A COMPARISON OF AUSTRALIA AND THE U.S ELECTRICAL INFRASTRUCTURE CYBER SECURITY STRATEGIES

Deo Gahiza, Pavol Zavarsky, Dale Lindskog, Ron Ruhl.
Department of Information Systems Security Management
Concordia University College of Alberta, Edmonton, Canada
dgahiza@student.concordia.ab.ca, {pavol.zavarsky, dale.lindskog, ron.ruhl} @ concordia.ab.ca
http://infosec.concordia.ab.ca

Abstract - **This study compares the protection of Electrical Infrastructure (EI) in Cyber Security Strategies (CSS) of the United States (U.S) and Australia. Employing three key indicators as interpretive frameworks – (I) Standards and guidelines, (II) policies and (III) security controls, this study takes on a risk-based approach using NIST Risk Management Framework (RMF) and Federal Information Processing Standards 200 (FIPS 200) as baselines. Drawing on secondary data, this study summarizes similarities and differences, and also identifies gaps in these two countries' CSS. The findings of this study may be relevant in the development of a checklist of security control areas for EI with potential use by countries that are yet to, or considering the development of, CSS for their EI or other key cyber critical infrastructure.**

Keywords – Cyber Security, CSS, EI, FIPS 200, NIST SP800-53A Controls, Frameworks, Electrical and Critical Infrastructure

I INTRODUCTION

In this age of wide scale digitization, cyber security has become a major concern for the protection of critical infrastructure. This has received considerable attention in recent years, especially after the known success of attacks carried out recently against U.S EI in 2009 by Chinese cyber spies, who left behind software programs that could be used to disrupt systems [19]. These attacks stroke directly on electricity grid in the U.S, which is an important part of EI. Having said this, providing security for this critical infrastructure is crucial, and having countermeasures in place to address these cyber security concerns about the Electrical Infrastructure cannot be overemphasized.

For the purpose of this paper, CSS will not only be defined as defense countermeasures (such as, but not limited to, standards, guidelines and security controls) to mitigate risks and attacks against cyber critical systems which support the functionality, reliability or operability of the EI, but also the prevention and detection of cyber threats. In other words, it is important that all three indicative security requirements are blended to have a comprehensive and robust CSS, with focus on prevention and detection which will mitigate the likelihood of harm.

Focusing on the prevention and detection of threats to cyber critical systems, this study compares and analyzes security strategies of the USA and Australia based on review of publicly available documents regarding cyber security protection, including risk mitigation techniques and protective measures which address security issues to EI, its control systems and distributed information networks.

A review of relevant documentation relating to security protection is necessary when addressing cyber security issues in the EI. Furthermore, the CSS presented in this study from both countries are based strictly on public available documents comprising of risk mitigation techniques and protective measures to EI. Table 1 below outlines key documents identified, which are used by both U.S and Australia in their CSS with regards to the protection of critical infrastructure.

TABLE .1 CRITICAL INFRASTRUCTURE CYBER SECURITY STRATEGIES

U.S.	Australia
NIST FIPS 200	Information Security Manual (AUS ISM)
NIST SP 800-53A	Critical Infrastructure Resilience Strategy
NERC CIP 002-009 Reliability Standard	Cyber Security Strategy
NIST Risk Management Framework	Information Security Core Policy
ISO/IEC 27002	AS/NZS ISO/IEC 27002:2005

The above mentioned documents are important standards and security guidelines used to address security issues in the protection of critical infrastructure. However, the scope of this study specifically targets security strategies for the protection of EI. Recognized internationally for its role in promoting innovative and industrial competitiveness, the U.S National Institute of Standards and Technology (NIST) helps all sectors, industries, and organizations enhance a strong security platform by developing standards and technology [23]. Notwithstanding, the NIST standards and guidelines documents (The NIST RMF; NIST SP 800-53A; and FIPS 200 standards) identified, are also part of the U.S CSS, but are not directly mandatory guidelines in U.S. EI as the CIP standards. Rather, they are general guidelines, standards, and recommendations that are widely accepted and used to promote critical infrastructure security resiliency. Hence, this study uses these documents in the comparison analysis to serve not only as baseline, but also as benchmark to examine and compare protective measures and mitigation techniques in the CSS of both U.S and Australia.

The protective measures and risk mitigation techniques identified in each of these countries' CSS are framed in the context of risk management, which is key element to an organization's security program. Moreover, an effective risk management framework helps organizations select appropriate controls necessary to protect people, operations and assets [18]. Having mentioned this, two documents, NIST RMF and FIPS 200, are employed in this study as a baseline for comparing the CSS in EI.

The NIST RMF establishes six - stages of methodology, with comparison being conducted at each stage of the framework. These are: (I) Categorization; (II) Selection; (III) Implementation; (IV) Assessment; (V) Authorization; and (VI) Monitoring showing similar and non-similar features in each country's CSS based on secondary data. The advantage of using the NIST RMF is that the output at various stages of the framework allows similar level comparisons for both countries. Furthermore, since the NIST RMF has been widely accepted and utilized worldwide by many sectors, using this framework in conjunction with the NIST FIPS 200 and NIST SP 800-53A *Recommended Security Controls* asserts that a risk-based approach to security selection and specification considers effectiveness and efficiency in comparing the two countries' CSS [18, 27].

Besides using the NIST RMF for similar level comparison, it is important to select the appropriate set of security controls to adequately mitigate risk while meeting the minimum security requirements of an organization. This process demonstrates an organization's commitment to security and the due diligence it exercises in protecting the Confidentiality, Integrity, and Availability (CIA) of organizational information and Information Systems [18]. The minimum security requirements are highlighted in FIPS 200 [26].

This paper uses NIST FIPS 200 as benchmark for comparison and categorization, because it is considered an internationally accepted standard which specifies minimum security requirements for Information System security. In addition FIPS 200 covers eighteen security-related areas with regards to the protection of Information Systems. This standard also promotes the development, implementation and operation of more secure Information Systems representing a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting Information Systems. Subsequent to using FIPS 200 for the security categorization process, selecting appropriate security controls necessary to satisfy the requirements set forth in the FIPS 200 standard is important [27].

However, in order to satisfy the minimum security requirement highlighted in FIPS 200, NIST SP 800-53A *Recommended Security Control* is used as a security baseline to compare standards, controls and identify gaps from (NERC CIP 002-009, ISO 27002, and AUS ISM controls) found in both the U.S and Australian CSS. Using NIST SP 800-53A provides a consistent, comparable and repeatable approach for selecting and specifying security controls, while at the same time, satisfying the breadth and depth of security requirements for Information Systems in the EI [26]. To clarify, the comparison carried out in this study will focus on the management and operational classes stipulated in NIST SP 800-53A, which applies to cyber security protection and management in the EI of both the U.S and Australia.

In the U.S, the North American Electric Reliability Council (NERC) caters solely to the EI, with its mandate to ensure reliability of the bulk power system. In addition, the NERC develops and enforce reliability standards and guidelines with focus on cyber security protection [1]. Since the twenty-first century, NERC has put forth consistent efforts in protecting cyber critical infrastructure in the energy industry by developing a number of cyber security standards and guidelines which address security issues in the EI. Examples of such standards are: the NERC 1200, replaced quite recently by the NERC 1300 [13]. However, this NERC 1300 is further broken into eight (8) separate standards called Critical Infrastructure Protection (CIP) ranging from CIP002 to CIP009. This standard establishes a set of baseline security requirements to implement and maintain a cyber security program and to protect cyber assets critical to reliable bulk electric system operation.

