National Cyber Security Centre and the Control Systems Security Information Exchange

Voluntary Cyber Security Standards for Control Systems Operators (VCSS-CSO)

Version 1

Document Control

Document History

Version	Date	Change(s)
1.0	2019	Initial Release

Approval

Name	Date
Control Systems Security Information Exchange (CSSIE)	

Contributors

Name	
Adrian van Hest	Peter McDowell
Jonathan du Preez	Peter Booth
Garry Lewis	Reyna Ramirez Montes
Jenni McNeil	Richard Tims
Mike Maclean	Stephen Allan
Matthew Cooper	Shaun Trewern
Nick Dean	Wenzel Huettner

Table of Contents

1.0 Introduction

1.1 Purpose

Much of New Zealand's critical infrastructure makes heavy use of Industrial Control Systems (ICS) technologies. The infrastructure of New Zealand is highly interconnected and interdependent. It is therefore more exposed to cyber threats and vulnerabilities, which could have major economic impacts, result in environmental damage or even loss of life. There are also potential physical and operational security factors that increase the requirement for system resilience and enhanced cyber security.

Critical National Infrastructure (CNI) is required to operate safely, continuously and reliably with defined controls and mechanisms that assist in protecting against adversaries. Increasingly however, the line between traditional operational technology (OT) environments that contain critical control systems and corporate information technology (IT) is being blurred. The rapid adoption of digital technologies and services, as well as efficiency drivers, means that the traditional hard separation between these two environments is being bridged. This trend will only increase through the adoption of modern technologies. Organisations need to remain focussed on understanding the different threats and risks in these distinct environments and protecting them using the appropriate controls. This includes maintaining adequate separation between the OT and IT environments with a managed boundary that provides the right choice of controls for any vulnerabilities or inherent design weaknesses.

New Zealand's government and industry organisations have responded to this increasingly hostile cyber environment by developing this standard. It is intended to support New Zealand's control systems operators in building resilient cyber security defences and practices.

The application of this standard will help prepare New Zealand's critical infrastructure to address cyber security threats considering the nature, origin, scale, complexity, intensity and duration of these risks.

1.2 Scope

The National Cyber Security Centre (NCSC) in partnership with the New Zealand Control Systems Security Information Exchange (CSSIE) has developed the Voluntary Cyber Security Standard for Control Systems Operators (VCSS-CSO) to recognise and address cyber security risks associated with the operation of ICS technologies.

This voluntary standard was developed using an industry-driven process and provides a foundational set of requirements designed to improve an organisations cyber resilience and secure the assets critical to the operation of New Zealand's control systems environments. These requirements are principally derived from international best practice standards created by the North American Electric Reliability Corporate (NERC) and the National Institute of Standards and Technology (NIST).

While the focus is on energy sector control systems, this standard can equally be applied to other sectors operating ICS technologies to assist in enhancing their cyber resilience. The primary objective is for all operators managing ICS technologies within New Zealand to adopt these foundational requirements across their entire organisation and integrate the baseline controls as part of an overall cyber security framework to ensure the reliable operation of the New Zealand electricity system.

This should be combined with a holistic approach to risk management and centralised governance supported by clearly defined roles and responsibilities.

It provides the framework for best practice cyber security controls which can be used to measure maturity and compliance within an organisation or a sector. It can be applied to provide a best practice foundation for cyber security across an organisation's IT and control systems environments with specific controls across ICS technologies.

The scope of the standard is all organisational activities, including controls systems, used in any industry to centralise the control and monitoring of technology assets that can be physically distributed. These control systems include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC). They support a wide range of industrial sectors, including energy (electricity, oil and gas) water, transport and a range of manufacturing sectors.

1.3 Compliance

Adherence to this standard is voluntary for all parties.

Each operator carries the responsibility for assessing, understanding, addressing and monitoring their compliance with this standard. This can be achieved using internal resources or an independent and suitably skilled external assessor. Similarly, it is recommended, but not mandatory, that capability maturity and compliance levels be shared with other members of the CSSIE.

1.4 Audience

This standard is specific to control systems operators covering the entire organisation including IT and control systems environments. The intended audience includes, but is not limited to the following:

- Information & Cyber Security Managers & Executives;
- Information & Cyber Security Professionals;
- ICS Engineers, Integrators & Architects;
- ICS Security Managers & Executives, and
- IT/ICS Risk Managers, Assurance Practitioners & Auditors.

1.5 National Cyber Security Centre Role Explained

The NCSC is part of the Government Communications Security Bureau (GCSB). The role of NCSC is to help New Zealand's most significant public and private sector organisations to protect their information systems from advanced cyber-borne threats.

Further information about NCSC can be obtained from the following website: https://www.ncsc.govt.nz.

The NCSC Security Information Exchange role is to provide a forum for information security professionals from organisations within a sector to meet and confidentially share information relating to threats that could potentially impact that sector. These forums focus on dissemination of critical information and awareness of key security issues among nationally significant organisations within NZ to reduce cyber security risks.

1.6 Control Systems Security Information Exchange Role Explained

The CSSIE is a forum tasked with improving the protection and cyber resilience of control systems and networks operated within New Zealand's CNI, from cyber-based threats.

The CSSIE is designed to facilitate the exchange of information between its members in a confidential and trusted environment, concerning threats, vulnerabilities and incidents of cyber-attacks on control systems networks and environments.

The membership of CSSIE is restricted to organisations that meet the following criteria:

- Operates a control system in support of New Zealand CNI.
- Meets the NCSC or New Zealand definition of CNI.
- Operates a security operations or incident response function for a New Zealand CNI.

1.7 Benefits of Compliance

When recognised as a business challenge, cyber security can be measured as an investment in improving capabilities and mitigating risk, rather than simply as an expense. This standard should not be about meeting a checklist of requirements, but rather managing cyber risk to an acceptable level through the adoption of this standard in a staged and measurable approach.

The benefits of adopting this standard include:

- **Strategic** - leadership decision-making is improved through the accurate identification of areas of high-risk exposure and the adoption of appropriate strategies to address them;
- **Financial** - providing a more robust and therefore effective basis for investing in cyber security. Spending funds strategically to mitigate potential losses and improved return on investment. It also aids cost avoidance by allowing rationalised decision making rather than unstructured reactions to newly identified vulnerabilities and threats, and
- **Operational Resilience -** organisations are better prepared for most eventualities, will be more resilient to threats and have well developed contingency plans and capabilities aiding business continuity.

This standard has been made publicly available to allow greater access, increased awareness, improved transparency and to promote good practice.

1.8 VCSS-CSO Definitions

To assist in achieving common understanding and application within the industry, the following common definitions are used:

- **Control Systems Operator (operator)** – any group, body or organisation that owns and/or is responsible for the operations of any industrial control systems environment.
- **Industrial Control Systems** – any system to centralise the control and monitoring of technology assets that can be physically distributed including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC).

- **Information Technology** – any technology or system used in the processing of information.
- **Operational Technology** – any technology or systems used to manage or maintain ICS environments.

2.0 Applying the VCSS-CSO

2.1 Overview of Structure

The VCSS-CSO is based on a foundation of best practice using the NIST Cyber Security Framework (CSF) with additional requirements adopted from the Critical Infrastructure Protection (CIP) Cyber Security Standards from NERC.

To support the implementation of this standard in an organisation, additional guidance has been included that covers:

- Governance & Roles;
- Risk Assessment & Management;
- Threat Modelling;
- Frameworks and Foundational Controls, and
- Compliance & Measurement.

