EA Technology

OpenLV Technical Security Standards

April 2020

Prepared by: *Rick Tahesh – Executive Principal Consultant*

Document Control

Document Version Control	
Document Classification:	CONFIDENTIAL
Client Name	EA Technology
NCCGP Document Reference:	NCC Group – EA Technology OpenLV Platform Security Standards
Document Title	OpenLV Platform Security Standards
Author Name:	Rick Tahesh
Technical Approval:	Arun Chidambaram

Document History			
Issue Number	**Issue Date**	**Issued By**	**Change Description**
0.1	07 April 2020	Rick Tahesh	Initial Draft
0.2	08 April 2020	Arun CV	QA Review
1.0	09 April 2020	Rick Tahesh	Final Version
1.1	24 April 2020	Rick Tahesh	Client Feedback Added

Document Distribution List	
Timothy Butler	Senior Consultant, EA Technology
Ray Burns	Consultant, EA Technology

Proprietary Information

Contents

1. Executive Summary

The OpenLV solution is expected to bring many benefits to a cross spectrum of stakeholders including operators and consumers of the energy sector. As this solution is aimed to monitor substation performance and electricity demand across regions within the United Kingdom, and integrate with third party products and applications, the security of the platform and the data generated, processed and transmitted are of paramount value and importance.

The objective from this assessment is to devise and put forward the baseline and enhanced security control standards that are required and expected to be in place for the deployment, management, operation and maintenance of the OpenLV Platform. In addition, it also provides the security controls that are needed to ensure secure development and connectivity from DNOs and other third parties.

The assessment has considered four Use Cases of OpenLV Platform deployment namely LV Monitoring, Limited Control, Enhanced LV Monitoring, and Full Capacity. Each Use Case builds on the previous in terms of connectivity, output and benefits.

In consideration of the baseline and enhanced security controls, this report has assessed the likely threats from external and internal threat actors to the OpenLV environment. The following table illustrates the potential threat level facing the OpenLV Platform:

#	Threat Actor	Capability	Motivation	Threat Rating
1	Organised Crime Group	High	Medium	**High**
2	Opportunist Hackers	Medium	High	**High**
3	Insider Threats	High	Low	**Moderate**
4	Terrorists	Medium	High	**High**
5	Hacktivists	Medium	Medium	**Moderate**
6	State Sponsored Groups	High	Medium	**High**
7	Competitors	High	Low	**Moderate**
8	Hostile Media	Low	Medium	**Low**
9	Partners, Vendors, Suppliers	High	Low	**Moderate**

Table 1: Threat Actors and their Ratings

In addition to the threat actors, this study has also assessed the impact to OpenLV Platform from a breach to or loss of Confidentiality, Integrity and Availability (CIA). The following table shows the impact to OpenLV based on the four Use Cases:

#	Use Case	Confidentiality	Integrity	Availability	Maximum Impact
1	LV Monitoring	Medium	Major	Minor	Major
2	Limited Control	Medium	Major	Major	Major

3	Enhanced LV Monitoring	Medium	Major	Medium	Major
4	Full Capacity	Medium	Major	Major	Major

Table 2: Use Cases CIA Impact

Based on the threats, security impact and risks to the OpenLV Platform, this assessment has detailed a set of technical security controls in the form of Baseline and Enhanced to support the mitigation of threats and risks. A summary of these outlining the domains and number of controls as shown in the table below:

#	Security Control Domains	# of Baseline Controls	# of Enhanced Controls
1	Identity and Access Management	9	2
2	Information and Data Processing	9	0
3	Server Security	9	3
4	Network Security	9	0
5	Application Security	7	2
6	Web Application Security	6	0
7	Cloud Security	5	0
8	End Point Security	7	1
9	Mobile and Remote Working	3	2
10	Threat and Vulnerability Management	5	0
11	Security Operations and Monitoring	6	3
12	Incident Management	6	1
13	Security Testing	5	0
14	Business Continuity	3	2

Table 3: Security Control Domains Summary

As the assessment shows that the impact to the OpenLV platform from a security incident originated by any or a number of threat actors is considered as Major, the proposed technical baseline and enhanced security controls would apply to all Use Cases of the OpenLV Platform.

Due to the inherent risks associated with a distributed intelligence platform environment and the impact these may have on the wider energy sector through DNOs and other third parties with access to the distributed intelligence platform environment, it is recommended that operating DNOs and third parties have stringent access management controls in place through the use of multifactor authentication, particularly for those with privileged and remote access, strong integrity controls through hashing and signing of data generated and transmitted, improved and secure software and applications development lifecycle with security by design and adherence to OWASP security best practice for web applications and services, with strong monitoring, logging, detection and incident response controls in place.

2. Introduction

2.1 Background

The UK has clear aspirations and its own legislation to drive towards a low carbon economy. Energy, and specifically electricity, has a key role in assisting this transition as generation decarbonises, and then through supporting heating and transport demands as these shift towards electricity. Great Britain has about 1,000,000 LV feeders. The LV networks are expected to see radical change as we, as customers, alter our behaviour and requirements stemming from the vehicles we drive, to the generation and storage devices we put onto and into our homes.

LV-CAP™ is an open source low cost software platform that can monitor substation performance and electricity demand. It is designed to integrate with third party products to enable network control and automation, and increase customer participation in network management.

The OpenLV Project is led by Western Power Distribution (WPD) and EA Technology and has installed LV-CAP™ devices in 80 low voltage substations across WPD's four licence areas, including substations where automated network control trials have successfully been undertaken. The project is collecting over 14 million data points per day. This data is being used by community groups, businesses, universities and the project team for a wide variety of purposes. Participating organisations have created apps that have been uploaded remotely onto the LV-CAP™ devices, or they are accessing data – real time and historical – for the benefit of community projects, the environment and the electricity system.

The OpenLV Project is expected to deliver a range of benefits to a broad spectrum of stakeholders including:

- End Customers such as households, small/medium businesses:
    - Negotiating power: visibility of aggregate demand and ability to use this to strike better deals with energy suppliers
    - Market access: a platform for the provision of services to Distribution Network Operators (DNO)
    - Reduced distribution use of system payments: resulting from improvements made by the DNO
    - Reduced connection costs: allows the LV customer to connect new forms of generation or demand in a more flexible way
- Distribution Network Operators:
    - Direct cost reduction: the use of a standardised single platform rather than multiple overlaying solutions; economies of scale in procurement
    - Improved flexibility: i.e. a platform rolled out for monitoring, can later be used to control the LV network, limiting the risk of stranded assets
- Third Party Developers
    - Hardware deployment: payment for every unit rolled out in a substation
    - App 'store' administration: payment by third party to manage apps; potentially also from end users to tailor apps for substations/community groups
- Platform Providers
    - Hardware deployment: payment for every unit rolled out in a substation

- App ‘store’ administration: payment by third party to manage apps; potentially also from end users to tailor apps for substations/community groups

2.2 High Level Architecture

The high-level architecture of the OpenLV solution is shown in the figure below:

