National Cyber Security Centre

Voluntary Cyber Security Standards for Industrial Control Systems v.1.0

www.gcsb.govt.nz
www.ncsc.govt.nz

Foreword

The national and economic security of New Zealand depends on the reliable functioning of critical infrastructure, like our electricity networks.

It is incumbent on infrastructure operators and those with an interest in national security to ensure practical steps are taken to protect and secure such corner stones of our economy.

The development of these voluntary security standards for industrial control systems provides an important base line of cyber security protections. Their production is a significant achievement and a great example of effective industry and government collaboration.

While developed with an emphasis on protection of the industrial control systems used in the electricity sector, the standards have been designed to be widely applicable across the spectrum of control systems used by New Zealand industry.

The standards are based on those developed for comparable international systems, and draw significantly from standards developed by the North American Electric Reliability Corporation (NERC). It is intended that they will be a starting point for further development and improvement.

I commend the New Zealand industry partners, and the staff from the National Cyber Security Centre (NCSC) for their initiative and commitment in developing and publishing these standards and encourage all operators of significant infrastructure to support their implementation.

The NCSC will continue to work closely with infrastructure operators to help maintain the integrity of our critical systems.

Ian Fletcher
Director

Government Communications Security Bureau.

Authors

Alan Harrop, Alun Evans, Andrew Hill, Bart Teekman, Callum Andrew, Carl Grayson, Chris Dodd, Craig Harris, Fritz Hildebrand, Geoff Bard, Grant Botting, , Ivan Murray, Jay Garden, Josh Symes, Keith Betts, Lana Tosic , Mark Holmberg, Mike Judge, Paul Matthews, Peter Galpin, Peter McDowell, Ravin Sami, Scott Oehm, Shaun Trewern, Stephen Allan, Stephen Jennings, Steve Collett, Subrin Shamsuddin, Vinay Ravji, Vish Viswanathan, Wayne Hosking.

Acknowledgements

The authors would like to acknowledge and express deep appreciation to their colleagues for their contribution and support in developing the NCSC Voluntary Cyber security Standards for Industrial Control Systems:

Alex Douglas, Andrew Marshall, Andy Hemming, Barry Brailey, Dave Mulder, Graham Dawson, David Glasgow, David Moore, David Osbourne, Duane Makin, Geoff Brown, Grant Dowson, Grant Lander, James Musgrave, John Cook, Kevin McVey, Paul de Munnik, Ross Mahon, Shane McMasters, Steve Gale, Terry Chapman, Tony Reeves, Vince De Roo, Wayne Redmond, Zhelyko Popovich.

The authors would particularly like to acknowledge:

Heather Ward, Principal Advisor, New Zealand National Cyber Policy Office, Department of Prime Minister and Cabinet,

Jason Smith, Technical Director, CERT Australia, Attorney-General's Department and

New Zealand SIS, who reviewed the NCSC Voluntary Cyber security Standards for Industrial Control Systems.

Their comments, recommendations, suggestions helped us clarify our terms and ideas to make these standards more coherent and accessible.

Introduction

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

CSSIE is a voluntary group, jointly led by industry and the NCSC.

These voluntary standards were developed using an industry-driven process and include a set of requirements designed to secure assets critical for the operation of New Zealand's industrial control systems.

This document is designed to provide high level guidance for securing ICS in the New Zealand environment and has been developed based on standards developed by the North American Electric Reliability Corporation (NERC)[1].

The standards have been developed to enhance the cyber security of electricity sector industrial control systems. The objective is to provide a cyber security framework to ensure the reliable operation of the New Zealand electricity system. While the standards have been developed with a focus on electricity sector systems, they may also be applied to other industrial control systems to enhance system cyber security.

Scope and Purpose

This document aims to establish common security countermeasures that can be applied to ensure reliable operation across and between critical infrastructure operations.

Adherence to this standard is voluntary for all parties.

Much of New Zealand's critical infrastructure makes heavy use of ICS technologies. The infrastructure of New Zealand is highly interconnected and interdependent and is consequently open to cyber threats and vulnerabilities, which could have major economic ramifications or result in environmental damage or loss of life. There are also potential physical and operational security factors that increase the requirement for system resilience and enhanced cyber security.

New Zealand national critical infrastructure is required to operate safely, continuously and reliably with established defensive standardised controls and mechanisms that assist in protecting against a malicious adversary. This document focuses on maintaining the integrity and continuity of both the control systems themselves and the communications between critical components at both the physical and logical levels.

The scope of this document includes ICS used in a wide range of industries to centralise the control and monitoring of technology assets that can be physically distributed. These ICSs include Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC), and support a wide range of industrial sectors, including energy (e.g. electricity, oil and gas) water, transport and a range of manufacturing sectors.

1 Although the standards developed by NERC are heavily oriented toward the energy sector, the principles are common across control systems generally and we would like to thank NERC for their work in this area.

Compliance

The definition of compliance has been established by the CSSIE and indicates self-compliance.
Each responsible entity should be responsible for monitoring their own compliance with the requirements and measures using internal resources or an appointed external auditor/assessor.