On the other side of the Pacific Ocean, the Australian Government has been aware of the great challenge that cyber security poses. A series of country-wide efforts have been made to ensure a healthy operational environment for national critical infrastructure. Among those, are the Critical Infrastructure Resilience Strategy (CIRS), Cyber Security Strategy, and Australian Government Information Security Core Policy (ISCP). The ISCP establishes the minimal requirements for all organizations based on three elements of Information Security (the CIA triad) [12, 24]. In addition to the already mentioned documents, the Information Security Manual (AUS ISM) was recently published and released by the Australian Government Department of Defence. All of these documents provide a framework for companies setting up their security controls to manage risk to critical Infrastructures, which Australia's EI is subject to as well [14]. Unlike the compliance requirement of AUS ISM, there is not a mandatory enforcement on AS/NZS ISO/IEC 27002:2005 standards in Australia; rather, it serves as recommendations to develop security management practice for agencies in all sectors [28].

While both countries seem to address cyber security concerns to EI in their respective CSS, their methods and approach are not quite the same? In view of this, the comparison of the two strategies can help identify the commonalities and distinctions in both countries' approach to securing EI. Furthermore, the findings and results of this study can contribute to selecting the appropriate cyber security countermeasures for other countries to follow when establishing their own CSS for their EI. Also, this paper will put forward a checklist based on the findings which could potentially be used by other countries and organizations worldwide in order to identify critical areas for selecting security controls when creating a comprehensive cyber security framework.

II METHODOLOGY

This study relied on secondary data obtained from two major sources. In order to capture essential comparative elements of CSS in the protection of EI in both the U.S and Australia, this study employed NIST RMF and FIPS 200 as baselines. As the NIST clearly states "the Risk Management Framework provides a structured process and information to help organizations identify the risks to their Information Systems, assess the risks, and take steps to reduce risks to an acceptable level". Similarly, the FIPS 200 document provides the minimum security requirements for federal information and Information Systems. Combining information from both documents allowed for a fair comparison of EI CSS in both countries based on standards and guidelines, policies, and security controls existent (or non-existent) in these countries. As the risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, or regulations, this study:

(i) Compared these two countries EI CSS following the RMF six (6) stage process. Using these processes as reference points, each country's CSS is validated against each step;
(ii) Identifies gaps if any based on the steps above, for each country;
(iii) Compared results from these countries' EI CSS against information from the baseline documents to create what could be an initial step in the development of a checklist for EI CSS in any country planning to move in this direction.

As this method, allows for the pulling of important information which would permit similar level comparisons at various stages of the framework, a description of these stages is provided as follows.

The first stage of the NIST RMF is Categorization. This stage groups specific security requirements for the protection of cyber systems that supports the reliability and functionality of the EI. Following the NIST FIPS 200 standard, agencies are require to categorize their Information Systems based on potential impact levels (low, moderate, or high) to address the security of EI and its control systems CIA [28]. Prior to the grouping of the minimum security requirements and the selection of the appropriate security controls for Information Systems, the determination of how much security is enough for Information Systems base on impact must be addressed. Having said that, the minimum security requirements outlined in FIPS 200 will serve as a benchmark for selecting controls. Accordingly, security requirement for cyber assets will be grouped into the following categories:

TABLE .2 NIST FIPS 200 SECURITY CONTROLS

1. Access Control	10. Media Protection
2. Awareness and Training	11. Physical and Environmental Protection
3. Auditing and Accountability	12. Planning
4. Certification, Accreditation, and Security Assessments	13. Personnel Security
5. Configuration Management	14. Risk Assessment
6. Contingency Planning	15. System Service Acquisition
7. Identification and Authentication	16. System and Communications Protection
8. Incident Response	17. System and Information Integrity
9. Maintenance	18. Program Management

The Categorizing process is critical for two reasons. It is the initial stage in the comparison process of both countries and it implements a comprehensive risk based approach for addressing risk to cyber Information Systems and groups of specific cyber security requirements.

Developing CSS is like driving a bus. The first stage points out a direction for the bus to go. The following two stages turn the ignition and push the gas paddle to get the bus moving.

The second stage of the NIST RMF is the Selection stage. The purpose of this stage is to set up a security baseline and then to tailor and select controls to meet it [16]. The Selection stage is based on the security categories divided by FIPS 200 and using NIST SP 800-53A *Recommended Security Controls* as the security baselines. This stage will map the two countries' existing standards and security controls and identify gaps made in the selection of controls to meet minimum cyber security requirements identified in the categorization.

In each security category, a table is deployed to reflect similarities and differences existing in the U.S and Australia. The first left column list a set of recommended security requirements use as baseline. Corresponding findings from each country are listed on the right. For instance gaps exist when neither the U.S nor Australia seems to have similar controls that map against the baseline. A total summary and important outcome will be provided in the "Comments" Column on the right.

TABLE. 3 SECURITY CATEGORY

NIST baseline controls	US Standards and Controls	AUS Controls	Comments

The third stage of RMF is Implementation. This stage addresses and compares the efforts the U.S and Australia have made to ensure required controls are implemented to protect their EI. In order to implement CSS, both countries have a series of plans, schedules and guidelines for industry to follow. Those efforts will be identified and compared in this stage.

Stages four to six provide assurance that the bus will not deviate from its selected route. Once rules are settled, one of the vital processes is to evaluate whether they are appropriate and accurate. Stage four, the Assessment stage, will measure whether required controls are in place. Who are the responsible entities evaluating and what are the outcomes from each country's assessment? Stage five, the Authorization stage, designates the authoritative entity for security operations. This stage compares different American and Australian authorities, which have power to approve changes and to implement standards and controls for risk mitigation in terms of critical infrastructure protection. The six and final stage of the NIST RMF is Monitoring. This stage addresses the enforcement programs such as auditing and compliance by comparing the monitoring efforts the US and Australia have made to ensure the compliance of all implemented security requirements and controls.

III COMPARISON

This study examines the contents of all six stages of NIST RMF. The first stage Categorization employs NIST SP FIPS 200 as a benchmark to specifically group minimum security requirements for cyber assets and will not be completed. Comparison will occur through the next five stages (Selection, Implementation, Assessment, Authorization, and Monitoring). This framework allows us to compare both countries.

3.1 Selection

After grouping cyber assets into different categories and identifying the critical areas in need of protection, minimum security controls must be selected in order to mitigate risks and to meet the security requirements stipulated.

In the U.S, NERC CIP standards are mandatory for EI protection. "The purpose of the NERC CIP standards is to ensure that all of the affected electric utilities which are responsible for the consistent and continued reliability of the US' electrical grid are properly protecting their critical cyber assets. As with most standards, the NERC CIP standard establishes the minimum requirements necessary to protect those critical cyber assets along with the exchange of any information" [22]. The standards address the security controls comparable to the requirements in the NIST SP 800-53A *Recommended Security Controls*. Also, because ISO 27002:2005 clearly defines the effective security areas and controls necessary to meet most regulatory compliance and most specifically the NERC CIP standards, it is well-accepted by energy and utilities companies [15]. The mapping between NERC CIP standards and ISO 27002 is shown as Figure 1 below [22].

In the case of Australia the EI does not have its own agency that develops security standards, guidelines and policies as NERC does for the U.S. All departments are subject to the Australian Government Information Security Manual (AUS-ISM). The purpose of this manual is to apply a risk management approach to the protection of Information Systems. Also, applying the security measures and procedures described will ensure companies/ organizations have effective information security governance arrangements [14]. It defines controls on information operations based on degrees of necessity.

