Tallinn University of Technology

Faculty of Information Technology

Department of Computer Science

TUT Center for Digital Forensics
and Cyber Security

# A Comparative Analysis of Cybersecurity Guidelines and Standards for Nuclear Power Plants

Master Thesis
ITC70LT

Student: Eve N Hunter
Student Code: 144705IVCM
Supervisor: Rain Ottis, Ph.D
Harry Kantola

Tallinn 2016

# Copyright Declaration

I hereby declare that I am the sole author of this thesis. The work is original and has not been submitted for any degree or diploma at any other University.
I further declare that material obtained from other sources has been duly acknowledged in the thesis.

..... .....

(Date) (Eve N Hunter)

**Abstract**

Guidelines and standards are imperative for ensuring strong cybersecurity at nuclear power plants worldwide. Yet operators and regulatory agencies lack comprehensive comparisons to adequately justify the implementation of one document over another. The goal of this project is to fill that gap with objective research and tailored recommendations based on level of cybersecurity maturity. It compares nine freely available cybersecurity guidance documents by mapping each document to the 2014 NIST Framework for Improving Cybersecurity of Critical Infrastructure, which was determined to be the most appropriate and comprehensive baseline for security controls. Techniques employed for this comparison of guidelines and standards include ANOVA test for variance, as well as standard deviations to determine fit to the 2014 NIST Framework. No document reviewed within the confines of this study would provide maximum cybersecurity; therefore a combination of documents surveyed is recommended. In the long term, it is strongly advised that a comprehensive, international standard for cybersecurity specifically tailored for nuclear energy facilities be created and enforced appropriately.

## Kokkuvõte

Tuumaelektrijaamade küberturbe kohustuslikuks osaks on juhised ja standardid. Samas puudub operaatoritel ja regulaatoritel kõikehõlmav võrdlusbaas, mille põhjal rakendamiseks sobivat dokumenti valida. Käesoleva lõputöö eesmärk on pakkuda olamasolevale küberturbe tasemele sobivat lahendust. Töös võrreldakse üheksat küberturbe juhendmaterjali 2014. aasta kriitilise infrastruktuuri küberturbe parendamise raamistikuga NIST-ilt, mis leiti olevat kõige sobivam ja põhjalikum alusdokument. Võrdluse läbiviimisel kasutati ANOVA lahknevuse testi ja standardhälbeid, et leida erinevus NIST-i 2014 raamistikuga. Ükski lõputöö raames võrreldud dokument ei andnud maksimaalset küberturbetaset, mistõttu soovitatakse mitme erineva dokumendi kombinatsiooni. Pikemas perspektiivis on soovitatav põhjaliku tuumaenergiajaamadele suunatud rahvusvahelise küberturbe standardi loomine ja jõustamine.

# Contents

# List of Figures

# List of Abbreviations and Terms

**ANOVA** Analysis of Variance . . . 43

**ANSI** American National Standards Institute . . . 66

**ANSI/ISA** American National Standards Institute/International Society of Automation . . . 64

**BSI** Federal Office for Information Security (Germany) . . . 31

**CCS CSC** Council on Cybersecurity Top 20 Critical Security Controls . . . 34

**CERT** Computer Emergency Response Team . . . 27

**CI** Critical Infrastructure . . . 13

**CIP** Critical Infrastructure Protection . . . 7

**CIIP** Critical Information Infrastructure Protection . . . 25

**CSIRT** Computer Security Incident Response Team . . . 52

**CSMS** Cyber Security Management System . . . 64

**DBT** Design Basis Threat . . . 50

**DCS** Distributed control systems . . . 22

**IAEA** International Atomic Energy Agency . . . 16

**I&C** Instrumentation and Control . . . 17

**ICS** Industrial control systems . . . 11

**IEEE** Institute of Electrical and Electronics Engineers . . . 40

**ISO** International Organization for Standardization . . . 31

**ISO/IEC** International Organization for Standarization/International Electrotechnical Commision . . . 34

**IT** Information technology . . . 11

**NEI** Nuclear Energy Institute . . . 39

**NERC** North American Electric Reliability Corporation . . . 62

**NIST** National Institute of Standards and Technology . . . . . 7

**NPP** Nuclear power plant . . . . . 7

**NRC** Nuclear Regulatory Commission . . . . . 39

**PLC** Programmable Logic Controller . . . . . 18

**PPP** Public-Private Partnership . . . . . 11

**PWR** Pressurized water reactor . . . . . 21

**SCADA** Supervisory control and data acquisition . . . . . 19

**US** United States . . . . . 11

**UK** United Kingdom . . . . . 11

**WINS** World Institute for Nuclear Security . . . . . 39

# Chapter 1

# Introduction

## 1.1. Problem Statement

Since computers have become the primary modus operandi for a variety of industries, governments have been working to ensure their security from outside infiltration or attack. The nuclear industry, however, upgraded its equipment from analog to digital relatively late. To this day, many plants continue to use aging analog technology. Whereas other critical industries have had to manage this threat for much longer, those in the nuclear industry have always assumed that the so-called 'air-gap' would protect them from remote cyber attacks. The focus has therefore been on the very real physical threats of threat and sabotage. Now that the situation has changed with the modernization of technology and the expanding number of nuclear reactors worldwide, the cybersecurity of the civil nuclear sector has been regarded as woefully lacking.

In September 2015, the world-reknowned London think tank, Chatham House, released a report disparaging the ability of current nuclear operators to manage the cyber threat in order to adequately maintain safe and secure operations at their plants.[1] The report concludes that there is a fundamental gap in the protection of civil nuclear facilities on almost every continent from modern cyber threats. Their conclusion is derived from a number of findings including lax procedural guidelines, contractual cybersecurity engineers, and increased know-how from potential threat actors (primarily states). The picture painted by this report is fairly bleak; there is a fundamental lack of cybersecurity expertise in the nuclear industry which is

making it vulnerable.

Chatham House's report has led to a number of nations coming forward to indicate that their security situation was unfairly depicted. Both the United States (US) and the United Kingdom (UK) have come forward to say that their facilities were very well prepared to defend against a cyber attack. [2], [3]

The Chatham House report assesses current industry practices; but this thesis works to assess the available resources for nuclear power plant operators and regulators to work from. There are many standards and guidelines that aim to increase security within Information technology (IT), Industrial control systems (ICS), and even NPPs in particular. The problem, therefore, is just that. There are too many potential guidelines to follow, and without proper recommendations and comparison, the choice on which to follow is not based on real comparative knowledge. Instead, the choice is instead based on the particular lead security employee's knowledge, for example. There is no resource that compares and evaluates the available guidance.

With the overall goal of improving cybersecurity of nuclear power plants worldwide, this study will provide a comparison of a variety of standards and guidelines available for NPP operators and regulators. This comparison will focus primarily on the substantive differences between documents and will provide recommendations for scenarios in which one piece of guidance may be preferred over another. A state-based Public-Private Partnership (PPP) approach, with enforcement capabilities, is endorsed by this project.

## 1.2. Scope

In order to address the problem of an oversaturated standards and guidance environment, chapter 2 first addresses the need for cybersecurity at nuclear facilities. This chapter reviews possible threat actors, vulnerabilities, threats, and known breaches of the cybersecurity of nuclear power plants. It furthermore discusses the variety of approaches governments can take to protect the cybersecurity of critical infrastructures, like nuclear energy.

Chapter 3 explains the selection processes of well-known, diverse, and comprehensive documents that could be applied to nuclear power plants. The author's consultation with IT experts at NPPs provides further analysis of the problem with existing

guidance. This section reviews the choice of the NIST Framework as a suitable baseline document from which to analyze other cybersecurity guidance. The following documents were chosen for their relevance to nuclear facilities, as well as their comprehensiveness as compared to other available guidance. There are many unassessed documents; reasons for their exclusion is included in chapter 3.

- IAEA Computer Security Guidelines[4]
- NEI 08-09 [Rev.6] Cyber Security Plan for Nuclear Power Plants [5]
- NRC Regulatory Guide 5.71 [6]
- NIST SP800-53 [7]
- WINS 4.3 Security of IT and IC Systems at Nuclear Facilities [8]
- IEEE 692-2013 [9]
- ISO/IEC 27001 [10], [11]
- NERC CIP v5 [12]
- ANSI/ISA 62443-2-1:2009 [13]
- ANSI/ISA 62443-3-3:2013 [14]

The author uses statistical analysis techniques to assess the above documents. The subsequent chapter 4 provides a qualitative assessment of each document, especially as compared to the NIST Framework. The final chapter, chapter 5, provides the combined results of both chapter 3 and chapter 4. The outputs of this study are analyses of the strengths and weaknesses of each studied document and recommendations for 1) the construction of new guidance for NPPs that will address the gamut of activities needed for excellent cybersecurity, and 2) what combinations of documents can be best utilized to create the strongest cybersecurity possible (based on situation).

Because of the large number of existing standards and guidelines for cybersecurity, there are a number of documents that are not included that would be useful for future research in this area. Furthermore, this work does not address the specific political environments that would be necessary to enact a strong, state-based regulatory environment; nor does it fully address privacy concerns that may be necessary to implement within a cybersecurity implementation.

# Chapter 2

# Background

## 2.1. Identifying Threat Actors

Although there are few non-state actors with the resources and knowledge to conduct a successful attack on critical facilities, the number of threat actors will only grow with time. Attribution remains a difficult challenge in the event of any cyber attack – even if the number of potential instigators is relatively low. It is important to have an adequate understanding of the threat landscape because the consequences of an attack on any Critical Infrastructure (CI) operators would be dangerous. An attack on a nuclear facility would be even more devastating.

Not only would disruption or sabotage of their services impact access to electricity, but the disturbance of nuclear materials in a NPP could seriously harm both human beings and the environment. The recent meltdown of the Hiroshima power plant in Japan illustrates just some of these consequences. Nuclear power plants are not impervious to attack, and have occasionally been at the receiving end of natural disasters, accidents, malfunctions, and intentional breaches. This section elaborates on potential motivation for intentional infiltrations of a power plant and, in particular, effects of computer-based problems in power plants. The aim of recounting such incidents is to demonstrate the reality of a cyber attack on a nuclear facilities and the potential for unfortunate consequences. This section focuses primarily on the various threat actors that may want to target a civil nuclear energy facility. It is important to note the motivations and methods of potential attackers because policies and controls implemented at the NPPs must take this information into consideration. This

particular section notes potential motivation of any attack (or accident) regardless of tactics (cyber or physical). Cyber criminals are not included in the following list of threat actors; financially motivated attacks are common in every business sector and are not specific to nuclear power plants. Theft of nuclear materials or NPP blueprints should be taken seriously. Ultimately, however, the recipients of nuclear material or information on how to attack a NPP would be included in one of the following categories of threat actors.

Incidents that are cyber-specific are included in the following section, 2.2.

### 2.1.1. Activists

Historically, nuclear plants have targets of radical activism. Nuclear power in itself is controversial; it is dangerous even barring intentional attacks. In order to demonstrate the insecurity of the sites, some activists take to disrupting the operation of plants. In 1982, on behalf of a radical political party, two individuals planted and detonated explosives in the newly commissioned Koeberg nuclear power plant in South Africa. As the fuel had not yet been loaded, the intent of the attack was not to spread radioactivity. This particular attack was unsuccessful in deterring the facility from coming online.[15] Certainly, however, modern hacktivists may also want to disrupt NPPs in order to prevent additional sites from being constructed.

As recently as 2014, hackers stole blueprints and test data from Korea Hydro and Nuclear Power Co. The data was leaked over Twitter with a warning to shut down three reactors or face 'destruction.' In the end, there was no physical damage to the plant but there is a clear will to target nuclear facilities. In this specific case, the activists' methods could have also compromised the security of the plant by providing detailed information to anyone interested in carrying out an attack on this plant, or one similar.[1]

In 2011, the French nuclear power group Areva, was purportedly affected by a virus. The details of the attack were never released in detail, however there were claims that the attackers had been in the system for up to two years. [16] The same company's website was taken down in 2015 by hacktivists associated with Anonymous in protest of the construction of a new nuclear power plant in France. [17]

### 2.1.2. Terrorists

Terrorism is on the rise; especially in European and North American countries that rely most on nuclear power. Violent extremists notoriously target members of an unsuspecting public, as that elicits the most overall fear. There certainly is reason to believe that nuclear power plants could be future targets for terrorists, especially given the increase in cyber capabilities of terror groups, like Daesh, for example. [18]

The US President George W. Bush said in his State of the Union address in 2002 that "diagrams of American nuclear power plants" were found in al-Qaeda materials. In fact, one al-Qaeda training manual highlights nuclear plants as some of the best targets for spreading fear among the American population.[19] The devastating consequences of an attack on a nuclear power plant are certainly cause for heightened security and concern, particularly given the increase of extremist attacks. It should be noted however, that the cyber threat to nuclear power plants was not thoroughly considered (at least publicly) until the Stuxnet malware hit Iran's Natanz facility. In fact, in 2005, the Congressional Research Service (CRS) provided a report to Congress detailing their vulnerability to terrorist attack, the possibility of a computer-generated attack was not even mentioned. [20]

### 2.1.3. Insiders

According to a 2014 paper by Matthew Bunn and Scott Sagan, insider threats are the most serious threat to nuclear facilities today. Insiders can also conduct a cyber attack from the inside; they have detailed knowledge of the systems being used and understand the crucial parts of that specific reactor. [21] The incident at the Ignalina reactor in Lithuania in 1992 is proof of that (section 2.2).

Bunn and Sagan provide numerous examples of insiders working to either steal nuclear material, or sabotage the plant; there is definite precedent for insider attack within the industry. In 2012, for example, a diesel generator was sabotaged at the San Onofre nuclear power plant in the US. Theft of nuclear material is also well-documented. Although the majority of NPPs currently use low-enriched uranium (LEU), which is very difficult to make into a nuclear bomb, some still use highly enriched uranium (HEU). HEU that is enriched to ninety percent is considered weapons-grade. Especially following the dissolution of the Soviet Union, there

were many times when HEU was stolen, almost always by an insider. There are undeniable motivations for an insider to also assist in a cyber attack - monetary (see above reference to cyber crime), revenge, or otherwise.[21]

The threat that insiders pose is robust. Guidance for cybersecurity at nuclear power plants should also specifically include methods that may mitigate that risk. The International Atomic Energy Agency (IAEA) has provided an entire document that focuses solely on neutralizing the insider threat, entitled *Preventive and Protective Measures against Insider Threats*. [22]

The insider threat does not just encompass malicious actions; accidental sabotage is also a potential result of the insider threat and will be addressed further in the following section.

### 2.1.4. Accidental

While not malicious, accidental incidents at a NPP could still be damaging to the facility. If an employee falls prey to a phishing attack, they could be unintentionally giving a malicious actor access to the facility, causing a loss of monitoring capabilities, or even provoking an emergency shutdown.

The most common causes of accidental insider threats were identified in a survey of the United States Department of Defense. As of January 2015, those threats were determined to be - phishing attacks (42%), incorrect use of an approved personal device (38%), accidentally deleting, corrupting or modifying critical data (38%), and copying data to a non-secure device (37%). Some of the underlying causes of these threats include lack of staff IT training, pressure to change configurations quickly, and use of mobile devices not limited to secure areas. Accidental cybersecurity incidents should be mitigated through thorough and enforced security policies and automated detection of suspicious behavior. [23]

### 2.1.5. Nation-State

The Geneva Convention should, in theory, deter nation-states from launching a deleterious attack on nuclear power plants. However, the uncertainty of attribution could provide a potential loophole in the articles that defend the rights of civilians

to be protected from the dangers of war. In that regard, Stuxnet (see 2.2) set a dangerous precedent. While this specific attack is assumed to be state-perpetrated (by the United States and Israel in particular), it cannot be said with absolute certainty. [24], [25]

India and Pakistan expanded upon the Geneva Convention and the Law of Armed Conflict with their 'India-Pakistan Non-Attack Agreement' which entered into force in 1991. In this document, both nations agree to not make nuclear electrical generating stations the target of attack when such an attack could release dangerous elements causing the suffering of a civilian population. [26] Hopefully, international agreements such as the one between India and Pakistan can deter nation-state level attacks, even if attribution is questionable.

## 2.2. Cyber Incidents at Nuclear Power Plants

To demonstrate the reality of the cyber threat in particular, I will provide a few examples of times when civil nuclear facilities were affected by a problem in their computer systems – either intentional or accidental. The Chatham House report mentioned earlier also chronicles each cyber security incident at nuclear facilities.[1]

First, in 1992, an employee of the Ignalina nuclear power plant in Lithuania introduced a virus into the ICS. He claimed his actions were intended to demonstrate the vulnerabilities of plants like Ignalina to basic viruses. This incident also highlights the importance of implementing security checks on staff members as well; an insider attack could be particularly devastating. [1]

Then, in 2003, a dormant nuclear power plant in Ohio (US), was infected by the Slammer worm through the plant's business network. Although the Instrumentation and Control (I&C) systems had been protected by a firewall, a consultant had created a vulnerability in order to access the internal systems from the office network. The worm itself generated malicious traffic, preventing employees from digitally monitoring the safety controls of the facility for approximately five hours.[27] The worm was being spread across the internet, exploiting a vulnerability in the Microsoft SQL 2000 database server software. The patch for this particular weakness had been released six months earlier, but had been applied to neither the business nor control system.[1]

Also in the United States, in 2006, an Alabama nuclear power plant's digital systems malfunctioned requiring a manual shutdown of the plant in order to avoid a meltdown. The communication process set up between a condensate demineralizer controller (a Programmable Logic Controller (PLC)) and a recirculation pump (using variable frequency drives) only allowed a limited amount of traffic. When the network began to create too much traffic for each of the devices to handle, both of them malfunctioned. This incident was unintentional but is evidence how a malfunction in a few digital components can lead to a potential meltdown. [28]

Two years later, an employee was installing an update on an enterprise computer that connected to the ICS of the Hatch nuclear plant in Georgia (US) in order to remotely monitor it. When the employee rebooted the computer to finalize the update, the data in the ICS was briefly set to zero, leading the ICS system to interpret that as an emergency situation, thus triggering an automatic shutdown.[1], [28]

A German nuclear facility was reported as having a virus within its computer system that monitored and visualized data regarding the movement of nuclear fuel rods in late April, 2016. The viruses found include "W32.Ramnit"' and "'Conficker"', which were discovered in 2010 and 2008, respectively. The system affected was retrofitted in 2008. Furthermore, there were 18 infected removable drives found in the plant's enterprise network. As of the completion of this project, the exact details of the virus are under investigation, but it appears that it was not specifically targeted towards the nuclear plant. Although there was no damage from this particular virus, there is a potential that even non-targeted malware could cause some damage to the operation of the facility. [29]

Of course, the most famous and most sophisticated attack on an ICS is the 2010 Stuxnet malware. Using infected flash drives, the attackers released an unprecedented type of malware that could exploit a vulnerability in Siemens equipment to cause physical damage. The worm specifically targeted the uranium-enriching centrifuges at Iran's Natanz facility. The flash drives were first deployed to five independent contractors believed to have direct connections to the Natanz facility. Stuxnet hit the computers operating at these businesses as well as the actual centrifuges at this plant. The success of this attack can be attributed to detailed intelligence as well as a method of physically delivering the flash drives to the companies. [30] But by targeting these intermediary sites, Stuxnet spread beyond its intended target, which inevitably led to its discovery. This piece of malware is also believed to have hit a Russian nuclear power plant in 2010.[1] This incident particularly highlights the need for strict policies against removable drives being allowed

inside nuclear facilities.