The specific additional controls that should be adopted are listed in the CIP requirement sections in the following format:

- **Overview** - provides an overview of each section, its purpose, audience and how it supports cyber security.
- **Requirements** - defines and provides the context for a particular CIP requirement, including purpose and structure of the requirements section.

To adopt this standard, an organisation can either establish the following sections specifically for their control systems environment or optimally map this standard into their existing information security landscape and apply it across the entire organisation. The benefit of consistent governance across the entire organisation is a holistic approach to risk-based management can be adopted that considers threats and how they impact both IT and control systems environments. This end-to-end application is shown in the diagram below.

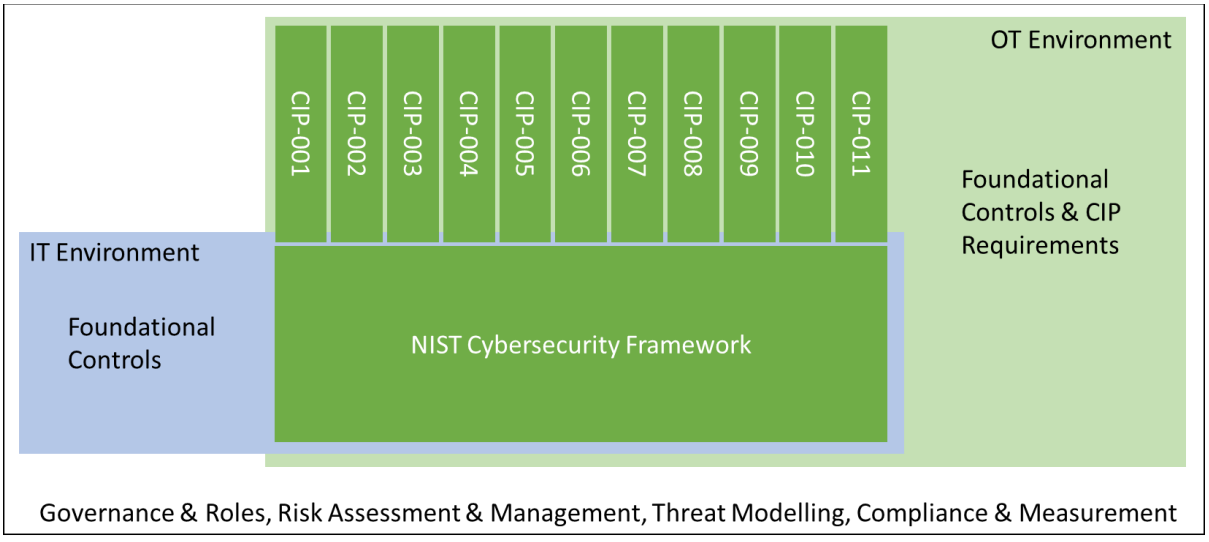

Figure 1: High Level Overview

2.2 Overview

- **Governance & Roles** – To effectively implement this standard within an organisation a governance framework must exist that clearly defines the applicable roles which at a minimum should encompass the operator and owner of Critical and Cyber Assets as well as the incident management and escalation points.
- **Risk Assessment & Management** – The driver to create, maintain and improve controls is ultimately justified by the risk that threats pose to the organisation. The requirements and recommendations in this standard should be considered in a risk context that will help establish the extent to which they need to be applied and prioritised.
- **Threat Modelling** – Ultimately risk is quantified based on the threats being faced by the organisation. A complete threat model relevant to the organisation should be developed based on the internal, local and global threat landscape and should be updated at least annually.
- **Framework & Foundational Controls** – The NIST CSF provides a best practice framework and foundation for applying cyber security controls across both IT and control systems environments. To support this a mapping has been provided where the relevant CSF subcategories are listed against the CIP requirements.
- **CIP Requirements** – these provide the recommended minimum standard required across control systems environments in addition to the foundational controls. These are clearly defined along with specific measures and operators can read the standard in a sequential manner or choose a component or aspect that best meets organisational needs, requirements and risk profile.
- **Assurance** – Overall a compliance and measurement regime should exist that provides assurance over the effectiveness of the foundational and CIP requirements.

2.3 Governance & Roles

To effectively manage cyber security threats and maintain an acceptable level of risk a governance framework with clearly defined roles must exist. This is the essential first step to applying the VCSS-CSO. This should include not just the Critical and Cyber Asset owners but also clearly identify the roles that are accountable and responsible for cyber security management across the organisation. This must be aligned with the organisational structure and have a clear line of sight to the executive and the board. Without a governance model in place, it is not possible to effectively manage and report risks and ensure that the organisation consciously defines an acceptable position around cyber security threats and their resultant risks. There are many guides available for establishing governance. The most important aspect, however, is that all the roles are clearly defined, and effective reporting is embedded into the governance model.

Governance should extend to consider supply chain risks including third-parties and outsourcing suppliers. It is important to note that it is not possible to outsource the organisations risks, and this will always need to be governed and managed internally. Governance should include the following minimum considerations for all third-parties and suppliers across the entire organisation and not just IT or control systems environments:

- A requirement to comply with the organisations policies and standards as well as best practice. For control systems environments this should include the CIP requirements;

- Ensuring accountability to manage the cyber security of any services provided to the organisation including vulnerability discovery and patch management;
- The requirement to notify the organisation of any cyber security incidents in a timely manner;
- The right to audit the third-party or supplier on a regular basis;
- The agreement to participate in cyber security testing;
- An acceptance of responsibility and liability should there be any cyber security incidents in their area of management affecting the confidentiality, integrity and availability of services delivered to the organisation;
- The right to terminate without penalty for ongoing non-compliance;
- Proactive and regular management of the performance of the third-party or supplier and clearly defined relationship ownership in the organisation, and
- There should also be an annual review of agreements which includes the requirements for third parties and suppliers to complete a self-assessment which may result in a full audit if results are not satisfactory.

2.4 Risk Assessment & Management

For control systems environments the biggest risk is often disruption to the availability of systems and therefore return to operations in a minimum timeframe is the primary driver. It is, however, important to consider a wider risk context for the management of cyber security controls and investments. A mature risk framework takes the threats faced by the organisation and portrays them in a context that is aligned to how the wider organisation manages and perceives risk. Managing risk is a continuous and ongoing process that requires the following:

- **Business Integration** – managing risks is only effective if those risks have clear owners and the organisational responsibilities and governance model are well embedded. Cyber security risks should be defined and reported in the same context as wider organisational risks like health and safety.
- **Continuous Assessment & Reporting** – risks must be continually assessed based on the changes in the threat landscape and the effectiveness of controls. Incidents should be aligned to threats and risks and be used to validate the effectiveness of controls.
- **Management Framework –** effective cyber security risk management should in the first instance adopt the existing organisational framework. If this has not been established, there are common standards available that can provide guidance.

2.5 Threat Modelling

There are many different methodologies and frameworks to represent the threats being faced by an organisation.

With regards to cyber risk, this standard adopts the definition according to the widely accepted standard ISO 27005: “**Threats** abuse **vulnerabilities** of **assets** to generate **harm** for the **organisation**”.

In more detailed terms, risk is considered as being composed of the following elements:

- **Threat** (Threat Actor Profile, Likelihood);
- **Asset** (Vulnerabilities, Controls), and
- **Impact** (Consequence).