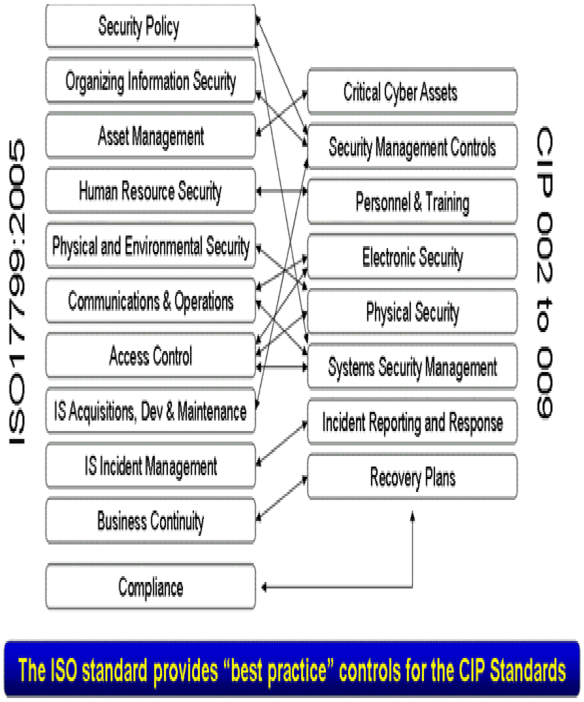
ISO17799:2005
Security Policy
Organizing Information Security
Asset Management
Human Resource Security
Physical and Environmental Security
Communications & Operations
Access Control
IS Acquisitions, Dev & Maintenance
IS Incident Management
Business Continuity
Compliance
Critical Cyber Assets
Security Management Controls
Personnel & Training
Electronic Security
Physical Security
Systems Security Management
Incident Reporting and Response
Recovery Plans
CIP 002 to 009
The ISO standard provides "best practice" controls for the CIP Standards

Figure 1

Since NIST 800-53A recommends that controls highly satisfy the minimum security requirements of FIPS200, the example below uses NIST 800-53A as a baseline to compare US NERC CIP standards and their associated security controls from ISO 27002 and controls from the AUS ISM. Gaps and analysis results will be provided in the “Comments” column. See the appendices section for the whole table.

TABLE.4 ACCESS CONTROLS

SP 800-53A Control	CIP Req #	US ISO 27002 controls	AUS IS Controls	Comments
AC-1 Access Control Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R5.3, CIP003-R5.1	5.1.1, 5.1.2, 11, 11.2,	Identification and Authentication 0413	

The 18 key areas of the NIST 800-53A *Recommended Security Controls* were used to set up a baseline for the comparison between the U.S NERC CIP standards and AUS ISM security controls. Of the 151 subset security controls compared, only 74 of them can be found in both the U.S NERC CIP standards and the AUS ISM. There were 77 items identified in the NIST 800-53A in which neither the U.S NERC CIP nor the AUS ISM had selected controls [27].

Results from the comparison show gaps in security controls selection in both countries. For instance, regarding Access Controls Security selection, both the U.S and Australia abide by the NIST 800-53A security requirements, but Australia seems to have a more comprehensive control on logging requirements, access enforcement and control session. In the Training and Awareness section, both countries seem to address these issues evenly.

In the Audit and Accountability section, Australia, unlike the U.S does not have any monitoring and reporting mechanism in place for audit activities; however, both the U.S and Australia fail to address audit storage and non-repudiation, both of which are very important to ensure accountability. A more complete detail of the comparison results is presented in the appendices section.

It is clear that the U.S and Australia have different areas of focuses when selecting controls. Differences also exist in the implementation stage.

3.2 Implementation

The U.S uses the NERC Cyber Security Standards CIP-002-009 to ensure that all stakeholders responsible for the reliability of bulk electric system in North America identify and protect cyber assets that could potentially impact the reliability of services. Furthermore, the implementation of these security standards for security controls is subject to a plan and a schedule which provides time for responsible stakeholders to examine their policies and processes to put together documentation and to meet the requirements needed [6].

The Australian Government Information Security Manual (AUS ISM) provides a “Rationale” section to explain to companies what to do [14]. However, there is nothing stipulated about an implementation schedule and compliance deadline. To add further, the manual serves for the general purpose of cyber security in all sectors. It is not specific to the EI. Related standards, guidelines, schedules and plans are either classified or not in place. If the second alternative is true, each company operates on its own. It is a very time-consuming and costly task to comply with the Australian Government’s requirements and also suit the industry’s needs. In the end, due to this diverse distinction between companies’ processes of implementing security controls, Australian IT auditors are prone to face more challenges than their American counterparts.

3.3 Assessment

Appropriate evaluation is an important technique in ensuring selected controls are implemented properly.

CIP standards, used in the U.S are mandatory Reliability Standards that are codified in the Federal Energy Regulatory Commission (FERC) regulations and are enforceable against all users, owners and operators of the bulk-power system. Each individual CIP standard also includes a "MEASURE" section for responsible personnel to evaluate whether all critical requirements from a standard is met. For example, CIP002 requires personnel to measure the following areas [6, 20]:

(i) The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.
(ii) The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.
(iii) The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.
(iv) The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

The Australian Government’s released measurement criteria in its Critical Infrastructure Resilience Strategy (CIRS) [7], includes effective engagement, government support, collaboration, investment resilient, positive relationship and awareness and training. However, the criteria only highlight the critical areas to evaluate. Where it pertains to the EI, a more detailed matrix for benchmarking is required. Currently this information is either classified or not in place.

3.4 Authorization

Besides choosing, implementing, and assessing appropriate controls, another very challenging problem for cyber security risk control is Authorization. Who is responsible for the critical cyber assets? Who has the authority to authorize mitigation controls over Information system operation based upon assessment of risk to the EI and its cyber assets? This section identifies the responsible parties and personnel in both US and Australia in terms of cyber security control of the EI.

In the U.S, the NERC CIP Standards emphasize the differing roles of management and decision making authorities to the operation of the Bulk Electric System, the criticality and vulnerability of cyber assets and the risks to which they are exposed [2, 6]. Accordingly, NERC defines the term of "Responsible Entity" in a more distributed manner. Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC and Regional Entity are all involved and share a part of the duties [6, 20].

For example, CIP-002-3 highlights that a senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology. This multiple authorizing mechanism ensures that not all responsibilities fall on one shoulder. It also minimizes single-point-of-failure, and increases possibilities of security breaches being found [6].

In Australia, the Information Security Core Policy requires that agency heads have the final authority and responsibility to ensure that controls are in place and being implemented [12]. However, information regarding authority distribution is not available.

3.5 Monitoring

In risk control management, monitoring is a vital process to ensure outcomes will not deviate. Therefore, enforcement programs, auditing and compliance need to be in place to supervise security control development.

In the U.S, the NERC Compliance Monitoring and Enforcement Program (CMEP) is developed under Section 215(c) of the Federal Power Act1 to establish and enforce Reliability Standards for the bulk power system, subject to review by the Federal Energy Regulatory Commission (FERC) and in the general accordance with the "Principles for an Electric Reliability Organization that can Function on an International Basis" [25]. The CMEP is designed to improve reliability through the effective and efficient enforcement of reliability standards. The compliance monitoring and enforcement process entails: compliance Audits, Self-Certifications, Spot Checking, Compliance Violation investigations, Self-Reporting and Complaints

NERC under its mandate has delegated authority to monitor and enforce compliance with reliability standards of owners, operators and users of the bulk power system to qualified regional entities. This delegation is governed by delegation agreements that have been approved by the appropriate regulatory authorities. These regional entities, under NERC's oversight, are responsible for carrying out the CMEP within their respective regions [21, 25].

Unlike the U.S, Australian auditing and compliance mechanisms have not yet been released. The Australian government created the strategy without telling companies and utilities how to achieve the goal. Tax payers expect to see more efforts by the government in this area. The industry needs more guidance and standards to ensure cyber assets are securely guarded.

IV FINDINGS AND RECOMMENDATIONS

Findings

The findings of this research study have shown differences and similarities in the U.S and Australia EI CSS.