Stuxnet provided a template for would-be ICS saboteurs to follow. Even more frightening is that exploit code for Supervisory control and data acquisition (SCADA) systems is widely available. [31] There is even a search engine, Shodan, designed specifically to find ICS devices, so even if an attacker might not initially be targeting a nuclear plant, he or she will have all potential damaging options laid out to them in a simple interface.[32] This is not to say that a successful attack on a nuclear plant is imminent; still the knowledge and resources needed to conduct such an attack are out of reach for most hackers (although not those with government-level resources). Regardless, steps taken to ensure comprehensive security now will pay-off in the long run when expertise on attacking critical systems becomes even more mainstream.

## 2.3. Threats to Nuclear Power Plants

Civil nuclear sites pose a serious threat for a number of reasons: they are a potential safety hazard for their employees and the surrounding inhabitants, a physical attack could destabilize the nuclear material, a pause in operation could leave an area completely without power, etc. The new threat now is the means in which many of these consequences could come about. Utilizing newer digital components in nuclear power plants, malicious actors could provoke a maelstrom of harmful effects; and yet the regulation of these digital aspects is still not globally accepted or implemented. To understand the need for the best possible standards and cybersecurity programs, there should be a clear understanding of what is at stake.

As shown in Figure 2.1, there are 30 countries worldwide operating 440 nuclear reactors for power generation. In fifteen countries, there are 65 reactors being built as of March 2016. Each of these plants, on average, creates $400 - 700$ permanent jobs.[34] However, this is not the complete number of individuals who would have access to any given plant. It is often said that the weakest part of any system is the human operating it. In this case, there are hundreds of humans available to compromise the operation of a nuclear plant, resulting in devastating consequences. Standards and guidelines for cybersecurity need to ensure thorough personnel reviews and clear behavior limitations. This is especially true given the number of nations that are pursuing nuclear power, or planning on expanding it.

Insiders aside, there are many more humans worldwide seeking to exploit specific

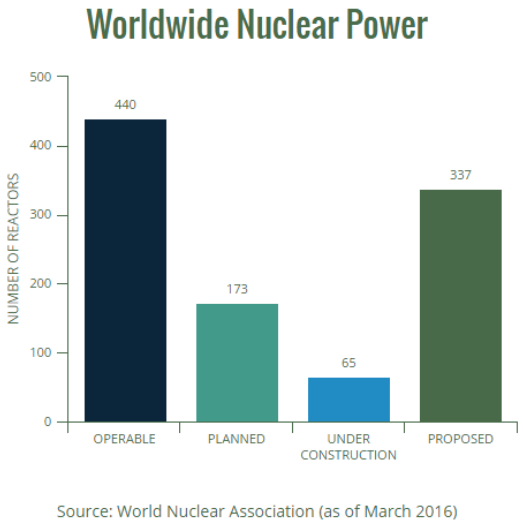


Figure 2.1. Current & Future Global Nuclear Power[33]

vulnerabilities(see 2.1). In 2014, there were over 200 sophisticated attacks on ICS in the Americas, 32% of those were focused on the energy sector. [35] The trend towards attacking critical infrastructure is one that is notably increasing; power plants should be prepared to defend against well-resourced and targeted attacks. Security at nuclear power plants specifically should be frequently checked and updated, in order to fend off increasingly sophisticated attacks.

The phenomenon of insecure systems at nuclear facilities is relatively new. Nuclear plants have been one of the last industries to modernize and introduce digital technologies alongside analog ones. With the exceptions of countries like Germany, Switzerland, and Sweden, that are phasing out nuclear power and are not modernizing existing control systems, digital technology is the future, both for the world and for industrial plants. [36] Although analog technologies are often heralded as an answer to cybersecurity problems, this is for the most part unfeasible in the modern world due to concerns over convenience as well as availability. [37] This evolution also means, however, that there are many modern vulnerabilities being discovered. The traditionally-trained nuclear engineers were not trained in cyber engineering and vice versa.[1] States therefore need to rely on the expertise of both nuclear power operators and cybersecurity experts in order to adequately defend against the attacks nuclear facilities.

### 2.3.1. Cyber Insecurities and the Need for Specialists

Nuclear engineers are more familiar with the operation of the plant, and therefore also more aware of its vulnerabilities. Understanding the process of energy generation through nuclear fission is one core aspect of preserving the continued operation of a plant. This section provides the readers a better understanding of how nuclear power plants operate, and which components in particular are vulnerable to cyber attacks.

The main types of nuclear reactors are: Pressurized water reactor (PWR), Boiling Water Reactors (BWR), Pressurized heavy water reactors (PHWR), Gas-cooled reactors (GCR), Light water graphite reactors (LWGR), and Fast Breeder Reactors (FBR). The PWR is by far the most prevalent type of reactor worldwide. [38]

Essentially, nuclear power plants are producing energy by producing heat. In the reactor core, the nuclear chain reaction occurs. Then, the heat is removed by water pumped through the core by the main circulation pumps. In a boiling-water reactor for example, water boils inside the core, then the steam generated is sent to a turbine generator to produce electricity. In a pressurized-water reactor, steam is produced through a cooling process. Overheating of the reactor fuel is what is generally referred to as a 'core meltdown' like the one that occurred at Chernobyl in 1986. Therefore, what the main threat to the core (which could release large amounts of heat and radioactive fuel) is a sabotage of the cooling process. The systems for cooling down the water and radioactive materials have numerous components and controlling parts that a malicious actor would want to target to produce the maximum damage to the plant and its surroundings. [39]

In their work on cyber-attack scenarios, Ahn et al. describe the components of a civil nuclear facility that could be targeted for a cyber attack. First, there is the enterprise network. This is the group of computers, printers, servers, switches, and more that manage the business aspects of the plant. These devices need connections to outside the facility for the Internet as well as for communicating with contractors and other stakeholders integral to business operation. These devices are connected then to the I&C systems, primarily for the purpose of monitoring. Because of this, ensuring that even the enterprise wireless networks and firewalls are properly configured is essential. The I&C systems consist of an internal server, a computerized work station for plant-employees to control and monitor the energy-generation process which would then link to the industrial control systems. These are the physical equipment,

sensors, and the control equipment - the PLC, Distributed control systems (DCS), or other control components. These are divided into safety systems and non-safety systems but due to their connection, all of these technologies should be monitored in order to prevent intruders from gaining dangerous levels of access to core operations of the plant. Communications between all of these I&C parts can be facilitated through Ethernet, an industrial fieldbus network, or a hardwired network. [27]

All of this equipment is primarily produced by a few internationally-known companies such as Siemens and Honeywell. Many operators of nuclear plants keep the default passwords on this equipment; this is a dangerous practice given how popular and widespread the equipment manufacturers are. Countries can no longer be sure that the hardware they buy from a private company in another country hasn't had a backdoor vulnerability installed. While countries like the United States may try to evade the inherent supply chain vulnerabilities through in-country production, most nations are much smaller and therefore cannot begin to produce all necessary equipment within the borders of their own national control. For this reason, integrity-checking mechanisms and policies to eradicate supply chain vulnerabilities should be included in the strongest standards and guidelines. [1]

Beyond this, much of the older control systems present in nuclear facilities were not designed with security in mind, nor the specific application at a nuclear plant as opposed to another facility. As reported by the Chatham House report, "'retrofitting' cyber security measures to these original systems now is technically challenging and expensive. " [1] After Stuxnet was revealed many industries utilizing ICSs checked their own systems and found malware on them. Perhaps a greater awareness among ICS operators will lead to further protections in the future. Still, as Joel Brenner warned in the Bulletin of Atomic Scientists , few companies are in fact willing to completely isolate their industrial control systems from the internet, taking the necessary steps to truly defending their critical services. [40]

Furthermore, these devices are running software that may need regular patching, and implementation of anti-virus software which would then increase the number of people and companies integral to securing access to the facility. This requires diligent administrators to ensure that all aspects of software management from personnel, to detection and monitoring and response are managed; if any vulnerabilities are found they should be immediately mitigated to prevent malicious hackers from capitalizing on outdated systems. [31] Security controls are especially crucial given there are companies selling zero-day vulnerabilities, which are vulnerabilities in software not yet discovered and therefore not yet patched. If one of them is exploited, there

should be a clear response plan in place; but if a patch has been already released for that vulnerability, the facility should ensure that a patch is installed in a timely manner. [41]

Nuclear systems are both complex and volatile. When IT specialists are generally unaware of the specific components, they are at a greater risk of unintentionally causing an error at the plant. There is certainly a need now for cyber experts who focus particularly on ensuring the safety and security of networked systems in a sensitive facility like a NPP. [1]

### 2.3.2. Attack Types

The attacks that are occurring are becoming increasingly sophisticated and targeted. This is true both at nuclear facilities and other facilities with ICS. Figure 2.2 below illustrates well some of the tactics ICS motivated hackers could use to disrupt or sabotage plant operation. The graph is based on companies that have reported intrusions into their systems but, as is well documented, this data likely only accounts for a small percentage of attacks. [42] To group specific methods such as code execution and buffer overflows, NIST from the US devised a useful categorization. For ICS, attacks can include control logic manipulation, control devices reprogramming, denial of control action, malware on control systems, modification of safety systems, and spoofed system status information. [43] Generally speaking, these are the primary issues vexing IT security specialists at nuclear plants. Any successful guidance implemented at a nuclear facility will address each of these threats and implement specific controls against them.

The IAEA released a timeline of known computer attacks that nuclear facility operators need to be diligently protecting against within their guidelines for computer security. [4] Unlike Figure 2.2, this graph includes methods for hackers to enter the system such as password guessing/cracking and back doors – as well as ways to interrupt it such as malicious code and morphing (a relatively new technique that alters the configuration of a system). Yet the broader purpose of Figure 2.3 is to illustrate how hacker know-how is no longer a prerequisite for advanced attacks. The downward-sloping dotted blue line indicates the necessary level of intruder knowledge, whereas the increasing red line indicates the growing level of attack sophistication. Even amongst the methods presented in Figure 2.2, many of them do not require high levels of skill or knowledge. When the entire situation is examined,

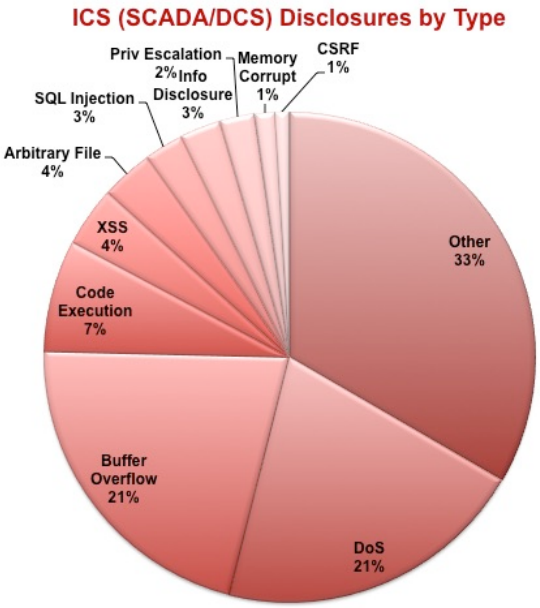


Figure 2.2. ICS Disclosures by Type

to include entry methods and tactics for disruption (or destruction), it is clear that the barrier for entry is not so high after all, and the humans behind the systems do in fact introduce many vulnerabilities.

The new normal is now a dangerous situation where human error is still blatantly present, but the number of actors who can exploit that vulnerability has risen exponentially. Because of this, the possible regimes and security controls that could be introduced have proliferated over the past several years. While this provides a depth of potential and knowledge, it is not always clear how to maneuver amongst all of these different guides and standards.

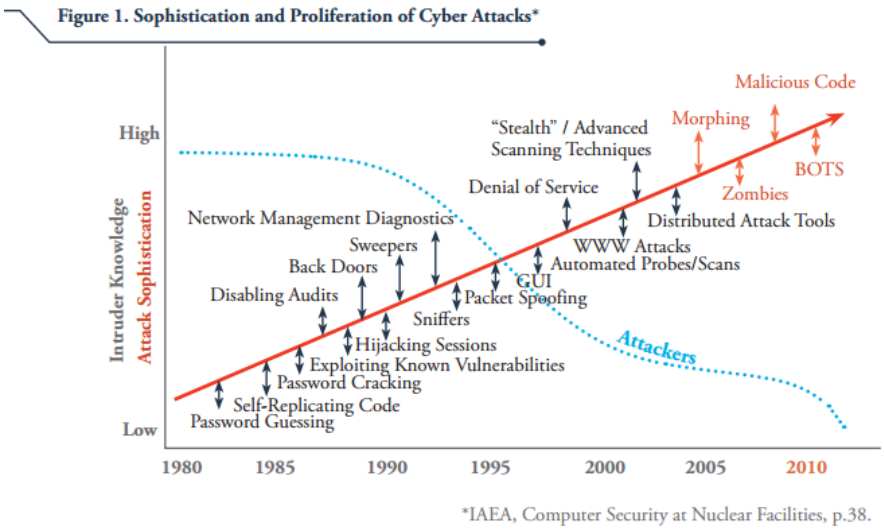


Figure 2.3. IAEA Computer Security at Nuclear Facilities [4]

## 2.4. Strategies for Critical Infrastructure Protection

The previous chapter made the case for decisionmakers at nuclear power plants investing strongly in cybersecurity. Cybersecurity implementation at these facilities is typically done through a combination of voluntary measures, meeting industry standards, information-sharing, and more. Even when discussing standard compliance in particular, there are a number of ways to achieve that, bureaucratically speaking. This thesis opines that government regulation is the most beneficial method for both operators and the implementing nation. This section will review the underpinnings of this recommendation, as well as other options for ensuring comprehensive cybersecurity is implemented at NPPs worldwide.

Over the past few decades, the cybersecurity of critical infrastructure has been increasingly regarded as one of the most essential activities of both the government and the private sector (where the majority of all CI is located). Despite the frequent animosity between the public and private sectors, governments tend to insist that public-private partnerships are essential for ensuring the security of national infrastructure, although they are not always regarded as the most ideal solution, particularly by the private sector(see subsection 2.4.1). This approach, termed 'network governance,' focuses on the government's role as facilitator and coordinator. The alternative, neoliberal governance, would transfer authority over critical infrastructure to the private sector. The neoliberal approach is seen as being more focused on efficiency, as it assumes that the private sector have much more effective ways of employing security measures and organizing amongst themselves to maintain situational awareness. [44] Of course, there is a varied continuum between these two approaches that Dan Assaf elaborated on in his 2008 article 'Models of Critical Information Infrastructure Protection.' The balance between public and private responsibility can be quite varied. [45]

The level of intervention from government in critical infrastructure protection activities varies quite widely. The Center for Security Studies at ETH Zurich has published a number of reports detailing the assorted approaches that governments take to protect critical infrastructure, and in particular critical information infrastructure. However, as the authors note, the two are inextricably linked. One cannot discuss CIP without an in depth discussion of Critical Information Infrastructure Protection (CIIP). This section will present approaches to CIIP in order to assess alternatives to government-led CIP. [46] The purpose is to describe the context within which civil nuclear plants can be analyzed as well as to provide a brief assessment

of the feasibility of a stronger government role in securing such facilities.

### 2.4.1. Private Sector

The private sector is known to advance much faster technologically, and therefore also in security capabilities. Given the concentration of critical infrastructure in the private sector, for some it makes sense to rely on the 'experts' of that field to decide the best security measures for them.

Some governments have actually implemented protections based on this philosophy. Australia, for example, is committed to the idea that the CI operators are the most knowledgeable regarding their own industries. Unless there is a special reason for state regulatory intervention, such as international obligations, they prefer to leave protection in the hands of the private sector. Notably, however, Australia does not have a nuclear power industry. Furthermore, the situations where governments agree to take a back seat on security issues is extremely rare.[46]

In theory, if the private sector organized well enough to enforce standards on its own members, a strictly private cybersecurity regime could be possible. There are examples of industry-led guidance and sharing of best practices. However without a clear authority this kind of collaboration among peers is unlikely to be successful. Furthermore, unless a specific security agency is formed for the private sector with the sole goal of thorough security, companies are likely to choose and enforce standards based on their effects on business success and continuity.

### 2.4.2. Government

State-based CIP is not entirely uncommon. Some nations treat critical infrastructure as first and foremost a matter of national security, and therefore it by default falls under the jurisdiction of a national authority. This also bars private industry from providing crucial services for citizens. Although this may be good from a security perspective (assuming governmental security is adequate), the private sector is known for its innovation and commitment to business continuity. While governments are expected to provide for its citizens, it is not quite so rigid a bond as that between a company and its customers.[46]

Brazil is one nation that chooses to keep its nuclear power in the hands of the government. It is state-owned and therefore obviously its protection is entirely in the hands of the state. As of 2015, Brazil has upheld its decision to deny private investment in nuclear power, although it has allowed in limited amounts for other areas of the electric grid. [47][48] This kind of blockade against private industry contributing to nuclear power is infeasible for most nations. Most nations either already rely on industry for critical services, or they simply don't have the capacity to manage the entirety of nuclear power production.

### 2.4.3. Public-Private Partnerships

PPPs are generally considered a more intermediate level of intervention by national governments. They utilize both the specialized knowledge of the private sector and the organizational capacity of the government. This study proposes a governmental authority be in charge of requiring and enforcing NPP compliance with standards and guidelines. It also acknowledges the expertise and obvious involvement of the private sector in this issue. A collaborative PPP led by a governmental body would be the best situation for cohesive enforcement of security implementations.

The reason this work recommends government be the leader of CIP is because a devastating attack on any nation's critical infrastructure would likely be considered an attack on that country itself (of which the government is in charge of defending against). John Locke argued that the condition under which government exists is that the citizens agree to abide by the law and the government works to provide for their wellbeing and security . In the United States Constitution, this idea is clearly stated in its preamble, in which it declares "to provide for the common defense." This is one of the key roles of any government. A national government could, therefore be considered to be shirking its duties if it transfers all responsibility of matters of security to the private sector. Most nations do in fact try to find a balance between the liberty of the private sector, and the government's role in ensuring the security of its citizens. For this reason, the government clearly does need to play a role in securing its critical infrastructure, although its involvement often varies.