Control Systems Top Threats

There is an increasing number of malicious adversaries or threat actors using sophisticated or organised cyber-attack methods to targeted control systems and critical infrastructures around the world. The first step to protecting against these threats is identifying them and the potential impact and consequences they may have on the assets of the organisation. As part of this is it also necessary to recognise the types of threat actors be they internal or external that could be behind these threats. Across the energy sector the following key threats are recognised as needing to be managed:

- **System and Application Attacks -** System and application attacks occur when a threat actor such as a hacker exploits a vulnerability or weakness to bypass logical system controls to gain unauthorised access to a service or system.
- **Unauthorised Access to Information -** Data breaches or information leakage occurs if commercially or sensitive operational data is disclosed to unauthorised parties by either malicious intent or an inadvertent mistake.
- **Misuse of Elevated Privileges -** Users who have elevated privileges to systems, beyond their normal role can install unlicensed or malicious software or remotely access critical infrastructure systems. These privileges if abused or obtained by an unauthorised party can enable a system compromise to occur.
- **Denial of Service (DOS) -** Attacks that can be launched externally or from internally compromised systems. DOS attacks can cripple network resources resulting in the inability to manage control systems or communicate with business partners. Services available via or dependant on the internet are highly vulnerable to a coordinated form of this attack called a Distributed Denial of Service (DDOS) attack which floods external systems with thousands and in extreme cases millions of individual source locations complicating service recovery if the attack is persistent.
- **Physical Manipulation/Damage/Theft/Loss of Asset -** Physical access presents a means to damage or access systems with information stored on them could be used to gain further access systems or disclose sensitive information.

Control Systems Top Threat Actors

It is important to recognise that the threat actors behind these threats to control systems are varied and could be malicious or inadvertent as well as internal or external. They can also be partners or any other providers in the supply chain. A general list of threat actors is:

- **Hackers –** Are generally motivated by prestige. They often target publicly available web services with known vulnerabilities with an aim to deface or obtain sensitive personal and business information.
- **Organised Crime –** Are usually motivated by financial gain as either individuals or part of larger organisations or syndicates. They will target systems based on financial

return which often includes financial / payment systems, personally identifiable information. They may use ransomware (malware) as an extortion method.

- **Insider (Inadvertent) –** Often as a result of trying to be helpful, lacking security awareness or intentionally negligent in their behaviour. Targeted by other threat actors as a weakness to bypass security controls or expose a vulnerability through human or configuration error.
- **Insider (Malicious) –** Can be motivated by personal advantage, monetary gain or professional revenge. Targets sensitive or restricted information, business operations, or personnel information.
- **Partner (Inadvertent or Malicious) -** Partners include any third-party, cloud service provider or outsourcer that has a business relationship with the operator. These can form part of the supply chain and can be targeted by other threat actors as a weakness to bypass security controls or expose a vulnerability through human or configuration error.
- **Hacktivist –** Generally motivated by wanting to pressure businesses to change their practices through political influence and social change. They target trade secrets, sensitive or restricted information, disrupts business activities using denial of service attacks.
- **Nation State -** Motivated by economic, political or military advantage. Targets trade secrets, sensitive information, disruption of business activities, emerging technologies and critical infrastructure.

Control Systems Top Consequences

The top consequences of these threats, combined with the threat actors, manifesting themselves in an organisation can be varied and specific to an organisation. Key consequences to consider are:

- Safety incident or loss of life;
- An interruption, loss of access or control occurs to control systems infrastructure;
- Destruction of control systems infrastructure or data;
- Leakage of sensitive control systems or customer related information;
- An interruption, loss of access or control of ICT systems which support control systems; infrastructure
- Destruction of information related systems or data, and
- Leakage of sensitive information from information technology related systems.

2.6 Framework & Foundational Controls

The CSF is an example of a framework of controls which can be implemented across an organisation. It is based on existing internationally recognised standards, guidelines, and best practices to better manage and reduce cyber security risk. In addition to helping organisations manage and reduce risks, it was designed to foster risk and cyber security

management communications amongst both internal and external organisational stakeholders.

The CSF will help an organisation to better understand, manage, and reduce its cyber security risks. It will assist in determining which activities are most important to assure critical operations and service delivery. In turn, that will help to prioritise investments and maximise the impact of each dollar spent on cyber security. By providing a common language to address cyber security risk management, it is especially helpful in communicating internally across the organisation and to external stakeholders. That includes improving communications, awareness, and understanding between and among IT, planning, and operating units, as well as senior executives of organisations. Organisations can also use the CSF to communicate current or desired cyber security posture between a buyer or supplier.

The CSF is a set of cyber security activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. An example of CSF outcome language is, "physical devices and systems within the organisation are inventoried." The CSF consists of five concurrent and continuous functions—Identify, Protect, Detect, Respond and Recover. When considered together, these functions provide a high-level, strategic view of the lifecycle of an organisation's management of cyber security risk. The CSF then identifies underlying key categories and subcategories for each function and matches them with example informative references, such as existing standards, guidelines, and practices for each subcategory. An additional mapping has been provided for the CIP requirements to the CSF and each CIP requirement has references to the relevant CSF subcategories.

Figure 3: The NIST CSF Functions

There are no "silver bullets" when it comes to cyber security and protecting an organisation. For instance, "Zero-day" attacks exploiting previously unknown software vulnerabilities are especially problematic. However, using the CSF to assess and improve management of cyber security risks should put organisations in a much better position to identify, protect, detect, respond to, and recover from an attack, minimising damage and impact. An organisation can use the CSF to establish a common foundation across the organisation to determine activities that are most important to critical service delivery and prioritise expenditures to maximise the impact of the investment.

2.7 Assurance

It is important that an ongoing programme of assurance is established to support the compliance and measurement of the overall governance of cyber security and the effectiveness of the controls deployed in the IT and controls systems environments. Especially for the CIP requirements, specific evidence and records of compliance should be maintained.

An assurance programme can include a range of activities including:

- **Security Assessments** – performed either internally or by an external specialist.
- **Security Audits** – carried out by either internal or external audit teams including:
  - Compliance Audits;
  - Self-Certification;
  - Spot Check Audits (conducted anytime using internal resources or an appointed external auditor / assessor);
  - Periodic Audit (conducted on a scheduled basis using either internal resources or an appointed external auditor / assessor), or
  - Triggered investigations following a major breach or system event.
- **Security Testing** – this can include a range of activities including:
  - Vulnerability Scanning;
  - Penetration Testing;
  - Table Top Exercises, or
  - Live Testing.

Organisations are also encouraged to establish internal controls like change and configuration management to ensure that controls effectiveness is maintained. This can be combined with the adoption of industry baselines or standards and should also include ongoing vulnerability scanning and management.

For all the controls the organisation should include consideration for the following:

- **Measures –** how will effectiveness be validated and what processes, records and metrics need to be established to provide continual and ongoing monitoring. This should include documentation on how each control is being managed, and
- **Retention –** how long does data and information need to be retained for to support both measurement and historical reporting.

3.0 CIP Requirements

The following sections cover the CIP requirements that have predominantly been reviewed and adapted from NERC. They are specific to control systems environments but there is no limitation to also applying them across the entire organisation including IT environments.

The requirements apply to any operator owning or operating control systems assets. The demarcation and exclusion are cyber assets associated with external communication networks and data communication links between discrete Electronic Security Perimeters (ESPs), which are not owned or operated by the operator.

3.1 CIP-001 Critical & Cyber Asset Identification

Overview

- **Purpose** - CIP-001 requires the identification and documentation of Critical and Cyber Assets. These critical assets are to be identified through the application of a risk-based assessment.
- **Objective** - Identifying Critical and Cyber Assets will enable the organisation to prioritise and direct effort and resources to ensure these assets are protected. The organisations should be able to:
    - Identify which systems are critical and understand why;
    - Include relevant systems measures commensurate with systems criticality;
    - Report on the effectiveness of specific security controls protecting systems critically, and
    - Apportion resource and effort to protect systems based on criticality (i.e. minimising over-commitment or under-commitment of resources).