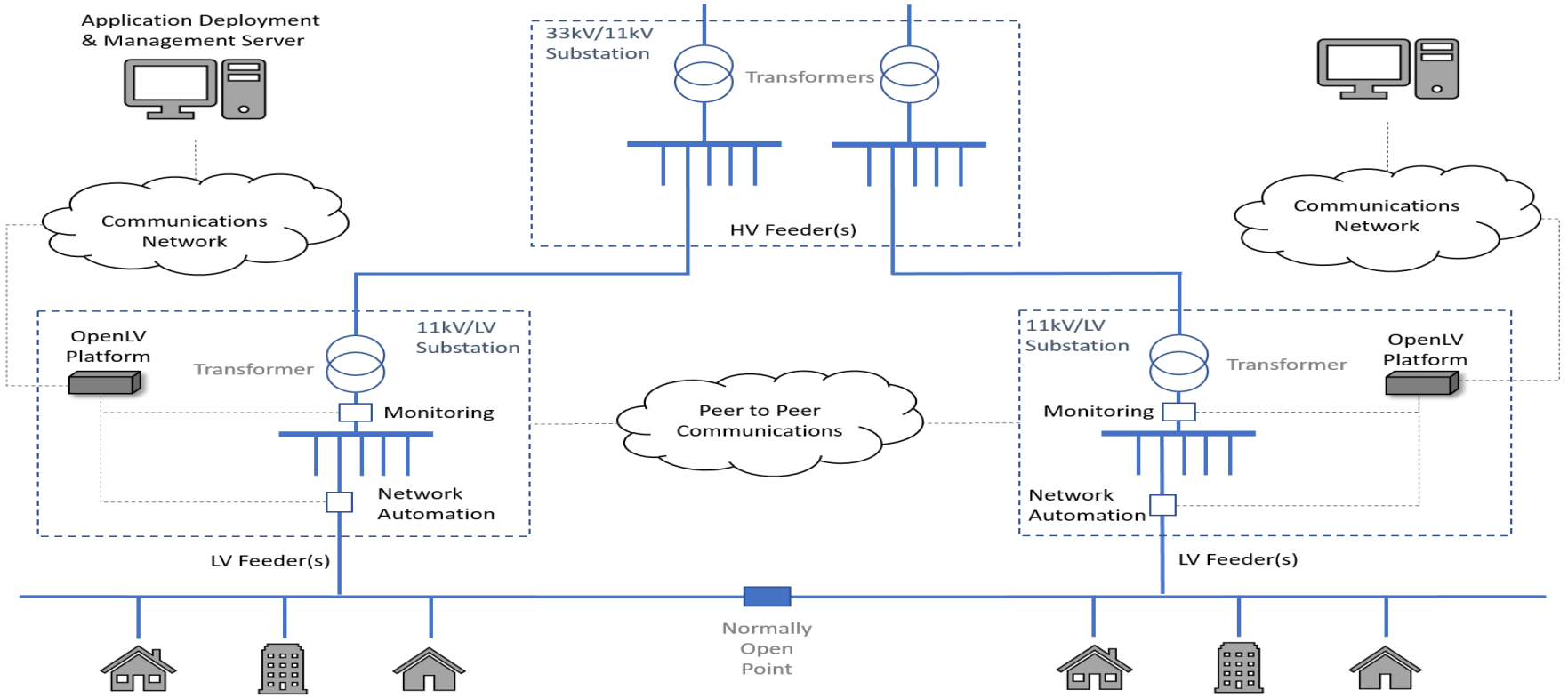

Figure 1: High Level Architecture[1]

[1] OpenLV-SDRC1-Specification-design-Testing-Version-1-1

The key components of the solution are as follows:

- **LV Network Automation:** These devices enable automated meshing of the LV network via an app or app(s) installed on the platform.
- **LV Monitoring Equipment:** This monitoring equipment utilises sensors to take electrical measurements from the LV busbar, the transformer and the outgoing feeder(s). In addition, temperature measurements are also taken from the transformer, and inside and outside substation(s). The monitoring equipment provides this LV monitoring data to the OpenLV Platform.
- **OpenLV Platform:** Consists of a ruggedised PC with a Linux based operating system running the Low Voltage-Common Application Platform (LV-CAP™). This platform receives, stores and processes data from external LV monitoring equipment. These devices have sufficient computational power to store and run multiple apps and can provide relevant information out via a communications link to centralised server(s).
- **Application Deployment & Management Server:** Enables management of the OpenLV Platform(s) that will be installed as part of the project. This includes the deployment of app(s) to devices in the field. It will also be utilised to store relevant data to enable the OpenLV trials to be assessed.
- **Cloud Hosted Server:** Enables LV monitoring data to be collected, stored, shared and visualised to provide benefits to communities and the wider industry.

3. Threat Assessment

The distributed intelligence platform threat assessment examines a number of threat actors, external and internal, and assesses their capability and motivation to do harm through unauthorised access to the platform and data generated, processed or transmitted. The table below outlines capabilities, motivation and likely threat rating for each threat actor.

Ref	Threat Actor	Capability Description	Motivation Description	Capability	Motivation	Threat Rating
TA-01	Organised Crime Group	Organised Criminal Groups (OCGs) have the resources to facilitate a highly sophisticated, technically capable and long-term approach to cyber-crime, and as such through targeting distributed intelligence platform directly, they can facilitate other crimes to disrupt power	OCGs are financially motivated, and therefore the extent of their intent is directly proportional to the potential reward to be gained from an attack. Several OCGs have successfully replicated the structures and processes deployed by large	High	Medium	High

Ref	Threat Actor	Capability Description	Motivation Description	Capability	Motivation	Threat Rating
		distribution and suppliers in a given region or network grid. In some instances, OCGs have been found to be co-operating or have been sponsored by Nation State actors. OCGs may in effect become a proxy to cause political or financial discourse in very discreet and targeted sectors, such as the power and financial industries. By virtue of these proxy relationships, they will often have access to resources and techniques that are highly advanced and can be difficult to detect/defend.	multinational companies, re-investing significant revenues into developing new capabilities. The cross-border nature of cyber-crime allows such operations to significantly reduce operational risk to the criminals. However, it is considered that OCGs will gain little financial gain from attacking distributed intelligence platforms and therefore, they are considered Low-to-Medium in terms of motivation.			
TA-02	Opportunist Hackers	Responsible for a large proportion of the attempted hacks against today's private and public sector organisations, this increasing group of threat actors are characterised by being high in volume, but with a moderate-low level of technical capability. Generally, they rely upon pre-configured hacking tools, which are freely available online. However, the distinction between opportunist hackers and OCGs is becoming increasingly blurred, as many of the same factors that have revolutionised enterprise IT such as cloud services have also benefited opportunist hackers, as the technical barriers to entry in terms of attack trade/craft have also been lowered.	It is likely that the power industry has experienced and will continue to experience, attacks from such individuals / groups. The generally low levels of capability mean that the majority of such threats are identified and prevented with reasonable ease; however, the rapid evolution of ransomware (and the anonymous crypto-currency infrastructure which facilitates this) has opened up new opportunities for amateur hackers to monetise their attacks with comparative ease. Additionally, it can be seen that many of the same factors which have revolutionised commercial IT operations (XaaS, increase in available data sources, decreasing	Medium	High	High

Ref	Threat Actor	Capability Description	Motivation Description	Capability	Motivation	Threat Rating
			technical barriers to entry, etc.) have also benefitted opportunist hackers, and resulted in an increasingly blurred boundary between this group and OCGs.			
TA-03	Insider Threats	Rogue insiders with legitimate access to distributed intelligence platform and infrastructure "especially those with privileged access", coupled with their inherent knowledge of the technology landscape, gives a significant advantage to the insider threat, allowing them to bypass security controls and avoid detection. There is also evidence to suggest that in recent years, a rogue employee or contractor may advertise their willingness to co-operate with more capable threat actors on public or dark-web criminal forums, presenting an exceptionally dangerous situation whereby key controls such as privileged access or secure remote connectivity could be bypassed with ease	This is a particularly difficult threat to assess and quantify, although it should be noted that if insider involvement (either intentional, malicious involvement, unintentional or 'user error') is one of the most commonly cited factors in successful attacks. The 'worst-case' scenario in this regard would be the active collaboration of an insider with another employee, Organised Criminal Group, or a competitor organisation. This could affect all aspects of distributed intelligence platform. However, the motivation of this type of threat actors in relation to the distributed intelligence platform is considered Low. Clearly 'human error' type incidents are devoid of motivation.	High	Low	Moderate
TA-04	Terrorists	The comparative rarity of terrorist attacks which combine an element of cyber suggests that there are limited capabilities available for use by these threat actors. Using cyber-attacks to gain access to national grid network and	The intent behind such a form of 'cyber terrorism' would most likely be to disrupt physical security systems with a view to causing mass casualties or network faults and power loss.	Medium	High	High

Ref	Threat Actor	Capability Description	Motivation Description	Capability	Motivation	Threat Rating
		facilities in order to carry out a conventional terrorist attack is a possibility, although to date, terrorist ability to combine cyber-attacks with conventional targeting (using bombs and bullets) has been very limited. However, if given the opportunity, a terrorist could seek to cause widespread damage and possible loss of life. Though with distributed intelligence platform, disruption to the power network could be accomplished through network breach or physical destruction of services and facilities.	That said, consideration should be given to the propaganda potential (and knock-on reduction in public confidence) of highly publicised, but non-lethal attacks and distributed intelligence platform operators and stakeholders should continue to monitor the threat landscape in relation to terrorists, their motivations and tools follow their desire to do physical harm.			
TA-05	Hacktivists	Hacktivist groups are typically comprised of a small number of determined and highly-skilled attackers, who will often co-operate with other like-minded individuals to achieve a specific objective or outcome, which is usually politically or socially motivated. Whilst their operative numbers are normally quite low, they have been known to inflict large-scale damage either through direct service disruption or the public disclosure of sensitive data/information. The past notoriety of groups such as Anonymous and LulzSec are primary examples where the capability of such attackers has seen to be highly advanced and unpredictable,	The objective of such groups is usually to inflict financial damage on the target organisation through influencing public opinion, or through disrupting operations. This could affect all aspects of distributed intelligence platform network. Most single-issue campaigning groups lack both the technical and organisational capacity to launch sophisticated attacks. Hacktivist groups allied to the objectives of nation states may, on occasion, be able to call on additional resources, increasing the threat.	Medium	Medium	Moderate