The Netherlands also created a number of public-private partnerships to address the issue of CIP. The Dutch government made it clear that there needs to be cooperation amongst a variety of actors such as the operators themselves, law enforcement, the intelligence services and Computer Emergency Response Teams (CERTs) in order

to protect CI from intentional attacks. One of their key observations was that the actual industry experts are unaware of the workings of other critical services and therefore are unaware of their dependencies. This is one argument for the inclusion of experts who specialize in critical infrastructure generally, in order to provide for a more cohesive response to threats. The government is one example of an entity who can work to establish effective collaboration across critical infrastructure industries. [46]

Given the US' role in kickstarting the field of critical infrastructure protection, an overview of the American approach to CIP is pertinent. The autonomy of the private sector remains a core value for much of society there. Because of this tendency, there is a strong focus on public-private partnerships and information-sharing as a solution for the defense of critical infrastructure. Still, in the case of a severe catastrophe the US military is authorized to take over operation of critical systems.[49] France implements a similar policy regarding crisis management. Article 22 of the French Military Planning attack gives the Prime Minister the authority to give orders that the private infrastructure operators "must implement."[50]

In Finland, there is one single organization that brings together public administration officials and business representatives in order to create concrete plans for securing the national infrastructure. The National Emergency Supply Council (NESC) is under the auspices of the government, but is a network of committees designated by industry. Approximately 800 people work there in order to "analyze threats against the country's security of supply, to plan measures to control these threats, and to promote readiness planning in individual industrial sites." [46][p.137]

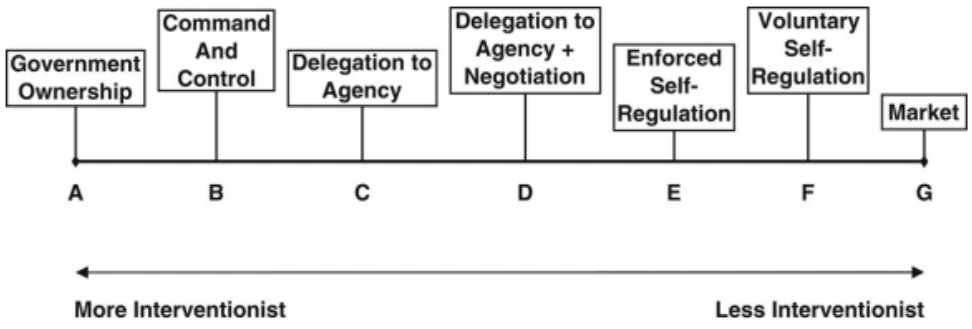


Figure 2.4. Range of Intervention in CIP

For the most part, experts agree that public-private partnerships, together with inter-industry collaboration, is the most effective way to ensure the safety of critical infrastructure.

Assaf clearly illustrates the wide range of governmental involvement in IT (see Figure 2.4). [45] Nations can choose to employ any number of approaches in order to secure their own infrastructure; however, in the very act of deciding on an approach, they accept responsibility for ensuring, to the extent possible, that a catastrophe does not occur, disrupting the heath and livelihood of citizens. The recommendation of this work is that governments employ a more interventionist PPP approach for nuclear facilities that requires and enforces compliance with specific cybersecurity standards and/or guidelines. A catastrophe would be bad not only for the national government but also businesses. Allowing the private sector to protect itself through additional security measures is ideal, but the government must also be involved to ensure that the private sector nuclear power plant operators hold up their end of the bargain. Determining the exact level of regulation and oversight for nations with nuclear power capabilities is beyond the scope of this work.

# Chapter 3

# Assessing Cybersecurity Guidelines and Standards for Nuclear Power

Guidelines and standards provide benchmarks for nuclear power plant operators to strive for to prevent cyber incidents. Compliance with standards can be one way of ensuring business continuity and can also be a tangible sign to customers to trust that company for reliable service. They can also be used by regulators to ensure cybersecurity is being properly managed at nuclear facilities.

Because nuclear power plants can be such a danger to employee and public safety, they have long needed to comply with strict regulations regarding handling of nuclear material, radiation detection, physical access control, etc. Now that nuclear plants are now needing to focus on cybersecurity, a number of standards and otherwise expert organizations have taken to devising guidelines or standards to follow. Guidelines in particular attempt to provide a step-by-step look at implementing cyber security controls. But the proliferation of these guides complicates the decision of how to secure the facilities. At present, there are eighteen countries that have plans to introduce nuclear power to their energy portfolio. [33] Given the current market and technological climate, available control systems are most likely digital and there is certainly an internet-connected enterprise network that needs to be managed. The questions that then need to be answered include the regulatory regime they will follow (2.4), whether or not they will create their own regulation based on guidelines, or just require power plants comply with specific standards. This section will review the choices available to nations in the process of developing nuclear power, as well as those modernizing and updating existing security frameworks. This thesis recommends establishing a Public-Private Partnership; but the

primary focus is on selecting the strongest possible standards and/or guidelines for adoption at a nuclear energy facility. The remainder of this work recommends paths forward for NPPs at various stages of development; regardless of the specific entity in the decision-making role.

Beyond what is examined here, there are additional resources for countries, organizations, or regulatory bodies to consult with for implementing a cybersecurity plan at a nuclear plant. Those documents considered here were specifically chosen for a number of reasons. First of all, they are more widely referenced than others and are all freely available to the public. Future studies could examine even more guides, recommendations and standards that are available for purchase. Secondly, there was a concerted effort to review comprehensive guidelines and standards. Certainly a compilation of specific standards or guidelines could be even more effective, but adding documents would also further complicate the process for the decision-making party. One example of that is the German Federal Office for Information Security (Germany) (BSI)'s 'IT-Grundschutz Methodology.' However that guide only refers to implementation of International Organization for Standardization (ISO) standards, and is not targeted towards critical infrastructure.[51] Lastly, this study chose documents that focus on the range of IT, ICS, and specifically nuclear guidance. By doing this, the essential differences between the types will be apparent and furthermore the most well-known and utilized documents will be assessed for their applicability to NPPs.

The NIST Framework for Improving Critical Infrastructure Cybersecurity (section 3.2) is the most recently developed guidance for cybersecurity and features a set of recommendations that are intended for broad use within all critical infrastructure providers (in the United States but also applicable elsewhere). It provides rather general goalposts for nations or operators to reach, therefore using this document for the baseline in a comparison was the logical choice. The Framework itself also includes mappings to some existing IT security standards. These mappings are used within this study when available.The full mapping can be found in Appendix C. The problem with the NIST Framework is that it is lacking in nuclear-specific guidance; its weaknesses are addressed further in the analysis of each examined document. A full analysis of the merits and faults of the NIST Framework can be found in section 3.2.

This project will present findings in a binary basis, either present in the NIST Framework or not. However, there are many nuances that cannot be captured by the presence or absence of a congruent recommendation. In those cases, a further

description will be included within chapter 4. Furthermore, if something is included in another document not mentioned in the NIST Framework, it will be noted in the subsequent chapter 4.

## 3.1. Expert Consultation

To obtain the perspectives of individuals most familiar with the assessed documents, I found 17 people who are employed in the cybersecurity sector of nuclear power plants, a nuclear regulatory body, and occasionally consultants for NPP. The questionnaire they were given asked them to assess their own knowledge of standards, the comprehensiveness of the documents, and based on their experiential knowledge, state which document was best for a variety of specific topics that should be included in a cybersecurity policy. The results were underwhelming. There are few people who actively work with these standards on a daily basis, after three weeks, with only seven final respondents, there could be no indicative analysis. Finding a significant number of individuals who have the expertise to assess a variety of standards/guidelines, and interpreting their knowledge of these documents is something that should be addressed in future work. Other IT employees who were contacted did not feel qualified to answer the questions because they were only following the standards and regulations they were told to follow, so their familiarity with a wide variety of documents was lacking.

Ultimately, the experts consulted worked Finland, Mexico, and the United States, they were knowledgable about the subject and had decades of experience in the nuclear field. Still, when looking at the results just from the United States, there was still no consensus. The United States has established a strict regulatory regime on cybersecurity, and yet the experts from the country had totally different perspectives on the quality and usefulness of the documents in question. The same was true of the other participants. There was no single question that resulted in any consensus.

The opinions of these experts, however, illustrates an important problem. If the cybersecurity experts of the nuclear industry are not in agreement about which standards are the most comprehensive, or well-respected, how can future regulatory bodies or plant operators make an educated decision about which guidance is suitable for their facilities? Because of this ambiguity, this project takes a statistical look and a more detailed qualitative look in order to provide objective recommendations as to which documents are the most thorough and appropriate for nuclear power

plants.

As multiple experts noted, it is a struggle to even complete the tasks of one standard; therefore the one that is chosen should be the best possible. This comparison is provided in order to give the decision-makers the most information possible about their options for cybersecurity implementation.

A full text of the questionnaire is found in Appendix D.

## 3.2. NIST Framework for Improving CI Cybersecurity (2014)

### 3.2.1. Overview

The NIST Framework [52] is a byproduct of President Barack Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." It is intended as a tool for all critical infrastructure providers, regardless of industry or size, to implement better cyber security. It specifically notes methods of protecting privacy and civil liberties. Although the NIST Framework is primarily intended for American critical infrastructure providers, the Framework is also mapped to international standards. This means that the Framework ideally acts to unite various international standards in a logical way for businesses. The structure is divided into "Tiers" that indicate different levels of cybersecurity maturity. The Framework does not recommend the highest tier for all businesses, only for those for whom the shift will significantly reduce cyber risk and be cost effective. The NIST Framework is a much more dynamic document than the majority of standards and guidelines as there is an open call for comments and suggestions for change with each iteration or update.

The instructions for implementing the guidelines clearly dictate that they "do not replace a risk management process," therefore showing that this particular document may be best utilized by facilities wanting to verify their cybersecurity risk management processes.

Figure 3.1 illustrates the categories that the Framework Core is divided into. Each category then includes an elucidation of the goals for each category. For example,

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

Figure 3.1. Organization of 2014 NIST Framework

'Access Control' (PR.AC) specifies the following: "Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions." These enumerations are useful for understanding the purpose of each specific category but ultimately are not as pertinent to this research as the even more detailed tasks, or subcategories, associated with each category. The detailed descriptions can be found in Appendix A; tasks can be seen in Appendix C.

Each of those subcategories are then mapped to a variety of standards:NIST SP800-53 [Rev.4], International Organization for Standarization/International Electrotechnical Commision (ISO/IEC) 27001:2013, COBIT 5, ANSI/ISA 62443-2-1:2009 and 62443-3-3:2013, and Council on Cybersecurity Top 20 Critical Security Controls (CCS CSC). This research utilizes the mappings of SP800-53, ISO/IEC 27001, and both ANSI/ISA standards.

The NIST Framework is unique in its clarity; the divisions among sections make implementing a risk-based cybersecurity program at a facility more manageable

and comprehensible than many other guidelines and standards available. Its introduction was particularly advantageous within the United States, where voluntary cooperation from the private sector is more desirable than increasing government regulation. The Framework itself encourages a multistakeholder approach to cybersecurity, including regulatory agencies, information-sharing networks, contractors and more.

The NIST Framework has earned a lot of respect from many different sectors and critical infrastructure providers because it has integrated many commonly accepted practices into its recommendations. By mapping each recommendation to international information technology standards it brands itself as internationally-acceptable and as an amalgamation of practices that are already common knowledge. For implementation, organizations are advised to first 'create a profile' based on sector-specific risks and existing practices, and then to compare that profile with the Framework in its entirety. Also included are designated 'tiers of cybersecurity maturity.' Tier designation provides a further benchmark for organizations to look at their own cybersecurity activities and determine if they exist at a primarily ad hoc level or if they are embedded in corporate culture and are frequently updated. (There are a total of four tiers found in Section 2.2 of the Cybersecurity Framework.

Below is a more detailed look at the Framework, as divided by function:

**Identify**

The NIST Framework, more than any other document, declares the need for identification of assets, risks, roles and responsibilities, policies, and more. Notably, it explicitly calls for the coordination of plant personnel. See, for example, ID.GV.2, which states that "information security roles & responsibilities are coordinated and aligned with internal roles and external partners." Other documents imply this cohesiveness among employees but are not nearly so explicit. While it is clear that the recommendations within this framework do not need to be implemented chronologically, nor in order, the tasks under the Identify function do provide a logical beginning for any respected risk management strategy.

**Protect**

Within the 'Awareness & Training' category, the Framework leaves much to be desired. It provided detail in relation to the stakeholders that should receive training. However, there is no clear guideline regarding the details of imparting the understanding of roles and responsibilities. Other standards and guidelines have specific recommendations for frequent trainings, or the need for simulation exercises. The

fact that there is not a hint of such thorough training processes emphasizes the need for the NIST Framework to certainly be accompanied by more detailed documents.

PR.AC-5 states "Network integrity is protected, incorporating *network segregation* where appropriate" [emphasis added]. The phrase 'network segregation' refers to the creation of zones within a network architecture to ensure that access to one area does not mean the entire operation of the NPP is compromised. One of the most commonly included security concepts in other guidance documents is a defense-in-depth strategy. Defense-in-depth is employed in order to create security levels with varied levels of defense to deter potential attackers. There are critiques of this system of defense – primarily that having a limited view of systems allows hackers to subvert detection systems that do not look for breaches in a holistic manner.[53]The defense-in-depth strategy is particularly relevant for nuclear energy facilities. Because of the volatility of the reactor core, this type of defense has been utilized as a way of creating fail-safes to prevent a catastrophic meltdown. It would be logical to mirror the physical defense-in-depth system within the digital systems present. This is a particular item that could be interpreted from the NIST Framework, but as it is not explicitly stated, could leave some NPPs without certain well-regarded security controls.

The NIST Framework also lacks a response to potential supply chain vulnerabilities. Whereas the Nuclear Energy Institute's plan has an entire section devoted to mitigating potential vulnerabilities with controls such as enforcing tamper-proof packaging for all systems[5], the NIST Framework has only one recommendation that could be construed as addressing this risk. PR.DS-6 states "integrity checking mechanisms are used to verify software, firmware, and information integrity." This specifically does not mention any hardware integrity checks or equipment acquisition policies. Given the sensitive nature of the equipment at a nuclear power plant in particular, this is an oversight that could have dangerous consequences.

It should also be noted that while the Framework does recommend that "[r]emovable media is protected and its use restricted according to policy," there is no mention of the physical disabling of unnecessary ports.

**Detect**

The NIST Cybersecurity Framework does not have specific mention of *automatic* detection/information-sharing capabilities (although this could be interpreted as being implicit within the tasks). Other than this minor issue, the Detection category is comprehensive enough even for a nuclear facility.

**Respond**

Regarding communication, the Framework recommends the frequent communication of roles and responsibilities of all personnel in all potential incidents (see RS.CO-4). This is an item that may frequently be overlooked by other groups; the importance of communication is very clear within the Framework. Generally speaking, the response category is intentionally vague. There is little that can be found in other guidance documents that so simply states "Response plan is executed during or after an event", as this is presumed obvious. Additionally, this Framework is not thorough in regard to ensuring proper documentation of all cyber incidents. While documentation is a standard practice for IT professionals, for the sake of comprehensiveness this aspect could be more adequately addressed.

**Recover**

Again, for the Recover function, the NIST Framework covers quite well a variety of activities from the actual technical recovery, to the improvement of recovery strategies and even to public reputation management. These items may frequently be considered under the purview of business leaders; however, in the case of a cyber incident there does need to be coordination amongst the entire workforce.

**Disadvantages**

Despite the advances that have been made due to the NIST Framework, there are certainly some disadvantages to providing only one Framework for all critical infrastructure providers. For nuclear facilities in particular, safety is a core component that must be considered in every aspect of security, both physical and cyber. This is briefly considered in ID.RM-3 –"The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis." This one mention of including sector-specific risk factors does not permeate the whole guidance in the way many documents specifically for nuclear facilities do. In that way, this document can only serve as guidance for nuclear power plants to a limited extent. With some effort, the managers or regulators of nuclear power plants can find further guidance on the matter but there would still be frequent reiterations of recommendations in the NIST Framework as well.

In general, the simplicity and streamlined package that the NIST Framework exhibits means that it leaves many nuances of cybersecurity up to interpretation. For example, the recommendations do not specifically reference how sensitive security information should be stored; nor do they specify that facilities should be tracking and documenting all incidents. There are many things that other guidelines include that the Framework does not; still, it remains an important piece of guidance for

many CIP.

*Recommendation:* This document should be utilized by organizations with a strong existing cybersecurity program, who use it only to ensure that they have not excluded any important aspect. In its current form, the Framework lacks the detail to be an inclusive implementation guide for those looking to take their security to the next level (or tier, as the Framework calls it). It provides a very strong baseline from which to look at other similar cybersecurity documents even if nuclear-specific guidance must be added.

### 3.2.2. Justification of Framework as Comparative Basis

As illustrated above, the NIST Framework is not an all-encompassing guideline for cybersecurity at nuclear facilities. There are perhaps areas where it over-emphasizes certain activities, and it certainly lacks recommendations that are necessary specifically for nuclear power plants. However, the Framework is constructed in such a manner that its recommendations cannot be unambiguously implemented; they encompass a variety of tasks that are included in other cybersecurity documents. In general, the NIST Framework has a solid base of activities that are consistently recommended for cyber risk mitigation implementations. The subsequent statistical analyses use the NIST Framework as a baseline for its overarching recommendations and comprehensiveness. The Framework's paucity of nuclear-specific guidance, or other more detailed recommendations, will be addressed by chapter 4's analyses.

## 3.3. Introduction to Assessed Guidance

The following section reviews the guidelines and standards chosen for comparison in this study.

### 3.3.1. Guidelines

Guidelines are intended as a way to steer companies into creating strong security practices and policies, without imposing a limiting and specific set of controls on

them. For most companies, this is a welcome freedom from the regulating exactness of national government. For others, taking guidelines and expanding them to a coherent and secure policy may be extremely taxing as opposed to implementing predetermined regulations. Other times, in the cases of Nuclear Energy Institute (NEI)'s and the Nuclear Regulatory Commission (NRC)'s guidelines, guidelines provide explicit instructions to fulfilling existing requirements.

Almost all guidance for cybersecurity for NPPs in particular is in the form of guidelines. International organizations such as the IAEA and World Institute for Nuclear Security (WINS) are key nuclear leaders with the experience and expertise to provide specific guidance. The NEI and NRC documents are based on the American regulation for cybersecurity at nuclear plants. Lastly, NIST's SP800-53 and SP800-82 are guidelines that focus on broad cybersecurity recommendations; the latter provides more granular ICS guidance.