Audience

This document covers cyber security aspects specific to the security of ICS. The intended audience includes the following:

- ICS engineers, integrators and architects
- ICS security executives
- Security and information assurance practitioners
- IT security professionals
- IT/ICS risk managers and auditors

NCSC Security Information Exchange role explained

The National Cyber Security Centre (NCSC) is a part of the Government Communications Security Bureau (GCSB) and contributes to the national security of New Zealand by:

- Ensuring the integrity, availability and confidentiality of official information through the provision of Information Assurance (IA) services to Government; and
- Assisting in the protection of the national critical infrastructure from cyber-based threats.

Further information about NCSC can be obtained from the following web site: http://www.ncsc.govt.nz.

The NCSC Security Information Exchange role is to coordinate efforts among New Zealand critical infrastructure owners, operators and vendors to reduce cyber security risks. These efforts include standards development, assessments of risk and preparedness, dissemination of critical information and awareness regarding key security issues. This role includes developing a standardised method and format for responding to suspected threats, as well as setting up trusted communication channels and collaboration across New Zealand.

New Zealand Control Systems Security Information Exchange role explained

The New Zealand Control Systems Security Information Exchange forum is dedicated to improving the protection and cyber security of control systems and networks, operated within New Zealand Critical National Infrastructure (CNI), from cyber based threats.

CSSIE was established to facilitate the exchange of information between its members, in a confidential and trusted environment, concerning threats, vulnerabilities and incidents of electronic attack on control system networks and environments.

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

- An organisation that operates a control system in support of NZ CNI.
- An organisation that meets the NCSC and/or NZ definition of CNI.

Understanding and Using the NCSC Voluntary Cyber Security Standards for Industrial Control Systems

There is an increasing number of very sophisticated cyber-attacks targeting ICS and critical infrastructure around the world.

The only means of mitigating against these attacks is to build in Information Assurance (IA) best practices and security measures through effective standards across the industry to counteract or minimise any negative outcomes.

The main drivers for the development of the NCSC Voluntary Cyber Security Standards for Industrial Control Systems include:

- An observed increase in the number of reported ICS-related cyber security and information technology incidents.
- Decrease the number and types of affected organisations.
- An enhanced awareness of the need for cyber security policies and practices as part of organisational risk management strategies.

The New Zealand Government and industry have responded to this increasingly hostile cyber environment by developing the following standards together in order to help and support New Zealand ICS infrastructure to build resilient cyber security defences and practices.

The standards describe baseline and minimum cyber security technical security standards for ICS. These technical cyber security standards will continue to be updated to help protect against existing threats. They will also outline the necessary roles and responsibilities in cyber information and systems security to support and maintain a more secure environment.

The desired outcome is to prepare New Zealand ICS critical infrastructure to effectively mitigate cyber security threats and risks regardless of their nature, origin, scale, complexity, intensity, and duration. This document is high-level; it is not comprehensive, and it should serve as a basic starting point for developing organisational cyber security protection and resilience.

Overview of Structure

The NCSC Voluntary Cyber Security Standards for Industrial Control Systems consist of nine Critical Infrastructure Protection Cyber Security Standards (CIP). Each CIP standard is broken down into five distinct sections:

- Section A – Introduction: Provides an overview of each standard, its purpose, audience and how it supports New Zealand's critical infrastructure cyber security.
- Section B – Requirements: Provides foundational requirements, defines and provides the context for that particular CIP requirement.
- Section C – Measures: Provides a list of steps to implement a particular requirement.
- Section D – Compliance: Provides specific guidance for Critical Infrastructure ICS compliance monitoring processes to indicate degrees of compliance.
- Appendices – The appendices provide resources to extend understanding and provide further reading.

Benefits

If recognised as a business issue, cyber security can be measured as an investment rather than an expensive business solution. The NCSC Voluntary Cyber Security Standards for Industrial Control Systems should not be about implementing a checklist of requirements, but rather managing cyber risks to an acceptable level.

The benefits of adopting the standards include:

Strategic
Corporate decision-making is improved through the high visibility of the high risk exposure across the whole of the organisation.

Financial
Providing financial benefit to the organisation through the reduction of losses and improved "value for money" potential, noting that cyber security threats and vulnerabilities and consequently cyber security incidents are a cost.

Operational
Organisations are prepared for most eventualities. Having measures and contingency plans in place provides reassurance and helps ensure business continuity.

These standards have been made publicly available to allow greater access, increase awareness, improve transparency and to share good practice.

How to Use the NCSC Voluntary Cyber Security Standards for Industrial Control Systems

Users can read the standards in a sequential manner or choose a particular component or aspect that best meets organisational needs and requirements.

Contents

NCSC CIP–001 — Critical Cyber Asset Identification

A. Introduction

1. **Title:** Critical Cyber Asset Identification

2. **Number:** NCSC CIP-001

3. **Purpose:** Standard NCSC CIP-001 requires the identification and documentation of Critical Cyber Assets (see Appendix A). These Critical Assets are to be identified through the application of a risk-based assessment.

4. **Applicability:**

   4.1. Within the text of Standard NCSC CIP-001, "Responsible Entity" should mean:

   4.1.1. Asset Owner

   and/or

   4.1.2. Asset Operator.

   4.2. The following are exempt from Standard NCSC CIP-001:

   4.2.1. Cyber Assets associated with external communication networks and data communication links between discrete Electronic Security Perimeters which are not owned or operated by the responsible entity.

B. Requirements

R1. Critical Cyber Asset Identification Method — The Responsible Entity should identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity should maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment should consider the following assets:

R1.2.1. Control centres and backup control centres performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the electricity system.