Ref	Threat Actor	Capability Description	Motivation Description	Capability	Motivation	Threat Rating
		making hacktivist groups a noteworthy adversary.				
TA-06	State Sponsored Groups	The most resourceful group of all the threat actors, state sponsored groups have proven to be a very insidious and prevalent threat in today's highly connected world. These groups often emerge from, or are linked to, Foreign Intelligence Services (FIS) and are typically part of a wider, government backed capability, which will develop, launch and sustain Advanced Persistent Threats (APTs) against their adversaries with a high-degree of technical craftsmanship. Nation States can be considered to be highly effective in their approach to the reconnaissance, delivery and exploitation of an attack and they will often go unnoticed or undetected.	It can sometimes be hard to determine the true source and motivation of an attacker. There will likely be a wide-range of motivations for Nation State actors to target distributed intelligence platform and connected systems. In the case of OpenLV, these may go after intellectual property, which makes OpenLV a possible target for a state sponsored attack for accessing operators and third parties systems. Foreign powers may also be interested in disrupting or manipulating the stability of the economy in the UK by targeting the services provided or supported by distributed intelligence platform. This element of Nation State activity can often be subtle and understated, but is typically part of a wider and longer-term campaign to erode or bring down the economic progress of an adversary. There is also evidence to suggest that Nation States have in recent years been 'proxying' their attacks through OCGs.	High	Medium	High

Ref	Threat Actor	Capability Description	Motivation Description	Capability	Motivation	Threat Rating
TA-07	Competitors	Whilst it is unlikely that Competitor organisations will have organic assets, which are capable of carrying out corporate cyber espionage/sabotage, it would be a credible scenario that such parties could procure external support to carry out an attack. This model is more recently becoming known as 'Cyber Attack as a Service', where a threat actor with malicious intent buys the services of a more skilled attacker from the Dark-Web to launch an attack against a competitor. As such, this skews the capability rating of this threat actor group and in the case of distributed intelligence platform, elevates the position to an overall Moderate rating.	Any potential attacker of this kind would stand to lose more than they gain if they were discovered. The most likely scenario would be to involve a competitor procuring the services of 'Hackers for Hire'. Whilst such resources are freely available via the dark web, the market is subject to significant friction: issues around trust and transparency make it potentially difficult for buyers to meet their requirements.	High	Low	Moderate
TA-08	Hostile Media	This threat actor group covers a broad spectrum of scenarios ranging from sensationalist and alarmist tabloid press who may actively engage in illegal activity, through to principled investigative journalists seeking to uncover information of genuine public interest. These groups are generally limited in terms of the technical capability, but will often employ methods such as social engineering to illicit sensitive information.	Although the Media usually point out profiteering on the expense of consumers, damage to the environments, etc. this threat is assessed to be Low. Having said this, however, there is a strong possibility that inaccurate / alarmist reporting could significantly exacerbate the effects of an attack from any of the threat actor groups identified above.	Low	Medium	Low

Ref	Threat Actor	Capability Description	Motivation Description	Capability	Motivation	Threat Rating
TA-09	Partners, Vendors, Suppliers	Partners, Suppliers and Vendors are often placed in the same grouping as Competitors given they are usually considered to be external entities, but their heightened levels of access can greatly affect the capability of such individuals to initiate an attack. As many third parties will have the opportunity to develop and deploy apps on OpenLV Platform, their capability has been assessed as High.	In the context of supply chain organisations in relation to distributed intelligence platform the motivation of this threat group is currently assessed to be Low. However, as an overall threat from this group, it is assessed as Moderate since of particular influence in this rating are the Nation State actors that exist within Vendors, Partners and Suppliers, who may seek to initiate an attack through the Supply Chain.	High	Low	Moderate

Table 4: Threat Actors Assessment

The following table provides a representation of the threat ratings that the above actors present to distributed intelligence platform:

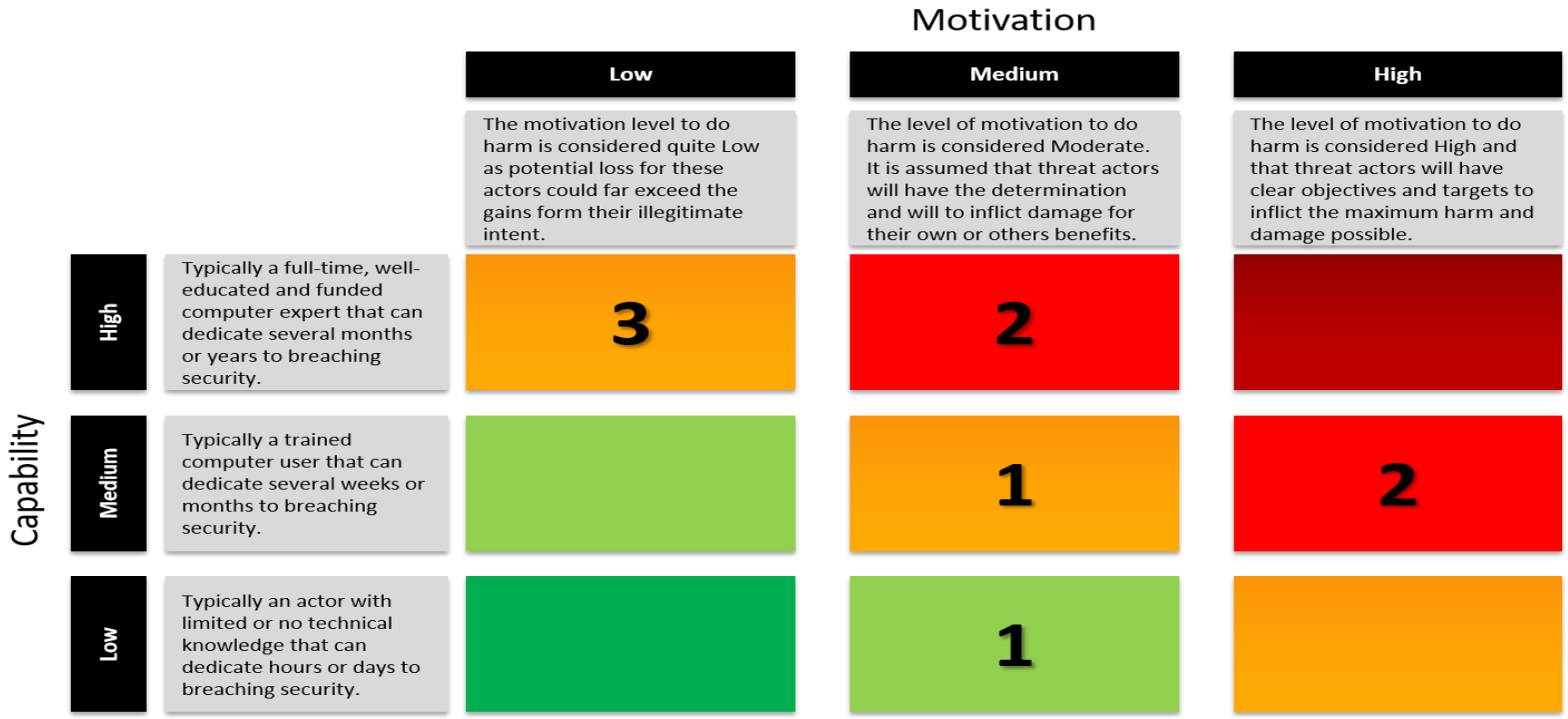

Figure 2: Threat Actors Ratings in Relation to OpenLV Platform

Based on Figure 2 above, the threat actors that present a significant threat to the OpenLV Platform are those with Medium and High Capability and Motivation levels.