Requirements

R1. **Critical Asset Identification Methodology** - The operator should identify and document a risk-based assessment methodology to identify its Critical Assets (ID-AM-5). The assessment should consider the following assets:

R1.1. Transmission substations that support the reliable operation of the NZ electricity system.

R1.2. Generation resources that support the reliable operation of the NZ electricity system.

R1.3. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.4. Systems and facilities critical to automatic load shedding under a common control system.

R1.5. Special protection systems that support the reliable operation of the NZ electricity system.

R1.6. Any additional assets that support the reliable operation of the NZ electricity system that the operator deems appropriate to include in its assessment.

R1.7. Any communication assets owned or operated by the operator required to support the reliable operation of the NZ electricity system

R1.8. Control centres or backup control centres used to control generation at plant locations, for any generation facility or group of generation facilities identified in criteria of these requirements.

R1.9. Control centres or backup control centres used to perform the functional obligations of the operator that includes the control of at least one asset identified in criteria of these requirements.

R2. **Assessment Methodology -** The operator should maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria (ID.AM-1).

R3. **Critical Asset Identification** - The operator should develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The operator should review this list at least annually and update it as necessary (ID.AM-2).

R4. **Cyber Asset Identification** - Using the list of Critical Assets developed from R1, the operator should develop a list of associated Cyber Assets and specifically identify any Critical Cyber Assets. Within the context of this standard the term Cyber Asset includes any Critical Cyber Assets for the purposes of applying the CIP requirements. Examples include:

- Control centres and backup control centres;
- Systems and facilities at master and remote sites that provide monitoring and control;
- Automatic generation control, and
- Real-time power system modelling and real-time inter-utility data exchange.

The operator should review this list at least annually and update it as necessary. For the purpose of this standard, Critical Cyber Assets are further qualified by having one of the following characteristics (ID.AM-3):

R4.1. The Cyber Asset uses a routable protocol to communicate outside the ESP or,

R4.2. The Cyber Asset uses a routable protocol within a control centre; or,

R4.3. The Cyber Asset can be accessed remotely.

R5. **Annual Approval** - The operator should approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Cyber Assets. The operator should keep a signed and dated annual approval record of the risk-based assessment methodology, the list of Critical Assets and the list of Cyber Assets (ID.AM-6).

3.2 CIP-002 Systems Security Management

Overview

- **Purpose -** CIP-002 requires operators to define methods, processes and procedures for securing those systems determined to be Cyber Assets and Critical Cyber Assets within the ESP.
- **Objective** - Implement robust practises to actively manage the risks related to Cyber Assets.

Requirements

R1. **Test Procedures** - the operator should ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls. For the purposes of CIP-002 a significant change should, at a minimum, include implementation of security patches, cumulative service packs, vendor releases and version upgrades of operating systems, applications, database platforms or other third-party software or firmware (ID.SC-5 & PR.IP-3).

R1.1. The operator should create, implement and maintain cyber security test procedures in a manner that minimises adverse effects on the production system or its operation (PR.DS-7).

R1.2. The operator should document that testing is performed in a manner that reflects the production environment (PR.IP-10).

R1.3. The operator should document test results.

R2. **Network Segregation** - The operator should establish, document and maintain network controls to ensure that remote access to all Cyber Assets within the ESP is restricted to only authorised users and ports required for normal and emergency operations. (PR.IP-1 & PR.PT-3).

R2.1. Cyber Assets within the ESP should be segregated from the corporate environment and where applicable each other based on risk assessment.

R2.2 The operator should enable only those ports and services required for normal and emergency operations.

R2.3. The operator should disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the ESP.

R2.4. In the case where unused ports and services cannot be disabled due to technical limitations, the operator should document compensating measure(s) applied to mitigate risk exposure.

R3. **Security Patch Management** - The operator, either separately or as a component of the documented configuration management process specified in CIP-003 R6, should establish, document and implement a security patch management programme for tracking, evaluating, testing and installing applicable cyber security software patches for all Cyber Assets within the ESP (PR.IP-12 & DE.CM-8).

R3.1. The operator should document the assessment of security patches and security upgrades for applicability within 30 calendar days of the availability of the patches or upgrades.

R3.2. The operator should document the implementation of security patches. Where a patch is not installed, the operator should document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Code Prevention - Where technically feasible the operator should use anti-virus software and other malicious software ("malware") prevention tools such as application whitelisting to detect, prevent, deter and mitigate the introduction, exposure and propagation of malware on all Cyber Assets within the ESP (DE.CM-4 & PR.PT-3).

R4.1. The operator should document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the operator should document compensating controls applied to mitigate risk exposure.

R4.2. The operator should document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R4.3. The operator should document and implement a process for the approval of applications to the application whitelist. The process must address testing the application for malicious code before approval.

R5. Account Management - The operator should establish, implement and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity and that minimise the risk of unauthorised system access.

R5.1. The operator should ensure that individual and shared system accounts and authorised access permissions are consistent with the concept of "Least Privilege" with respect to work functions performed (PR.AC-4).

R5.2. The operator should ensure that user accounts are implemented as approved by designated personnel. Refer to CIP-003 R5 (ID.GV-2).

R5.3. The operator should establish methods, processes and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days (PR.AC-1 & DE.CM-3).

R5.4. The operator should review, at least annually, user accounts to verify access privileges are in accordance with CIP-003 R5 and CIP-009 R4.

R5.5. The operator should implement a policy to minimise and manage the scope and acceptable use of administrator, shared and other generic account privileges including factory default accounts (PR.AT-2 & PR.AC-7).

R5.5.1. The policy should include the removal, disabling or renaming of such accounts where possible. For such accounts that must remain enabled, passwords should be changed prior to putting any system into service.

R5.5.2. The operator should identify those individuals with access to shared accounts.

R5.5.3. Where such accounts must be shared, the operator should have a policy for managing the use of such accounts that limits access to only those with authorisation, an audit trail of the account use (automated or manual) and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.5.4. Where technically feasible or where interactive remote access is implemented, the operator should enable Multi Factor Authentication (MFA) to reduce the risk of unauthorised access through password cracking or compromise.

R5.6. For password-only authentication the operator should, at a minimum and as technically feasible, require and use passwords subject to the following:

R5.6.1 Each password should be a minimum of 10 characters.

R5.6.2 Each password should consist of a combination of alpha, numeric and "special" characters.

R5.6.3 Each password should be changed at least annually or more frequently based on risk.

R6. Security Status Monitoring - The operator should ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organisational process controls to monitor system events that are related to cyber security (DE.AE-2, DE.AE-3, DE.AE-5 & DE.CM-1).

R6.1. The operator should implement and document the organisational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the ESP.

R6.2. The security monitoring controls should be implemented according to the principle of defence in depth with two or more methods for detecting known or suspected malicious communications for both inbound and outbound communications, including but not limited to Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection, application layer firewall etc.

R6.3. The security monitoring controls should issue automated alerts for detected cyber security incidents.

R6.4. The operator should maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in CIP-007.

R6.5. The operator should retain all logs specified in R6 for ninety calendar days online, with offline retention of logs for 12 months.

R6.6. The operator should review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment - The operator should establish and implement formal methods, processes and procedures for disposal or redeployment of Cyber Assets within the ESP as identified and documented in CIP-004 (PR.DS-3).