R1.2.3. Generation resources that support the reliable operation of the electricity system.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system.

R1.2.6. Special protection systems that support the reliable operation of the electricity system.

R1.2.7. Any additional assets that support the reliable operation of the electricity system that the Responsible Entity deems appropriate to include in its assessment.

R1.2.8. Any communication assets owned or operated by the responsible entity required to support the reliable operation of the NZ electricity system.

R2. Critical Cyber Asset Identification — The Responsible Entity should develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity should review this list at least annually and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity should develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centres and backup control centres include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modelling and real-time inter-utility data exchange. The Responsible Entity should review this list at least annually and update it as necessary. For the purpose of Standard NCSC CIP-001, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or

R3.2. The Cyber Asset uses a routable protocol within a control centre; or

R3.3. The Cyber Asset is accessible remotely.

R4. Annual Approval — The Responsible Entity should approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2 and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity should keep a signed and dated annual approval record of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null).

C. Measures

M1. The Responsible Entity should make available all documentation of its current risk-based assessment methodology, list of Critical Assets, list of Critical Cyber Assets and records of annual approvals.

D. Compliance

1. **Compliance Monitoring Process**

1.1. Self Compliance Enforcement
Each Responsible Entity should be responsible for monitoring its own compliance using either internal resources or an appointed external auditor / assessor.

1.2. Compliance Monitoring and Enforcement

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.3. Data Retention

1.3.1. The Responsible Entity should keep documentation required by Standard NCSC CIP-001 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2. The Compliance Enforcement Authority in conjunction with the Responsible Entity should keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1. NCSC and CSSIE to assist and advise on the interpretation and the further development of these standards.

NCSC CIP–001 — Critical Cyber Asset Identification

Appendix A

Critical Cyber Asset Criteria

To avoid adverse impacts on the reliable operation the New Zealand electricity system, the following are considered Critical Assets:

1.1. Each generating site defined by the Asset Operator as critical.

1.2. Each generation facility that the Asset Operator designates to the Generator Owner or Generator Operator as essential.

1.3. Each blackstart resource identified by the Asset Operator's restoration plan.

1.4. The facilities required to operate the blackstart resource to the first interconnection point of the NZ power generation system as identified by the Asset Operator's restoration plan.

1.5. Transmission facilities identified by the Asset Operator as critical.

1.6. Switching stations or substations identified by the Asset Operator as critical.

1.7. Transmission facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in the loss of the assets identified by any Asset Owner.

1.8. Each system or facility that performs automatic load shedding as identified by the Asset Operator as required by the regional load shedding requirements.

1.9. Each control centre or backup control centre used to control generation at plant locations, for any generation facility or group of generation facilities identified in criteria 1.1, 1.3or 1.4 of this appendix.

1.10. Each control centre or backup control centre used to perform the functional obligations of the Asset Operator that includes the control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8 and , 1.9 of this appendix.

Standard NCSC CIP–001 — Critical Asset Identification

Version History

Version	Date	Action	Change Tracking	
1.0	04/12/2013	Approved		CSSIE Group

Standard NCSC CIP–002 — Systems Security Management

A. Introduction

1. **Title:** Systems Security Management

2. **Number:** NCSC CIP-002

3. **Purpose:** Standard NCSC CIP-002 requires Responsible Entities to define methods, processes and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard NCSC CIP-002 should be read in conjunction with Standards NCSC CIP-001 through to NCSC CIP-009.

4. **Applicability:**

   4.1. Within the text of Standard NCSC CIP-002, "Responsible Entity" should mean:

   4.1.1. Asset Owner

   and/or

   4.1.2. Asset Operator.

   4.2. The following are exempt from Standard NCSC CIP-002:

   4.2.1. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters not owned or operated by the Responsible Entity.

B. Requirements

R1. Test Procedures — The Responsible Entity should ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For the purposes of Standard NCSC 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.

R1.1. The Responsible Entity should create, implement and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity should document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity should document test results.

R2. Ports and Services — The Responsible Entity should establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity should enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity should disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity should document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in NCSC CIP-003 Requirement 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 Electronic Security Perimeter(s).

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

R3.2. The Responsible Entity should document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity should document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity should use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter and mitigate the introduction, exposure and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity 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 Responsible Entity should document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity 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.

R5. Account Management — The Responsible Entity should establish, implement and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity should ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "Least Privilege" with respect to work functions performed.

R5.1.1. The Responsible Entity should ensure that user accounts are implemented as approved by designated personnel. Refer to Standard NCSC CIP-003 Requirement R5.

R5.1.2. The Responsible Entity 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.

R5.1.3. The Responsible Entity should review, at least annually, user accounts to verify access privileges are in accordance with Standards NCSC CIP-003 Requirement R5 and NCSC CIP-009 Requirement R4.

R5.2. The Responsible Entity should implement a policy to minimize and manage the scope and acceptable use of administrator, shared and other generic account privileges including factory default accounts.

R5.2.1. 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.

R5.2.2. The Responsible Entity should identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity should have a policy for managing the use of such accounts that limits access to only those with authorization, 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).

R5.3. At a minimum, the Responsible Entity should require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password should be a minimum of six characters.