4. OpenLV Platform Asset Assessment

This section assesses the impact of unauthorised access or security breach to distributed intelligence platform in relation to the Confidentiality, Integrity and Availability (CIA) of data generated, processed and transmitted. The impact is measured based on a range of ratings; from Negligible to Catastrophic. In the context of distributed intelligence platform environment, the CIA are defined as follows:

- Confidentiality – protection against unauthorised access or disclosure of data and information generated, stored or transmitted by the distributed intelligence platform
- Integrity – protection against unauthorised modifications (e.g. changes, deletion, or amendment) of data generated, stored or transmitted by the distributed intelligence platform
- Availability – protection against loss or unavailability of data and information at the time of need and at the frequency required by DNOs and/or third parties

Ref	*Asset Use Case*	*Description*	*Confidentiality*	*Integrity*	*Availability*	*Max Impact*
A-01	LV Monitoring	• Platform deployed for the purposes of basic LV monitoring only. • There is minimal data processing undertaken, primarily for reducing data storage requirements. Data is recorded, and stored locally for a short period, with processed 'key information' (max, min and average loads, and voltages) periodically reported to the DNO. • Key information is recorded, but only uploaded when 'requested' rather than on a regular schedule. • Local intelligent algorithms analyse the data in real (or near to real) time, triggering priority alert messages if necessary. • Data (both actual and processed) can be manually accessed, or automatically transmitted in response to network alerts.	Medium	Major	Minor	Major

Ref	Asset Use Case	Description	Confidentiality	Integrity	Availability	Max Impact
A-02	Limited Control	• Monitored data is processed, generating 'key information' for transmission on a schedule defined by the DNO. • Key information is not considered to be urgently required, so likely to be collated and uploaded on a regular schedule. • Local intelligent algorithms analyse the data in real time, determining whether any available actions can benefit the local network. (E.g. Active voltage control, automated network switching, charge / discharge of local battery storage). • Implement actions if viable (and notify the DNO if configured to do so). • Data is recorded, and stored locally for a short to moderate period, with processed 'key information' (max, min and average loads, and voltages), and records of implemented actions, periodically reported to the DNO. • Data and information is available to all applications running on the platform.	Medium	Major	Major	Major

Ref	Asset Use Case	Description	Confidentiality	Integrity	Availability	Max Impact
A-03	Enhanced LV Monitoring	• Monitored data is processed, generating 'key information' for transmission on a schedule defined by the DNO. • Key information is not considered to be urgently required, so likely to be collated and uploaded on a regular schedule. Local intelligent algorithms analyse the data in real time, triggering priority alert messages if necessary. • Actual recorded data can be manually accessed, or automatically transmitted in response to network alerts. • Recorded data can be stored for a longer period, and the processed information for longer still. • Data and information is available to all applications running on the platform. • DNO and 3rd Party applications can be deployed to the platform for multiple purposes - E.g. prediction of network conditions or enhanced calculations on asset state. • Apps may communicate externally to non-DNO servers with the potential to indirectly affect the distribution network. (E.g. informing local communities of network loading, or signalling EV's to commence, or curtail charging).	Medium	Major	Medium	Major

Ref	Asset Use Case	Description	Confidentiality	Integrity	Availability	Max Impact
A-04	Full Capacity	• Monitored data is processed, generating 'key information' for transmission on a schedule defined by the DNO. • Key information is not considered to be urgently required, so likely to be collated and uploaded on a regular schedule. • Local intelligent algorithms analyse the data in real time, triggering priority alert messages if necessary. • Actual recorded data can be manually accessed, or automatically transmitted in response to network alerts. • Recorded data can be stored for a longer period, and the processed information for longer still. • Data and information is available to all applications running on the platform. • DNO and 3rd Party applications can be deployed to the platform for multiple purposes - E.g. prediction of network conditions or enhanced calculations on asset state. • Apps may communicate externally to non-DNO servers with the potential to indirectly affect the distribution network. (E.g. informing local communities of network loading, or signalling EV's to commence, or curtail charging). • Local intelligent algorithms analyse the data in real time, determining whether any available actions can benefit the local network. (E.g. Active voltage control, automated network switching, charge / discharge of local battery storage). • Implement actions if viable (and notify the DNO if configured to do so).	Medium	Major	Major	Major

Table 5: CIA OpenLV Platform Use Case Assessment

5. Risk Assessment

The following set of risks were considered for the OpenLV Platform. The security controls to mitigate these risks have also been referenced based on the detailed Technical Security Controls, Section 6 of this report.

Ref.	Adversarial / Accidental / Environmental	Threat	Risk Description	Mitigation Controls Ref.
ACC001	Accidental	Behavioural	Authorised individuals cause incidents through error (accidental or negligent), mishandling of data, or through loss of information systems.	IAM01, IAM02, IAM03, IDP03, BCO01
ACC002	Accidental	Process failure	Incidents are caused as a consequence of process failures, for example through undesirable effects of change, misconfiguration or errors in maintenance of OpenLV Platform.	SSE01, SSE02, SSE11, SSE12
ACC003	Accidental	Technology failure	Incidents caused by malfunctions in software (either internally or externally generated) or through accidental physical damage to OpenLV Platform and supporting systems.	ASE01, ASE02, ASE05, ASE06, WAS01
ADV001	Adversarial	Authentication Attack	Incidents caused by malicious individuals through session hijacking (taking control of authentic and authorised sessions) or through gaining unauthorised access to legitimate authentication credentials.	IAM01, IAM02, IAM04, IAM07, IAM08, IAM11
ADV002	Adversarial	Authorisation Attack	The threat exploits vulnerabilities in the authorisation mechanisms of DNO's information systems in order to gain access to OpenLV Platform and other systems part of the network.	IAM01, IAM03, IAM05, IAM09, IDP06, CSE04, MRW05
ADV003	Adversarial	Communications attacks	The threat gains unauthorised access to OpenLV data in transit (i.e. 'sniffing'), and potentially alters information while it is being transmitted.	IAM07, IAM08, IDP05, SSE08, NSE05
ADV004	Adversarial	Denial of Service (DoS)	The threat deliberately impairs the availability or performance of DNOs and third parties through breach of the security of OpenLV Platform and devices (e.g. Distributed Denial of Service). Having an insecure network that is open to network traffic / attacks such DDoS and network floods, XSS and Ransomware / Unauthorised access present a major vulnerability to the OpenLV Platform.	SSE02, NSE01, NSE02, NSE05, NSE06, NSE07, WAS03
ADV005	Adversarial	Information Leakage	The threat exploits insecure disposal of OpenLV devices and data.	IDP03, IDP06
ADV006	Adversarial	Malware	The threat introduces malware to DNOs and third parties through compromise of OpenLV Platform.	SSE01, SSE02

Ref.	Adversarial / Accidental / Environmental	Threat	Risk Description	Mitigation Controls Ref.
			Malware and/or APT's gain access to deployed Containers.	
ADV007	Adversarial	Misconfiguration	Exploit misconfigured network devices, systems, design or configuration issues in DNOs and third parties remote access service (e.g. VPNs), or poorly-designed network architecture. Docker uses kernel level multi-tenancy, which relies on insecure Linux namespaces to virtualise networking / process tables / hostnames etc. to provide what looks like a dedicated environment. Docker images are typically packaged and distributed with open permissions. Running bad or insecure container images.	SSE01, SSE03, SSE09, SSE11, NSE02, NSE03
ADV008	Adversarial	Misuse	The threat misuses legitimately-assigned access privileges to perform unauthorised actions on information systems.	IAM01, IAM03, IAM05, IAM09, IDP06, CSE04, MRW05
ADV009	Adversarial	Physical	The threat gains unauthorised physical access to OpenLV Platform and uses this access to gain logical access and cause physical damage.	IDP05, SSE04, NSE02
ADV011	Adversarial	Social engineering	The threat manipulates persons within the DNOs or as part of the supply chain into carrying out harmful actions, or inserts individuals into the supply chain, or conducts phishing attacks.	IAM05, IAM09, CSE04, CSE05, MRW04
ADV012	Adversarial	Software exploitation	The threat exploits coding bugs or design flaws (e.g. buffer overflows, improper validation of input) in OpenLV in order to gain unauthorised access. Mixing of more secure traditional VM based non-Docker services with less secure Docker services. Poor DevOps practices and lack of end-to-end security in the Build / Ship / Run development cycles.	ASE02, ASE05, ASE08, WAS01, WAS03, WAS04, WAS05, WAS06, STE02,
ADV013	Adversarial	Supplier compromise	The threat compromises information systems at a key third party or business partner of a DNO in order to gain access to the OpenLV information assets.	IAM08, IAM09, MRW04, MRW05
ENV006	Environmental	Infrastructure Failure	A power failure (or fluctuation), damage to or loss of communications channels, failures in environmental control systems, hardware malfunctions, or structural fire (typically caused by faulty electrical equipment or similar).	BCO01, BCO02, BCO03

Table 6: OpenLV Risk Assessment

6. Technical Security Controls – Baseline and Enhanced

The purpose of this section is to detail the required technical security controls, in the form of baseline and enhanced, to address and mitigate the threats and risks highlighted in previous sections of this report. Baseline and enhanced security controls are defined as follows:

- Baseline controls are the minimum set of security controls that are expected to be in place prior to deployment and operation of distributed intelligence platform. These controls are designed to be mandatory in nature to meet business and regulatory requirements.
- Enhanced controls are additional controls that can be implemented, on top of the baseline controls, to strengthen the security environment of distributed intelligence platform and to mitigate against Advanced Persistent Threats (APTs). Therefore, these should be considered in-line with changing threat and risk landscape and implemented at earliest opportunity.