The guiding documents being considered for nuclear power plants (or more generally ICS) are as follows:

- IAEA Computer Security Guidelines[4]
- NEI 08-09 [Rev.6] Cyber Security Plan for Nuclear Power Plants [5]
  - NRC Regulatory Guide 5.71 [6]
- NIST SP800-53 [7]
  - NIST SP800-82 [43]
- WINS 4.3 Security of IT and IC Systems at Nuclear Facilities [8]

Each of these, with the exception of NIST SP800-53 and SP800-82, can be seen as standalone guides to implementing cybersecurity at a nuclear power plant. This section will look at each individually as well as comparatively in order to give an accurate assessment of strengths and weaknesses of each document.

### 3.3.2. Standards

Standards provide more certainty within a facility, because compliance is rewarded with a certification. While compliance should not be the operators' sole objective,

providing a target to reach can be effective for incentivizing increased and hardened cybersecurity.

There are few standards available specifically for nuclear energy facilities. The majority of advice available for such facilities is currently in the form of guidance documents or national regulations. This study aims to look at the most comprehensive standards available. There are numerous standards for information technology that have been studied in much more depth because of their wide applicability. For that reason, the IT standard being compared in this study is the highly regarded ISO 27001. Other similar standards are documented in the NIST Cybersecurity Framework and other NIST publications. Therefore the ISO standard will represent a range of IT standards.

Beyond IT standards, there are few standards that address the gamut of potential cybersecurity issues within an ICS or nuclear facility. Many of them are control-specific, such as the Institute of Electrical and Electronics Engineers (IEEE) Standards. The IEEE organization is well-known for creating standards for a wide range of technologies in use today such as the Wi-Fi or 802.11 standard.[54] Still, this organization that is clearly very knowledgeable about the threats and opportunities present with digital technology has their guidance for nuclear power plants divided in a highly segmented manner. The United States North American Electric Reliability Corporation (NERC) also openly publishes its standards for energy producers. Their guidance is widely available and has been recently updated to reflect increased knowledge. Therefore this study will also include an analysis of the NERC CIPv5 standard group. [12] The International Electrotechnical Commission (IEC) created a cybersecurity standard specifically for nuclear power facilities. Unfortunately this standard is not freely available, therefore an analysis of IEC 62645:2014 is recommended for future studies. [55]

Standards examined in this work:

- IEEE 692-2013 [9]
- ISO/IEC 27001 [10], [11]
- NERC CIP v5 [12]
- ANSI/ISA 62443-2-1:2009 [13]
- ANSI/ISA 62443-3-3:2013 [14]

## 3.4. Statistical Analysis

This research project provides sound judgment and recommendations for use of cybersecurity guidance. To do so, it must in turn produce a unequivocally objective assessment. The following section utilizes a combination of the mappings already provided by the NIST Framework and the author's own mappings to provide a clear assessment of the issues present in each standard or guideline see Appendix C. By utilizing a statistical analysis, this project introduces an objective measure of variation amongst documents, thus providing a clear analysis of the available landscape of cybersecurity guidance for nuclear power plants. This method furthermore is necessary for a thorough analysis of the strengths and weaknesses of each document by function, and by category.

The first section looks at the specific methods used for the following analyses. The subsequent sections are divided based on the aspect of the documents that are being investigated.

### 3.4.1. Methods

Once the guidelines and standards were chosen, the next step was to create a way to be able to understand the content (or lack thereof) within those documents. The typical method of comparison for standards is a mapping. This is done particularly when a new document or framework is released to make it clear to the end users of the document what is new and what they have already implemented. Many have used this technique to illustrate the connection between standards; while others still have used this technique to determine how well each document conforms to privacy guidance. [56], [57]

The NIST Framework, as mentioned in 3.2.2, is ideal for this kind of comparison because it included a basic mapping to multiple standards and one guideline. To complete the mappings for nuclear specific documents, the specific sections that included implementation guides were chosen in order to identify the activities that will fall into the subcategories of the NIST Framework. Hence, the process for creating the mapping was examine each section of the particular document and find where in the NIST Framework that is addressed. If the document included multiple, more detailed instructions, those were included directly within the mapping, but not

in the statistical analysis because the NIST Framework itself does not provide a high level of detail. Items that were either not at all mentioned in the Framework or were examples of extremely detailed instructions were noted down and are included in chapter 4.

To interpret those mappings into quantifiable data, if there were any matching items present for a given subcategory, that document would get one point for that subcategory. There are many instances of there being more sections referenced for a single subcategory, however number of sections does not delineate depth of coverage, therefore quantity of congruent sections are not included in this research. Total points were then summed for each category and for each document as seen in Figure 3.2 below. This particular table demonstrates the difference between the NIST Framework and the standards/guidelines examined in this study. Figure 3.3 in the following subsection provides a further comparison of each category's presence in all of the documents.

| GUIDELINE & STANDARD ASSESSMENT | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Function | Category Unique Identifier | Category | # of Subcategories (NIST Framework) | Guideline Documents Compared | | | | | Standards Compared | | | |
| | | | | IAEA CSG | NEI 08-09 | NRC 5.71 | NIST SP800-53 | WINS 4.3 | ISO/IEC 27001 | NERC CIPv5 | ANSI/ISA 62443-2-1:2009 | ANSI/ISA 62443-3-3:2013 |
| IDENTIFY (ID) | ID.AM | Asset Management | 6 | 5 | 5 | 6 | 6 | 6 | 4 | 5 | 2 | |
| | ID.BE | Business Environment | 5 | 1 | 2 | 0 | 5 | 4 | 3 | 0 | 1 | 0 |
| | ID.GV | Governance | 4 | 3 | 1 | 3 | 4 | 4 | 3 | 1 | 3 | 0 |
| | ID.RA | Risk Assessment | 6 | 3 | 5 | 5 | 6 | 6 | 4 | 2 | 4 | 0 |
| | ID.RM | Risk Management Strategy | 3 | 2 | 1 | 2 | 3 | 3 | 0 | 0 | 2 | 0 |
| PROTECT (PR) | PR.AC | Access Control | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 |
| | PR.AT | Awareness and Training | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 3 | 5 | 0 |
| | PR.DS | Data Security | 7 | 2 | 5 | 7 | 7 | 4 | 7 | 0 | 1 | 6 |
| | PR.IP | Information Protection Processes and Procedures | 12 | 7 | 10 | 12 | 12 | 9 | 11 | 6 | 10 | 5 |
| | PR.MA | Maintenance | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 0 |
| | PR.PT | Protective Technology | 4 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 2 | 4 |
| DETECT (DE) | DE.AE | Anomalies and Events | 5 | 2 | 5 | 2 | 5 | 3 | 1 | 1 | 3 | 2 |
| | DE.CM | Security Continuous Monitoring | 8 | 5 | 8 | 8 | 8 | 6 | 5 | 6 | 3 | 4 |
| | DE.DP | Detection Processes | 5 | 1 | 3 | 5 | 5 | 3 | 5 | 3 | 5 | 2 |
| RESPOND (RS) | RS.RP | Response Planning | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| | RS.CO | Communications | 5 | 2 | 3 | 3 | 5 | 4 | 3 | 3 | 4 | 0 |
| | RS.AN | Analysis | 4 | 0 | 3 | 2 | 4 | 3 | 4 | 1 | 3 | 2 |
| | RS.MI | Mitigation | 3 | 1 | 3 | 3 | 3 | 2 | 3 | 3 | 2 | 1 |
| | RS.IM | Improvements | 2 | 0 | 1 | 2 | 2 | 1 | 1 | 2 | 1 | 1 |
| RECOVER (RC) | RC.RP | Recovery Planning | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| | RC.IM | Improvements | 2 | 0 | 1 | 2 | 2 | 0 | 0 | 2 | 0 | 0 |
| | RC.CO | Communications | 3 | 0 | 1 | 1 | 1 | 2 | 0 | 0 | 0 | 0 |
| | | Total Congruent Recommendations | 98 | 50 | 72 | 81 | 96 | 77 | 74 | 50 | 62 | 33 |
| | | Percentage of NIST Framework | 100 | 51.0 | 73.5 | 82.7 | 98.0 | 78.6 | 75.5 | 51.0 | 63.3 | 33.7 |

Figure 3.2. Primary Data Table: Comparison of Overall Congruence with NIST Framework

**Analysis of Variance:** This technique is used to determine the variation between two or more means. In this specific project, the null hypothesis is that there is no difference between the documents; the alternative hypothesis is that there is a significant different between documents. The process is as follows. First, calculate the means for each document. Next, calculate the overall mean. The next step is to

calculate the sum of squares of both between the documents, and within the group.

$$F = \frac{between - groupvariability}{within - groupvariability}$$

Finally, the F-ratio is compared to a table of p-values to determine whether the null or alternative hypothesis is confirmed.

**Average:**

$$\mu = \sum(\frac{x}{N})$$

The average $\mu$ is an indicator on how many topics in the mean can be mapped to the NIST framework $x$ equal the mapped values of the individual standards and guidelines whereas $N$ is the number of guidelines we looked at in total.

**Variance:**

$$\sigma^2 = \frac{\sum(X - \mu)^2}{N}$$

The variance $\sigma^2$ measures how far a set of numbers are spread out. A variance of zero indicates that all the values are identical. Variance is always nonnegative: a small variance indicates that the data points tend to be very close to the mean (expected value) and hence to each other, while a high variance indicates that the data points are very spread out around the mean and from each other.

**Standard deviation:**

$$\sigma = \sqrt{\frac{\sum(X - \mu)^2}{N}}$$

The standard deviation $\sigma$ indicates how far data deviates from the mean $\mu$. The standard deviation has the same dimension as the data, and is therefore comparable to deviations from the mean.

### 3.4.2. Overall Comparison

As mentioned in the above section, the Analysis of Variance (ANOVA) method measures the variance between guidelines and standards. This test was run both on the group of guidelines, and the group of standards. For guidelines, the F-ratio determines whether the average for each document differ significantly. The initial hypothesis is that the each of the documents are different enough that their variation can also be shown using statistics. Between the guideline documents in particular the F-ratio is 2.35. To determine if this number is statistically significant, the p-

value is then found. In this case the p-value is .044838, and because the p-value must be less than .05 to be considered statistically signficant, it can be determined that the differences between guideline documents is considerable.

Amongst the standards included in this study, the F-value (5.3) implicates an even larger discrepancy between standards than there is between guidelines. The associated p-value is then .0006, illustrating the apparent incompatibilities between cybersecurity standards available to NPPs.

This analysis clearly demonstrates that the options available to nuclear facility operators and potentially the organizations tasked with regulating them are not created equally. They are statistically different from each other; the strengths of the documents are varied amongst different categories or tenets of a cybersecurity implementation.

### 3.4.3. Comprehensiveness

Based on the assessment of the NIST Framework as the currently most comprehensive cybersecurity guidance available for NPP, the level of compatibility of a document with the NIST Framework is therefore one measure of how comprehensive it itself is. Although the NIST Framework is not an exhaustive document, specifically for nuclear facilities, it does address the core aspects of cybersecurity that need to be practiced in any CI facility.

Figure 3.2 shows the percentage of each document that matches with the NIST Framework. Take the IAEA Computer Security Guidelines, for example. [4] Even though there may be valuable information about how to tailor a cybersecurity plan to be specific for the needs of a NPP, it does not come close to being as comprehensive as the NIST Framework, which means it could is not recommended to be implemented on its own as the primary guiding document for cybersecurity at a facility. At the same time, however, just because NIST SP800-53 matches more closely with the NIST Framework does not mean that it is therefore the most ideal instrument to base a cybersecurity regime off of. There are further details that cannot be covered by this data set. The nuances of each document is reviewed in the next chapter (chapter 4).

The total congruence between the chosen documents and standards and the NIST

Framework moreover demonstrates the incompleteness of the standards. Any standard chosen does not address all issues that the NIST Framework does, and therefore surely there are areas of a security implementation that must be sacrificed through the mere act of choosing a particular standard to comply with.

### 3.4.4. Individual Security Controls

In order to compare the documents' level of completeness within each category, the average, variance, and standard deviation was calculated. The categories represent important groups of security controls that should be implemented in any (critical IT) facility. The first standard deviation as shown in the chart below compares the documents to each other based on the mean. From this information it can be shown which categories are the most variable amongst the assessed guides. For example, access control is thoroughly addressed in nearly all of the documents. However, whether a document recommends extensive risk assessment measures depends greatly on which one is chosen. For example, one cannot assume that any of the documents chosen will have similarly complete Information Protection Processes and Procedures due to the high deviation within the guides. The same can be said of the Business Environment category as well as Data Security. For decision-makers, this data means that when selecting a guide for cybersecurity at a NPP, they should ensure that a solid range of activities is recommended. If not, it is perhaps wise to augment that document with another with a stronger record for the deficient categories. This comparison acts as an initial step to understanding the strengths and weaknesses of the guides available.

| Document | IDENTIFY (ID) | | | PROTECT (PR) | | | | DETECT (DE) | | | | RESPOND (RS) | | | | RECOVER (RC) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Asset Management | Business Environment | Governance | Risk Assessment | Risk Management Strategy | Access Control | Awareness and Training | Data Security | Information Protection Processes and Procedures | Maintenance | Protective Technology | Anomalies and Events | Security Continuous Monitoring | Detection Processes | Response Planning | Communications | Analysis | Mitigation | Improvements | Recovery Planning | Improvements | Communications |
| NIST CSF | 6 | 5 | 4 | 6 | 3 | 5 | 5 | 7 | 12 | 2 | 4 | 5 | 8 | 5 | 1 | 5 | 4 | 3 | 2 | 1 | 2 | 3 |
| IAEA CSG | 5 | 1 | 3 | 3 | 2 | 5 | 5 | 2 | 7 | 2 | 4 | 2 | 5 | 1 | 0 | 2 | 0 | 1 | 0 | 0 | 0 | 0 |
| NEI 08-09 | 5 | 2 | 1 | 5 | 1 | 5 | 4 | 5 | 10 | 1 | 4 | 5 | 8 | 3 | 1 | 3 | 3 | 3 | 1 | 0 | 1 | 1 |
| NRC 5.71 | 6 | 0 | 3 | 5 | 2 | 5 | 5 | 7 | 12 | 2 | 4 | 2 | 8 | 5 | 1 | 3 | 2 | 3 | 2 | 1 | 2 | 1 |
| NIST SP800-53 | 6 | 5 | 4 | 6 | 3 | 5 | 5 | 7 | 12 | 2 | 4 | 5 | 8 | 5 | 1 | 5 | 4 | 3 | 2 | 1 | 2 | 1 |
| WINS 4.3 | 6 | 4 | 4 | 6 | 3 | 5 | 5 | 4 | 9 | 2 | 3 | 3 | 6 | 3 | 1 | 4 | 3 | 2 | 1 | 1 | 0 | 2 |
| ISO/IEC 27001 | 6 | 3 | 3 | 4 | 0 | 5 | 5 | 7 | 11 | 2 | 4 | 1 | 5 | 5 | 1 | 3 | 4 | 3 | 1 | 1 | 0 | 0 |
| NERC CIP v5 | 4 | 0 | 1 | 2 | 0 | 5 | 3 | 0 | 6 | 2 | 4 | 1 | 6 | 3 | 1 | 3 | 1 | 3 | 2 | 1 | 2 | 0 |
| ANSI/ISA 62443-2-1:2009 | 5 | 1 | 3 | 4 | 2 | 5 | 5 | 1 | 10 | 2 | 2 | 3 | 3 | 5 | 1 | 4 | 3 | 2 | 1 | 0 | 0 | 0 |
| ANSI/ISA 62443-3-3:2013 | 2 | 0 | 0 | 0 | 0 | 4 | 0 | 6 | 5 | 0 | 4 | 2 | 4 | 2 | 0 | 0 | 2 | 1 | 1 | 0 | 0 | 0 |
| Average | 5.00 | 1.78 | 2.44 | 3.89 | 1.44 | 4.89 | 4.11 | 4.33 | 9.11 | 1.67 | 3.67 | 2.67 | 5.89 | 3.56 | 0.78 | 3.00 | 2.44 | 2.33 | 1.22 | 0.56 | 0.78 | 0.56 |
| Variance (mean) | 1.56 | 3.06 | 1.80 | 3.43 | 1.36 | 0.10 | 2.54 | 6.67 | 5.88 | 0.44 | 0.44 | 2.00 | 2.99 | 2.02 | 0.17 | 1.78 | 1.58 | 0.67 | 0.40 | 0.25 | 0.84 | 0.47 |
| Standard Deviation (mean) | 1.25 | 1.75 | 1.34 | 1.85 | 1.17 | 0.31 | 1.59 | 2.58 | 2.42 | 0.67 | 0.67 | 1.41 | 1.73 | 1.42 | 0.42 | 1.33 | 1.26 | 0.82 | 0.63 | 0.50 | 0.92 | 0.68 |
| Variance (NIST) | 2.56 | 13.44 | 4.22 | 7.89 | 3.78 | 0.11 | 3.33 | 13.78 | 14.22 | 0.56 | 0.56 | 7.44 | 7.44 | 4.11 | 0.22 | 5.78 | 4.00 | 1.11 | 1.00 | 0.44 | 2.33 | 6.44 |
| Standard Deviation (NIST) | 1.60 | 3.67 | 2.05 | 2.81 | 1.94 | 0.33 | 1.83 | 3.71 | 3.77 | 0.75 | 0.75 | 2.73 | 2.73 | 2.03 | 0.47 | 2.40 | 2.00 | 1.05 | 1.00 | 0.67 | 1.53 | 2.54 |
| Percentage Variation | 0.27 | 0.733 | 0.51 | 0.47 | 0.6 | 0.1 | 0.4 | 0.53 | 0.3143 | 0.4 | 0.2 | 0.5 | 0.3 | 0.41 | 0.5 | 0.48 | 0.5 | 0.4 | 0.5 | 0.7 | 0.8 | 0.8 |

Figure 3.3. Complete Assessment of Standard Deviation for Standards & Guidelines

Figure 3.3 furthermore displays the deviation from the NIST Framework for each category. Rather than showing the variability just between the available documents, the data in this case highlights the categories for which documents can vary substantially from the NIST Framework. Still, as mentioned before, there are differences between documents not addressed by this data set (but will be covered in chapter 4). However, what this information does provide is an initial understanding of the categories for which the NIST Framework recommends a more comprehensive plan, and where a decision-maker needs to pay close attention if aiming to utilize a document at least as thorough as the NIST Framework. Because the standard deviation could be misleading given the disparity between the size of each category, the percentage variation was added for additional clarity.