R5.3.2. Each password should consist of a combination of alpha, numeric and "special" characters.

R5.3.3. Each password should be changed at least annually or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity should ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity should implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls should issue automated or manual alerts for detected cyber security incidents.

R6.3. The Responsible Entity should maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard NCSC CIP-007.

R6.4. The Responsible Entity should retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity should review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity should establish and implement formal methods, processes and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard NCSC CIP-004.

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

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

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

R8. Cyber Vulnerability Assessment — The Responsible Entity should perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment should include, at a minimum, the following:

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 Electronic Security Perimeter 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 Responsible Entity should review and update the documentation specified in Standard NCSC CIP-007 at least annually. Changes resulting from modifications to the systems or controls should be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity should make available documentation and records of its security test procedures, ports and services used, security patch management program, malicious software prevention program, account management program, security status monitoring program, program for the disposal or redeployment of Cyber Assets, annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) and the review and update process.

M2. The Responsible Entity should consider implementation of recommended mitigation strategies developed by external standards agencies (see Appendix A).

D. Compliance

1. Compliance Monitoring Process

1.1. Self Compliance Enforcement
Each Responsible Entity should be responsible for monitoring its own compliance using either internal resources or an appointed external auditor / assessor.

1.2. Compliance Monitoring and Enforcement Processes

- Compliance Audits
- Self-Certifications
- Self Spot Checking
- Self Compliance Violation Investigations
- Self-Reporting
- Complaints

1.3. Data Retention

1.3.1. The Responsible Entity should keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2. The Responsible Entity should retain security-related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard NCSC CIP-007 Requirement R2.

1.3.3. The Compliance Enforcement Authority in conjunction with the Registered Entity should keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1. NCSC and CSSIE to assist and advise on the interpretation and the further development of these standards.

Standard NCSC CIP–002 — Systems Security Management

Appendix A

The document entitled *The Top 4 Strategies to Mitigate Targeted Cyber Intrusions* outlines the most effective security controls an organisation can implement at this point in time based on our current visibility of the cyber threat environment. The Australian Signals Directorate, previously known as the Defence Signals Directorate, assesses that implementing the Top 4 strategies should mitigate at least 85% of the intrusion techniques.

The Top 4 Strategies document provides specific implementation information on the mitigation strategies, including some technical guidance for IT system administrators on planning and implementing the Top 4 Strategies in a typical Windows environment.

The Top 4 Mitigation Strategies document is available through the following link:
http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

Standard NCSC CIP–002 — Systems Security Management

Version History

Version	Date	Action	Change Tracking	
1.0	04/12/2013	Approved		CSSIE Group

Standard NCSC CIP–003 — Security Management Controls

A. Introduction

1. **Title:** Security Management Controls

2. **Number:** NCSC CIP-003

3. **Purpose:** Standard NCSC CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard NCSC CIP-003 should be read in conjunction with Standards NCSC CIP-001 through to NCSC CIP-009.

4. **Applicability:**

   4.1. Within the text of Standard NCSC CIP-003, "Responsible Entity" should mean:

   4.1.1. Asset Owner

   and/or

   4.1.2. Asset Operator.

   4.2. The following are exempt from Standard NCSC CIP-003:

   4.2.1. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters not owned or operated by the Responsible Entity.

B. Requirements

R1. Cyber Security Policy — The Responsible Entity should document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity should, at a minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards NCSC CIP-001 through NCSC CIP-009, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R2. The Responsible Entity should assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, adherence to and annual review of the cyber security policy Standards NCSC CIP-001 through NCSC CIP-009.

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 Standards NCSC CIP-001 through NCSC CIP-009, 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 Responsible Entity's cyber security policy. These exceptions must be documented within thirty days of being authorized, 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. 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. The Responsible Entity should implement and document a programme to identify and protect information associated with Critical Cyber Assets as follows:

R4.1. The Critical Cyber Asset information to be protected should, at a minimum and regardless of media type, include operational procedures; lists as required in Standard NCSC CIP-001; network topology or similar diagrams; floor plans of computing centres that contain Critical Cyber Assets; equipment layouts of Critical 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 Responsible Entity should identify information to be protected under this programme based on the sensitivity of the Critical Cyber Asset information.

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

R5. The Responsible Entity should document and implement a programme for managing personnel access to protected Critical Cyber Asset information as follows:

R5.1. The Responsible Entity should maintain a list of designated personnel who are responsible for authorizing 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 authorizing access.

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

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

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

R6. Change Control and Configuration Management — The Responsible Entity should establish and document a process of change control and configuration management for adding, modifying, replacing or removing Critical 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 Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity should make available documentation of its cyber security policy as specified in all requirements.

D. Compliance

1. **Compliance Monitoring Process**

1.1. Self Compliance Enforcement
Each Responsible Entity should be responsible for monitoring its own compliance using either internal resources or an appointed external auditor / assessor.

1.2. Compliance Monitoring and Enforcement Processes

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.3. Data Retention

1.3.1. The Responsible Entity should keep documentation required by Standard NCSC CIP-003 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2. The Compliance Enforcement Authority and the Responsible Entity should keep the last audit records including all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1. CSSIE and NCSC to assist and advise on the interpretation and the further development of these standards.