Both of these countries have their own sets of controls corresponding to security baselines. Through the comparison explained previously, it was determined that each country's controls consist of required minimum security controls which need to be in place. Access Control, Certification, Accreditation, Security Assessment and Risk Assessment are the areas in which both the U.S and Australia have the most in common with the NIST SP 800-53A security baseline.

However, distinctions do exist in each stage of the framework. There were significant gaps found in both the U.S NERC CIP-002-009 security controls and the AUS ISM security controls when compared to the baseline NIST 800-53A *Recommended Security Controls.*

Using the NIST SP 800-53A *Recommended Security Controls* as a baseline to compare how the U.S and Australia select security controls it becomes clear that the two countries have significant differences. The U.S, being the country with an already established council – NERC - which provides cyber security guidance for the EI through its CIP standards and guidelines, was found to be lacking key areas identified by the NIST SP 800-53A in its security controls. A typical example is the gap identified in the "System and Services Acquisition", which also applies to Australia. Another big gap was identified in the "System and Communications Protection" controls. Analyzing the controls specified in this section, it was found that, out of the 23 security controls highlighted by NIST 800-53A, only 6 areas were addressed by both CIP and AUS-ISM as they failed to address technical and operational details. Another significant finding was identified in the "Program Management" controls section, where both the U.S CIP standard and AUS ISM failed to enforce project management techniques to their security management process. Instead, they divide security management into a series of individual units. These examples point out the need for both countries, and their respective guidelines, especially the U.S' NERC CIP-002-009, to update its security controls. Another significant finding was that both the U.S and Australia have made tremendous efforts to implement, evaluate, and authorize selected controls.

In this area, there is a big difference between the U.S and Australia. In the U.S, the CIP standards stipulate that implementation of security controls are subjected to a plan and schedule. Unlike the U.S, the Australians do not address this in their security requirements. Also, in both the "Assessment" and "Authorization" stages of the RMF, it is seen clearly that the U.S is in a better position than their Australian counterparts. The U.S CIP standard outlines measures to evaluate whether all critical requirements are met and proper authority is delegated to the rightful individual. Australia's CIRS and ISCP, however, only highlight critical areas to evaluate, mentioning nothing about authority distribution.

In addition to the differences identified in CSS already mentioned, it was also found that the U.S EI through the NERC mandate has delegated authority to monitor and enforce compliance to CIP standards, while Australia is yet to release its compliance enforcement mechanism specifically for the EI.

To further augment the findings, the U.S seems to have a well-defined set of strategies to improve cyber security in the EI. NERC was established to create standards, guidelines and procedures for the electricity industry. Most requirements in the NERC CIP standards correspond to the NIST SP 800-53A security baseline controls. ISO 27002:2005, an effective tool, has been adopted for the CIP standards implementation and compliance.

On the other hand, in Australia, the national government is responsible for creating policies and objectives, and only general information is published. However, the EI needs more clear guidelines. Finally, it can be clearly seen that Australia at times looks to the U.S for experience and guidance in dealing with cyber security issues relating to critical infrastructure protection. Also Australian businesses that run "critical infrastructure" have been earmarked for at least $35,000 from the Federal Government to attend cyber-security training course organized by the U.S [4].

Recommendations

- Similar to the U.S which has a central body, the NERC which caters solely to security protection in the EI, Australia should establish its own specific body which will directly oversee security protection of the EI and its Information Systems. This body should be able to develop standards, guidelines and policies which can be adapted by both private and public parties responsible for the protection of the EI in Australia.
- Also, based on the successful implementation experience of ISO/IEC 27002 in EI protection of the U.S., Australia can encourage and accelerate the usage of its own AS/NZS ISO/IEC 27002:2005 to salvage existing gaps in security controls development.
- Based on the findings of this research study, gaps exist in the current selected controls of both the U.S and Australia's EI cyber security. A cyber security checklist which addresses all areas of security controls found in the mapping of the NIST 800-53A *Recommended Security Controls* with the U.S CIP standards and AUS ISM needs to be developed. This checklist can be used as a benchmark for security requirement for the EI of other countries that are trying to develop their own CSS for this sector.

CONCLUSION

This study used NIST RMF as a method to review and compare the security measures outline in the CSS of both the U.S and Australia. Based on published data, the methodology employed in this study allowed for the extraction of information at various stages in the framework which permitted similar levels of comparison for both countries.

In addition, FIPS200 was selected as a benchmark to group security requirements in 18 key areas. The NIST SP 800-53A *Recommended Security Controls,* which outlines security requirements, was used to compare US NERC CIP standards and their associated security controls from ISO 27002 and controls from AUS ISM to satisfy requirements in FIPS 200. The comparison pointed out similarities and differences in both countries' CSS, while, at the same time, identifying gaps in security requirements.

This method proved to provide a consistent, comparable and repeatable approach for comparing security controls. A careful examination of the results show significant distinctions in CSS based on key indicators used for this analysis. Therefore, developing a checklist of security control areas will serve as a benefit to other nations planning to develop similar CSS for the protection of their EI or other critical infrastructures.

FUTURE RESEARCH/WORK

This study was carried out using public available documents. This research came up with a checklist highlighting critical security controls areas in the EI that needs attention. However, future work can be carried out to provide a detail list of security controls for critical areas in the EI, and also how to implement them, how to prioritize them, how to evaluate them, and what are the key performance indicators. In addition, in the interest of being thorough, the author would like to see further research conducted into Australian cyber security strategies and security controls for EI protection.

REFERENCES

[[1] United States Depart of Energy, North America Electric Reliability Council, URL: http://www.nerc.com. [Accessed Dec, 2010]

[2] North America Electric Reliability Council, "Security Guidelines for the Electricity Sector," 2007. [Accessed Jan, 2011]

[3] United States General Accounting Office Reliability Council, "Cybersecurity for Critical Infrastructure Protection," URL: http://www.gao.gov/new.items/d04321.pdf**,** May 2007

[4] B. Grubb, " Australia looks to US for Infrastructure Security Training," *S C Magazine*, Sep, 2009. URL:http://www.securecomputing.net.au/News/155152,australia-looks-to-us-for-infrastructure-security-training.aspx. [Accessed Feb, 2011]

[5] Federal Energy Regulatory Commission, "NERC Reliability Standards," Oct, 2010, URL: http://www.ferc.gov/industries/electric/indus-act/reliability/standards.asp**.** [Accessed Jan, 2010]

[6] North America Electric Reliability Council, "Reliability Standards for the Bulk Electric Systems of North America," URL:http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf. [Accessed Feb, 2011]

[7] Australian government, "Australia Critical Infrastructure Resilience Strategy, Dec, 2009.URL: http://www.tisn.gov.au. [Accessed Nov, 2010]

[8] United States Department of Commerce, "Guide for Assessing Security Controls in Federal Information System, July, 2008.URL: http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf. [Accessed Jan, 2011]**:**

[9] North America Electric Reliability Council, "System Security Management," May, 2009. URL: http://www.nerc.com/files/CIP-007-2.pdf. [Accessed Dec, 2010]**//**

[10] NCircle, "NERC Critical Infrastructure Protection Compliance",http://www.ncircle.com/index.php?s=solution_regcomp_NERC. [Accessed Dec, 2010]

[11] S. Harris, "CISSP All-in-one Exam Guide 5th edition, pp. 51-55, January, 2010istpubs

[12] Australian Government, Attorney-General's Department, "Protective Security Policy Framework," January, 2011. http://www.ag.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_ProtectiveSecurityPolicyFrameworkDownloads. [Accessed Feb, 2011]