As the risk profile is quite similar for the four Use Cases; LV Monitoring, Limited Control, Enhanced Monitoring and Full Capability, the following baseline and enhanced security controls apply to all these Use Cases.

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
			IAM01	**ROLE BASED ACCESS CONTROL:** Adopt a policy of least privilege access (business need to know), ensuring that administration rights are only granted on the host, end-point, application, etc. where there is a justified business or operational reason for granting such access. This may include the allocation of user rights and permissions for non-functional or system based accounts.	**Y**	
			IAM02	**PRIVILIGED USER ACCESS MANAGEMENT:** Controls should be in place to manage, control and monitor users with elevated privileges/rights. This may include provisions for the aggregation and monitoring of admin user sessions. Controls should include the following: • Establish elevated roles mapped to privileged operations	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
IAM	Identity & Access Management	Ensure that there is appropriate controls in place for uniquely identifying and authenticating users, including any specific requirements for restricting, monitoring or logging access to distributed intelligence platform and other supporting systems.		• Roles may include trusted device, privileged local user, system administrator, trusted application, and trusted gateway • Implement and enforce technical and policy mechanisms to restrict administrator ability to track location or other sensitive attributes of system users • Implement access controls and logging procedures to prevent insiders from disabling these controls without the system logging the event • Minimise privileged operations that run as root and do not run network services (e.g., web servers) as root		
			IAM03	**LIMITING ADMINISTRATIVE USE** Users should use unprivileged accounts when there is no requirement for administrative account usage. This will help constrain the potential for inadvertent changes being applied. In addition, all admin users should access the IoT system with their normal user credentials and switch to admin privileges when required.	Y	
			IAM04	**AUTHENTICATION SERVICES:** There should be a dedicated authentication service used for accessing the distributed intelligence platform and the systems used to manage these.	Y	
			IAM05	**JOINERS, LEAVERS & MOVERS:** An effective process for the granting and revoking of user access rights/permissions should be in place within DNOs and third parties to ensure that as employees or contractors commence, change or leave the role their access rights are initiated, amended or terminated within an appropriate time frame. This also includes the requirement for individuals or suppliers to return assets to the hiring organisations once their employment or contract agreement has been terminated.	Y	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
			IAM06	**UNIQUE IDs:** Each employee or contractor with access to the distributed intelligence platform environment shall be allocated a unique user ID to ensure that where appropriate, their actions can be logged, traced and retrieved as necessary. This may include the allocation of user IDs for non-functional or system based accounts.	**Y**	
			IAM07	**SECURE AUTHENTICATION:** The organisation has in place the means to securely authenticate users based upon the requirement for a passphrase or password to be submitted which meets appropriate complexity and validity criteria (e.g. a minimum of 12 alpha-numeric characters, changes on a quarterly basis as per the defined policy, appropriate warnings for privacy/confidentiality purposes, lock out requirements for unattended use/inactivity, forgotten/incorrect password attempts etc.).	**Y**	
			IAM08	**MULTI-FACTOR AUTHENTICATION:** • The organisation has in place appropriate provisions for multi-factor authentication (MFA) where privileged or administrative access is granted, including domain administration. • MFA provisions may include smart cards, certificates, one time passwords or biometrics. • Use of MFA should also be included for any remote access solution to the corporate network used to then access the Distributed intelligence platform environment.	**Y**	
			IAM09	**THIRD PARTY ACCESS:** Policies and procedures for third party access and management of IoT devices should be established: • This includes data that can be transmitted out of the organisation (e.g. instrumentation data), authorised roles, and minimum access security requirements for	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
				management of the devices within organisation's networks Enforce these controls and monitor for misuse		
			IAM10	**CONFIGURATION INTEGRITY:** All configuration files for IoT devices should be documented: • Digitally sign those files and store them in a secure repository • Use these digitally signed files to restore devices • Validate the digital signature of the file after provisioning to the device		**Y**
			IAM11	**SECURE COMMUNICAITON:** Certificates should be used to authenticate transactions instead of the native username/password capability.		**Y**
IDP	**Information & Data Protection**	Ensure that appropriate controls are in place to protect information and data wherever it is processed, stored or transmitted within and from distributed intelligence platform to DNOs and other third	**IDP01**	**DATA MAPPING:** The organisation has a good understanding of where distributed intelligence platform data is processed, stored or transmitted across the technology estate, including network, end-point, host and other ingress/egress points. These 'data flows' are documented with key areas of risk identified and governed through the risk management process.	**Y**	
			IDP02	**DATA CLASSIFICATION:** The organisation has in place a system of data/information classification, in line with restricting access to those with a business 'need to know' requirement.	**Y**	
			IDP03	**DATA DISPOSAL:** The organisation has in place appropriate policies and capabilities for the secure disposal/deletion of assets (including removable media) where they are used to process, store or transmit classified data/information.	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
		parties, in accordance with any relevant compliance obligations or risk mitigation objectives.	**IDP04**	**PROTECTION OF DATA AT REST:** There is an appropriate means of encrypting classified or sensitive data/information, which is at rest using strong cryptography to prevent misuse or access by those without a justifiable business reason to do so. This includes the need to protect information residing on laptops, desktops or removable media.	**Y**	
			IDP05	**PROTECTION OF DATA IN TRANSIT:** There is an appropriate means of encrypting classified or sensitive data/information in transit using strong cryptography to prevent unauthorised access. This includes the requirement for robust procedures to be in place for custody of assets/hard copy data that are physically transported from one location to another. This should also include operational data regarding management of ICS components as well as data egress out of the ICS environment into the corporate network.	**Y**	
			IDP06	**DATA LOSS PREVENTION:** Controls in place to detect and prevent the unauthorised exfiltration of sensitive data/information from the distributed intelligence platform environment. This should include coverage on storage, end-point and network based components.	**Y**	
			IDP07	**KEY MANAGEMENT:** There are effective management procedures for the validity and replacement of encryption keys to ensure that access to any data/information at rest or in transit cannot be easily compromised, including consideration for specified 'crypto periods' that may be appropriate to the ongoing safeguarding of such assets.	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
			IDP08	**CERTIFICATE MANAGEMENT:** The organisation has in place an effective capability for the issue and validation of security certificates as appropriate to the ingress and/or egress of classified information/data.	**Y**	
			IDP09	**API KEYS:** API keys and other credentials must not be stored in public-facing source control systems (e.g. gitlab). • Publish procedures for the secure handling of API keys. • Do not hardcode API keys into firmware, mobile applications, or any client-based application. • Monitor at least quarterly to verify that API keys and other credentials are not stored in public-facing source control systems.	**Y**	
SSE	**Server Security**	Ensure that the organisation has in place a range of controls to manage the risks associated with the processing, storage or transmission of data/information on ICS components and systems that are used to support them.	**SSE01**	**SECURE CONFIGURATION:** The organisation uses standardised security hardened builds for initial deployment of hosts/servers/components, ensuring that any insecure protocols or configuration items are addressed. This would include any requirement for connectivity to the enterprise wide security controls/tools (e.g. FIM, HIDS/HIPS, SIEM, patching, Vulnerability Scanning etc.). Critically, the build standards for each Operating System are reviewed on a regular basis to ensure that they address any recent incidents, vulnerabilities or other attack vectors. Hosts should also take their system time from one secure, synchronised time source.	**Y**	
			SSE02	**ANTI-VIRUS & ANTI-MALWARE:** The organisation has deployed technical measures to prevent virus or malware infections on the host/server estate, including consideration for any process/procedural requirements that describe how such events are to be handled from a recovery and cleaning perspective.	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
			SSE03	**VIRTUALISATION:** The organisation has in place appropriate controls to secure the hypervisor as part of a component virtual architecture, ensuring that any security controls at the host/server level are also implemented at the management layer.	Y	
			SSE04	**BACKUPS:** Suitable technical and process provisions are in place for the suitable protection of backups, including considerations for physical security, encryption of data at rest (stored) as well as when they are transmitted across the network. This also considers necessary provisions for the use of cloud services and remote backups.	Y	
			SSE05	**PRIMARY FUNCTION:** The organisation takes consideration of the network location and public exposure of a host within the environment to determine potential risk of attack and ensures that the host is appropriately built and used for a single primary function.	Y	
			SSE06	**REMOTE ADMIN:** Secure channels are used when remotely administrating all hosts/servers within the organisation. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption are only used if they are established over a secondary encryption channel, such as SSL, TLS or IPSEC.	Y	
			SSE07	**MANAGEMENT RESILIANCE:** Adequate resilience is in place to provide continual operational management, monitoring, logging and alerting should any primary service become unavailable.	Y	
			SSE08	**FILE INTEGRITY:** File integrity monitoring controls in place to detect unauthorised changes to key files within the server.		Y