R7.1. Prior to the disposal of such assets, the operator should destroy or erase the data storage media to prevent unauthorised retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the operator should, at a minimum, erase the data storage media to prevent unauthorised retrieval of sensitive cyber security or reliability data.

R7.3. The operator should maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment - The operator should perform a cyber vulnerability assessment of all Cyber Assets within the ESP at least annually. The vulnerability assessment should include, at a minimum, the following (PR.IP-12 & ID.RA-1):

R8.1. A document identifying the vulnerability assessment process.

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the ESP are enabled.

R8.3. A review of controls for default accounts.

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment and the execution status of that action plan.

R9. Documentation Review and Maintenance - The operator should review and update any documentation specified at least annually. Changes resulting from modifications to the systems or controls should be documented within thirty calendar days of the change being completed.

3.3 CIP-003 Security Management Controls

Overview

- **Purpose -** CIP-003 requires operators have minimum security management controls in place to implement this standard and protect their Cyber Assets.
- **Objective** – To continually improve the cyber security posture and resilience of the organisation through the implementation and maintenance of security management controls.

Requirements

R1. **Cyber Security Policy -** The operator should document and implement a cyber security policy that represents management's commitment to implement this standard and any additional cyber security requirements. The operator should, at minimum, ensure the following (ID.GV-1):

R1.1. The cyber security policy addresses the guidance on applying this standard and its requirements.

R1.2. The cyber security policy is readily available to all personnel involved in cyber security governance and management and those who have access to or are responsible for Cyber Assets.

R2. **Senior Governance** – The operator should assign a single senior manager with overall responsibility and authority for leading and managing the implementation of, adherence to and annual review of the cyber security policy (ID.GV-2).

R2.1. The senior manager should be identified by name, title and date of designation.

R2.2. Changes to the designated senior manager must be documented.

R2.3. Where allowed by this standard, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations should be documented in the same manner as R2.1 and R2.2 and approved by the senior manager.

R2.4. The senior manager [or delegate(s)], should authorise and document any exception from the requirements of the cyber security policy. These exceptions must be documented within 30 days of being authorised, must include an explanation as to why the exception is necessary, the expected timeframe for the exception and if any compensating or alternative measures have been applied.

R3. **Exceptions** - Any exceptions must be reviewed and approved annually by the senior manager [or delegate(s)] to ensure the exceptions are still required and valid.

R4. **Cyber Security Programme** - The operator should implement and document a programme to implement the controls identified through the cyber security policy and identify and protect information associated with Cyber Assets as follows (ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-5, PR.IP-1 & PR.IP-9):

R4.1. The Cyber Asset information to be protected should, at a minimum and regardless of media type, include operational procedures; lists as required in CIP-001; network topology or similar diagrams; floor plans of computing centres that contain Cyber Assets; equipment layouts of Cyber Assets; disaster recovery plans; incident response plans and security configuration information (i.e. permitted protocols, admin accounts. remote access and management, etc.).

R4.2. The operator should identify information to be protected under this programme based on the sensitivity of the Cyber Asset information.

R4.3. The operator should, at least annually, assess adherence to its Cyber Asset information protection programme, document the assessment results and implement an action plan to remediate deficiencies identified during the assessment.

R5. Personnel Management - The operator should document and implement a programme for managing personnel access to protected Cyber Asset information as follows (PR.AC-1, PR.AC-2, PR.AC-3 & PR.AC-4):

R5.1. The operator should maintain a list of designated personnel who are responsible for authorising logical or physical access to protected information.

R5.1.1. Personnel should be identified by name, title and the information for which they are responsible for authorising access.

R5.1.2. The list of personnel responsible for authorising access to protected information should be verified at least annually.

R5.2. The operator should review, at least annually, the access privileges to protected information to confirm that access privileges are correct and that they correspond with the operator's needs and appropriate personnel roles and responsibilities.

R5.3. The operator should assess and document, at least annually, the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management - The operator should establish and document a process of change control and configuration management for adding, modifying, replacing or removing Cyber Asset hardware or software and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Cyber Assets pursuant to the change control process (PR.IP-3).

3.4 CIP-004 Electronic Security Perimeter

Overview

- **Purpose** - CIP-004 requires the identification and protection of the ESP inside which all Cyber Assets reside, as well as all access points on the perimeter.
- **Objective** - To continually improve the cyber security posture and resilience of the organisation through the identification and implementation of protection measures relating to Cyber Assets within an ESP and its access points.

Requirements

R1. **Electronic Security Perimeter** - The operator should ensure that every Cyber Asset resides within an ESP. The operator should identify and document the ESP and all access points to the perimeter(s) (ID.AM-1, ID.AM-2 & ID.AM-3),

R1.1. Access points to the ESP should include any externally connected communication end point (e.g. routers, network connections) terminating at any device within the ESP.

R1.2. For a dial-up accessible Cyber Assets that uses a non-routable protocol, the operator should define an ESP for that single access point at the dial-up device.

R1.3. Communication links connecting discrete ESP's should not be considered part of the ESP. However, end points of these communication links within the ESP should be considered access points to the ESP.

R1.4. Any Cyber Asset within a defined ESP should be identified and protected pursuant to the requirements of CIP-004.

R1.5. Cyber Assets used in the access control and/or monitoring of the ESP should be afforded the protective measures as specified in CIP-003; CIP-004 R2 and R3; CIP-005 R3; CIP-002 R1 and R3 through R9; CIP-007; and CIP-008.

R1.6. The operator should maintain documentation of every ESP, all interconnected Cyber Assets within the ESP, all electronic access points to the ESP and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. **Electronic Access Controls** - The operator should implement and document the organisational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESP (PR.AC-3, PR.AC-4, PR.AC-6, PR.IP-1 & DE.CM-3).

R2.1. These processes and mechanisms should use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the ESP, the operator should enable only ports and services required for operations and for monitoring Cyber Assets within the ESP, and should document individually or by specified grouping, the configuration of those ports and services.

R2.3. The operator should implement and maintain a procedure for securing any form of remote access to the ESP.

R2.4. Where external interactive access into ESP has been enabled, the operator should implement strong procedural and technical controls at the access points to ensure authenticity of the accessing party pursuant to the requirements of CIP-002 R5.2.

R2.5. The operator should enable external interactive access into the ESP only for the time period such access is required, and access should be monitored during use pursuant to the requirements of CIP-002 R6.2.

R2.6. The required documentation should, at least, identify and describe:

R2.5.1. The processes for access request and authorisation.

R2.5.2. The authentication methods, in accordance with CIP-002 R5.

R2.5.3. The review process for authorisation rights, in accordance with CIP-010 R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.5.5. Appropriate Use Banner - Electronic access control devices should display an appropriate use banner on the user screen upon all interactive access attempts, where technically feasible.

R3. Monitoring Electronic Access - The operator should implement and document processes for continuously monitoring and logging access at access points to the ESP (DE.CM.1, DE.CM-4, DE.DP-1 & DE.DP-4):

R3.1 For remotely accessible Cyber Assets that use non-routable protocols, the operator should implement and document monitoring processes at each access point to the remotely accessible device.

R3.2. The security monitoring processes should detect and alert for attempts at or actual unauthorised accesses. These alerts should provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the operator should review or otherwise monitor access logs for attempts at or actual unauthorised accesses at least every sixty calendar days.

R4. Cyber Vulnerability Assessment - The operator should perform a cyber vulnerability assessment of the electronic access points to the ESP at least annually. The vulnerability assessment should include, at a minimum, the following (PR.IP-12 & ID.RA-1):

R4.1. A document detailing the vulnerability assessment process.