[13] United States Homeland Security, "A Comparison of Electrical Sector Cyber Security Standards and Guidelines," Oct, 2004. URL:http://www.us-cert.gov/control_systems/pdf/electrical_comp1004.pdf. [Accessed Dec, 2010]

[14] Australian Government Department of Defense, "Australian Information Security Manual," Nov, 2010. URL: http://www.dsd.gov.au/publications/Information_Security_Manual_2010.pdf. [Accessed Jan, 2011]

[15**]** J. Kennedy, "Achieving NERC CIP compliance utilizing ISO 17799:2005", June,2007. URL: http://www.continuitycentral.com/feature0482.htm. [Accessed Feb, 2011]

[16] S. Katzke, K.Stouffer, National Institute of Standards & Technology (NIST),"Applying NIST SP 800-53 to Industrial Control Systems", Aug, 2006. URL: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/Apply-SP-800-53-ICS-final-22Aug06.pdf. [Accessed Jan, 2011]

[17] C. Anderson, Information Systems Security Association (ISSA), "Successful Security Control Selection Using NIST SP 800-53", July, 2009 URL: http://www.noblis.org/NewsPublications/Publications/PublicationsandPresentations/Documents/ISSA0709_Using%20NIST%20SP%20800-53.pdf. [Accessed Dec, 2010]

[18] National Institute of Standard and Technology, "Risk Management Framework", June, 2010. URL: http://csrc.nist.gov/groups/SMA/fisma/framework.html. [Accessed Jan, 2011]

[19] The Wall Street Journal, "Electricity Grid in U.S. Penetrated by Spies", April, 2009. URL: http://online.wsj.com/article/SB123914805204099085.html. [Accessed Nov, 2010]

[20] North America Electric Reliability Council, "Standard CIP-002-3-Cyber-Security-Critical Cyber Asset Identification", Dec 16, 2009, URL: http://www.nerc.com/files/CIP-002-3.pdf, [Accessed Jan, 2011]

[21] SERC Reliability Corporation "SERC Reliability Corporation 2011 Implementation Plan", Dec 1 2010, URL: http://www.serc1.org/documents/Compliance/2011%20Program/2011%20SERC%20CMEP%20Implementation%20Plan%2012-1-10%20rev%2012-10-10.pdf. [Accessed Jan, 2011]

[22] Jim Kennedy, "Achieving NERC CIP Compliance Utilizing ISO 17799:2005, Jun 28 2007, URL: http://www.continuitycentral.com/feature0482.htm, [Accessed Dec, 2010]

[23] National Institute of Standard and Technology, "Public and Business Affairs", June, 2010. URL: http://www.nist.gov/public_affairs/general_information.cfm [Accessed, Feb, 2011]

[24] Australian Government, "Cyber Security Strategy, Nov, 2009.URL: http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity. [Accessed Nov, 2010]

[25] Reliability First Corporation, "Compliance" URL: https://www.rfirst.org/compliance/Pages/CMEPImplementationPlans.aspx. [Accessed, Dec, 2010]

[26] NIST, "Recommended Security Controls for Federal Information Systems and Organizations", 2006, URL: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf. [Accessed March, 2011]

[27] NIST, Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems ", 2008, URL: http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf. [Accessed March 2011]

[28] Australian government, " AS/NZS ISO/IEC 27002:2005".URL: http://en.wikipedia.org/wiki/ISO/IEC_27002 [Accessed March, 2011]

APPENDIX I

COMPARISON OF SECURITY STANDARDS AND CONTROLS IN THE EI

ACCESS CONTROL

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
AC-1 Access Control Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R1.3, CIP003-R5, CIP003-R5.3, CIP003-R5.1	5.1.1, 5.1.2, 11, 11.2, 11.4, 11.5, 11.6	Identification and Authentication 0413	• In most areas, CIP standards and AUS ISM correspond to the SP 800-53 controls. • CIP standards do not have any controls on Access Enforcement. However, AUS ISM requires that agencies must enforce authorizations on systems and remote privilege access must not be allowed. • Least Privilege is an important control to ensure entities have enough rights to perform their assignments without leaking sensitive information. In AUS ISM, this issue is not addressed properly. • AUS ISM contains more complete logging requirements than those of CIP standards. Unsuccessful logon attempts and logon notification info is recorded • CIP standards lack controls on sessions. AUS ISM addresses those issues better.
AC-2 Account Management	CIP003-R5.1, CIP003-R5.2, CIP004-R4.1 CIP005-R2.5, CIP007-R5.1.3, CIP007-R5.2	11, 11.2, 11.2.1, 11.2.2, 11.2.3, 11.4, 11.5, 11.5.1, 11.5.2, 11.5.3, 11.5.4, 11.5.5, 11.5.6, 11.6	Identification and Authentication 0973, 0415, 0416,	
AC-3 Access Enforcement	N/A		System Access 0856, 0985, Remote Access 0446, 0447	
AC-4 Information Flow Enforcement	N/A		N/A	
AC-5 Separation of Duties	N/A		N/A	
AC-6 Least Privilege	CIP007-R5.1	11.5, 11.5.1, 11.5.2, 11.5.3, 11.5.4, 11.5.5, 11.5.6,	N/A	
AC-7 Unsuccessful Logon Attempts	N/A		Event Logging and Auditing 0986, 0582, 0583, 0584	
AC-8 System Use Notification	CIP005-R2.6, CIP005-R5.1	5.1.2, 11.4, 11.5, 11.6, 15.2.2,	Identification and Authentication 0408, 0979, 0980	
AC-9 Previous Logon Notification	N/A		Identification and Authentication 0977	
AC-10 Concurrent Session Control	N/A		N/A	
AC-11 Session Lock	N/A		Identification and Authentication 0427, 0428	

AC-12 Session Termination	N/A		Identification and Authentication 0853	- There are 7 out of 20 items on which neither CIP nor AUS ISM have selected controls.
AC-13 Supervision and Review-Access Control	N/A		Identification and Authentication 0429, 0430, 0431	
AC-14 Permitted Actions without Identification or Authentication	N/A		N/A	
AC-15 Automated Marking	N/A		N/A	
AC-16 Automated Labelling	N/A		N/A	
AC-17 Remote Access	CIP005-R1.1, CIP005-R2.3, CIP005-R2.4, CIP005-R2.5, CIP005-R5.1	5.1.2, 11.1.1, 11.4, 11.5, 11.6, 15.2.2,	Remote Access 0858, 0706, 0985, 0709	
AC-18 Wireless Access Restrictions	CIP005-R2.4, CIP005-R5.1,	5.1.2, 11.4, 11.5, 11.6, 15.2.2,	Wireless LAN 0536-0545, 1010-13, 0860, 1081	
AC-19 Access Control for Portable and Mobile Devices	CIP005-R2.4, CIP005-R5.1	5.1.2, 11.4, 11.5, 11.6, 15.2.2,	Mobile Devices 1082, 0687, 1083, 1047, 0693, 0694,	
AC-20 Use of External Information Systems	N/A		N/A	

Awareness and Training

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
AT-1 security Awareness and Training Policy & Procedures	CIP004-R1, CIP004-R2	8.2.2,	Information Security Awareness and Training 0252, 0251, 0922	• Both CIP standards and AUS ISM require awareness training to personnel. • AUS ISM requires training degrees in which content should be based on the roles and responsibilities of trainees. CIP standards do not fill that gap. • Training activities should be documented. AUS ISM has lack of documentation in this area. • There is 1 out of 4 areas on which neither CIP nor AUS ISM have selected controls.
AT-2 Security Awareness and Literacy Training	CIP003-R1.2	5.1.1,	Information Security Awareness and Training 0256, 0257	
AT-3 Specialized Security Training	N/A		Information Security Awareness and Training 0253	
AT-4 Security Training Records	CIP004-R2.3	8.2.2	N/A	
AT-5 Contacts with Security Groups & Associations	N/A		N/A	