Standard NCSC CIP–003 — Security Management Controls

Version History

Version	Date	Action	Change Tracking	
1.0	04/12/2013	Approved		CSSIE Group

Standard NCSC CIP–004 — Electronic Security Perimeter(s)

A. Introduction

1. **Title:** Electronic Security Perimeter(s)

2. **Number:** NCSC CIP-004

3. **Purpose:** Standard NCSC CIP-004 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard NCSC CIP-004 should be read in conjunction with Standards NCSC CIP-001 through NCSC CIP-009.

4. **Applicability:**

   4.1. Within the text of Standard NCSC CIP-004, "Responsible Entity" should mean:

   4.1.1. Asset Owner

   and/or

   4.1.2. Asset Operator.

   4.2. The following are exempt from Standard NCSC CIP-004:

   4.2.1. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters not owned or operated by the responsible entity.

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity should ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity should identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) should include any externally connected communication end point (for example, remote access devices) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a remote accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity should define an Electronic Security Perimeter for that single access point at the remote device.

R1.3. Communication links connecting discrete Electronic Security Perimeters should not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) should be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter should be identified and protected pursuant to the requirements of Standard NCSC CIP-004.

R1.5. The Responsible Entity should maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity should implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

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 Electronic Security Perimeter(s), the Responsible Entity should enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and should document individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity should implement and maintain a procedure for securing remote access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity should implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party.

R2.5. The required documentation should, at least, identify and describe:

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

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard NCSC CIP-009 Requirement R4.

R2.5.4. The controls used to secure remote accessible connections.

R2.6. 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. The Responsible Entity should maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity should implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For remotely accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity should implement and document monitoring process(es) at each access point to the remotely accessible device, where technically feasible.

R3.2. The security monitoring process(es) should detect and alert for attempts at or actual unauthorized accesses, where technically feasible. These alerts should provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity should review or otherwise monitor access logs for attempts at or actual unauthorized accesses at least every sixty calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity should perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment should include, at a minimum, the following:

R4.1. A document identifying 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 Electronic Security Perimeter.

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 Responsible Entity should review, update and maintain all documentation to support compliance with the requirements of Standard NCSC CIP-004.

R5.1. The Responsible Entity should ensure that all documentation required by Standard NCSC CIP-004 reflect current configurations and processes and should review the documents and procedures referenced in Standard NCSC CIP-004 at least annually.

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

R5.3. The Responsible Entity should retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents should be kept in accordance with the requirements of Standard NCSC CIP-007.

C. Measures

M1. The Responsible Entity should make available documentation about the Electronic Security Perimeter(s), the electronic access controls to the Electronic Security Perimeter(s), controls implemented to log and monitor access to the Electronic Security Perimeter(s), documentation of its annual vulnerability assessment, access logs and documentation of review, changes and log retention.

D. Compliance

1. Compliance Monitoring Process

1.1. Self Compliance Enforcement
Each Responsible Entity should be responsible for monitoring its own compliance using either internal resources or an appointed external auditor / assessor.

1.2. Compliance Monitoring and Enforcement Processes

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.3. Data Retention

1.3.1. The Responsible Entity should keep logs for a minimum of ninety calendar days, unless:

e) longer retention is required pursuant to Standard NCSC CIP-007, Requirement R2;

f) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2. The Responsible Entity should keep other documents and records required by Standard NCSC CIP-004 from the previous full calendar year.

1.3.3. The Compliance Enforcement Authority in conjunction with the Registered Entity should keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1. NCSC and CSSIE to assist and advise on the interpretation and the further development of these standards.

Standard NCSC CIP–004 — Electronic Security Perimeter(s)

Version History

Version	Date	Action	Change Tracking	
1.0	04/12/2013	Approved		CSSIE Group

Standard NCSC CIP–005 — Physical Security

A. Introduction

1. **Title:** Physical Security of Critical Cyber Assets

2. **Number:** NCSC CIP-005

3. **Purpose:** Standard NCSC CIP-005 is intended to ensure the implementation of a physical security programme for the protection of Critical Cyber Assets. The requirements detailed in Standard NCSC CIP-005 are the minimum protective physical security requirements. Standard NCSC CIP-005 should be read in conjunction with Standards NCSC CIP-001 through to NCSC CIP-009.

4. **Applicability:**

   4.1. Within the text of Standard NCSC CIP-005, "Responsible Entity" should mean:

   4.1.1. Asset Owner

   and/or

   4.1.2. Asset Operator.

   4.2. The following are exempt from Standard NCSC CIP-005:

   4.2.1. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters not owned or operated by the responsible entity.

B. Requirements

R1. Threat and risk assessment should be conducted and reviewed yearly using the appropriate standards ie. ISO 31000 and HB 167 Security Risk Management.

R2. When selecting suitable locations the Responsible Entity should consider Crime Prevention Through Environmental Design principles 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 Responsible Entity 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 Electronic Security Perimeter should reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity 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 Requirement 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 authorization requests and revocation of access authorization, in accordance with NCSC CIP-004 Requirement R4.

R3.6. A visitor control programme for visitors (personnel without authorized 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 authorize 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 unauthorized physical access.