R4.2. A review to verify that only ports and services required for operations at these access points are enabled.

R4.3. The discovery of all access points to the ESP.

R4.4. A review of controls for default accounts, passwords and network management community strings.

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment and the execution status of that action plan.

R5. Documentation Review and Maintenance - The operator should review, update and maintain all documentation to support compliance with the requirements of CIP-004.

R5.1. The operator should ensure that all documentation required by CIP-004 reflects current configurations and processes and should review the documents and procedures referenced in CIP-004 at least annually.

R5.2. The operator should update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The operator should retain electronic access logs for at least ninety calendar days online, with offline retention of logs for 12 months. Logs related to reportable incidents should be kept in accordance with the requirements of CIP-007.

3.5 CIP-005 Physical Security

Overview

- **Purpose** - To ensure the implementation of a physical security programme for the protection of Cyber Assets. The requirements detailed in CIP-005 are the minimum protective physical security requirements.
- **Objective** - To continually improve the cyber security posture and resilience of the organisation through the implementation and maintenance of physical security controls.

Requirements

R1. **Threat & Risk Assessment** – These should be conducted and reviewed yearly using the appropriate standards i.e. ISO 31000 and HB 167 Security Risk Management (ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, PR.AT-5, PR.IP-5 & DE.CM-2)

R2. **Design Principles** - When selecting suitable locations, the operator should consider Crime Prevention through Environmental Design principles (CPTED) that assist in deterring crime. The design of these facilities should also utilise multiple levels of security creating defence in depth.

R3. **Physical Security Plan** - The operator should document, implement and maintain a physical security plan, approved by the senior manager or delegate(s) that should address, at a minimum, the following:

R3.1. All Cyber Assets within an ESP should reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the operator should deploy and document alternative measures to control physical access to such Cyber Assets.

R3.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R3.3. Processes, tools and procedures to monitor physical access to the perimeter(s).

R3.4. Appropriate use of physical access controls as described in R4 including visitor pass management, responses to loss of access devices and prohibition of inappropriate use of physical access controls.

R3.5. Review of access authorisation requests and revocation of access authorisation, in accordance with CIP-004 R4.

R3.6. A visitor control programme for visitors (personnel without authorised unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R3.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R3.6.2. Continuous escort of visitors within the Physical Security Perimeter.

R3.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls or logging controls.

R3.8. Annual review of the physical security plan.

R4. **Protection of Physical Access Control Systems** - Cyber Assets that authorise and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, should:

R4.1. Be protected from unauthorised physical access.

R4.2. Be afforded the protective measures specified in CIP-003 & CIP-009 R3, CIP-004 R2 and R3, CIP-005 R4 and R5, CIP-002, CIP-007 and CIP-008.

R5. **Protection of Electronic Access Control Systems** - Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) should reside within an identified Physical Security Perimeter.

R6. **Physical Access Controls** - The operator should document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The operator should implement one or more of the following physical access methods:

- **Key Card** - A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- **Special Locks** - These include, but are not limited to, locks with “restricted key” systems, electronic locks that can be operated remotely and “man-trap” systems.
- **Identification** - Visual identification where practicable.
- **Security Personnel** - Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- **Other Authentication Devices** - Biometric, keypad, token, or other equivalent devices that control physical access to Cyber Assets.
- **Multi Factor Authentication** – Strong authentication using multiple factors should be considered for Critical and Cyber Assets.
- **Fail Safe Defaults** - Provision and or procedures should be in place to ensure security in the event of prolonged power outage or system failure.

R7. **Monitoring Physical Access** - The operator should document and implement the technical and procedural controls for continuously monitoring physical access at all access points to the Physical Security Perimeter(s). Unauthorised access attempts should be reviewed immediately and handled in accordance with the procedures specified in the requirements of CIP-008. One or more of the following monitoring methods should be used:

- **Alarm Systems** - Systems that alarm to indicate a door, gate or window has been opened without authorisation. These alarms must provide for immediate notification to personnel responsible for response. Alarm systems should comply with the AS/NZS 2201.1:2007 and AS/NZS 2201.5:2008.

- **Human Observation of Access Points** - Monitoring of physical access points by authorised personnel as specified in R4.

R8. **Logging Physical Access** - Logging should always record enough information to uniquely identify individuals' access. The operator should implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- **Computerised Logging** - Electronic logs produced by the operator's selected access control and monitoring method.
- **Video Recording** - Electronic capture of video images of sufficient quality to determine identity.
- **Manual Logging** - A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorised to control and monitor physical access as specified in R4.

R9. **Access Log Retention** - The operator should retain physical access logs for at least ninety calendar days online, with offline retention of logs for 12 months. Logs related to reportable incidents should be kept in accordance with the requirements of CIP-007.

R10. **Maintenance and Testing** - The operator should implement a maintenance and testing programme to ensure that all physical security systems under R4, R5, and R6 function properly. The programme must include, at a minimum, the following:

R10.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R10.2. Retention of testing and maintenance records for the cycle determined by the operator in R8.1.

R10.3. Retention of outage records regarding access controls, logging and monitoring for a minimum of one calendar year.

3.6 CIP-006 Threat Levels & Incident Reporting

Overview

- **Purpose** – To ensure the operator has implemented a Threat Alert Level (TAL) framework to be able to rapidly categorise both response and reporting actions. This includes increasing the level of preparedness internally, mobilising response teams and escalating to external agencies in accordance with agreed plans. External agencies include the NCSC and where appropriate the wider CSSIE community, NZ Police and CERT NZ. Cyber security incident reporting to the NCSC does not replace any existing operational or compliance reporting processes, procedures and requirements. The identity of the critical infrastructure operator will not be disclosed beyond the NCSC unless authorised by the operator and as part of the TAL process using the Traffic Light Protocol (TLP) guideline.
- **Objective** - To continually improve the cyber security posture and resilience of the organisation through maintaining internal threat alert levers and participating in incident reporting to ensure the industry sector at a whole is adequately protected and minimising the impact of any downstream incident from occurring.

  Reporting cyber security incidents helps NCSC to develop a better picture of the threat environment for government systems and CNI and assists other agencies who may also be at risk. Cyber security incident reports are also used for developing new policies, procedures, techniques and training measures to help prevent future incidents. Reporting cyber security incidents to NCSC through the appropriate communication channels ensures that appropriate and timely assistance can be provided. The purpose of recording cyber security incidents in a register is to identify the nature and frequency of the cyber security incidents so that mitigation actions can be taken.

Requirements

R1. **Cyber Security Incident Identification** - Have procedures to ensure operating personnel are aware of, and able to recognise, major cyber security incident events (PR.AT-3, PR.AT-4, PR.AT-5).

R1.1 Cyber security incidents include but are not limited to:

- Attempts to gain unauthorised access to a Critical Asset, Cyber Asset or computer system or its information;
- Unwanted disruption or denial of service;
- Unauthorised use of a system for processing or storing information, and
- Changes to system hardware, firmware or software without the knowledge or consent of the system owner.

R1.2 Cyber security incidents can range in severity and/or be part of a broader security emergency. Major cyber security incidents severely impact information infrastructures and services of major organisations or numerous organisations of national importance. The impact may be complex and difficult to contain. The incident has wide or significant detrimental implications for national interests.

R2. Incident Response Procedures – The operator should provide its operating personnel with cyber security incident response and reporting procedures or guidelines. See also CIP-007 (RS.CO-1).

R2.1 operator must detail cyber security incident responsibilities and procedures for each system in the relevant standard operating procedures.