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
			SSE09	**HRDENING:** Where applicable, all builds shall be hardened in line with the relevant CIS Benchmark configuration guideline. *Note: CIS Benchmarks offer benchmark security build guidelines that can be found here - https://www.cisecurity.org/cis-benchmarks/*.	Y	
			SSE10	**ABSENCE OF HARDENING GUIDELINES:** Where no CIS Benchmark exists the service provider / manufacturer shall be approached to provide the required hardening guidelines.		Y
			SSE11	**GOLD BUILDS:** • Maintain secure images or templates (Gold Builds) for all systems supporting the distributed intelligence platform environment, based on organisation's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates. • An up to date documented process will exist, detailing the process for creating and maintaining Gold Builds. • Hashes should be taken on Gold Builds for integrity purposes. • Hashes should be stored securely. • Before installing from a Gold Build the hash should be verified to ensure the integrity of the Gold Build. • Gold builds must be updated on a quarterly basis to include the delta of any new security fixes that have been released. • For host & kernel security use, RHEL SELinux or other tools such as AppArmor or SECCOMP to lock kernel level multi-tenancy down and enforce access controls.	Y	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
			SSE12	**GOLD BUILDS ENHANCED CONTROLS:** • Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible. • Deploy system configuration management tools that would automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. • Utilise a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		**Y**
NSE	**Network Security**	Ensure that suitable controls are in place to detect and prevent internal or external network attacks that may have an adverse effect upon normal business activities or could enable unauthorised access to or the extraction of, data/information across the organisation.	**NSE01**	**NETWORK TOPOLOGY:** The organisation has a good understanding of the network topology with documented, diagrammatic representation of the estate. The information is frequently reviewed and revalidated to ensure that it is up to date and reflects any changes.	**Y**	
			NSE02	**NETWORK ZONING:** • The organisation deploys an effective model of network separation to ensure that assets or groups of assets that have different criticality and/or store or transmit sensitive information/data are physically/logically kept apart. • Access between zones is only permitted with an appropriate business or operational requirement and concept of trust between defined zones is deployed to ensure that a high-risk area cannot directly connect to a sensitive internal network segment, which contains sensitive data/information and/or systems. This should include situations where VLANs are used and whether ACLs have been defined and how rigid these are.	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
			NSE03	**SECURE CONFIGURATION:** The organisation has defined a secure configuration standard for common network components (e.g. Load Balancers, Firewalls, Switches, Routers, etc.), ensuring that any vendor default passwords or insecure protocols are addressed. This includes the requirement for clocks to be synchronised with an anti-tamper configuration across the organisation and that unrequired services are disabled.	**Y**	
			NSE04	**WIRELESS:** The organisation deploys wireless networks in a secure manner, ensuring that strong encryption channels are enabled (e.g. AES, WPA2) and that system default configuration settings are changed prior to deployment.	**Y**	
			NSE05	**FIREWALLS:** • The organisation has deployed effective perimeter/boundary controls to prevent unauthorised connectivity from external sources directly into the organisation. • Where firewall technologies have been deployed, they are securely configured and are effectively managed/maintained to ensure that they meet stated security and operational requirements. • Firewall ruleset reviews are carried out on a frequent basis to ensure that access is maintained with continued business or operational justification and any invalid rules are removed as required.	**Y**	
			NSE06	**NETWORK IDS/IPS:** The organisation has deployed capabilities to detect potentially nefarious network traffic within the IT estate and has put in place detection and/or preventative (blocking/filtering) policies.	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
			NSE07	**DDOS PROTECTION:** The organisation has suitable technical controls in place to ensure that the distributed intelligence platform environment is resilient against various types of DDoS events.	**Y**	
			NSE08	**ATTACK MITIGATION:** Measures have been implemented to protect the ICS control networks for attack from any other connected network, whether that be an internal or external network.	**Y**	
			NSE09	**NETWORK LOGGING & MONITORING:** Logs for all network devices are generated for security events at a minimum and are stored in a secure way to prevent modification. Events are reviewed on a daily basis to detect and respond to potentially malicious activity.	**Y**	
ASE	**Application Security**	Ensure that appropriate provisions are in place to secure the development, deployment and maintenance of applications that are used to process, store or transmit data/information across the organisation.	**ASE01**	**SECURITY REQUIREMENTS:** A common set of functional and non-functional security requirements are defined by the organisation for the development of secure applications and these standard requirements are considered both within initial delivery and ongoing operational development cycles.	**Y**	
			ASE02	**SECURE DEVELOPMENT LIFECYCLE:** Security risk is considered within the software delivery lifecycle that is deployed within the organisation and there is appropriate governance hold/check points in place to ensure that insecure applications/products are not released to market/service without proper risk assessment and acceptance by the business. Where applicable, applications software development is conducted in line OWASP controls.	**Y**	
			ASE03	**ENVIRONMENT SEPARATION:** The organisation has in place appropriate controls for the separation of production and non-production systems. Similarly,	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
				production based data shall not be used within a non-production environment.		
			ASE04	**SEGREGATION OF DUITES:** The organisation ensures that roles/responsibilities on production and non-production systems are distinct from an access, deployment and maintenance perspective.	**Y**	
			ASE05	**APPLICATION TESTING:** Automated or manual code reviews of applications that are developed and deployed by the organisation are performed to ensure that any common security vulnerabilities are addressed prior to deployment and routinely throughout the lifecycle of the product or service.	**Y**	
			ASE06	**TRAINING & AWARENESS:** Specific training for application developers and operational support teams is in place and is kept up to date with the latest industry developments/issues for security using such sources as the OWASP Top 10.	**Y**	
			ASE07	**LOGGING & MONITORING:** Application level logging is enabled on the systems deployed and such events are aggregated to a central log monitoring service.	**Y**	
			ASE08	**THIRD PARTY DEVELOPMENT:** The organisation has in place provisions for the commensurate control and review of third party developed applications, including contractual provisions. This could include but is not limited to undertaking code reviews (e.g. manual or using static application code analysis tools) and third party audits of code review practices.		**Y**
			ASE09	**AUDITING/LOGGING DESIGN**: The type and depth of logging that is required needs to be identified and agreed. Business critical systems should have their		**Y**