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 Responsible Entity 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 Responsible Entity should implement one or more of the following physical access methods:

- Card Key: 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.
- 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 the Critical Cyber Assets.
- Dual Authentication should be considered for critical assets.
- Provision and/or procedures should be in place to ensure security in the event of a prolonged power outage.

R7. Monitoring Physical Access — The Responsible Entity should document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts should be reviewed immediately and handled in accordance with the procedures specified in Requirement NCSC 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 authorization. These alarms must provide for immediate notification to personnel responsible for response. Alarm systems should comply with the AS/NZS 2201 set 2008.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R8. Logging Physical Access — Logging should record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity 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:

- Computerized Logging: Electronic logs produced by the Responsible Entity'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 authorized to control and monitor physical access as specified in Requirement R4.

R9. Access Log Retention — The Responsible Entity should retain physical access logs for at least ninety calendar days. Logs related to reportable incidents should be kept in accordance with the requirements of Standard NCSC CIP-007.

R10. Maintenance and Testing — The Responsible Entity should implement a maintenance and testing programme to ensure that all physical security systems under Requirements 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 Responsible Entity in Requirement R8.1.

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

C. Measures

M1. The Physical Security measures are important elements of an appropriate protective security environment, therefore physical security measures must be supported by comprehensive policies and procedures.

M2. The Responsible Entity should make available documentation of the physical security plan, the implementation and review and updating of the plan including methods for monitoring physical access.

D. Compliance

1. **Compliance Monitoring Process**

1.1. Self Compliance Enforcement
Each Responsible Entity should be responsible for monitoring its own compliance using either internal resources or an appointed external auditor / assessor.

1.2. Compliance Monitoring and Enforcement Processes

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.3. Data Retention

1.3.1. The Responsible Entity should keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2. The Compliance Enforcement Authority in conjunction with the Registered Entity should keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1. The Responsible Entity should not make exceptions in its cyber security policy to the creation, documentation or maintenance of a physical security plan.

1.4.2. NCSC and CSSIE to assist and advise on the interpretation and the further development of these standards.

Standard NCSC CIP–005 — Physical Security

Version History

Version	Date	Action	Change Tracking	
1.0	04/12/2013	Approved		CSSIE Group

Standard NCSC CIP–006 — Cyber Security Incident Reporting

A. Introduction

1. **Title:** Incident Reporting

2. **Number:** NCSC CIP-006

3. **Purpose:** Upon identifying a major cyber security incident or breach affecting critical infrastructure, the Responsible Entity (see 4.1) should report the incident to the National Cyber Security Centre (NCSC). 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 asset will not be disclosed beyond the NCSC unless authorised by the Responsible Entity. See also New Zealand Information Security Manual (ref. Chapter 7, Information Security Incidents).

4. **Applicability:**

   4.1. Within the text of Standard NCSC CIP-006, "Responsible Entity" should mean:

   4.1.1. Asset Owner

   and/or

   4.1.2. Asset Operator.

B. Requirements

Each Responsible Entity to whom this standard is applicable should:

R1. Have procedures to ensure operating personnel are aware of, and able to recognise, major cyber security incident events.

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

- Attempts to gain unauthorised access to a computer system or its information;
- Unwanted disruption or denial of service;
- Unauthorised use of a system for processing or storing information;
- 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. Incidents can have wide or significant detrimental implications for national interests.

R2. Provide its operating personnel with cyber security incident response and reporting procedures or guidelines. See also Standard NCSC CIP-007.

R2.1. The Responsible Entity should detail cyber security incident responsibilities and procedures for each system in the relevant standard operating procedures.

R2.1.1. The Responsible Entity should document 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.

R3. Have procedures for the communication of information concerning cyber security incident events to appropriate parties operating within the interconnected systems of the infrastructure asset.

R3.1. The Responsible Entity should have procedures, if an event is assessed to be a major cyber security incident, to report immediately to the National Cyber Security Centre (NCSC) and/or where relevant, New Zealand Police. All incident reports provided to the NCSC (see Appendix A) will be treated in the strictest confidence.

C. Measures

M1. Each Responsible Entity should have and provide upon request procedures or guidelines (either electronic or hard copy) and relevant information relating to the implementation of these procedures and guidelines.

D. Compliance

1. **Compliance Monitoring Process**

1.1. Self Compliance Enforcement

1.1.1. Each Responsible Entity should be responsible for monitoring its own compliance with the Requirements (Section B) and Measures (Section C) using either internal resources or an appointed external auditor / assessor – known as the Compliance Monitor.

1.1.2. NCSC and CSSIE to assist and advise on the interpretation and further development of these standards.

1.2. Compliance Monitoring and Enforcement Processes

One or more of the following methods should be used to verify compliance:

1.2.1. Self-certification.

1.2.2. Spot Check Audits (conducted anytime by the Responsible Entity using internal resources or an appointed external auditor / assessor).

1.2.3. Periodic Audit (conducted on a scheduled basis every three years by the Responsible Entity using either internal resources or an appointed external auditor / assessor).

1.2.4. Triggered investigations following a major breach or system event.

1.2.5. A review after twelve months following a triggered investigation (1.2.5).

1.3. Recording Cyber Security Incidents

1.3.1. Evidence used as part of a triggered investigation should be retained by the Responsible Entity for one year from the date that the investigation is closed or as determined by the Compliance Monitor. The Compliance Monitor should retain the most recent periodic audit report and all requested and submitted subsequent compliance records.