The percentage in the lowest row in Figure 3.3 provides the amount that documents typically stray from the NIST Framework. When looking specifically at the Awareness and Training category, there is on average a 40% difference between the document and the NIST Framework. The numbers are much larger in the Recover function, however because the amount of subcategories is so few, the high percentages are less meaningful (although the lack of guidance regarding recovery is an issue that should be considered when choosing to follow a guide.) The least deviation from the NIST Framework occurs in Access Control, Protective Technology, Asset Management, and Security Continuous Monitoring. For these categories, there is a higher chance that a chosen document will have sufficient recommendations. The categories in which the documents tend to differ the most from the Framework are: Business Environment, Response Planning, Communications, Data Security, Risk Management Strategy, and Governance. The disparities between the documents based on category are striking. Evaluating which guide to implement would be incredibly taxing for an operator or regulatory body. The differences on these few categories could make a large impact on the security of the facility, so thoroughness is necessary, and as previously mentioned, another document may need to be utilized to offset any deficiencies in a particular category.

### 3.4.5. Results

The concrete results and recommendations that have been elicited through the statistic methods used on this data set are the following:

1. **The documents are in fact significantly different from one another.** By identifying the discrepancy amongst the selected guides, the need for this comparison becomes even more evident. There must be a simplified process for those making decisions about the cybersecurity of nuclear power plants, otherwise there is a chance an implementation will be put into place without full recognition of its weaknesses.

2. **Certain categories are more likely to differ amongst documents.** Such categories should be examined especially well to ensure that the necessary security activities are completed. This implies the need for a thorough selection process as not every document provides adequate instruction on Data Security, for example.

3. **Certain categories stray further from the NIST Framework than is desirable.** Those utilizing the guidance from these documents for a cybersecurity regime should ensure that the majority of the NIST Framework is addressed, at a minimum. At present, this means utilizing multiple documents and potentially even others to account for flaws in the NIST Framework itself.

The following chapter addresses each document's idiosyncracies and nuances that could not be included in this statistical analysis. The final section will combine them to produce recommendations for current and future arbiters of cybersecurity at NPPs.

# Chapter 4

# Comprehensive Analysis of Guidelines and Standards

The previous chapter provided a broad, statistical overview of the documents being considered for this research. The purpose of this chapter, on the other hand, is to complement those values with qualitative assessments in order to highlight the wide range and complexity of each document. The NIST Framework, though the most comprehensive Framework currently available, is not all-inclusive for cybersecurity implementations at NPPs.[52] The subsequent analyses will first provide general information about the guide in question, an overall comparison to the NIST Framework, then address each function (Identify, Protect, Detect, Respond, Recover). Not every subcategory will be mentioned; they will be included only if they differ significantly from other guidance. If there are aspects that are incongruent with the NIST Framework but are still worth consideration, they will be included at the end. Finally, a recommendation for use of this specific document will be provided. Further recommendations can be found in the final chapter.

## 4.1. Guidelines

The guidelines investigated below are primarily nuclear focused but also cover more general IT/ICS guidance. The reasons for their selection are included in section 3.3.

### 4.1.1. IAEA Computer Security Guidelines

The International Atomic Energy Agency published in 2011 a technical guidance document for computer security at nuclear facilities. The IAEA used the collective knowledge of willing member countries and international experts to compile these recommended controls. The purpose behind this document was to acknowledge that many guidelines for cybersecurity are not directly applicable to nuclear facilities. This international document illustrates cybersecurity implemention methods at nuclear facilities specifically. Moreover, this guidance has a targeted focus on preventing malicious actions that could lead to a breakdown in physical safety of the employees, the environment, or the general populace. The IAEA Guidelines place a much lesser emphasis on business continuity and reputation than publications for a more industry-specific audience, like the NIST Framework. The overall similarities between the IAEA Guidelines and the NIST Framework are presented in Figure 4.1 below.

| Comparison between IAEA Computer Security Guidelines & NIST Framework (baseline) | | | | | | |
|---|---|---|---|---|---|---|
| Function | IDENTIFY (ID) | PROTECT (PR) | DETECT (DE) | RESPOND (RS) | RECOVER (RC) | Totals |
| NIST Framework | 24 | 35 | 18 | 15 | 6 | 98 |
| IAEA CSG | 14 | 25 | 8 | 3 | 0 | 50 |
| Δ | 10 | 10 | 10 | 12 | 6 | Δ 48 |
| % Similarity | 58.33 | 71.43 | 44.44 | 20.00 | 0.0 | 51.02 |

Figure 4.1. NIST Framework and IAEA Computer Security Guidelines by Function

The above chart demonstrates the lack of detail and comprehensive guidance across the board in all five functions presented by the NIST Framework. From this perspective, the IAEA Guidelines are not particularly instructive; however they are one of few documents that chiefly target the controls necessary for nuclear systems.

Security levels are an important aspect of these guidelines, as they indicate separation amongst different systems within a plant, based on how important the provided function is. The assessment presented here is based on the Implementation Guide of the IAEA Guidelines; many of the controls that are noted in the document are categorized based on security level. Accordingly, throughout the recommendations there is a significant focus on ensuring best practices even for systems that are not as critical as others.

#### Identify

The Identify function is reasonably well-populated by advice from the IAEA. This section is also supplemented by other resources, such as a list of potential threat actors and vulnerabilities.

Business continuity is not at all mentioned in this guide, so for the majority of NPP owners, this can be considered a substantial drawback.

**Protect**

Within the nuclear industry, maintenance is something that must be done with the utmost of care. Item 7.4 in the guidelines implores the organization to make a distinction between normal maintenance and system modifications that would require the equipment be retested or recertified. These guidelines also provide a comparison of IT security as opposed to ICS security that includes information as to difference in the norms of maintenance, of receiving outside support for components, the prioritization of functions, and more.

As to this document's risk assessment recommendations, it follows the general path that the NIST Framework does, with identification, protection, mitigation and recovery techniques. There are many similarities in the protection function, for example (as seen in 4.1). The NIST Framework has 35 subcategories for which the IAEA Guidelines have 25 similar recommendations.

**Detect**

Unfortunately, not specifically naming tasks such as detecting unauthorized malicious or mobile code, could mean that some power plants will not place adequate emphasis on these issues, thus leaving them in a weakened state of security.

**Response & Recovery**

The downside of this document, though understandable, is the lack of attention to response and recovery. While a nuclear meltdown or other extreme loss of control at a nuclear facility would be disastrous, there should still be sufficient guidance on response, especially for the investigation of suspicious activities or alerts. Any incident with the potential to have such a large impact on the community around it should be addressed systematically, ideally curbing some of the damage before it affects a wider area.

Where the IAEA advice differs is in its explicit recommendation that attack scenarios are constructed. The motivation of the attacker plays a much more important role in these guidelines than in generic or primarily IT-focused ones. This is common for nuclear security, where the Design Basis Threat (DBT) is a necessary calculation.

Deficiencies in this document can be attributed to assumption that they would be included through other security activities, or are more generally assumed as in the

case of response and recovery.

*Recommendation:*
Despite not being a fully comprehensive document, this is necessary reading for security officers with knowledge of IT standard practices, but need further education on securing ICS and specifically nuclear equipment. The IAEA Computer Security Guidelines would furthermore be useful for newly founded nuclear regulatory authorities as this document addresses the roles of legal and regulatory frameworks in conjunction with technical guidance.

### 4.1.2. NEI 08-09 [Rev.6] Cybersecurity Plan for Nuclear Power Plants

This guiding document for nuclear power plants was created by the independent Nuclear Energy Institute (NEI) in the United States. Its original intention was to be a tool for plant operators to use to meet federal mandate 10 CFR 73.54. [58] Where the regulation is vague, the NEI document breaks the requirement down into smaller tasks. 10 CFR 73.54 established 18 requirements for facilities and NEI details how to achieve them by focusing on detailed technical tasks. NEI's ultimate purpose for creating this guide was, like the IAEA's and this thesis', to prevent substantial harm from being inflicted on the environment or on human beings. The guidance has two appendixes that give detailed guidance for plant security personnel. The first, Appendix D, provides technical security controls while Appendix E provides organizational and management level recommendations.

The figure below demonstrates the guide's compatibility with the NIST Framework.

| Comparison between NEI 08-09 & NIST Framework (baseline) | | | | | | |
|---|---|---|---|---|---|---|
| Function | IDENTIFY (ID) | PROTECT (PR) | DETECT (DE) | RESPOND (RS) | RECOVER (RC) | Totals |
| NIST Framework | 24 | 35 | 18 | 15 | 6 | 98 |
| NEI 08-09 | 14 | 29 | 16 | 11 | 2 | 72 |
| Δ | 10 | 6 | 2 | 4 | 4 | Δ 26 |
| % Similarity | 58.33 | 82.86 | 88.89 | 73.33 | 33.3 | 73.47 |

Figure 4.2. NIST Framework and NEI 08-09 Guidelines by Function

**Identify**
Within NEI's guidelines, there is not a focus on the risk management process. Instead, the items that correspond with the Identify function are a part of response and protection activities; rather than being highlighted separately.

**Protect**

There is a large emphasis on items within the Protect function. Key among these are the sections that focus on ensuring functioning security tools, access control capabilities, and security training for personnel. It specifically recommends lengths of passwords, how to protect databases where passwords are stored, setting a limit for number of unsuccessful login attempts. Like the IAEA's guidelines, special emphasis is also given to the scheduling and implementation of software upgrades. As illustrated by the shutdown at the Hatch nuclear plant in 2008 (section 2.2), patches can be extremely disruptive for plant functioning. This aspect is something that is included in almost all guidance for nuclear facilities but is not found in guidance for critical infrastructure more broadly.

The NEI Plan additionally houses an entire section focused on hardening against potential supply chain vulnerabilities (see Appendix E, 3.7 and 11). This includes ensuring a high level of trust in the equipment security (including software) and the validation of all vendors.

Furthermore, unlike the NIST Framework, NEI does not specifically recommend that senior executives understand their roles and responsibilities in the event of an incident.

**Respond**

From an organizational perspective, this document continues to be extremely detailed. Instead of merely calling for testing of response plans, this guide indicates a recommended frequency for those tests and insists that there be announced and unannounced tests in order to ensure a maximum level of preparedness amongst the staff. In fact, this document is extremely strong in its response-planning. As shown in Figure 4.2 NEI 08-09 corresponds with the majority of the subcategories in the Respond (RS) category of the NIST Framework (11 out of 15). However unlike the NIST document, NEI details the formation of a Computer Security Incident Response Team (CSIRT) to respond to incidences and requires there be response personnel available 24 hours a day, every day of the year. This in itself is a much stronger recommendation, though it blatantly provides less room for creativity than the baseline Framework.

**Recover**

There is very little in this document that focuses on recovery and reputation management (2 out of 6 of the NIST recommendations.) It is in these instances that the goal of preventing a major nuclear disaster seems to usurp other goals that will

be essential for business operation. Particularly given that neither reputation management nor the knowledge of senior executives are specifically mentioned, there is much to be desired from a business continuity perspective.

The NEI 08-09 is more detailed than many other guidance documents reviewed in this work. That is true primarily because of the requirements enforced by the American Nuclear Regulatory Commission. In order for a nuclear facility to continue operating, it is imperative that they reach these requirements. For that reason it is far more comprehensive and detailed than other guidelines.

Lastly, this guide provides many requirements focused on preserving data confidentiality and integrity and on ensuring proper documentation of any and all incidents. Recommendations such as the one found in Appendix E (5.6) that requires documentation of all physical access to the facility or to the equipment is essential, particularly for investigating incidents and performing forensic analysis. [5] This harks back to the fact that thorough documentation is required by 10 CFR 73.54; however adequate documentation will also increase accountability and will provide additional information for future investigations into incidents.

The NEI Plan maps closely to the NIST Cybersecurity Framework. If it were to be expanded to have items focused on mapping organizational communication, on protecting civil liberties, continuous improvement and incident recovery plans, this guide could in fact be considered one of the most comprehensive for cybersecurity at nuclear energy facilities. Some of the deficiencies in NEI's guidance can be seen in the comparison in Figure 4.2.

*Recommendation:*
Because of the included in the NEI 08-09 [Rev. 6] Plan, it would be ideal for first-time plant operators beginning to institute cybersecurity measures. Similar to the IAEA Guidelines, it is something that is more useful from a government perspective than a business one but would regardless reduce the chance of a major incident occurring.

Note: The NEI 08-09 Plan is very similar to the NRC Regulatory Guide 5.71 intended to provide a guide to implementing 10 CFR 73.54. While there are some differences between the two guidance documents, they both do not warrant full coverage. However the mapping of both to the NIST Framework can be found in Appendix C.

### 4.1.3. NIST SP800-53 [Revision 4]

NIST created SP800-53, or 'Security and Privacy Controls for Federal Information Systems and Organizations,' as a non-binding guide for ensuring security within federal information systems. As stated within the guidance itself, it is intended as a tool for operators to exercise necessary due diligence (as opposed to mere compliance) when implementing cyber security plans. This document does not recommend immediate implementation of suggested guidance; rather, it encourages caution and a risk-based approach when implementing any new controls. Despite the fact that SP800-53 is intended for federal information systems in the United States, and recommends compliance with specific American regulations, it also is unique in that it addresses the need for privacy controls in conjunction with a solid cybersecurity plan. This aspect could be beneficial for other nations that may perhaps have stricter privacy regulations in place.

This document is complex, lengthy, and is an excellent guide for IT systems, but not necessarily for ICS or nuclear facilities. It has become clear through the analysis of nuclear specific recommendations that there are certain practices or policy items that are unusual for a typical cybersecurity implementation. Therefore SP800-53 near congruence with the NIST Framework means that it is also lacking guidance that may be specifically useful for nuclear energy facilities. The only items for which the NIST Framework is more thorough are RC.CO-1 and 2 ("Public relations are managed" and "Reputation after an event is repaired.")

SP800-53 goes into far more detail than the NIST Framework. Clearly, the number of items it that map to a single phrase in the Framework make it evident that SP800-53 is a thorough implementation guide, and can be used as such. (See Figure 4.3). Where it is less thorough, for example, in sector-specific, ICS-based facilities like NPP, the creators of the standard recommend further overlays that would eliminate the need for unnecessary redundancy amongst standards.

| Comparison between NIST SP800-53 & NIST Framework (baseline) | | | | | | |
|---|---|---|---|---|---|---|
| | IDENTIFY (ID) | PROTECT (PR) | DETECT (DE) | RESPOND (RS) | RECOVER (RC) | Totals |
| NIST Framework | 24 | 35 | 18 | 15 | 6 | 98 |
| NIST SP800-53 | 24 | 35 | 28 | 15 | 4 | 96 |
| Δ | 0 | 0 | 0 | 0 | 2 | Δ 2 |
| % Similarity | 100.00 | 100.00 | 155.56 | 100.00 | 66.7 | 97.96 |

Figure 4.3. NIST Framework and NIST SP800-53 by Function

Structurally speaking, SP800-53 provides a standard-like format that can be implemented in order to ensure no aspects of security were overlooked. It also provides

varied levels that allow facilities to tailor the recommendations to their individual situations. Below each recommendation the document offers supplemental guidance for implementing the control.

*Recommendation:*
A cyber security team with experience in nuclear facilities could take this document and apply it successfully to a plant. For ensured comprehensiveness, this document would need to be implemented in conjunction with ICS and/or nuclear guidance, such as NIST SP800-82. Even though it is intended for use within the federal government, its applicability extends far beyond that, potentially even to other regions of the world.

### 4.1.4. NIST SP800-82

The NIST SP800-82 document is an add-on for SP800-53 that addresses specific controls that are necessary for protecting ICS operation as opposed to IT operation. It was most recently updated in 2015. The security objectives present in this document are strongly aligned with the NIST Cybersecurity Framework as well as nuclear-specific guidance.[43] They are as follows:

- Restricting logical access to the ICS network and network activity
- Restricting physical access to the ICS network and devices
- Protecting individual ICS components from exploitation
- Restricting unauthorized modification of data
- Detecting security events and incidents
- Maintaining functionality during adverse conditions
- Restoring the system after an incident

As this document is based on SP800-53, this analysis will look at the specifically ICS-related recommendations provided by this document. The IAEA's Computer Security Guidelines in fact include a chart from this document that clarifies the differences between typical information technology systems and industrial control

systems.[4] Incidentally, this means that when conducting a risk assessment or designing the initial system, there should be special consideration given to the fact that ICS require different protections be put in place. For example, because a disruption of service of ICS could result in physical damage, there must be a clear establishment of risk tolerance.

Although this guidance recommends a review of SP800-53 when selecting security controls, it also includes instructions for an ICS specific security architecture (Section 5). This includes how to effectively segregate and protect various areas based on their varying criticality levels. SP800-82 also recommends a defense-in-depth strategy. When the guide reviews recommended security controls, it first addresses the general control then adds an additional field that alerts readers to potential differences in ICS. Figure 4.4 illustrates the format and typical addition for that tailored guidance. In general, this is helpful guidance, but is also appears to simply be a reminder that IT security cannot be equated with ICS security.

**6.2.17 System and Information Integrity**

Maintaining system and information integrity assures that sensitive data has not been modified or deleted in an unauthorized and undetected manner. The security controls that fall within the NIST SP 800-53 System and Information Integrity (SI) family provide policies and procedures for identifying, reporting, and correcting information system flaws. Controls exist for malicious code detection, spam and spyware protection, and intrusion detection, although they may not be appropriate for all ICS applications. Also provided are controls for receiving security alerts and advisories, and the verification of security functions on the information system. In addition, there are controls within this family to detect and protect against unauthorized changes to software and data, provide restrictions to data input and output, and check for the accuracy, completeness, and validity of data as well as handle error conditions, although they may not be appropriate for all ICS applications.

Supplemental guidance for the SI controls can be found in the following documents:

- NIST SP 800-40 provides guidance on security patch installation [40].
- NIST SP 800-94 provides guidance on Intrusion Detection and Prevention (IDP) Systems [55].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

**ICS-specific Recommendations and Guidance**

Controls exist for malicious code detection, spam and spyware protection, and intrusion detection, although they may not be appropriate for all ICS applications. ICS-specific recommendations and guidance for these controls are included in Sections **Error! Reference source not found.**and 0.

Figure 4.4. NIST SP800-82

Moreover, unlike other guidance documents for critical infrastructure or nuclear facilities, SP800-82 addresses both business and safety concerns. It makes a strong case for the importance of cybersecurity to business continuity and success. One section (4.14), titled "Presenting the Business Case to Leadership," even recommends strategies and plans that could convince upper-level management to invest in security.

*Recommendation:*
This document is sufficient for plant operators that have already introduced secure IT controls and principles. While this particular scenario is unlikely, SP800-82 is more accommodating for facilities that are improving security for the purpose of increasing business or ensuring business continuity. If used in conjunction with NIST SP800-53, this would be ideal for general critical infrastructure. However, to ensure adequate for a nuclear plant in particular, a separate guide for NPPs should be consulted.