Audit and Accountability

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
AU-1 Audit and Accountability Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R1.3 CIP005-R3, CIP005-R5.1 CIP007-R5, CIP007-R5.2.3	5.1.1, 5.1.2, 10.10.1-10.10.6, 11.2.1-11.2.3, 11.5.1-11.5.6, 15.2.2	Event Logging and Auditing 0580, 0582, 0109, 0987,	• AUS ISM does not have any monitoring and reporting mechanism in place for audit activities. • AUS ISM does actively take controls to protect audit information. CIP standards do not cover this area. • There are 4 out of 11 areas on which neither CIP nor AUS ISM has selected controls. Audit storage and non-repudiation are two important areas needing controls in place to ensure accountability.
AU-2 Auditable Events	CIP005-R3.1, CIP005-R5.1, CIP007-R5.1.2, CIP007-R5.2.3, CIP007-R6.1, CIP007-R6.3	10.10.1-10.10.6 5.1.2, 11.2.1-11.2.3, 11.5.1-11.5.6, 15.2.2, 15.3	Event Logging and Auditing 0109	
AU-3 Content of Audit Records	CIP007-R5.1.2, CIP007-R5.2.3	11.2.1-11.2.3, 11.5.6,	Event Logging and Auditing 0986, 0582, 0583, 0584, 0987,	
AU-4 Audit Storage Capacity	N/A		N/A	
AU-5 Response to Audit Processing Failures	N/A		N/A	
AU-6 Audit Monitoring, Analysis, and Reporting	CIP005-R3.2, CIP005-R5.1, CIP007-R6.5, CIP007-R6.2,	10.10.1-10.10.6, 15.3	N/A	
AU-7 Audit Reduction and Report Generation	N/A		N/A	
AU-8 Time Stamps	N/A		Event Logging and Auditing 0585	
AU-9 Protection of Audit Information	N/A		Event Logging and Auditing 0586, 0989, 0587	
AU-10 Non-repudiation	N/A		N/A	
AU-11 Audit Record Retention	CIP005-R5.3, CIP007-R5.1.2, CIP007-R6.4, CIP008-R2,	10.10.2, 10.10.3, 13.2, 13.2.1-13.2.3 15.3	Event Logging and Auditing 0859, 0990, 0991	

Certification, Accreditation, and Security Assessments

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
CA-1 Certification, Accreditation, and Security Assessment Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R1.3,	5.1.1, 5.1.2,	System Accreditation	• AUS ISM does require each agency to have accreditation and certification controls in place at the policy level. • AUS ISM fails to control from a trusted zone to an un trusted zone outside of an organization's perimeter. • CIP standards have better defined project management plans than AUS ISM. However, CIP standards are lack of continuous monitoring controls.
CA-2 Security Assessments	CIP005-R4, CIP005-R5.1, CIP006-R6 CIP007-R1, CIP007-R8	12.6, 12.6.1, 10.3	System Accreditation 0807 Information Security Monitoring 0911, 0105, 0909	
CA-3 Information System Connections	CIP005-R2, CIP005-R5.1, CIP003-R4.3,	11.4, 11.5, 11.6, 7.2, 7.2.1, 7.2.2,	N/A	
CA-4 Security Certification	N/A		System Accreditation 1142, 0100	
CA-5 Plan of Action and Milestones	CIP003-R4.3, CIP005-R4.5, CIP005-R5.1 CIP007-R8.4	7.2, 7.2.1, 7.2.2, 12.6, 12.6.1, 5.1.2,	N/A	
CA-6 Security Accreditation	CIP003-R2.3, CIP003-R4.3	6.1, 6.1.1 7.2, 7.2.1, 7.2.2,	System Accreditation 0791, 0064, 0065, 0086	
CA-7 Continuous Monitoring	N/A		Information Security Monitoring 0119	

Configuration Management

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
CM-1 Configuration Management Policy & Procedures	CIP003-R6, CIP003-R1.3,	5.1.1, 5.1.2 10.1.1-10.1.4, 10.3, 10.3.1, 10.3.2	Network Security 0513, 0515, 1007	• AUS ISM does not have a comprehensive set of configuration management policies and procedures in place and only emphasizes configuration in networking. • AUS ISM needs a control on monitoring configuration changes. • AUS ISM does not address the issue of least functionality. Agencies may have enough capability to perform duties. • CIP standards contain more controls corresponding to NIST security baselines in configuration management. • There are 2 out of 8 items on which neither CIP nor AUS ISM have selected controls.
CM-2 Baseline Configuration and System Component Inventory	CIP007-R9	5.1.1, 5.1.2	N/A	
CM-3 Configuration Change Control	CIP005-R5.2, CIP007-R3, CIP007-R9	5.1.2 12.5.2, 12.5.3 15.2.2	Change Management 0115, 0117, 0912, 0809	
CM-4 Monitoring Configuration Changes	CIP007-R1	10.3	N/A	
CM-5 Access Restrictions for Change	N/A		N/A	
CM-6 Configuration Settings	N/A		N/A	
CM-7 Least Functionality	CIP005-R2.2, CIP005-R5.1 CIP007-R2	11.4-11.6 5.1.1, 5.1.2 10.6.1	N/A	
CM-8 Information System Component Inventory	CIP002-R3, CIP002-R4	7.2, 7.2.1, 7.2.2 15.2.1, 15.2.2	N/A	

Contingency Planning

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
CP-1 Contingency Planning Policy & Procedures	CIP003-R1.3, CIP009-R1	5.1.1, 5.1.2, 14.1.1, 14.1.2, 14.1.3,	Business Continuity and Disaster Recovery	• AUS ISM does not have control in place to enable agencies to develop their contingency planning policies. • Even though both CIP standards and AUS ISM have a personnel training section, contingency training is not emphasized. • Contingency plans need to be updated on a timely basis. AUS ISUM is lacking of controls to ensure the updating process. • There are 3 out of 10 items, on which neither CIP nor AUS ISM have selected controls.
CP-2 Contingency Plan	CIP009-R1.1, CIP009-R1.2	14.1.1, 14.1.2, 14.1.3,	Business Continuity and Disaster Recovery 0913	
CP-3 Contingency Training	N/A		N/A	
CP-4 Contingency Plan Testing and Exercises	CIP009-R2	14.1.4, 14.1.5,	Business Continuity and Disaster Recovery 0118	
CP-5 Contingency Plan Update	CIP009-R3	14.1.5	N/A	
CP-6 Alternate Storage Site	N/A		N/A	
CP-7 Alternate Processing Site	N/A		N/A	
CP-8 Telecommunications Services	N/A		N/A	
CP-9 Information System Backup	CIP009-R4, CIP009-R5	10.5.1	Business Continuity and Disaster Recovery 0119	
CP-10 Information System Recovery and Reconstitution	CIP009-R4	10.5.1	Business Continuity and Disaster Recovery 0913, 0914	

Identification and Authentication

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
IA-1 Identification and Authentication Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R1.3, CIP007-R5,	5.1.1, 5.1.2, 11.5, 11.5.1-11.5.6, 11.2, 11.2.1-11.2.3,	Identification and Authentication 0413	• CIP standards and AUS ISM have similar controls over identification and authentication on users but not devices. Authenticating feedback and protection mechanisms are not emphasized. • There are 4 out of 7 items on which neither CIP nor AUS ISM have selected controls.
IA-2 User Identification and Authentication	CIP005-R2.4, CIP005-2.5, CIP005-R5.1	6.1, 6.1.1-6.1.3 5.1.1,	Identification and Authentication 0414, 0416	
IA-3 Device Identification and Authentication	N/A		N/A	
IA-4 Identifier Management	N/A		N/A	
IA-5 Authenticator Management	CIP007-R5.2.1, CIP007-R5.3,	11.5.2, 11.5.3, 11.2.3	Identification and Authentication 0423, 0424, 1055	
IA-6 Authenticator Feedback	N/A	N/A	N/A	
IA-7 Cryptographic Module Authentication	N/A	N/A	N/A	

