREMENT LANGUAGE	Account Management
	DOE CPLEDS 2.4	GENERAL CYBERSECURITY PROCUREMENT LANGUAGE	Session Management
	DOE CPLEDS 2.5	GENERAL CYBERSECURITY PROCUREMENT LANGUAGE	Authentication/Password Policy and Management
B.3 Data Security			
	DHS CSPLCS 10.1	REMOTE ACCESS	Dial-up Modems
	DHS CSPLCS 10.2	REMOTE ACCESS	Dedicated Line Modems

	DHS CSPLCS 10.3	REMOTE ACCESS	TCP/IP
	DHS CSPLCS 10.4	REMOTE ACCESS	Web Based Interfaces
	DHS CSPLCS 10.5	REMOTE ACCESS	Secure Virtual Private Networks
	DHS CSPLCS 10.6	REMOTE ACCESS	Serial Communications Security
	DHS CSPLCS 13.1	WIRELESS TECHNOLOGIES	Bluetooth Technologies
	DHS CSPLCS 13.2	WIRELESS TECHNOLOGIES	Wireless Closed-Circuit TV Technology
	DHS CSPLCS 13.3	WIRELESS TECHNOLOGIES	Radio Frequency Identification Technology
	DHS CSPLCS 13.4	WIRELESS TECHNOLOGIES	802.11 Technology
	DHS CSPLCS 13.5	WIRELESS TECHNOLOGIES	ZigBee Technology
	DHS CSPLCS 13.6	WIRELESS TECHNOLOGIES	WirelessHART Technology
	DHS CSPLCS 13.7	WIRELESS TECHNOLOGIES	Mobile Radios
	DHS CSPLCS 13.8	WIRELESS TECHNOLOGIES	Wireless Mesh Network Technology
	DHS CSPLCS 13.9	WIRELESS TECHNOLOGIES	Cellular Technology
	DHS CSPLCS 13.10	WIRELESS TECHNOLOGIES	WiMAX Technology
	DHS CSPLCS 13.11	WIRELESS TECHNOLOGIES	Microwave and Satellite Technology
	DOE CPLEDS 2.1	GENERAL CYBERSECURITY PROCUREMENT LANGUAGE	Software and Services
	DOE CPLEDS 6.1	WIRELESS TECHNOLOGIES	General Wireless Technology Provisions
	DOE CPLEDS 7.1	CRYPTOGRAPHIC SYSTEM MANAGEMENT	Cryptographic System Documentation
	DOE CPLEDS 7.2	CRYPTOGRAPHIC SYSTEM MANAGEMENT	Cryptographic Key and Method Establishment, Usage, and Update
B.4 System Security			
	DHS CSPLCS 2.1	SYSTEM HARDENING	Removal of Unnecessary Services and Programmes
	DHS CSPLCS 2.4	SYSTEM HARDENING	Hardware Configuration
	DHS CSPLCS 2.6	SYSTEM HARDENING	Installing Operating Systems, Applications and Third-Party Software Updates
	DHS CSPLCS 3.1	PERIMITER PROTECTION	Firewalls
	DHS CSPLCS 7.1	MALWARE DETECTION AND PREVENTION	Malware Detection and Prevention
	DHS CSPLCS 8.1	HOST NAME RESOLUTION	Network Addressing and Name Resolution
	DHS CSPLCS 9.1	END DEVICES	Intelligent Electronic Devices
	DHS CSPLCS 9.2	END DEVICES	Remote Terminal Units
	DHS CSPLCS 9.3	END DEVICES	Programmable Logic Controllers
	DHS CSPLCS 9.4	END DEVICES	Sensors, Actuators and Meters
	DOE CPLEDS 2.8	GENERAL CYBERSECURITY PROCUREMENT LANGUAGE	Malware Detection and Protection
	DOE CPLEDS 3.4	THE SUPPLIER'S LIFE CYCLE SECURITY PROGRAM	Patch Management and Updates
	DOE CPLEDS 4.1	INTRUSION DETECTION	Host Intrusion Detection
	DOE CPLEDS 4.2	INTRUSION DETECTION	Network Intrusion Detection
B.5 Resilient Networks & Systems			
	DHS CSPLCS 2.5	SYSTEM HARDENING	Heartbeat Signals