### 4.1.5. WINS 4.3 Security of IT and I&C Systems at Nuclear Facilities

The World Institute for Nuclear Security (WINS) is an international non-governmental organization whose aim is to create best practice guides to improve nuclear security worldwide. The Best Practice Guide 4.3 (Revision 3) was published in April 2014.[8] Compared to other guidelines, this WINS guide is structured in a way that is targeted at individuals looking for a basic education on cyber security techniques for nuclear facilities. Although it includes similar amounts of information, its effectiveness may be dampened because it is far less task-based than other guides. While including many of the same general recommendations as the NIST Framework, WINS 4.3 typically does not advise its readers to frequently update plans, processes, and strategies and incorporate lessons learned into those plans.

| Comparison between WINS 4.3 Best Practice Guide & NIST Framework (baseline) | | | | | | |
|---|---|---|---|---|---|---|
| | IDENTIFY (ID) | PROTECT (PR) | DETECT (DE) | RESPOND (RS) | RECOVER (RC) | Totals |
| NIST Framework | 24 | 35 | 18 | 15 | 6 | 98 |
| WINS 4.3 | 23 | 28 | 12 | 11 | 3 | 77 |
| Δ | 1 | 7 | 6 | 4 | 3 | Δ 21 |
| % Similarity | 95.83 | 80.00 | 66.67 | 73.33 | 50.0 | 78.57 |

Figure 4.5. NIST Framework and WINS 4.3 Best Practice Guide by Function

#### Identify
WINS has put together a program that correllates strongly with the tasks in the Identify function. This is primarily due to the fact that it suggests a risk-based approach. In this section, WINS advises the inclusion of cybersecurity threats into the Design Basis Threat DBT). DBT is commonly referred to among nuclear security experts - it is defined by the IAEA as "a comprehensive description of the motivation, intentions and capabilities of potential adversaries against which protection systems are designed and evaluated." [59]

This Best Practice Guide also recognizes the need to examine the business rationale for security investments, much like NIST SP800-82.

**Protect**

On a more granular level, there are aspects where the NIST Framework would provide stronger security because of its explicitness. For example, data protection is addressed in the NIST document whereas it is only tangentially mentioned by WINS.

However, there are a number of areas where WINS provides more specific recommendations than even other nuclear-focused documents. This document discusses the need to promote a security culture in the facility. Nuclear security culture is a well-studied and well-implemented topic, particularly by international nuclear bodies such as the IAEA, WINS, and the Institute of Nuclear Materials Management (INMM).[60] The idea of a cyber security culture is not so specifically developed and would perhaps be considered along the same lines as cyber hygiene. WINS furthermore recommends personnel be trained and tested, with the results of assessments being reported to responsible leaders. In the NIST Framework, this kind of assessment of training and knowledge of users is not emphasized nor does it include recommendations to update and improve training programs.

Similar to other nuclear guidance, WINS recommends firewalls, whitelisting and disabling unnecessary ports and protocols. The differences between management of enterprise networks as opposed to administration of control systems was specifically noted as a vulnerability of nuclear facilities. This acknowledgment reflects many of the noted vulnerabilities noted by other security assessments of ICS as well as the Chatham House report's recommendations. Unfortunately, due to its format, WINS' guidance and cannot be directly taken as any kind of instructive measure.

**Respond**

The WINS Respond function is well-populated. The areas which it is not as thorough are: voluntary information-sharing (RS.CO-5), the mitigation of newly-discovered vulnerabilities (RS.MI-3), and incorporating lessons learned into response plans (RS.IM-1). As mentioned earlier, this is indicative of a lack of attention on the necessary updating and improving processes that are necessary for cybersecurity.

**Other**

No other guidance or standard considered in this thesis mentioned the idea of penetration testing. While penetration testing is standard for nearly all other industries

reliant on computer-based technologies, it is almost never mentioned in relation to nuclear power. WINS also notes that safeguards must be put in place prior to penetration testing. This is something that more plants should be looking into, as it will help organizations and governments better understand the risk likelihoods and therefore improve cybersecurity. Classic nuclear industry 'two-person rules' are also applied in terms of cyber threat mitigation.

*Recommendation:*
The WINS 4.3 Best Practice Guide is not specific enough to use on its own. Its tone and wording however make the necessary tasks understandable especially for leadership and management who perhaps are less familiar with the cybersecurity needs of nuclear facilities. Its recommendation for carefully-implemented penetration testing should also be included in future guidance documents or new regulations.

### 4.1.6. Forthcoming Guidance

The biennial Nuclear Industry Summit took place from March 30 – April 1 2016. The working group focused on 'managing cyber threats' published a report detailing progress and recommendations for future enhancements to improve cybersecurity management at nuclear facilities. In 2014, the working group issued a report recommending the creation common guiding framework for the entire industry. This particular group encouraged the IAEA to be the unifying organization to take on this task. To display the progress towards reaching a more unified understanding of cybersecurity at nuclear plants, the group compiled the following table. Figure 4.6 details upcoming guidance documents that will assist existing and future power plant operators to implement comprehensive cybersecurity regimes at their facilities. These documents will also need to be assessed for their applicability to NPPs when they are released.[61]

| DOCUMENT | STATUS |
|---|---|
| **TECDOC NST 037 - Conducting Computer Security Assessments**<br><br>Provides good practices for organizing and conducting cyber security assessments associated with nuclear security. | Document Complete<br>Publication in 2016 |
| **TECDOC – NST038 Computer Security Incident Response**<br><br>Provides good practices for implementing cyber security incident response processes between competent authorities, operators, and technical support organizations. | Document Complete<br>Publication in 2016 |
| **Nuclear Security Series Technical Guidance – NST036 Computer Security of Instrumentation and Control Systems at Nuclear Facilities.**<br><br>Provides guidance on implementing cyber security controls across the life cycle of nuclear instrumentation and control systems. | Approved for Publication<br>Publication in 2016 |
| **Nuclear Security Series Implementing Guide – NST045 Computer Security for Nuclear Security**<br><br>Provides overarching guidance to assist Member States in implementing cyber security as a component of their nuclear security regime. | Under Development |
| **Nuclear Security Series Technical Guidance – NST047 Computer Security Techniques for Nuclear Facilities**<br><br>Provides discussion on good practices for implementing cyber security associated with digital technologies at nuclear facilities. | Under Development |

Figure 4.6. Forthcoming guidance for cybersecurity at NPPs

## 4.2. Standards

Standards for primarily ICS or IT systems will be examined below. Further information about their selection can be found in subsection 3.3.2.

### 4.2.1. IEEE Standards

The IEEE has created a wide range of standards for nuclear power plants. This project looks only briefly at 692-2013, which has a greater level of comprehensiveness than others. A more comprehensive list of active standards for nuclear power facilities can be found in Appendix B.

**692-2013 – Criteria for Security Systems for Nuclear Power Generating Systems**[9]

The 692-2013 standard promotes the creation of an integrated security system that will detect any potential threats and notify the appropriate personnel of their presence. The primary goal of this standard, however, is to ensure physical security of the facility. Cyber security is mentioned only briefly as a necessary consideration in an overall security plan. For more detailed information on the topic, this 692-2013 suggests 10 CFR 73.54 [58], NEI 08-09 (subsection 4.1.2), and NRC Regulatory Guide 5.71. Given the IEEE's standing in the cyber/IT community and their large number of standards for nuclear power plants, it is certainly unusual that they refer readers to a US-specific regulation rather than contributing to the landscape of standards for cybersecurity at nuclear facilities.

### 4.2.2. ISO/IEC 27001

The ISO 27001 certification is one of the best known IT security standards; certification that an organization is compliant with this standard goes a long way in ensuring regulators, investors, and consumers of a business' maturity and security practices. The full title of this standard is "ISO/IEC 27001:2013; Information technology - Security techniques - Information security management systems – Requirements."

Quite evidently, even with full compliance, this standard would not be sufficient for a nuclear power plant or other facility with ICS. Its international reputation, however, means that it is certainly a meaningful step towards security any facility. The introduction of 27001 furthermore specifically notes that it can be used as either a step towards improved security or as the basis for introducing cybersecurity to a system with no existing controls implemented.

| Comparison between ISO/IEC 27001 & NIST Framework (baseline) | | | | | | |
|---|---|---|---|---|---|---|
| | IDENTIFY (ID) | PROTECT (PR) | DETECT (DE) | RESPOND (RS) | RECOVER (RC) | Totals |
| NIST Framework | 24 | 35 | 18 | 15 | 6 | 98 |
| ISO/IEC 27001 | 16 | 34 | 11 | 12 | 1 | 74 |
| Δ | 8 | 1 | 7 | 3 | 5 | Δ 24 |
| % Similarity | 66.67 | 97.14 | 61.11 | 80.00 | 16.7 | 75.51 |

Figure 4.7. NIST Framework and ISO/IEC 27001 by Function

**Identify**

When compared to the NIST Framework, the sector-specific references are logically

excluded from 27001. Risk tolerance is also an item that is not explicitly considered within the standard.

**Protect**

The protection criteria PR.IP-7 in the NIST Framework which recommends protection processes be continuously improved is surprisingly lacking in the ISO standard. Similarly, the items that encourage the updating and incorporation of lessons learned into the response and recovery plans are missing from 27001.

**Detect**

A few critical detection items such as DE.CM-1 and DE.CM-2 which advise the network and physical environment be 'monitored to detect potential cybersecurity events' are also not present in the standard.

**Respond**

For response, ISO 27001 matches up nearly perfectly with the NIST Framework. However it does not place an emphasis on information-sharing or coordination. Although ISO 27001 includes incorporating lessons learned into response plans, it does not mention updating them. This is a case where the statistical analysis does not imply a serious deficiency within the ISO document. Incorporating lessons learned by default implies that the response plans must be updated.

**Recover**

ISO 27001 only tangentially mentions recovery processes.

*Recommendation:*

An internationally renowned standard such as 27001 is valuable for all organizations. Steps for compliance with this standard could be taken in the enterprise network of a power plant, while a separate nuclear-focused standard could be applied to the critical assets within the system. Either way, working towards compliance with ISO 27001 will demonstrate that due diligence for cybersecurity is being pursued.

### 4.2.3. NERC CIPv5

The North American Electric Reliability Corporation (North American Electric Reliability Corporation (NERC)), which requires compliance with its standards from American electricity providers, updated its standards for critical infrastructure pro-

tection in June of 2015. There is an exhausting number of documents that can be considered a part of this standard.[12] This project, however, looked only at Standard-Specific Training recommendations. These documents reviewed provide actionable items that match well with other standards and guidelines. Although this standard is not specific to nuclear energy production, it is required for most energy providers in the United States.

Articles aiming to prepare operators to comply with the latest version of this standard focus on the more stringent requirement for compliance, which unlike the previous version, requires both a plan and actual implementation.[62]

| Comparison between NERC CIP v5 & NIST Framework (baseline) | | | | | | |
|---|---|---|---|---|---|---|
| | IDENTIFY (ID) | PROTECT (PR) | DETECT (DE) | RESPOND (RS) | RECOVER (RC) | Totals |
| NIST Framework | 24 | 35 | 18 | 15 | 6 | 98 |
| NERC CIP v5 | 7 | 20 | 10 | 10 | 3 | 50 |
| Δ | 17 | 15 | 8 | 5 | 3 | Δ 48 |
| % Similarity | 29.17 | 57.14 | 55.56 | 66.67 | 50.0 | 51.02 |

Figure 4.8. NIST Framework and NERC CIP v5 by Function

**Protect**

Based on the comparison to the NIST Framework, there are some key aspects that are left out of this standard. There are four separate recommendations that users understand their roles and responsibilities in the NIST Framework. The Cyber Security Training Program of CIP v 5, however, is only addressed towards privileged users and not third-party stakeholders, senior executives, or physical security personnel. In fact, the item that suggests the monitoring of third-party individuals with access to systems is not specifically mentioned in the NERC standard either.

However, as shown in Figure 4.8, this standard is very strong on managing access control (especially with regard to access revocation). It furthermore included a lot of detail on log retention and the testing of physical security equipment. Similar to many other nuclear guidance, it also provided specific guidance on password requirements. Its strong record on access control goes hand-in-hand with the requirement that a senior CIP manager must be appoints, and that access controls be based on levels of trust throughout the organization.

As mentioned in section 3.2, the NIST Framework is particularly deficient in mentions of frequent documentation as well as in restricting unnecessary ports. NERC CIP v5 makes explicit both of those things.

*Recommendation:*
NERC CIPv5 provide adequate cybersecurity for the American electric grid. Still, there remain some nuances of security management that are not elucidated, therefore making this standard not a candidate as a baseline for any nuclear plant or energy producer. This document does, however, make sense for nuclear facilities located in the United States who comply with this standard as well as 10 CFR 73.54 [58]. Its emphasis on Access Revocation in 004-05 would however be a good addition to other guidance for cybersecurity at nuclear facilities or in ICS.

### 4.2.4. ANSI/ISA 62443-2-1:2009

This standard, entitled "Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program" was released by the American National Standards Institute (ANSI) and the International Society of Automation (ISA). ANSI also releases a number of more granular nuclear-focused standards for nuclear facilities (including research reactors). For the purposes of this study, the fourth section of ANSI/ISA 62443-2-1:2009, 'Elements of a Cyber Security Management System (CSMS)' will be examined.

This standard in fact contains far more detailed instructions than the NIST Framework. The mapping included in Appendix C is an expanded version of that present in the NIST Framework Core itself. It is clear however, that there is rarely a blatant intuitive link between the actions designated in the American National Standards Institute/International Society of Automation (ANSI/ISA) 2009 Standard that are supposedly congruent with items in the NIST Framework.

| Comparison between ANSI 62443-2-1:2009 & NIST Framework (baseline) | | | | | | |
|---|---|---|---|---|---|---|
| | IDENTIFY (ID) | PROTECT (PR) | DETECT (DE) | RESPOND (RS) | RECOVER (RC) | Totals |
| NIST Framework | 24 | 35 | 18 | 15 | 6 | 98 |
| ANSI/ISA 62443-2-1:2009 | 15 | 25 | 11 | 11 | 0 | 62 |
| Δ | 9 | 10 | 7 | 4 | 6 | Δ 36 |
| % Similarity | 62.50 | 71.43 | 61.11 | 73.33 | 0.0 | 63.27 |

Figure 4.9. NIST Framework and ANSI/ISA 62443-2-1:2009 by Function

**Protect**
For example, PR.IP-7 in the NIST document states "Protection processes are continuously improved." The Framework then liberally claims that this recommendation includes: "Assign an organization to manage and implement changes to the CSMS; Evaluate the CSMS periodically; Establish triggers to evaluate CSMS; Identify and implement corrective and preventive actions; Review risk tolerance; Monitor and

evaluate industry CSMS strategies; Monitor and evaluate applicable legislation relevant to cyber security; Request and report employee feedback on security suggestions."

The utility of the NIST Framework is again called into doubt because it fails to go into detail, instead referring to other standards which may provide more explicit instructions. In the case of ANSI/ISA 62443-2-1:2009, however, a decision to instead rely on this standard would be wise. It is very thoroughly put together; where it is lacking is in recovery recommendations, protecting communication and control networks, restricting removable media, putting in place integrity checking mechanisms, and a few more. Still, despite lacking such important recommendations, it remains is a far more comprehensive document than the majority reviewed in this study.

*Recommendation:*
The detail present in this standard makes it suitable option for implementing a new regulation or for starting a cybersecurity program from scratch. Furthermore, although it doesn't specifically acknowledge nuclear power facilities, it does seriously take into account needs for network segmentation and defense in depth. Some considerations such as controls for environmental impact may be necessary; therefore compliance with this standard as well as implementing recommendations from a nuclear-specific guidance document would be ideal.

### 4.2.5. ANSI/ISA 62443-3-3:2013

Far less comprehensive than the 2009 standard reviewed above, this 2013 standard adds some elaborating components to ICS cybersecurity despite it's lack of detail as compared to the NIST Framework (see below).

| Comparison between ANSI 62443-3-3:2013 & NIST Framework (baseline) | | | | | | |
|---|---|---|---|---|---|---|
| | IDENTIFY (ID) | PROTECT (PR) | DETECT (DE) | RESPOND (RS) | RECOVER (RC) | Totals |
| NIST Framework | 24 | 35 | 18 | 15 | 6 | 98 |
| ANSI/ISA 62443-3-3:2013 | 2 | 19 | 8 | 3 | 0 | 32 |
| Δ | 22 | 16 | 10 | 12 | 6 | Δ 66 |
| % Similarity | 8.33 | 54.29 | 44.44 | 20.00 | 0.0 | 32.65 |

Figure 4.10. NIST Framework and ANSI/ISA 62443-3-3:2013 by Function

**Protect**
The 2009 standard was, for example, lacking in the requirements PR.DS-1 & 2 that recommend data-at-rest and data-in-transit be protected. In the 2013 document. There are multiple instructions that specifically address this issue. Fur-

ther, where the 2009 standard was without recommendations for integrity checking mechanisms (PR.DS.-6), American National Standards Institute (ANSI)/ISA 62443-3-3:2013 provided multiple action items (although none specifically addressing firmware security).

Actually, instances where the 2013 standard can assist the 2009 standard are few and far between. Risk management, response and recovery strategies, personnel requirements for cybersecurity were all not addressed within the later document.

*Recommendation:*
This standard in particular is advised to only be used in conjunction with either ANSI/ISA 62443-1-1:2009 or another extremely comprehensive standard. Achieving compliance with this standard alone would be not indicate a strong level of cybersecurity.

# Chapter 5

# Results and Conclusions

## 5.1. Results

The cybersecurity of nuclear power plants is crucial to avoid a major disaster. The first step is to ensure that the security implemented is as thoroughly as possible. Plants and regulators utilize guidelines and standards from reputable organizations to serve as baselines or even requirements for the operation of the nuclear power plant. In order to supplement the choice of document to base a cybersecurity implementation on, this project provides a comparison of major documents for nuclear power plants or other IT systems. This section compiles the results of the statistical analyses from chapter 3 and the qualitative results from chapter 4. Final recommendations and resources for decision-makers are provided in section 5.2.

The results from the data generated by the mapping of guidelines and standards can be instructive, although there are limits. The figure below highlights the documents that are most compatible with the NIST Framework, organized by category.