Incident Response

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
IR-1 Incident Response Policy & Procedures	CIP003-R1, CIP008-R1, CIP008-R1.2, CIP008-R1.4, CIP008-R1.5,	5.1.1, 5.1.2 13.1, 13.1.1,13.1.2	Incident Response Plans 0058, 0059	• AUS ISM only defines what should be included in incident response plans but does not define how to train, handle, monitor and guide agencies to implement the plans. • CIP standards are lacking of training and monitoring processes for personnel on incident response either. • There are 4 out of 7 items, on which neither CIP nor AUS ISM have selected controls.
IR-2 Incident Response Training	N/A		N/A	
IR-3 Incident Response Testing and Exercises	CIP008-R1.6	13.1.1, 13.1.2	N/A	
IR-4 Incident Handling	CIP008-R1.1	13.1	N/A	
IR-5 Incident Monitoring	N/A		N/A	
IR-6 Incident Reporting	CIP008-R1.3	13.1.1	N/A	
IR-7 Incident Response Assistance	N/A		N/A	

Maintenance

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
MA-1 System Maintenance Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R1.3, CIP006-R6,	5.1.1, 5.1.2	Product Maintenance and Repairs 1079, 0305	• CIP standards have fewer controls over maintenance than AUS ISM does. • There are 3 out of 6 items on which neither CIP nor AUS ISM have selected controls.
MA-2 Controlled Maintenance	N/A		N/A	
MA-3 Maintenance Tools	N/A		N/A	
MA-4 Remote Maintenance	N/A		Product Maintenance and Repairs 0310, 0944	
MA-5 Maintenance Personnel	N/A		Product Maintenance and Repairs 0306	
MA-6 Timely Maintenance	N/A		N/A	

Media Protection

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
MP-1 Media Protection Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R1.3, CIP007-R7	5.1.1 10.7.1-10.7.4	Media Security	• AUS ISM has a complete set of media security controls, except transportation. • CIP standards fail to implement controls over media access, labeling, storage and transport.
MP-2 Media Access	N/A		Media Usage 0341, 0342, 0343	
MP-3 Media Labeling	N/A		Media Handling 0322, 0325, 0330, 0331, 0335	
MP-4 Media Storage	N/A		Media Usage 0338	
MP-5 Media Transport	N/A		N/A	
MP-6 Media Sanitization and Disposal	CIP007-R7.1, CIP007-R7.2, CIP007-R7.3		Media Sanitization & Disposal	

Physical and Environmental Protection

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
PE-1 Physical and Environmental Protection Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R1.3, CIP003-R5.3 CIP006-R1	5.1.1, 5.1.2 11.2, 11.5, 11.6	Physical Security	• CIP standards do not address physical access authorization issues, or have enough controls over system locations. Cabling management is another issue not being covered • Both CIP standards and AUS ISM have basic physical protections, but environmental protections, such as backup power, humidity, temperature, and lighting are not addressed properly. • There are 8 out of 19 items on which neither CIP nor AUS ISM have selected controls.
PE-2 Physical Access Authorizations	N/A		Physical Security 0164, 0919	
PE-3 Physical Access Control	CIP006-R2, CIP006-R3	9.1.2, 9.1.3	Physical Security 0812, 0813, 1074, 0150, 0151	
PE-4 Access Control for Transmission Medium	N/A		N/A	
PE-5 Access Control for Display Medium	N/A		Physical Security 0164, 0919	
PE-6 Monitoring Physical Access	CIP006-R4	9.1.2, 10, 12, 13,	Physical Security 0173	
PE-7 Visitor Control	CIP006-R1.4	9.1.1	Personnel Security 0166, 0169, 0170, 0171	
PE-8 Access Records	CIP006-R5	10.	Personnel Security 0169, 0170, 0171	
PE-9 Power Equipment and Power Cabling	N/A		Cable management Fundamentals	
PE-10 Emergency Shutoff	N/A		Emergency Procedures 0062	
PE-11 Emergency Power	N/A		N/A	
PE-12 Emergency Lighting	N/A		N/A	
PE-13 Fire Protection	N/A		N/A	
PE-14 Temperature and Humidity Controls	N/A		N/A	
PE-15 Water Damage Protection	N/A		N/A	
PE-16 Delivery and Removal	N/A		N/A	
PE-17 Alternate Work Site	N/A		N/A	
PE-18 Location of Information System Components	N/A		Network Infrastructure 0156, 1070,	
PE-19 Information Leakage	N/A		Physical Security for systems 0160-0163, 1056	

Planning

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
PL-1 Security Planning Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R1.3	5.1.1, 5.1.2,	Information Security Policy 0049, 0890	• Both CIP standards and AUS ISM do not address acceptable behavior properly. Privacy impact assessment needs to be in place. • There are 2 out of 6 items, on which neither CIP nor AUS ISM has selected controls.
PL-2 System Security Plan	CIP003-R3, CIP003-R3.1, CIP003-R3.2	5.1.2,	System Security Plans 0895, 0067	
PL-3 System Security Plan Update	CIP003-R3.3	5.1.2,	System Security Plans 0067	
PL-4 Rules of Behavior	N/A		N/A	
PL-5 Privacy Impact Assessment	N/A		N/A	
PL-6 Security-Related Activity Planning	CIP007-R1.1	10.3	N/A	

Personnel Security

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
PS-1 Personnel Security Policy & Procedures	CIP003-R1, CIP004-R3	5.1.1, 8.1, 8.1.1-8.1.3, 8.2, 8.2.1, 8.2.3,	Personnel Security	• AUS ISM has more focus on how to grant permissions to authorized personnel properly, but do not address the termination issue. Third-Party Role needs and responsibilities need to be clearly identified. • CIP needs to implement controls over personnel roles and responsibilities. • There are 2 out of 8 items on which neither CIP nor AUS ISM have selected controls.
PS-2 Position Categorization	N/A		Role and Responsibilities	
PS-3 Personnel Screening	CIP004-R3	8.1, 8.1.1-8.1.3,	N/A	
PS-4 Personnel Termination	CIP004-R4.2 CIP007-R5.2.3	8.3.3, 11.5.3, 11.2.2	N/A	
PS-5 Personnel Transfer	CIP004-R4.1, CIP004-R4.2 CIP007-R5.2.3	8.3.3, 11.2, 11.3.2	N/A	
PS-6 Access Agreements	N/A		N/A	
PS-7 Third-Party Personnel Security	CIP004-R4.1	8.3.3, 11.2, 11.3, 11.5.2	N/A	
PS-8 Personnel Sanctions	N/A		N/A	

Risk Assessment

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
RA-1 Risk Assessment Policy & Procedures	CIP002-R1, CIP002-R1.1 CIP003-R1 CIP005-R4, CIP005-R5.1	6.1.1, 6.1.2 6.2.1 14.1.2 15.1.1-15.1.6 12.6, 12.6.1	Security Risk Management Plans 0788, 0893 Vulnerability Management 0911, 0909	• AUS ISM is lacking of a proper procedure to perform risk assessment and does not provide enough guidelines. • There is 1 out of 5 items on which neither CIP nor AUS ISM have selected controls. RA is an on-going process. Updates are required on a timely basis.
RA-2 Security Categorization	CIP003-R4, CIP004-R4.1, CIP004-R4.2	7.2, 7.2.1, 7.2.2	N/A	
RA-3 Risk Assessment	CIP002-R1.2, CIP005-R4.1, CIP005-R5.1	6.1.1-6.1.2	N/A	
RA-4 Risk Assessment Update	N/A		N/A	
RA-5 Vulnerability Scanning	CIP005-R4.2, CIP005-R4.3, CIP005-R4.4 CIP005-R5.1 CIP007-R3.1, CIP007-R8	12.6, 12.6.1, 12.5.2, 12.5,3, 12.5.4,	Vulnerability Management 0911, 0909, 0113, 0112	