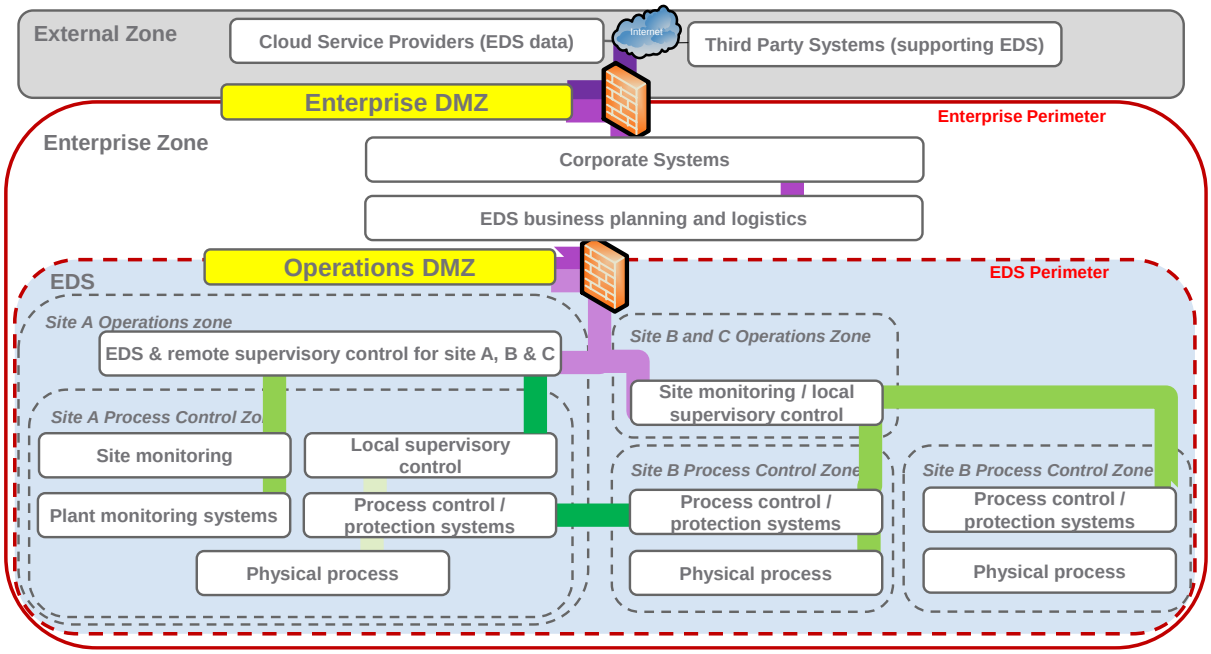
	DHS CSPLCS 5.1	CODING PRACTICES	Coding for Security
	DHS CSPLCS 11.1	PHYSICAL SECURITY	Physical Access of Cyber Components
	DHS CSPLCS 11.2	PHYSICAL SECURITY	Physical Perimeter Access
	DHS CSPLCS 11.3	PHYSICAL SECURITY	Manual Override Control
	DHS CSPLCS 11.4	PHYSICAL SECURITY	Intra Perimeter Communications
	DHS CSPLCS 12.1	NETWORK PARTITIONING	Network Devices
	DHS CSPLCS 12.2	NETWORK PARTITIONING	Network Architecture
	DOE CPLEDS 2.7	GENERAL CYBERSECURITY PROCUREMENT LANGUAGE	Communication Restrictions
	DOE CPLEDS 2.9	GENERAL CYBERSECURITY PROCUREMENT LANGUAGE	Heartbeat Signals
	DOE CPLEDS 2.10	GENERAL CYBERSECURITY PROCUREMENT LANGUAGE	Reliability and Adherence to Standards
B.6 Staff Awareness & Training			
		N/A	None identified
C.1 Security Monitoring			
	DHS CSPLCS 2.2	SYSTEM HARDENING	Host Intrusion Detection Systems
	DHS CSPLCS 3.2	PERIMITER PROTECTION	Network Intrusion Detection System(s)
	DHS CSPLCS 3.3	PERIMITER PROTECTION	Canaries (and/or Honey Pots)
	DOE CPLEDS 2.6	GENERAL CYBERSECURITY PROCUREMENT LANGUAGE	Logging and Auditing
	DOE CPLEDS 5.1	PHYSICAL SECURITY	Physical Access to Energy Delivery System Components
	DOE CPLEDS 5.2	PHYSICAL SECURITY	Perimeter Access
	DOE CPLEDS 5.3	PHYSICAL SECURITY	Communications inside the Physical Security Perimeter
C.2 Proactive Security Event Discovery			
		N/A	None identified
D.1 Response and Recovery Planning			
		N/A	None identified
D.2 Lessons Learned			
		N/A	None identified