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
				logs integrated into SIEM for log aggregation and investigation purposes. Logs should be maintained as per requirement either by business, legal or regulatory or compliance to a globally recognised standard (such as ISO 27001) and or business and security requirements.		
WAS	**Web Application Security**	Ensure that controls are in place for any for the development, management and secure maintenance of web applications to safeguard the confidentiality, integrity	**WAS01**	**INHOUSE DEVELOPMENT:** • All web applications developed in-house shall prevent Cross-Site Request Fraud (CSRF) by including an unpredictable token in the body or URL of each HTTP request. • All web applications developed in-house shall avoid the use of redirects and forwards. If their use is necessary, do not involve user parameters in calculating the destination. • Web applications shall not rely on client-side functions, such as AJAX, to exercise control logic with security implications. All such control logic shall be implemented on the server side.	**Y**	
			WAS02	**USER-SUBMITTED DATA:** All applications shall be designed such that user-submitted data are not directly used by an application to specify access to resources such as filenames, network addresses, environment variables, database records, Operating System commands.	**Y**	
			WAS03	**CROSS-SITE SCRIPTING** • Cross-Site Scripting (XSS) attacks shall be tested against by carrying out input validation of web data in forms. • Additionally for XSS, handle the output to the client by either using escaping sequences or encoding. Escaping all untrusted data based on the HTML context (body, attribute, JavaScript, CSS, or URL).	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
		and availability of data and information		• Use secure libraries and encoding frameworks that provide protection against XSS issues, such as Microsoft Anti-Cross-Site Scripting, OWASP ESAPI Encoding Module and Apache Wicket.		
			WAS04	**PARAMETER SECURITY** • Either mask or cryptographically protect (encrypt / hash) exposed parameters, especially query string key value pairs. • Validate the input (change in the object / parameter value) to ensure that the change is allowed as per the whitelist). • Perform multi-access control and authorisation checks every time a parameter is changed. If a direct object reference shall be used, first ensure that the user is authorised to do so. • Ensure that all data that are output to HTML (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.	**Y**	
			WAS05	**ERROR HANDLING** • Ensure that all output encoding/error handling controls are implemented on the server side. • Ensure that output encoding /error handling controls encode all characters not known to be safe for the intended interpreter. • Ensure that for each type of output encoding/error handling performed by the application, there is a single security control for that type of output for the intended destination. • Implement failsafe by redirecting all errors to a generic error page and logging it for later review.	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
			WAS06	**DOCKER SERVICES** The organisation uses techniques such as Domain Driven Design (DDD) to separate more secure traditional VM based non-Docker services with less secure Docker services into different and segregated domains i.e. using 'bounded contexts' for controlled entry/egress points for any network communication or sharing data between container pods.	**Y**	
CSE	**Cloud Security**	Ensure that controls are in place for end-to-end mitigation of risk associated with the use of private and/or public cloud services which may be used in the processing, storage or transmission of data/information across the organisation.	**CSE01**	**CONTROL OWNERSHIP:** The organisation has a good understanding of what controls need to be implemented as part of the use of the cloud services and who has responsibility for the provision and maintenance of any controls as it relates to SaaS, PaaS and/or IaaS services as well as the deployment model adopted (e.g. Public, Private, Hybrid, etc.).	**Y**	
			CSE02	**DATA PROTECTION:** Specifically, the organisation has a good understanding of how data/information is protected within the cloud hosting environments or software/application providers that they utilise, for both data in transit or at rest. There is also a good understanding of the appropriate public/private key exchange requirements associated with data at rest and in transit between the organisation and the cloud provider(s).	**Y**	
			CSE03	**MULTI TENANCY:** The organisation has a good understanding of the multitenancy arrangements that apply to their consumption of cloud services, such that in the event of a compromise, there is clarity around whether or not their data/information has been affected.	**Y**	
			CSE04	**GOVERNANCE:** The organisation has a good understanding on who owns, or has the ability to access, copy or delete data that is stored in cloud based service providers. Additionally, the organisation is clear on how the cloud service provider(s) can comply with their policies	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
				and there are robust provisions in place to ensure that service performance metrics include consideration for security.		
			CSE05	**TERMS OF SERVICE:** When engaging with cloud service providers, the organisation has robust security provisions included within any contract terms, including breach notification and a right to audit.	**Y**	
EPS	**End Point Security**	Ensure that the organisation has in place a range of controls to reduce the risk of potential data loss from end user or end point devices, which may be used in the processing, storage or transmission of data/information across the organisation.	**EPS01**	**SECURE CONFIGURATION:** The organisation uses standardised security hardened builds for end point devices (i.e. laptops and desktops) ensuring that any insecure protocols or configuration items are addressed. This would include any requirement for connectivity to the enterprise wide security controls/tools (e.g. HIDS, Personal FW, patching etc.). Critically, the build standards for each Operating System are reviewed on a regular basis to ensure that they address any recent incidents, vulnerabilities or other attack vectors.	**Y**	
			EPS02	**ANTI-VIRUS & ANTI-MALWARE:** The organisation has deployed technical measures to prevent virus or malware infections on the end-point estate, including consideration for any process/procedural requirements that describe how such events are to be handled from a recovery and cleaning perspective.	**Y**	
			EPS03	**WEB BROWSERS:** Only fully supported web browsers operate within the organisation, ensuring that the latest versions are installed with the most up to date security features and patches deployed. Unnecessary scripting languages or other plug-ins are disabled and access to known malicious file/data transfer websites is blocked.	**Y**	
			EPS04	**E-MAIL HYGEINE:**	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
				The organisation has in place a capability that is able to identify and quarantine/block unhealthy e-mail traffic being received into or sent from the organisation.		
			EPS05	**END-POINT DRIVE ENCRYPTION:** The organisation has in place appropriate provisions for the protection of sensitive data/information on user end-point devices, with deployment of an appropriate encryption solution being considered where sensitive data is at rest.	**Y**	
			EPS06	**LOCAL ADMIN RIGHTS:** The organisation ensures that local administration rights on user end-points are removed by default and are only granted by exception with a valid business or operational justification.	**Y**	
			EPS07	**REMOTE ADMIN:** Remote administration to systems used to manage ICS systems must be tightly controlled and must use secure protocols. Communications must be encrypted and activity performed by the remote administrator must be approved by the local user and must be captured.	**Y**	
			EPS08	**LOGGING & MONITORING:** The organisation has the ability to put in place log collection and monitoring provisions for specific end user scenarios, where appropriate to the level of the risk.		**Y**
MRW	**Mobile & Remote Working**	Ensure that the organisation has in place robust controls for remote access to the corporate network or data/information, either on mobile devices or via other	**MRW01**	**PERMISSIBLE DEVICES:** The organisation has in place a mobile security policy and has defined a range of supporting security measures (e.g. configuration, control and monitoring, etc.) that addresses the risks associated with the use of mobile devices.	**Y**	
			MRW02	**MOBILE DEVICE MANAGEMENT:** The organisation has in place a capability that ensures they are able to deploy, monitor and maintain the specified controls	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
		public/private networks to support legitimate business use.		identified and can remotely lock, locate or wipe a device that is found to be in contravention of policy.		
			MRW03	**REMOTE ACCESS:** The organisation has in place a policy and supporting security measures that ensure the risks associated with remote access are understood and managed, including authentication, device configuration and any other control or monitoring requirements.	**Y**	
			MRW04	**THIRD PARTY ACCESS:** The organisation has in place a policy and supporting security measures that ensure the risks associated with access to key systems by 3rd parties (e.g. suppliers, outsource partners, developers, etc.) are understood and managed, including any authentication, monitoring arrangements or other specific controls subject to risk assessment.		**Y**
			MRW05	**REMOTE AUTHORISATION AND ACCESS** • All Virtual Private Networks (VPNs) should be configured with routing controls to restrict external network traffic to only specified authorised parts of Pepper Group's resources. • Endpoint tethering should be turned off while a VPN connection is active. • VPN sessions should be restricted to one session per user only. • Remote Access Services (RAS) should be restricted to one RAS platform.		**Y**
	Threat & Vulnerability Management		**TVM01**	**THREAT AWARENESS:** The organisation has in place a means of determining what threats are present within the organisation based upon the range of software, devices and other IT/ICS elements they have deployed. Sources of threat intelligence may range from vendor	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
TVM		Ensure that the organisation has in place controls to take proactive and reactive measures in the response to and remediation of, emerging threats/vulnerabilities, which may pose a risk to the organisation at a system, application, network and/or infrastructure layer.		communications, consolidated feeds or open source/dark-web. Information is effectively categorised and prioritised.		
			TVM02	**ASSET DATA:** Asset inventory data is co-ordinated within the organisation for consideration with regards to threat intelligence and vulnerability management activities, to ensure effective coverage and relevance across the IT estate.	Y	
			TVM03	**COMMUNICATIONS:** Where relevant threat intelligence is brought to the attention of the organisation, it is communicated and acted upon in an appropriately prioritised manner. This may include an incident response based approach to quickly react to issues that present a clear and present threat to the organisation.	Y	
			TVM04	**INFRASTRUCTURE SCANNING:** The organisation has in place the appropriate capability to scan infrastructure elements, both internally and externally, in order to determine whether they are patched and configured securely (i.e. vulnerability management and penetration testing).	Y	
			TVM05	**REMEDIATION:** Further to findings of any internal and external based scans, the organisation has in place provisions to ensure that critical and high risk findings are remediated and retested within appropriate timescales. This may include the provision of automated patch deployment solutions or the assignment of frequent maintenance windows where routine updates can be applied or ad-hoc, emergency patches can be deployed.	Y	
SOM	**Security Operations & Monitoring**	Ensure that there are sufficient controls in place for the operational	SOM01	**SERVICE TOPOLOGY/CATALOGUE:** The organisation maintains a good inventory of where operational security services are deployed in terms of coverage and scope. This may take the form of a set of design topology diagrams that	Y	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
		maintenance and monitoring of security controls, which are deployed to mitigate the risk of the potential loss of data/information across the organisation.		show where the various elements of the solution are deployed in the estate, along with any asset data or console level information.		
			SOM02	**BAU OPERATING PROCEDURES:** A set of operational level processes, procedures and/or work instructions are available and kept up to date for the services in scope. This should include an indication of the routine operational tasks that may apply in terms of the daily, weekly, monthly, quarterly, annual, etc. activities that are required to keep the service operating and compliant where applicable.	**Y**	
			SOM03	**SERVICE LEVEL AGREEMENTS:** The organisation maintains a set of service level agreements for each of the operational security services that are in scope. This includes an agreement with consuming or other parties that may be affected by a potential problem or breakdown of the service as to response and resolution times. Where applicable, a set of Operational Level Agreements are also identified within the organisation (including suppliers) to ensure that any end-to-end Service Level Agreements can be met.	**Y**	
			SOM04	**OPERATIONAL REPORTING:** Regular reporting information is made available to the consuming parties of, or those potentially impacted by, the services in scope as to how well individual solutions/functions are performing. This may include reporting data as to how well the operational team are meeting their SLA objectives, as well as how well the functionality of the service is performing.	**Y**	
			SOM05	**MANAGEMENT REVIEW:** Based upon the operational reporting that is provided as to the performance of the security services within the organisation, regular management reviews are carried out to ensure that any shortcomings or failures are responded to accordingly, as well as	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
				identifying any trends or repeat occurrences of previous issues so that they can be handled accordingly.		
			SOM06	**LOG COLLECTION & STORAGE:** The organisation has appropriate provisions for the central aggregation of security based log events across the IT estate. These logs are secured in an appropriate container with access only being provided on a business needs basis. The logs are protected from any tampering or inadvertent or deliberate deletion and are retained in accordance with appropriate policy and compliance requirements as may be applicable.		**Y**
			SOM07	**LOG MONITORING:** The organisation carries out daily reviews of the security relevant log events that are collected, looking for appropriate Indicators of Compromise across the IT estate. Where the volume of logs collected for review are sizeable, the organisation has deployed appropriate automation technology (e.g. SIEM or big data analytical tools) to make the process of review easier, quicker and more effective.		**Y**
			SOM08	**TRIAGE PROCESS:** Where log events received from across the various operational security services provide an indication of potential compromise or attack, a triage process is in place to validate that the evidence collected is true and that the event(s) can be considered an incident for escalation and response. Typically, some form of independent verification on the analysts findings are carried out to ensure that there is a second set of eyes on the findings.	**Y**	
			SOM09	**CONTINUOUS IMPROVEMENT:** Continuous improvement is embodied by the pro-active and reactive steps taken by management and the security team (with tangible documented evidence). This may be verified by the		**Y**