Figure 5.1 provides a visual illustration of the strengths and weaknesses of each document. It demonstrates how well the assessed standards and guidelines fit the NIST Framework and therefore their strengths among categories. The bright orange color indicates full congruence with the NIST Framework, the lighter color indicates the difference of only one subcategory. For example, the IAEA Computer Security Guidelines are strongest in the categories of: Access Control, Awareness and Training, Maintenance, Protective Technology as well as Asset Management, Governance,

| Document | IDENTIFY (ID) | | | PROTECT (PR) | | | DETECT (DE) | | | RESPOND (RS) | | | | RECOVER (RC) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Asset Management | Business Environment | Governance | Risk Assessment | Risk Management Strategy | Access Control | Awareness and Training | Data Security | Processes and Procedures | Information Protection | Maintenance | Protective Technology | Anomalies and Events | Security Continuous Monitoring | Detection Processes | Response Planning | Communications | Analysis | Mitigation | Improvements | Recovery Planning | Improvements | Communications |
| NIST CSF | 6 | 5 | 4 | 6 | 3 | 5 | 5 | 7 | 12 | 2 | 4 | 5 | 8 | 5 | 1 | 5 | 4 | 3 | 2 | 1 | 2 | 3 |
| IAEA CSG | 5 | 1 | 3 | 3 | 2 | 5 | 5 | 2 | 7 | 2 | 4 | 2 | 5 | 1 | 0 | 2 | 0 | 1 | 0 | 0 | 0 | 0 |
| NEI 08-09 | 5 | 2 | 1 | 5 | 1 | 5 | 4 | 5 | 10 | 1 | 4 | 5 | 8 | 3 | 1 | 3 | 3 | 3 | 1 | 0 | 1 | 1 |
| NRC 5.71 | 6 | 0 | 3 | 5 | 2 | 5 | 5 | 7 | 12 | 2 | 4 | 2 | 8 | 5 | 1 | 3 | 2 | 3 | 2 | 1 | 2 | 1 |
| NIST SP800-53 | 6 | 5 | 4 | 6 | 3 | 5 | 5 | 7 | 12 | 2 | 4 | 5 | 8 | 5 | 1 | 5 | 4 | 3 | 2 | 1 | 2 | 1 |
| WINS 4.3 | 6 | 4 | 4 | 6 | 3 | 5 | 5 | 4 | 9 | 2 | 3 | 3 | 6 | 3 | 1 | 4 | 3 | 2 | 1 | 1 | 0 | 2 |
| ISO/IEC 27001 | 6 | 3 | 3 | 4 | 0 | 5 | 5 | 7 | 11 | 2 | 4 | 1 | 5 | 5 | 1 | 3 | 4 | 3 | 1 | 1 | 0 | 0 |
| NERC CIP v5 | 4 | 0 | 1 | 2 | 0 | 5 | 3 | 0 | 6 | 2 | 4 | 1 | 6 | 3 | 1 | 3 | 1 | 3 | 2 | 1 | 2 | 0 |
| ANSI/ISA 62443-2-1:2009 | 5 | 1 | 3 | 4 | 2 | 5 | 5 | 1 | 10 | 2 | 2 | 3 | 3 | 5 | 1 | 4 | 3 | 2 | 1 | 0 | 0 | 0 |
| ANSI/ISA 62443-3-3:2013 | 2 | 0 | 0 | 0 | 0 | 4 | 0 | 6 | 5 | 0 | 4 | 2 | 4 | 2 | 0 | 0 | 2 | 1 | 1 | 0 | 0 | 0 |

| Key: | |
|---|---|
| | NIST TARGET -1 (where target ≠ 1) |
| | NIST TARGET |

Figure 5.1. Documents Most Congruent with NIST Framework (by Category)

Risk Management Strategy. ANSI/ISA 62443-3-3:2013 on the other hand is strong only in Protective Technology, Access Control and Data Security.

Figure 5.1 clearly displays the overlap amongst the standards and guidelines. In order to weed out the documents that are perhaps weaker in a certain category than others the following will utilize the information presented in chapter 4. For each category the documents that are most appropriate will be selected.

IDENTIFY

- **Asset Management:***ISO/IEC 27001 & NIST SP800-53*
  The only four documents that fully matched the NIST Framework were the NRC Regulatory Guide 5.71, WINS Best Practice Guide, ISO 27001 and NIST SP800-53. The NRC Regulatory Guide only required strong asset management for 'low impact systems.' This is not comprehensive enough to ensure protection for even the enterprise section of the system. The WINS Best Practice Guide includes asset management recommendations only in regard to detection and response activities. Both ISO 27001 and SP800-53 very clearly require inventory of assets and their categorization.

- **Business Environment:***NIST SP800-53 (+ SP800-82) & WINS 4.3*
  The business concerns addressed in SP800-53 are made even more evident if combined with the ICS-focused SP800-82. The WINS Best Practice Guide while not a full-blown implementation guide, does provide valuable guidance for encouraging management to invest in cybersecurity.

- **Governance:***NIST SP800-53 & NERC CIP v5*
  Both NIST SP800-53 and the WINS Best Practice Guide were similar to the NIST Framework. And although the WINS Guide did provide congruent recommendations, once again the Governance tasks were mentioned tangentially with response activities. Furthermore, it does not compare to the Governance guidance provided by NERC CIP v5, which dictates a necessary delegation of authority in its 003 Guide focused solely on policy development. NIST SP800-53 meets all criteria of the NIST Framework and provides in depth recommendations regarding the Governance tasks of creating a policy and disseminating roles and responsibilities.

- **Risk Assessment and Risk Management Strategy:***NIST SP800-53 & WINS 4.3*
  NIST SP800-53 is one of the few documents that urges caution when im-

plementing security controls. In its introduction it firmly recommends that implementation should be risk-based and cautious, to avoid any adverse effects that may arise due to large scale system configurations. In that way, and more specifically in its recommendations, SP800-53 integrates risk assessment through its entirety. Other documents are less explicitly focused on risk assessment as a crucial activity for implementing security controls. The WINS Guide, partially due to its advisory format and more explanatory nature, best describes the need for risk assessment and controls based on those assessments at NPPs. Risk Assessment and Risk Management Strategy were combined; logically documents cannot explicitly call for risk management management unless they first require risk identification and assessment.

PROTECT

- **Access Control:** *NEI 08-09 & ANSI/ISA 62443-2-1:2009*
  The data provides no strong differential amongst documents in the category of Access Control; however, this is not the case from a qualitative perspective. Of the included guidance documents, the NEI 08-09 Plan for Nuclear Power Plants provides the most thorough guidance on access control. Of the various categories included in the plan, Access Control (Appendix D, 1) is the longest and most detailed section. However, ANSI/ISA 62443-2-1:2009 provides the broadest depiction of access control procedures. Whereas the NEI limits itself to access control for information systems, ANSI/ISA discusses both physical and virtual access control in great detail.

- **Awareness and Training:** *WINS 4.3*
  Even though the documents nearly all document address Awareness and Training more generally, as the NIST Framework does, none provided such clear reasoning and recommendations for this category than the WINS Best Practice Guide. Overall, the WINS Guide provided the best outline for a complete awareness and training program because it emphasized the need to build a culture, to encourage reporting of potential malicious insiders and to ensure that senior leaders understood the necessity of strong investment in cybersecurity. Furthermore, WINS' recommendations are focused on nuclear facilities in particular and build on existing practices related to physical protection at those facilities.

- **Information Protection Processes and Procedures:** *NRC 5.71 & ISO/IEC 27001*

NRC 5.71 is very detailed and clear about protecting information, about ensuring personnel security. It also clearly matched well with the NIST Framework. The ISO 27001 document did not fully match with the Framework, nor is it specific to nuclear or even ICS facilities, however it still provided very detailed processes to follow in this category.

- **Data Security:***NIST SP800-53 & ANSI/ISA 62443-3-3:2013*
  Not all of the documents examined included explicit consideration of both data-at-rest and data-in-transit (NIST Framework, ISO 27001, NIST SP800-53, NEI 08-09, ANSI/ISA 62443-3-3:2013, and NRC Regulatory Guide 5.71.) Of those, NIST SP800-53 and ANSI/ISA 62443-3-3:2013 addressed the issue specifically and in a more detailed manner than the rest.

- **Maintenance:***NRC 5.71 & NEI 08-09*
  Nuclear guidance is more sensitive to maintenance concerns at a NPP than other more generic documents. Although other nuclear documents discuss the need to verify all security patches; these provide the most detailed security controls. For example, NRC 5.71 specifically mentions the evaluation of maintenance and testing personnel.

- **Protective Technology:***ANSI/ISA 62443-3-3:2013 & NERC CIP v5 &NRC 5.71 & NEI 08-09*
  This category differs from the Information Protection in that it focuses on protections such as restricting removable media and encourages thorough documentation. Nearly all of the documents are congruent with the NIST Framework; however the NIST Framework itself does not adequately address the need for disabling unnecessary ports or removing unnecessary services. Most of the documents would be in fact better than the NIST Framework in this category but the latest ISA standard is actually quite thorough. In general, nuclear documents are stronger in this category (with the exception of the IAEA and WINS guidelines which did not have as much guidance as the other more step-by-step control-based documents indicated here.

DETECT

- **Anomalies and Events:***NIST SP800-53, NRC 5.71, NEI 08-09, ISO/IEC 27001*
  The majority of documents reviewed did not discuss the need for specifically "automated" detection systems. This is certainly an oversight as automated detection is necessary to ensure no breach is overlooked during off-hours. For

this reason, and for the documents most congruent to the NIST Framework, NIST SP800-53, NRC Regulatory Guide 5.71, and NEI 08-09 are considered by this work to be the best guidelines for the detection of anomalies. Of the standards, ISO 27001 provides simple but broad-reaching requirements for compliant organizations.

- **Security Continuous Monitoring:***NIST SP800-53 & NRC 5.71 & NEI 08-09*
  These are the top ranked documents in the Security Continuous Monitoring project, they also contain the most detailed documentation for this category.
- **Detection Processes:***ISO 27001 & NRC 5.71*
  Both ISO 27001 and the NRC Regulatory Guide have clear guidelines for the gamut of detection processes. The two documents provide more specific recommendations regarding automated detection processes and utilizing information about potential incidents from a variety of sources.

RESPOND

- **Response Planning:***All but IAEA Computer Security Guidelines & ANSI/ISA 62443-3-3:2013*
  There is only one task in this category: "Implement an incident response plan." This is a basic recommendation and any of the documents (besides those mentioned here) would provide that advice.
- **Communications:***NIST SP800-53 & WINS 4.3 & ANSI/ISA 62443-2-1:2009*
  Because the NIST Framework fully covers recommendations for communications as an aspect of the Respond function, the best documents for this category are those most closely linked with it.
- **Analysis:***NEI 08-09 & NRC 5.71 & ISO 27001*
  Each of these documents is very explicit in their recommendations to the facilities to document all incidents, as they may be useful in forensics and in managing an ongoing incident.
- **Mitigation:***NEI 08-09 & NRC 5.71 & ANSI/ISA 62443-2-1:2009*
  NEI 08-09 and NRC Regulatory Guide 5.71 contained the most well-formed recommendations for response planning. Both advise the creation of a CSIRT as well as 24/7 available response assistance. ANSI/ISA (2009) specifically focuses on fixing the vulnerability that was exploited during an incident and applying preventive measures as a part of the response plan.

- **Improvements:** *All but IAEA Computer Security Guidelines*
  The majority of documents will either imply or specifically state the need to improve response plans and capabilities (with the exception of the IAEA Computer Security Guidelines which is not as focused on the response and recovery aspects of cybersecurity management).

RECOVER

- **Recover Categories:** *NIST SP800-53 & NERC CIP v5 (& NIST Framework)*
  Recovery was, for obvious reasons, not emphasized nearly as much as the other categories. Even though NIST SP800-53, and NERC CIPv5 placed the most targeted attention on recovery techniques in their documents, neither of them were on par with the NIST Framework, which in fact provided the most specific recommendations regarding recovery. Any recovery plans should include the recommendations of the NIST Framework - to execute a recovery plan, communicate that plan, manage reputation and public relations as a part of that plan, and eventually to update the recovery strategy to reflect lessons learned.

The above recommendations are visualized in Figure 5.2.

| Document | IDENTIFY (ID) | | | PROTECT (PR) | | | DETECT (DE) | | | RESPOND (RS) | | | | DETECT (DE) | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Asset Management | Business Environment | Governance | Risk Assessment | Risk Management Strategy | Access Control | Awareness and Training | Data Security | Processes and Procedures | Maintenance | Protective Technology | Anomalies and Events | Security Continuous Monitoring | Detection Processes | Response Planning | Communications | Analysis | Mitigation | Improvements | Recovery Planning | Improvements | Communications |
| NIST CSF | 6 | 5 | 4 | 6 | 3 | 5 | 5 | 7 | 12 | 2 | 4 | 5 | 8 | 5 | 1 | 5 | 4 | 3 | 2 | 1 | 2 | 3 |
| IAEA CSG | 5 | 1 | 3 | 3 | 2 | 5 | 5 | 2 | 7 | 2 | 4 | 2 | 5 | 1 | 0 | 2 | 0 | 1 | 0 | 0 | 0 | 0 |
| NEI 08-09 | 5 | 2 | 1 | 5 | 1 | 5 | 4 | 5 | 10 | 1 | 4 | 5 | 8 | 3 | 1 | 3 | 3 | 3 | 1 | 0 | 1 | 1 |
| NRC 5.71 | 6 | 0 | 3 | 5 | 2 | 5 | 5 | 7 | 12 | 2 | 4 | 2 | 8 | 5 | 1 | 3 | 2 | 3 | 2 | 1 | 2 | 1 |
| NIST SP800-53 | 6 | 5 | 4 | 6 | 3 | 5 | 5 | 7 | 12 | 2 | 4 | 5 | 8 | 5 | 1 | 5 | 4 | 3 | 2 | 1 | 2 | 1 |
| WINS 4.3 | 6 | 4 | 4 | 6 | 3 | 5 | 5 | 4 | 9 | 2 | 3 | 3 | 6 | 3 | 1 | 4 | 3 | 2 | 1 | 1 | 0 | 2 |
| ISO/IEC 27001 | 6 | 3 | 3 | 4 | 0 | 5 | 5 | 7 | 11 | 2 | 4 | 1 | 5 | 5 | 1 | 3 | 4 | 3 | 1 | 1 | 0 | 0 |
| NERC CIP v5 | 4 | 0 | 1 | 2 | 0 | 5 | 3 | 0 | 6 | 2 | 4 | 1 | 6 | 3 | 1 | 3 | 1 | 3 | 2 | 1 | 2 | 0 |
| ANSI/ISA 62443-2-1:2009 | 5 | 1 | 3 | 4 | 2 | 5 | 5 | 1 | 10 | 2 | 2 | 3 | 3 | 5 | 1 | 4 | 3 | 2 | 1 | 0 | 0 | 0 |
| ANSI/ISA 62443-3-3:2013 | 2 | 0 | 0 | 0 | 0 | 4 | 0 | 6 | 5 | 0 | 4 | 2 | 4 | 2 | 0 | 0 | 2 | 1 | 1 | 0 | 0 | 0 |

Key: RECOMMENDED

Figure 5.2. Recommendations by Category

## 5.2. Conclusions

Thus far, this project has evaluated the nine guidelines and standards using statistical data combined with qualitative information from each document. By selecting the strongest documents in each of these categories, operators or regulators have a chance to utilize the best possible sections of each guide in order to ensure the most comprehensive security in their own facilities. This section summarizes the results into concrete recommendations that will be useful for decision-makers at current and future nuclear power plants. It further recommends the development of a comprehensive, international standard for cybersecurity at nuclear power plants and describes future work to add on to this research.

### 5.2.1. Recommendations

Figure 5.2 identified the recommended documents for each category. However, combining all of them, at least at this point, is not feasible. The figure below provides situations that a decision-maker may find him or herself in. Recommendations for a combination of documents to address their concerns are included on the right.

| PURPOSE | RECOMMENDATION |
|---|---|
| *Improve cybersecurity (outside of existing regulations)* | • Compare current practices to NIST Framework;<br>• Consult either the combination of NIST SP800-53 and SP800-82 or ANSI/ISA 62443-2-1:2009 and ANSI/ISA 62443-3-3:2013 for specific implementations |
| *Improve cybersecurity (no existing documents utilized)* | • Implement NIST SP800-53 and SP800-82;<br>• Augment with NEI 08-09 Plan;<br>• Incorporate the guidance of the WINS Best Practice Guide |
| *Create a national regulation on the basis of* | • NERC CIPv5, NEI 08-09, NRC Regulatory Guide 5.71;<br>• Ensure thoroughness for basic IT Standards using ISO/IEC 27001<br>• Double check compatibility with NIST Framework<br>• Check applicability for nuclear systems with IAEA Computer Security Guidelines |
| *Adapt existing cybersecurity controls to be specific to nuclear power plants* | • Implement NEI 08-09 and/or NRC 5.71<br>• Incorporate lessons learned from IAEA CSG and WINS Best Practice Guide |
| *Upgrade a nuclear plant from analog to digital* | • Implement NIST SP800-53 and SP800-82<br>• Where relevant, include controls provided by NEI 08-09 and NRC 5.71 |
| *Educate IT Specialists on the differences between IT, ICS, and Nuclear* | • Make required reading: IAEA Computer Security Guidelines, WINS 4.3, and ANSI/ISA 62443-3-3:2013 |
| *Implement a cybersecurity plan that includes business recommendations* | • Both ANSI/ISA documents<br>• Reference WINS 4.3 Best Practices Guide |

Figure 5.3. Recommendations for Decision-makers

This chart explored the scenarios that a decision-maker may face when working to

implement cybersecurity for nuclear power facilities. Those scenarios are chosen as the most likely and most perplexing scenarios for which a thorough comparison such as the one provided with this project would be necessary. Recommendations here are provided for the sake of simplicity, based on the results above. The ideal scenario is for the management making the decision to look at Figure 5.3 then ensure the recommendations are the right one for them based on either a particular document's analysis or the assessment based on category provided in the above section 5.1.

For example, the first scenario would apply to NPP operators and regulatory agencies in countries like the UK, US and Canada that have strong existing regulations. To improve the cybersecurity of a specific plant, or of nuclear facilities nationwide, they could compare current practices to the NIST Framework. Once any deficiencies are determined, either the combination of NIST 800-53 and SP800-82 or the combination of ANSI/ISA 62443-2-1:2009 and ANSI/ISA 62443-3-3:2013 can be used for specific implementation of security controls. This method ensures that any gaps in cybersecurity are known and mitigated. To develop cybersecurity expertise in more detail, it is advised that the decision-makers take note of the *"'Educate IT Specialists"'* recommendations to require the reading of the guidelines from the IAEA, WINS and the 2013 ANSI/ISA 62443-3-3 standard. Implementing these recommendations for advanced nations may be arduous; however cybersecurity is a noble investment of resources that can always be strengthened. These recommendations regarding standard or guideline implementation (*"'Create a national regulation"'*) are particularly vital for nations that are in the process of establishing nuclear power. They have the opportunity to introduce strong cybersecurity standards from the beginning, eliminating the challenges that come with retrofitting analog technology.