R2.1.1 Documenting responsibilities and procedures for cyber security incidents in relevant standard operating procedures to ensure that when a cyber security incident does occur, personnel can respond in an appropriate manner.

R2.1.2 Understand the procedures when reporting cyber security incidents as part of the their CSSIE membership.

R3. Communications Plans – The operator should have procedures for the communication of information concerning cyber security incident events to appropriate internal and external stakeholders (ID.BE-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.CO-5).

R3.1 Have procedures, if an event is assessed to be a major cyber security incident, to report immediately to the NCSC and/or where relevant NZ Police. All incident reports provided to the NCSC will be treated in the strictest confidence.

R4. Incident Register - The operator should ensure that all cyber security incidents are recorded in a register. This register should be used as a reference for future security risk assessments and continuous improvement. The operator should include, at the minimum, the following information in their register:

- The date the cyber security incident was discovered
- The date the cyber security incident occurred
- A description of the cyber security incident and whether it was reported
- Any reference details to assist with improved ongoing reporting and management.

R5. Threat Alert Level (TAL) Framework – The operator should implement a framework for internal threat alert levels that represent the current threat level to the organisation. This level should be re-evaluated based on any changes in the internal or external threat landscape based on the impact of the threat, the criticality of assets potentially impacted and the effectiveness of controls and/or countermeasures. Useful guidance on threat alert levels can be found here - https://www.cisecurity.org/cybersecurity-threats/alert-level/. Any high or severe threat levels should trigger an escalation to the NCSC and potentially advising NZ Police, CERT NZ and other CSSIE members.

3.7 CIP-007 Incident Response and Handling

Overview

- **Purpose** - Ensures the identification, classification, response and reporting of cyber security incidents related to Critical and Cyber Assets. The New Zealand Security Incident Management Guide for CSIRT's, available from www.ncsc.govt.nz/resources, provides detailed information on best practices and basic framework for NZ Government and CNI organisations when establishing or reinforcing existing incident management and response capabilities.
- **Objective** - To continually improve the cyber security posture and resilience of the organisation through the implementation and maintenance of procedures to ensure that operating personnel are aware of, and able to recognise, major cyber security incident events, manage them effectively and report these to appropriate parties in the instance of a major cyber security breach. This aims to support cyber security posture by ensuring record keeping and accurate documentation processes take place at every stage. This standard should be considered with understanding of the requirements presented in their entirety.

Requirements

R1. **Cyber Security Incident Response Plan** - The operator should develop and maintain a Cyber Security Incident Response Plan and implement the plan in response to cyber security incidents. The Cyber Security Incident Response Plan should address, at a minimum, the following (PR.IP-9, RS.RP-01):

R1.1. Procedures to characterise and classify events as reportable cyber security incidents (DE.AE-4, RS.AN-1, RS-AN-2).

R1.2. Response actions, including roles and responsibilities of cyber security incident response teams, cyber security incident handling procedures and communication plans (DE.DP-1, RS.CO-1, RS-AN-4).

R1.3. A process for reporting cyber security incidents to the NCSC. The operator should ensure that all reportable cyber security incidents as defined in R1.1 are reported to the NCSC either directly or through an intermediary (RS.CO-2, RS.CO-3, RS.CO-4)

R1.4 A process for reporting cyber security incidents to participating CSSIE members following identification of a major cyber security incident.

R1.5. A process for updating the Cyber Security Incident Response Plan within thirty calendar days of any changes.

R1.6. A process for ensuring that the Cyber Security Incident Response Plan is reviewed at least annually (RS.IM-2).

R1.7. A process for ensuring the Cyber Security Incident Response Plan is tested at least annually. A test of the Cyber Security Incident Response Plan can range from a paper drill to a full operational exercise (PR.IP-10).

R2. **Cyber Security Incident Documentation** - The operator should keep relevant documentation related to cyber security incidents reportable per R1.1 for three calendar years.

3.8 CIP-008 Recovery Planning

Overview

- **Purpose** – To ensure that recovery plans are put in place for Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.
- **Objective** - To continually improve the cyber security posture and resilience of the organisation through the implementation and maintenance of recovery plans. This helps to ensure that should a cyber incident occur; the operator can adequately recover from the incident.

Requirements

R1. **Recovery Plans** - The operator should create and annually review recovery plans for Cyber Assets. The recovery plan(s) should address at a minimum the following (PR.IP-9, RC.RP-1):

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plans.

R1.2. Define the roles and responsibilities of responders.

R2. **Exercises** - The recovery plans should be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill to a full operational exercise. (PR.IP-10, RC.IM-2).

R3. **Change Control** - Recovery plans should be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates should be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed (RC.IM-1).

R4. **Backup and Restore** - The recovery plans should include processes and procedures for the backup and storage of information required to successfully restore Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, etc.

3.9 CIP-009 Training & Personnel Development

Overview

- **Purpose** – To ensure that personnel having authorised cyber or authorised unescorted physical access to Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training and security awareness.
- **Objective** - To continually improve the cyber security posture and resilience of the organisation through establishing, documenting, implementing and maintaining a security awareness programme.

Requirements

R1. The operator should establish, document, implement and maintain a security awareness programme to ensure personnel having authorised cyber or authorised unescorted physical access to Cyber Assets receive on-going reinforcement in sound security practices. The programme should include security awareness reinforcement on at least an annual basis using mechanisms such as (PR.AT-5):

- Direct communications (e.g., emails, memos, computer-based training etc.);
- Indirect communications (e.g., posters, intranet, brochures etc.);
- Management support and reinforcement (e.g. presentations, meetings etc.).

R2. The operator should establish, document, implement and maintain an annual cyber security training programme for personnel having authorised cyber or authorised unescorted physical access to Cyber Assets. The cyber security training programme should be reviewed annually, at a minimum, and should be updated whenever necessary (PR.AT-5).

R2.1. This programme should ensure that all personnel having access to Cyber Assets, including contractors and service vendors, are trained prior to being granted access, except in specified circumstances such as an emergency.

R2.2. Training should cover the policies, access controls and procedures as developed for the Cyber Assets covered by CIP-001, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Cyber Assets.

R2.2.2. Physical and electronic access controls to Cyber Assets.

R2.2.3. The proper handling of Cyber Asset information.

R2.2.4. Action plans and procedures to recover or re-establish Cyber Assets and access thereto following a cyber security incident.

R2.3. The operator should maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. The operator should have a documented personnel risk assessment programme for personnel having authorised cyber or authorised unescorted physical access to Cyber

Assets. This personnel risk assessment should be conducted prior to the cyber security training programme (R2) and prior to personnel being granted access to Cyber Assets (PR.IP-11). The personnel risk assessment programme should at a minimum include:

R3.1. The operator should ensure that each personnel risk assessment at a minimum include positive identity verification and a criminal background check.

R4. The operator should maintain lists of personnel with authorised cyber or authorised unescorted physical access to Cyber Assets, including their specific electronic and physical access rights to Cyber Assets (PR.AC-1). This should include:

R4.1. Reviewing the list(s) of personnel who have such access to Cyber Assets annually and ensuring the list is properly maintained.

R4.2. Revoking access to Cyber Assets as soon as possible within 24 hours for those personnel, contractors and service vendors whose services have been terminated.

3.10 CIP-010 Managing Confidentiality

Overview

- **Purpose** - To ensure confidentiality relevant to the organisation and any involved parties, relating to the security posture of those business activities.
- **Objective** - This standard intends to support the security posture by ensuring establishment, implementation, adherence and maintenance of confidentiality of Cyber Assets. It will enable an organisation to establish, document, implement and maintain a confidentially programme for authorised personnel and suppliers. This aim is ensuring record keeping and accurate documentation processes take place at every stage.