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
				holding of regular meetings to focus on security system innovation/improvements or the targeting of specific risk reduction objectives, including get well programmes in particular areas of concern (e.g. spear phishing simulation or simulated DDoS attacks etc.).		
IMA	**Incident Management**	Ensure that appropriate procedures are in place for the handling of security incidents within the organisation, including communications and provision for the regular testing and improvement of such arrangements.	**IMA01**	**INCIDENT HANDLING:** The organisation has a formalised incident management process in place for instances where security events or events that could endanger the public are identified. Appropriate resources are deployed and coordinated from a central point where necessary (e.g. through a SIRT) to investigate, respond, record all aspects of the incident.	**Y**	
			IMA02	**FORENSIC CAPABILITIES:** The organisation has in place appropriate forensic capabilities and resources to ensure that any requirement for the preservation of evidence in terms of future internal investigations or legal action (e.g. internal disciplinary procedures, co-operation with law enforcement agencies, etc.) can be met. This may include any obligations for third party involvement as part of a specific contractual or compliance mandate as applicable.	**Y**	
			IMA03	**INTERNAL COMMUNICATIONS:** The organisation has an effective process for communicating with internal stakeholders, employees, contractors or other suppliers to ensure that in the event of an incident/breach, any affected parties or teams are notified at the appropriate time. In addition, the organisation issues clear guidance to employees, contractors and suppliers should they be approached for any information in relation to the incident, so that a consistent messaging can be provided by the organisation.	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
			IMA04	**EXTERNAL COMMUNICATIONS:** The organisation has an effective process for communication with external stakeholders or other interested parties to ensure that in the event of an incident, consistent messaging is provided by the organisation.	**Y**	
			IMA05	**REPORTING:** Following a security incident, an appraisal is carried out and the findings are documented for management review. This may include further insight as to the root cause of the incident as well as any periphery factors or other risks, including details of what might have been impacted or potentially affected with recommendations as to prevent reoccurrence.	**Y**	
			IMA06	**ANNUAL EXERCISE:** The organisation frequently performs an exercise on the effectiveness of the incident management processes and other associated provisions to determine their suitability, robustness, etc. and identify any areas for improvement. Typically, this would involve an exercise being carried out on an/bi-annual basis, but this may vary depending upon the size, scale and risk appetite of the organisation.	**Y**	
			IMA07	**CONTINUOUS IMPROVEMENT:** As part of the organisation's commitment to continuous improvement, a lessons learned activity is carried out following a security incident to ensure that the possibility for reoccurrence is reduced and that the root cause of any incident is identified and flagged to management for further attention/remedial action.		**Y**
STE	**Security Testing**	Ensure that provisions are in place for the performance of routine and ad-hoc security	**STE01**	**SCOPING:** The organisation carries out security testing of applications, infrastructure and other system components to ensure that any exploitable vulnerabilities from the perspective of an internal or	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
		testing of applications and systems, which may process, store or transmit data/information, including robust arrangements for the tracking and remediation of any findings.		external attack scenario are identified, risk assessed and mitigated.		
			STE02	**ROUTINE TESTING:** Security Testing is carried out on a frequent basis to ensure that any operational risks that the organisation may be exposed to are identified, risk assessed and mitigated in a timely manner.	**Y**	
			STE03	**ADHOC TESTING:** Security Testing is carried out prior to the deployment of any new systems or capabilities to ensure that any risks associated with the change that the organisation may be exposed to are identified, risk assessed and mitigated in a timely manner.	**Y**	
			STE04	**REMEDIATION:** The findings associated with the performance of any security testing carried out by the organisation are remediated in a timely manner, ensuring that any Critical or High risk findings are prioritised and mitigated in accordance with the potential severity of the finding being exploited.	**Y**	
			STE05	**REPORTING & GOVERNANCE:** Findings of security testing activities performed are reported to management with appropriate action being taken in the case where any Critical or High risk findings are specified for remediation and have fallen behind plan in terms of agreed remediation.	**Y**	
			BCO01	**BUSINESS CONTINUITY PLANNING:** The organisation is able to identify business critical and other important services that are provided to support business operations/units fulfil their objectives as it relates to the systems used to support the ICS components. Additionally, the organisation is able to determine appropriate recovery time and	**Y**	

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
BCO	Business Continuity	Ensure that appropriate controls are in place to ensure that systems remain available for business use or can be recovered in accordance with the service continuity objectives that have been defined by the business.		recovery point objectives (RTO/RPO) for those systems which require specific business continuity plans to be set in place.		
			BCO02	**DISASTER RECOVERY:** Based upon the prioritised view of business critical systems, the organisation has developed and documented disaster recovery plans such that the individual RTO/RPOs for the specific systems can be reasonably achieved, should there be a systemic or individual failure of the system. These plans are also tested upon initial release to ensure that they are operationally robust, fit for purpose and most importantly achievable.	Y	
			BCO03	**ANNUAL EXERCISE:** The organisation frequently performs an exercise on the effectiveness of the disaster recovery planning and other associated provisions to determine their suitability, robustness, etc. and identify any areas for improvement. Typically, this would involve an exercise being carried out on an annual basis, but this may vary depending upon the size, scale and risk appetite of the organisation, as well as the criticality of the business system for which the plan is intended, past failures or incidents/near misses, etc.	Y	
			BCO04	**REPORTING:** Following a disaster recovery situation, an appraisal is carried out and the findings are documented for management review. This may include further insight as to the root cause of the outage/breakage as well as any periphery factors or other risks, including details of what might have been impacted or potentially affected with recommendations as to prevent reoccurrence.		Y
			BCO05	**CONTINUOUS IMPROVEMENT:** As part of the organisation's commitment to continuous improvement, a lessons learned activity is carried out following a		Y

Domain ID	Control Domain	Control Objective	Control ID	Sub-Controls	Baseline	Enhanced
				disaster recovery situation to ensure that the possibility for reoccurrence is reduced and that the root cause of any outage/breakage is identified and flagged to management for further attention/remedial action.		

As can be seen from the detailed technical security controls, the baseline controls are designed to provide appropriate protection to distributed intelligence platform and ensure the confidentiality, integrity and availability of data and information for the effective use by DNOs and third parties. The enhanced security controls would provide these parties with added security maturity and assurance, and safeguard against persistent threat actors.

7. Recommendations

Based on the detailed threat assessment and assets impact and risk assessment, it is recommended that DNOs and third parties looking to operate, access and develop apps for the OpenLV Platform to ensure the following are met and in place:

- Treat all four Use Cases the same from security threat and risk perspective
- Continuously monitor the cyber security threat landscape and determine its impact on the OpenLV Platform
- Ensure high level of integrity and availability controls are in place at all times
- Implement proposed Baseline Security Controls, as minimum, to ensure secure operation and management of OpenLV
- Consider the implementation of Enhanced Security Controls as these will add additional layer of security to baseline controls
- Implement multifactor authentication especially for privileged and third party users
- Adopt role based access controls with appropriate levels of network segregation
- Ensure separation of duties with clearly defined roles and responsibilities
- Ensure there are strong controls around software development lifecycle and applications development backed up by appropriate governance and operational procedures
- Adhere to the OWASP security best practices for the development of web applications
- Implement strong operational security controls for the monitoring, logging and review of events
- Ensure effectiveness of security incident and recovery processes and plans