System and Services Acquisition

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
SA-1 System and Services Acquisition Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R1.3	5.1.1,	Product Selection and Acquisition 0279	• CIP and AUS ISM do not have proper controls over system and service acquisition. This gap needs to be filled. • There are 10 out of 11 items on which neither CIP nor AUS ISM have selected controls.
SA-2 Allocation of Resources	N/A		N/A	
SA-3 Life Cycle Support	N/A		N/A	
SA-4 Acquisitions	N/A		N/A	
SA-5 Information System Documentation	N/A		N/A	
SA-6 Software Usage Restrictions	N/A		N/A	
SA-7 User Installed Software	N/A		N/A	
SA-8 Security Engineering Principles	N/A		N/A	
SA-9 External Information System Services	N/A		N/A	
SA-10 Developer Configuration Management	N/A		N/A	
SA-11 Developer Security Testing	N/A		N/A	

System and Communications Protection

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
SC-1 System and Communications Protection Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R1.3 CIP005-R2, CIP005-R5.1	5.1.1, 5.1.2, 11.4, 11.5,	System Security Plans 0895, 0067, Communications Security	• AUS ISM has more detailed controls in this area than CIP does. However, there are still very big gaps with the NIST security control baseline. CIP and AUS ISM only provide high level guidelines. Technical and operational details are not addressed. • There are 17 out of 23 items, on which neither CIP nor AUS ISM has selected controls.
SC-2 Application Partitioning	N/A		N/A	
SC-3 Security Function Isolation	N/A		N/A	
SC-4 Information Remnants	N/A		N/A	
SC-5 Denial of Service Protection	N/A		Communications Security 1135 Network Security 1019, 1020	
SC-6 Resource Priority	N/A		N/A	
SC-7 Boundary Protection	CIP005-R1, CIP005-R1.2, CIP005-R1.3, CIP005-R1.4, CIP005-R1.6 CIP005-R2 CIP005-R5.1	11.1.1, 11.4, 11.5, 11.6 5.1.2, 15.2.2,	Physical Security 0152, 0153, 0157	
SC-8 Transmission Integrity	N/A		N/A	
SC-9 Transmission Confidentiality	N/A		Network Security Communications Security Cryptography	
SC-10 Network Disconnect	N/A		N/A	
SC-11 Trusted Path	N/A		N/A	
SC-12 Cryptographic Key Establishment and Management	N/A		Key Management Internet Protocol Security	
SC-13 Use of Cryptography	N/A		Cryptography	
SC-14 Public Access Protections	N/A		N/A	
SC-15 Collaborative Computing	N/A		N/A	
SC-16 Transmission of Security Parameters	N/A		N/A	
SC-17 Public Key Infrastructure Certificates	N/A		N/A	
SC-18 Mobile Code	N/A		N/A	
SC-19 Voice Over	N/A		N/A	

Internet Protocol				
SC-20 Secure Name / Address Resolution Service (Authoritative Source)	N/A		N/A	
SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)	N/A		N/A	
SC-22 Architecture and Provisioning for Name/Address Resolution Service	N/A		N/A	
SC-23 Session Authenticity	N/A		N/A	

System and Information Integrity

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
SI-1 System and Information Integrity Policy & Procedures	CIP003-R1, CIP003-R1.1, CIP003-R1.3	5.1.1, 5.1.2	N/A	• CIP has high level controls to implement integrity check policies but not detailed controls over input and out validation. • AUS ISM does not have a specific section related to integrity protection. However, integrity check is required within system protection, software protection and network security sections. • There are 6 out of 12 items on which neither CIP nor AUS ISM have selected controls.
SI-2 Flaw Remediation	CIP007-R3.2	12.5.2, 12.5.3, 12.5.4,		
SI-3 Malicious Code Protection	CIP007-R4, CIP007-R4.2	10.4	Cyber Security Incidents 0824	
SI-4 Information System Monitoring Tools and Techniques	CIP007-R4.1 CIP007-R6	10.4 10.10.2, 15.3	N/A	
SI-5 Security Alerts and Advisories	N/A		N/A	
SI-6 Security Functionality Verification	N/A		N/A	
SI-7 Software and Information Integrity	N/A		N/A	
SI-8 Spam Protection	N/A		Network Security 1152	
SI-9 Information Input Restrictions	N/A		Software Security 0401	
SI-10 Information Accuracy, Completeness, Validity, and Authenticity	N/A		N/A	
SI-11 Error Handling	N/A		N/A	
SI-12 Information Output Handling and Retention	N/A		N/A	

Program Management

SP 800-53A Control	NERC CIP Req.	US ISO 27002 Controls ID	AUS ISM Control #	Comments
PM-1 Information Security Program Plan	N/A		N/A	• AUS ISM outlines requirements to identify different roles and responsibilities within a security development team. CIP standard controls do not address this issue. • CIP standards require responsible Entities to ensure evidence of controls are in place. • Both CIP standards and the AUS ISM fail to enforce project management techniques to security management, and development but divide security management into a series of individual units. • There are 6 out of 11 items on which neither CIP nor AUS ISM have selected controls.
PM-2 Senior Information Security Officer	N/A		Chief IS Officer 0714-0721, IT Security Officer 0772-0773	
PM-3 Information Security Resources	N/A		N/A	
PM-4 Plan of Action and Milestone Process	N/A		N/A	
PM-5 Information System Inventory	N/A		N/A	
PM-6 Information Security Measures and Performance	CIP002-009 Measures		N/A	
PM-7 Enterprise Architecture	N/A		N/A	
PM-8 Critical Infrastructure Plan	CIP002-R1, CIP002-R2	6.1.1, 6.1.2	N/A	
PM-9 Risk Management Strategy	N/A		Security Risk Management Plans 0009, 0788, 0893, 0894	
PM-10 Security Authorization Process	N/A		N/A	
PM-11 Mission/Business Process Definition	N/A		N/A	

APPENDIX II

CHECKLIST FOR EI BASED ON SECURITY STANDARDS AND CONTROLS COMPARISON

The proposed cyber security checklist is intended to be used as a comprehensive guide listing all vital domains which should be addressed by cyber security planning. All stakeholders responsible for security management in Electrical Infrastructure should take necessary steps to minimize their vulnerability to cyber attacks.

The security domains outlined in the checklist have been grouped into 20 sections based on the NIST SP 800-53 *Recommended Security Controls* use as part of the methodology comparison process. They intend to mitigate the existing gaps within the NERC CIP standards and Australia's security controls.

The "Findings" column will contain all discovered evidence and existing controls by the cyber security developing team. If an area has been evaluated, it will be marked by a "√" in the "CHECK" column.

CHECKLIST FOR EI		
Security Domains	**Findings**	**Check**
Cyber Asset identification		
Security Management		
Personnel Training & Awareness		
Personnel Security & Role management		
Electronic Security Perimeter		
Physical Security & Environmental Protection		
Systems Security		
Incident Reporting & Response		
Contingency & Disaster Recovery Planning		
Audit and Accountability		
Certification, Accreditation, and Security Assessments		
Systems Configuration Management		
Authentication and Authorization Management		
Maintenance Management		
Media Protection		
Life cycle development planning		
Risk Assessment		
System and Service Acquisition		
Communications Protection		
System and Information Integrity		