Requirements

R1. **Confidentiality Arrangement –** The operator should establish arrangements that ensure a party must not disclose the other party's confidential information except as permitted by other agreement and should not use the other party's confidential information except to perform its obligations and take the intended benefit of its rights.

R1.1. The terms of disclosure and use of information should be followed as per negotiations or arrangement between parties.

R1.2. Confidentiality agreements may be determined to align with an organisations internal confidentiality arrangement or to align subject to an organisations information classification methods.

R2. **Use of Another Party's Confidential Information** — The operator should establish arrangements to determine safe keeping, disclosure or destruction of another party's confidential information. This should be arranged between the parties with consideration of existing arrangements, confidentiality agreements or policies of each party (PR.DS-1, PR.DS-2).

R3. **Return of Confidential Information –** The operator should liaise with other parties to determine the procedures and terms of information destruction, return or other means in instances such as ceasing working relationship, termination or finishing agreed upon work, as well as considering CIP-008 for business continuity in the instance of disaster to arrange recovery techniques and practices. This arrangement should be aligned to any parties involved and should be treated as unique and flexible across its application (PR.IP-6).

R4. **Official Information Act –** The operator should make arrangements to ensure that the organisation and/or third parties and suppliers to manage any requests for official information (as defined in the Official Information Act 1982 ("OIA")) in a timely manner (ID.GV-4).

R5. **Confidentiality Agreement -** The operator should work with relevant stakeholders and/or third parties to develop an appropriate confidentiality agreement, and clearly communicate/enforce what this involves. This confidentiality agreement should be aligned to the Cyber Security Policy deployed by the operator as per CIP-003 R1.

3.11 CIP-011 Connected Devices & IoT

Overview

- **Purpose** - Require the identification and management of IoT cyber security risks that could impact or form part of an organisations Cyber Assets. Appropriate controls should be identified and implemented through a detailed risk assessment. For purposes of CIP-011 the US Department of Homeland Security (USDHS) definition of IoT has been adopted:

  "IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems."

  As there is currently no universally agreed framework or standards for IoT, CIP-011 may be updated in future to align to industry standards.

- **Objective** - Where IoT devices are deployed, the identification and implementation of appropriate controls will ensure that Cyber Assets remain protected. In complying with this section and applying the principles outlined in CIP-011, an organisation will limit the potential impacts of any security incidents that may emanate or propagate from IoT devices. The requirements below align with the USDHS "Strategic Principles for Securing the Internet of Things", Version 1.0 dated November 2016 and have been summarised for the purposes of this standard. Further details can be found at https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Requirements

R1. The operator should incorporate security at the design phase.

R1.1. The operator should enable security by default through unique, hard to crack usernames and passwords.

R1.2. The operator should build the device using the most recent operating system that is technically viable and economically feasible.

R1.3. The operator should use hardware that incorporates security features to strengthen the protection and integrity of the device.

R1.4. The operator should design with system and operational disruption in mind.

R2. **Security Updates & Vulnerability Management** - The operator should promote security updates and vulnerability management.

R2.1. The operator should consider ways in which to secure the device over network connections or through automated means.

R2.2. The operator should coordinate software updates among third-party vendors to address vulnerabilities and security improvements to ensure consumer devices have the complete set of current protections.

R2.3. The operator should develop automated mechanisms for addressing vulnerabilities.

R2.4. The operator should develop a policy regarding the coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities.

R2.5. The operator should develop an end-of-life strategy for IoT products including assessing product sunset issues ahead of time and communicating to manufacturers and consumer's expectations regarding the device and the risks of using a device beyond its usability date.

R3. Security Practices - The operator should build on recognised security practices.

R3.1. The operator should start with basic software security and cyber security practices and apply them to the IoT ecosystem in flexible, adaptive, and innovative ways.

R3.2. The operator should refer to relevant sector-specific guidance, where it exists, as a starting point from which to consider security practices.

R3.3. The operator should practice defence in depth and employ a holistic approach to security that includes layered defences against cyber security threats.

R3.4. The operator should participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.

R4. Prioritise Measures - The operator should prioritise security measures according to potential impact.

R4.1. The operator should know and understand a device's intended use and environment, where possible.

R4.2. The operator should perform testing, where developers actively try to bypass the security measures needed at the application, network, data, or physical layers.

R4.3. The operator should identify and authenticate the devices connected to the network, especially for industrial consumers and business networks.

R5. Promote Transparency – The operator should promote transparency across IoT.

R5.1. The operator should conduct end-to-end risk assessments that account for both internal and third-party vendor risks, where possible.

R5.2. The operator should consider creating a publicly disclosed mechanism for using vulnerability reports, e.g. Bug Bounty programmes.

R5.3. The operator should consider developing and employing a software bill of materials that can be used as a means of building shared trust among vendors and manufacturers to help understand and manage their risk and patch any vulnerabilities immediately following any incident.

R6. Due Care - The operator should connect carefully and deliberately.

R6.1. The operator should advise IoT users on the intended purpose of any network connections.

R6.2. The operator should make intentional connections. There are instances when it is in the user's interest not to connect directly to the Internet, but instead to a local network that can aggregate and evaluate any critical information.

R6.3. The operator should build in controls to allow manufacturers, service providers, and consumers to disable network connections or specific ports when needed or desired to enable selective connectivity.

4.0 References

National Cyber Security Centre – role of the agency and resources – https://www.ncsc.govt.nz/resources

NIST Cybersecurity Framework – Framework definition and details - https://www.nist.gov/cyberframework

ISO27001 Information Security Standard – Best practice framework - https://www.iso.org/isoiec-27001-information-security.html

ISO27005 Risk Management Standard – Information security risk standard - https://www.iso.org/standard/75281.html

ISO31000 Risk Management Guidelines – General guidelines for enterprise risk management - https://www.iso.org/standard/65694.html

FAIR – Quantitative risk management - https://www.fairinstitute.org/

European Union Agency for Network and Information Security (ENISA) – Threat landscape report - https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

AS/NZS 2201.1:2007 – Intruder alarm systems - https://shop.standards.govt.nz/catalog/2201.1%3A2007%28AS%7CNZS%29/view

AS/NZS 2201.5:2008 – Alarm systems transmission - https://shop.standards.govt.nz/catalog/2201.5%3A2008%28AS%7CNZS%29/view

New Zealand Computer Emergency Response Team (CERT) – Advice and escalation https://cert.govt.nz

New Zealand Police – Cybercrime unit - https://www.police.govt.nz/

Traffic Light Protocol (TLP) – Definition and levels - https://www.first.org/tlp/

Center for Internet Security (CIS) Cybersecurity Threat Alert Levels – Overview and examples - https://www.cisecurity.org/cybersecurity-threats/alert-level/

New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTSs) - https://www.ncsc.govt.nz/assets/NCSC-Documents/New-Zealand-Security-Incident-Management-Guide-for-Computer-Security-Incident-Response-Teams-CSIRTs.pdf

DHS IoT Principles – Department of Homeland Security strategic IoT security principles - https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

5.0 Appendices

5.1 Reporting Cyber Security Incidents

A government organisation or CNI organisation that has encountered or suspects a cyber incident, should contact NCSC and/or download, complete and return an Incident Reporting Form from https://www.ncsc.govt.nz/incidents/.

Organisations should also ensure that any third-parties or suppliers inform them of all cyber security incidents to allow them to formally report to NCSC and/or relevant law enforcement agencies.

Phone	04 498-7654
Email	Incidents@ncsc.govt.nz