E. Supplementary guidance

When applying the reference model to EDS it is important to realise that systems are not equal in security definition. The function, operation and architecture will define the security zone, security level and security requirements for any EDS or IACS sub-system. A high-level architecture of an EDS is provided to demonstrate the application of key IACS concepts to support application of this guidance.

The arrangement in Figure 7 shows an application of the EDS-CSRM for an EDS with three control areas, A, B and C. Overall network management is performed from site A which has separate monitoring and local control room and control systems; Site B and C are remotely managed from a control room (site B & C operations zone) near to their processes with local control systems at site B and C respectively. The communications within the areas are all different protocols and connection types (various colours) to highlight that there is no one size fits all approach to security in this environment.

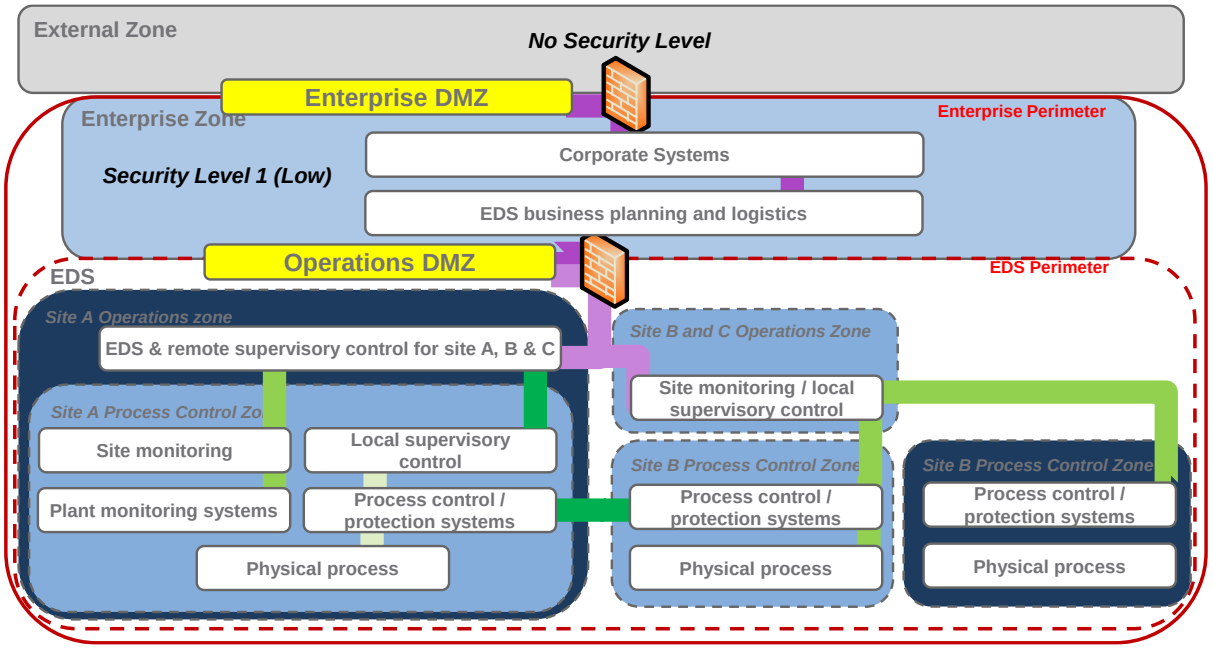
Figure 7 EDS-CSRM applied to example EDS in a good practice architecture



E.1. Reference model EDS Security levels (SGIS risk mapping)

Now taking the above, and applying example security levels, where site C is evaluated as being critical to the business, and the regional control of Site A, B and C, affects a large customer base.

Figure 8 Security levels applied using to example EDS



Energy Networks Association
6th Floor, Dean Bradley House
52 Horseferry Road, London SW1P 2AF

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