1.3.2. Each Responsible Entity should retain up-to-date documents as evidence of compliance with the Requirements and Measures outlined in NCSC CIP-006. If a Responsible Entity is found to be non-compliant with any one of the Requirements or Measures, it should record the steps taken to address this situation, retaining this information until found compliant or for two years, whichever is longer.
(See Appendix A)

Standard NCSC CIP–006 — Reporting Cyber Security Incidents

Appendix A

Reporting cyber security incidents to NCSC

Reporting cyber security incidents helps NCSC to develop a threat environment picture for government systems and Critical National Infrastructure (CNI) and assist 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. The NCSC provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.

Reporting cyber security incidents to NCSC through the appropriate communication channels ensures that appropriate and timely assistance can be provided.

If you are a government organisation or Critical National Infrastructure organisation and you have encountered or suspect a cyber threat, please contact NCSC and/or download, complete and return an Incident Reporting Form from www.ncsc.govt.nz

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

Recording cyber security incidents

The purpose of recording cyber security incidents in a register is to identify the nature and frequency so that mitigation actions can be taken.

- The Responsible Entity should ensure that all cyber security incidents are recorded in a register.
- The Responsible Entity should include, at the minimum, the following information in its 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,
  - The file reference.

The Responsible Entity should use their register as a reference for future security risk assessments.

Outsourcing and cyber security incidents

When a Responsible Entity outsources information technology services and functions, they are still responsible for the reporting of cyber security incidents. The Responsible Entity must ensure that the service provider informs it of all cyber security incidents to allow it to formally report to NCSC and /or where relevant, NZ Police.

Responsible Entities that outsource their information technology services and functions must ensure that the services provider consults with the Responsible Entity when a cyber security incident occurs.

Standard NCSC CIP–006 — Cyber Security Incident Reporting

Version History

Version	Date	Action	Change Tracking	
1.0	04/12/2013	Approved		CSSIE Group

Standard NCSC CIP–007 — Incident Response Planning

A. Introduction

1. **Title:** Incident Reporting and Response Planning

2. **Number:** NCSC CIP-007

3. **Purpose:** Standard NCSC CIP-007 ensures the identification, classification, response and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard NCSC CIP-007 should be read in conjunction with Standards NCSC CIP-001 through to NCSC CIP-009 (see Appendix A for more information on managing incidents).

4. **Applicability:**

   4.1. Within the text of Standard NCSC CIP-007, "Responsible Entity" should mean:

      4.1.1. Asset Owner

      and/or

      4.1.2. Asset Operator.

   4.2. No-one should be exempt from Standard NCSC CIP-007.

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity 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:

R1.1. Procedures to characterize and classify events as reportable cyber security incidents.

R1.2. Response actions, including roles and responsibilities of cyber security incident response teams, cyber security incident handling procedures and communication plans.

R1.3. A process for reporting cyber security incidents to the NCSC. The Responsible Entity should ensure that all reportable cyber security incidents as defined in NCSC CIP-007 R1.1 are reported to the NCSC either directly or through an intermediary.

R1.4. A process for updating the Cyber Security Incident Response Plan within thirty calendar days of any changes.

R1.5. A process for ensuring that the Cyber Security Incident Response Plan is reviewed at least annually.

R1.6. 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, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity should keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity should make available all documentation relating to its Cyber Security Incident Response Plan including details of the review and updating process, testing of the plan and test records.

D. Compliance

1. Compliance Monitoring Process

1.1. Self Compliance Enforcement

Each Responsible Entity should be responsible for monitoring its own compliance using either internal resources or an appointed external auditor / assessor.

1.2. Compliance Monitoring and Enforcement Processes

- Compliance Audits
- Self-Certifications
- Self Spot Checking
- Self Compliance Violation Investigations
- Self-Reporting
- Complaints

1.3. Data Retention

1.3.1. The Responsible Entity should keep documentation, other than that required for reportable Cyber Security Incidents for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2. The Compliance Enforcement Authority in conjunction with the Registered Entity should keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1. The Responsible Entity should not make exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.4.2. The Responsible Entity should not make exception in its cyber security policies to reporting Cyber Security Incidents to the NCSC.

1.4.3. NCSC and CSSIE to assist and advise on the interpretation and the further development of these standards.

Standard NCSC CIP–007 — Incident Response Planning

Appendix A

Managing Cyber Security Incidents

The New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs), provides detailed information on best practices and basic frameworks for NZ government and CNI organisations when establishing or reinforcing existing incident management and response capabilities.

The New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs) is available from the following link:
http://www.ncsc.govt.nz/resources.html

Standard NCSC CIP–007 — Incident Response Planning

Version History

Version	Date	Action	Change Tracking	
1.0	04/12/2013	Approved		CSSIE Group

Standard NCSC CIP–008 — Recovery Plans for Critical Cyber Assets

A. Introduction

1. **Title:** Recovery Plans for Critical Cyber Assets

2. **Number:** NCSC CIP-008

3. **Purpose:** Standard NCSC CIP-008 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard NCSC CIP-008 should be read in conjunction with Standards NCSC CIP-001 through to NCSC CIP-009.

4. **Applicability:**

   4.1. Within the text of Standard NCSC CIP-008, "Responsible Entity" should mean:

      4.1.1. Asset Owner

      and/or

      4.1.2. Asset Operator.

   4.2. The following are exempt from Standard NCSC CIP-008:

      4.2.1. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters not owned or operated by the Responsible Entity.

B. Requirements

R1. Recovery Plans — The Responsible Entity should create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) should address, at a minimum, the following:

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

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

R2. Exercises — The recovery plan(s) should be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) 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.

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

C. Measures

M1. The Responsible Entity should make available all documentation of its recovery plan(s), records documenting required exercises, changes to the recovery plan(s), backup and storage of information and testing of backup media.

D. Compliance

1. **Compliance Monitoring Process**

1.1. Self Compliance Enforcement

Each Responsible Entity should be responsible for monitoring its own compliance using either internal resources or an appointed external auditor / assessor.

1.2. Compliance Monitoring and Enforcement Processes

- Compliance Audits
- Self-Certifications
- Self Spot Checking
- Self Compliance Violation Investigations
- Self-Reporting
- Complaints

1.3. Data Retention

1.3.1. The Responsible Entity should keep documentation required by Standard NCSC CIP-008 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2. The Compliance Enforcement Authority in conjunction with the Responsible Entity should keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1. NCSC and CSSIE to assist and advise on the interpretation and the further development of these standards.

Standard NCSC CIP–008 — Recovery Plans for Critical Cyber Assets

Version History

Version	Date	Action	Change Tracking	
1.0	04/12/2013	Approved		CSSIE Group

Standard NCSC CIP–009 — Personnel and Training

A. Introduction

1. **Title:** Personnel & Training

2. **Number:** NCSC CIP-009

3. **Purpose:** Standard NCSC CIP-009 requires that personnel having authorized cyber or authorised unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training and security awareness. Standard NCSC CIP-009 should be read in conjunction with Standards NCSC CIP-001 through to NCSC CIP-008.

4. **Applicability:**

   4.1. Within the text of Standard NCSC CIP-009, "Responsible Entity" should mean:

   4.1.1. Asset Owner

   and/or

   4.1.2. Asset Operator.

   4.2. The following are exempt from Standard NCSC CIP-009:

   4.2.1. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters not owned or operated by the responsible entity.

B. Requirements

R1. The Responsible Entity should establish, document, implement and maintain a security awareness programme to ensure personnel having authorized cyber or authorized unescorted physical access to Critical 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:

- 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 Responsible Entity should establish, document, implement and maintain an annual cyber security training programme for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training programme should be reviewed annually, at a minimum, and should be updated whenever necessary.

R2.1. This programme should ensure that all personnel having access to Critical 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 Critical Cyber Assets covered by NZ NCSC CIP-009, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

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

R2.2.3. The proper handling of Critical Cyber Asset information; and

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

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

R3. The Responsible Entity should have a documented personnel risk assessment programme for personnel having authorized cyber or authorized unescorted physical access to Critical 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 Critical Cyber Assets.

The personnel risk assessment programme should, at a minimum, include:

R3.1. Positive identity verification and if appropriate, a criminal background check.

R4. The Responsible Entity should maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity should review the list(s) of its personnel who have such access to Critical Cyber Assets annually and should ensure the list is properly maintained.

R4.2. The Responsible Entity should revoke access to Critical Cyber Assets as soon as possible within 24 hours for those personnel, contractors and service vendors whose services have been terminated.

C. Measures

M1. The Responsible Entity should make available documentation of its security awareness and reinforcement programme, cyber security training programme, review, personnel risk assessment programme and access revocation documentation.

D. Compliance

1. **Compliance Monitoring Process**

1.1. Self Compliance Enforcement
Each Responsible Entity should be responsible for monitoring its own compliance using either internal resources or an appointed external auditor / assessor.

1.2. Compliance Monitoring and Enforcement Processes

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.3. Data Retention

1.3.1. The Responsible Entity should keep documentation required by Standard NCSC CIP-009 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2. The Compliance Enforcement Authority in conjunction with the Responsible Entity should keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1. NCSC and CSSIE to assist and advise on the interpretation and the further development of these standards.

Standard NCSC CIP–009 — Personnel and Training

Version History

Version	Date	Action	Change Tracking	
1.0	04/12/2013	Approved		CSSIE Group

Resources and References

New Zealand Guidance

- New Zealand's Cyber Security Strategy, June 2011
  http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf
- New Zealand Information Security Manual (NZISM) v 1.01, June 2011
  http://www.gcsb.govt.nz/newsroom/nzism/NZISM_2011_Version_1.01.pdf
- New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)
  http://www.ncsc.govt.nz/resources
- Security in the Government Sector
  http://www.security.govt.nz/publications/security-in-the-government-sector/

The following websites offer additional information about organisations involved in the security of government and national critical infrastructure systems:

- http://www.gcsb.govt.nz
- http://www.nzsis.govt.nz
- http://www.police.govt.nz
- http://www.mfat.govt.nz
- http://www.dia.govt.nz
- http://www.e.govt.nz
- http://www.standards.govt.nz
- http://www.privacy.org.nz
- http://www.dpmc.govt.nz
- http://www.auditnz.govt.nz
- http://www.oag.govt.nz
- http://www.justice.govt.nz

High-level information relating to physical security is also contained in:
Protective Security Manual (PSM), and ISO/IEC 27002:2013.