These recommendations, in combination with the statistical and qualitative analyses in this study, simplify the process for deciding upon an appropriate regime for cybersecurity at existing and future nuclear power plants. However, as elaborated on in the section below, a much more comprehensive standard for cybersecurity at nuclear power plants worldwide so that a complex combination of existing documents is unnecessary.

### 5.2.2. Further Considerations & Future Work

While the information provided here contributes to the current landscape of cybersecurity guidance for nuclear power plants, this is not a feasible system in the

long term. Regulators and operators should not have to piece together the most effective cybersecurity guidance, it should be provided in order to ensure international security from a devastating nuclear incident. In the long run, a standard (not a guideline) should be created to ensure that each of these sections is exhaustive and specifically tailored for nuclear power plants. This document should be even more comprehensive than the NIST Framework but include many of the categories discussed within it.

It is also important that this be an international effort. This project included many American standards and guidelines; although they are well-known there should still be a more international outlook on the issue of cybersecurity, especially at NPPs. The current practice of each nation developing their own regulations for the cybersecurity at NPP is creating redundant work. If an international standards organization could work together with multiple nations, and solicit expertise as NIST did for the development of its Framework, there would be a stronger cybersecurity regime at NPPs worldwide. This is especially important for nations just beginning their nuclear power programs. The IAEA, for example, could periodically certify their compliance with an international cybersecurity standard, thus taking a lot of the insecurity and guesswork out of initial security measures. Implementation of any of the assessed documents is not an easy process; ensuring that the chosen framework to implement is comprehensive would eliminate some of the redundant work completed due to discrepancies between guidance.

Still, even if this document is created, enforcement is a problem. Most IT experts can verify that compliance with standards is subjective and is largely dependent on self-reporting of processes. Regulatory bodies as well as the IAEA need to employ cybersecurity experts who can guarantee that the technical security controls are in place, in conjunction with security policies and risk management processes.

In the future, there should be further studies on the processes behind developing cybersecurity regulation and how developing nuclear power capable nations approach the overall issue of security in their facilities. A comprehensive study regarding the choice of documents would also be valuable for ensuring that the best guides are utilized, although the results of such a study may be extremely varied.

# Bibliography


[1] C. Baylon, D. Livingstone, and R. Brunt, "Cyber security at civil nuclear facilities: Understanding the risks", Chatham House, Oct. 2015. [Online]. Available: https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks (visited on 03/20/2015).

[2] C. McGoogan, "UK nuclear plants 'not threatened' by cyber attacks", Wired, Ed., Oct. 2016. [Online]. Available: http://www.wired.co.uk/news/archive/2015-10/05/uk-nuclear-cybersecurity-risk (visited on 03/20/2016).

[3] B. Gross, "On chatham house and nuclear cyber security", NEI Nuclear Notes, Ed., Oct. 2015. [Online]. Available: http://neinuclearnotes.blogspot.com.ee/2015/10/chatham-house-nuclear-cyber-security.html (visited on 03/20/2016).

[4] *Computer security at nuclear facilities*, Nuclear Security Series No. 17, International Atomic Energy Agency, 2011.

[5] *NEI 08-09 [Rev 6] cyber security plan for nuclear power reactors*, Nuclear Energy Institute, Apr. 2010. [Online]. Available: http://www.nrc.gov/docs/ML1011/ML101180437.pdf.

[6] *Regulatory guide 5.71*, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Jan. 2010. [Online]. Available: https://scp.nrc.gov/slo/regguide571.pdf.

[7] *SP 800-53: Recommended security controls for federal information systems*, National Institute of Standards and Technology, 2003.

[8] *WINS international best practice guide 4.3: Security of IT and IC systems at nuclear facilities, rev. 3.0*, World Institute for Nuclear Security, Apr. 2014.

[9] *692-2013: IEEE standard for criteria for security systems for nuclear power generating stations*, IEEE Standards Association, Aug. 2013. [Online]. Available: https://standards.ieee.org/findstds/standard/692-2013.html.

[10] *ISO/IEC 27001:2013*, International Standards Organization, 2013. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=54534.

[11] D. Ochel, *Comparing NIST's cybersecurity framework with ISO/IEC 27001*, Seculibrium, Feb. 2014. [Online]. Available: http://www.secuilibrium.com/news/comparing-isoiec-27001-with-nists-cybersecurity-framework.

[12] *Implementation study final report: CIP version 5 transition program*, North American Electric Reliability Corporation, Oct. 2014. [Online]. Available: http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPv5_Implem_Study_Final_Report_Oct2014.pdf.

[13] *ANSI/ISA-62443-2-1: 2009 security for industrial automation and control systems part 2-1: Establishing an industrial automation and control systems security program*, American National Standards Institute/International Society of Automation, Jan. 2009. [Online]. Available: https://www.americanbar.org/content/dam/aba/administrative/law_national_security/nistframework/NIST%20Cybersecurity%20Framework%20Core%20-%20ISA%2062443-2-1-2009.authcheckdam.PDF.

[14] *ANSI/ISA-62443-3-3: 2013 security for industrial automation and control systems part 3-3: System security requirements and security levels*, American National Standards Institute/International Society of Automation, Aug. 2013. [Online]. Available: https://www.americanbar.org/content/dam/aba/administrative/law_national_security/nistframework/NIST%20Cybersecurity%20Framework%20Core%20-%20ISA%2062443-3-3-2013.authcheckdam.pdf.

[15] M. Bunn, "Beyond crises: The unending challenge of controlling nuclear weapons and materials", in *Nuclear Weapons Security Crises: What Does History Teach?*, H. D. Sokolski, Ed. Strategic Studies Institute, 2013, pp. 253–278.

[16] C. Brook, *Report: French nuclear company areva hit by virus*, Threat Post, Ed., Oct. 2011. [Online]. Available: https://threatpost.com/report-french-nuclear-company-areva-hit-virus-103111/75825/.

[17] J. Stone, *Anonymous' #OpGreenRights hack team knocked nuclear corporation areva offline, leaked world trade organization emails*, International Business Times, Ed., May 2015. [Online]. Available: http://www.ibtimes.com/anonymous-opgreenrights-hack-team-knocked-nuclear-corporation-areva-offline-leaked-1909527.

[18] *Hacking for ISIS: The Emergent Cyber Threat Landscape*, Flashpoint, Apr. 2016. [Online]. Available: https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_HackingForISIS_April2016.pdf (visited on 03/20/2015).

[19] Council on Foreign Relations, Ed., *Targets for terrorism: Nuclear facilities*, Jan. 2006. [Online]. Available: http://www.cfr.org/homeland-security/targets-terrorism-nuclear-facilities/p10213.

[20] *Nuclear Power Plants: Vulnerability to Terrorist Attack*, Congressional Research Service, Feb. 2005. [Online]. Available: https://fas.org/irp/crs/RS21131.pdf (visited on 04/20/2015).

[21] *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes*, American Academy of Arts and Sciences, 2014. [Online]. Available: https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf (visited on 04/20/2015).

[22] *Preventive and Protective Measures against Insider Threats*, IAEA Nuclear Security Series No. 8, International Atomic Energy Agency, 2008. [Online]. Available: http://www-pub.iaea.org/books/IAEABooks/7969/Preventive-and-Protective-Measures-against-Insider-Threats (visited on 04/20/2015).

[23] K. McCaney, *The accidental hackers: Insiders post the top threat to dod networks*, Defense Systems, Ed., Jan. 2015. [Online]. Available: https://defensesystems.com/articles/2015/01/29/dod-insider-threats-it-security-survey.aspx.

[24] V. Manzo, *Stuxnet and the dangers of cyberwar*, The National Interest, Ed., Jan. 2013. [Online]. Available: http://nationalinterest.org/commentary/stuxnet-the-dangers-cyberwar-8030?page=2.

[25] M. Poznansky and E. Perkoski, *Attribution and secrecy in cyberspace*, War on the Rocks, Ed., Mar. 2016. [Online]. Available: http://warontherocks.com/2016/03/attribution-and-secrecy-in-cyberspace/.

[26] *India-Pakistan Non-Attack Agreement*, Nuclear Threat Initiative, 1988. [Online]. Available: http://www.nti.org/learn/treaties-and-regimes/india-pakistan-non-attack-agreement/.

[27] W. Ahn, M. Chung, B.-G. Min, and J. Seo, "Development of cyber-attack scenarios for nuclear power plants using scenario graphs", *International Journal of Distributed Sensor Networks*, vol. 2015, 2015.

[28] B. Kesler, "The vulnerability of nuclear facilities to cyber attack", *Strategic Insights*, vol. 10, no. 1, pp. 15–25, 2011.

[29] C. Steitz and E. Auchard, *German nuclear plant infected with computer viruses, operator says*, Reuters.com, Apr. 2016.

[30] K. Zetter, "An unprecedented look at stuxnet, the world's first digital weapon", *Wired.com. November*, vol. 3, p. 14, 2014.

[31] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare", *Computers & Security*, vol. 31, no. 4, pp. 418–436, 2012.

[32] R. Piggin, "Industrial systems: Cyber-security's new battlefront", *Engineering & Technology*, vol. 9, no. 8, pp. 70–74, 2014.

[33] *World Nuclear Power Reactors & Uranium Requirements*, World Nuclear Association, Mar. 2016. [Online]. Available: http://world-nuclear.org/information-library/facts-and-figures/world-nuclear-power-reactors-and-uranium-requireme.aspx (visited on 04/20/2015).

[34] *Nuclear Power Plants Benefit State and Local Economies*, Nuclear Energy Institute, Feb. 2015. [Online]. Available: http://www.nei.org/Master-Document-Folder/Backgrounders/Fact-Sheets/Nuclear-Power-Plants-Contribute-Significantly-to-S (visited on 04/20/2015).

[35] Trend Micro, "Organization of american states (2015) report on cybersecurity and critical infrastructure in the americas", 2015.

[36] J. Kanter, *Switzerland decides on nuclear phase-out*, The New York Times, May 2011. [Online]. Available: http://www.nytimes.com/2011/05/26/business/global/26nuclear.html?_r=0.

[37] D. Sax, *In the age of cybercrime, the best insurance may be analog*, Bloomberg Businessweek, Mar. 2016. [Online]. Available: http://www.bloomberg.com/news/articles/2016-03-10/cybersecurity-the-best-insurance-may-be-analog.

[38] *The nuclear power deception*, Apex Press, 1999. [Online]. Available: http://www.%20ieer.%20org/reports/npd.%20html.

[39] O. Bukharin, "Upgrading security at nuclear power plants in the newly independent states", *The Nonproliferation Review*, vol. 4, no. 2, pp. 28–39, 1997.

[40] J. F. Brenner, "Eyes wide shut: The growing threat of cyber attacks on industrial control systems", *Bulletin of the atomic scientists*, vol. 69, no. 5, pp. 15–20, 2013.

[41] T. Fox-Brewster, *Want some nuclear power plant 'zero day' vulnerabilities? yours for just 8,000usd*, Forbes, Ed., Oct. 2015. [Online]. Available: http://www.forbes.com/sites/thomasbrewster/2015/10/21/scada-zero-day-exploit-sales/#63813a5d96c9.

[42] SCADAhacker.com, Ed., *Home*, 2015. [Online]. Available: https://scadahacker.com/index.html.

[43] *SP800-82: Guide to industrial control systems (ICS) security, final public draft*, National Institute of Standards and Technology, 2008.

[44] M. Dunn-Cavelty and M. Suter, "Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection", *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 179–187, 2009.

[45] D. Assaf, "Models of critical information infrastructure protection", *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 6–14, 2008.

[46] *International CIIP handbook 2008/2009*, Center for Security Studies, ETH Zurich, 2008.

[47] World Nuclear Association, Ed., *Nuclear power in brazil*, Oct. 2015. [Online]. Available: http://world-nuclear.org/information-library/country-profiles/countries-a-f/brazil.aspx.

[48] Tech in Brazil, Ed., *The brazilian energy distribution system*, Jan. 2016. [Online]. Available: http://techinbrazil.com/the-brazilian-energy-distribution-system.

[49] *Joint Publication 3-12(R) Cyberspace Operations*, Joint Chiefs of Staff, Feb. 2013. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[50] *National Cyber Security Organisation: France*, NATO Cooperative Cyber Defence Centre of Excellence, 2015. [Online]. Available: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_FRANCE_032015_0.pdf.

[51] *BSI standards*, Federal Office for Information Security. [Online]. Available: https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html.

[52] *Framework for improving critical infrastructure cybersecurity, version 1.0*, National Institute of Standards and Technology, Feb. 2014.

[53] P. E. Small, "Defense in depth: An impractical strategy for a cyber world", *SANS Institute, Bethesda*, 2011.

[54] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai, "IEEE 802.11 wireless local area networks", *IEEE Communications Magazine*, vol. 35, no. 9, pp. 116–126, 1997.

[55] *IEC 62645:2014*, International Electrotechnical Commission, Mar. 2015. [Online]. Available: https://webstore.iec.ch/publication/7311.

[56] C. Kuligowski, "Comparison of it security standards", Master's thesis, Cybersecurity Academy, 2009. [Online]. Available: http://www.federalcybersecurity.org/CourseFiles/WhitePapers/ISOvNIST.pdf.

[57] P. Agcaoili, *Cybersecurity framework vPA092813*, Oct. 2013. [Online]. Available: https://app.box.com/s/2qd8fs7d9xxdgmg7euhc.

[58] U.S. Code of Federal Regulations, "U.S. code §5195c - critical infrastructures protection", 2001. [Online]. Available: https://www.law.cornell.edu/uscode/text/42/5195c (visited on 03/20/2016).

[59] *Development, use and maintenance of the design basis threat*, 10, International Atomic Energy Agency, 2009.

[60] *Home*, Institute of Nuclear Materials Management. [Online]. Available: https://www.inmm.org/Home.htm.

[61] Working Group 1, *WG1: Report managing cyber threats*, Nuclear Industry Summit, Mar. 2016. [Online]. Available: http://nis2016.org/wp-content/uploads/2016/02/Working-Group-1-Report-Managing-Cyber-Threats.pdf.

[62] S. Parker, *Introduction to NERC CIP version 5*, Power Magazine, Jun. 2014. [Online]. Available: http://www.powermag.com/introduction-to-nerc-cip-version-5/?pagenum=3.

# Appendices

# Appendix A

# NIST Framework Category Descriptions

**Identify (ID)**

- Asset Management(ID.AM)
  The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
- Business Environment(ID.BE)
  The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- Governance(ID.GV)
  The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
- Risk Assessment(ID.RA)
  The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- Risk Management Strategy(ID.RM)

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

**Protect(PR)**

- Access Control(PR.AC)
  Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
- Awareness and Training (PR.AT)
  The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
- Data Security (PR.DS)
  Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Information Protection Processes and Procedures(PR.IP)
  Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance (PR.MA)
  Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
- Protective Technology (PR.PT)
  Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

**Detect(DE)**

- Anomalies and Events (DE.AE)
  Anomalous activity is detected in a timely manner and the potential impact of events is understood.

- Security Continuous Monitoring (DE.CM)
  The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection Processes (DE.DP)
  Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

**Respond(RS)**

- Response Planning (RS.RP)
  Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
- Communications (RS.CO)
  Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- Analysis (RS.AN)
  Analysis is conducted to ensure adequate response and support recovery activities.
- Mitigation(RS.MI)
  Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
- Improvements (RS.IM)
  Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

**Recover(RC)**

- Recovery Planning (RC.RP)
  Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
- Improvements (RC.IM)
  Recovery planning and processes are improved by incorporating lessons learned into future activities.

- Communications (RC.CO)
  Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

# Appendix B

# List of Active IEEE Nuclear Power Standards for ICS

7-4.3.2-2016 - Approved Draft Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations

308-2012 - Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations

336-2010 - Recommended Practice for Installation, Inspection, and Testing for Class 1E Power, Instrumentation, and Control Equipment at Nuclear Facilities

338-2012 - Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety

497-2010 - Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations

572-2006 - Qualification of Class 1E Connection Assemblies for Nuclear Power Generating Stations

577-2012 - Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations

583-1982 - Standard Modular Instrumentation and Digital Interface System (CAMAC) (Computer Automated Measurement and Control)

596-1982 - Standard Parallel Highway Interface System (CAMAC) (Computer Automated Measurement and Control)

627-2010 - Qualification of Equipment Used in Nuclear Facilities

675-1982 - Standard Multiple Controllers in a CAMAC Crate (Computer Automated Measurement and Control)

692-2013 - Criteria for Security Systems for Nuclear Power Generating Stations

758-1979 - Standard Subroutines for Computer Automated Measurement and Control (CAMAC)

845-1999 - Guide for the Evaluation of Human-System Performance in Nuclear Power Generating Stations

960/1177-1993 - Standard FASTBUS Modular High-Speed Data Acquisition and Control System and IEEE FASTBUS Standard Routines

1023-2004 - Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities

1082-1997 - Guide for Incorporating Human Action Reliability Analysis for Nuclear

Power Generating Stations

1289-1998 - Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations

# Appendix C

# Detailed Comparison of Standards and Guidelines

## C.1. Guidelines

| NIST CSF 2014 | | WINS 4.3 Best Practices Guide | NIST SP800-53 | | NEI 08-09 | | IAEA Computer Security Guidelines | | NRC Reg Guide 5.71 | |
|---|---|---|---|---|---|---|---|---|---|---|
| *ID* | *Task* | *Section* | *ID* | *Task* | *ID* | *Task* | *ID* | *Task* | *ID* | *Task* |
| ID.AM-1 | Physical devices and systems within the organization are inventoried | Detecting attacks | CM-8 | Information System Component Inventory | Appendix D 4.5; Appendix E 10.9 | Device Identification and Authentication; Component Inventory | 5.3 | Asset Analysis and Management | A.3.1.3, C.11.3, C.11.9 | Identification of Critical Digital Assets, Baseline Configuration, Component Inventory |
| ID.AM-2 | Software platforms and applications within the organization are inventoried | Detecting attacks | CM-8 | Information System Component Inventory | Appendix D 5.1; Appendix E 10.9 | Removal of Unnecessary Services and Programs; Component Inventory | 5.3 | Asset Analysis and Management | A.3.1.3, B.5.1, C.11.3, C.11.9 | Identification of Critical Digital Assets, Removal of Unnecessary Services and Programs, Baseline Configuration, Component Inventory |
| ID.AM-3 | Organizational communication and data flows are mapped | Detecting attacks | AC-4, CA-3, CA-9, PL-8 | Information Flow Enforcement, System Interconnections, Internal System Connections,Information Security Architecture | | | 5.3 | Asset Analysis and Management (Dataflow analysis) | C.11.9 | Component Inventory |
| ID.AM-4 | External information systems are catalogued | Detecting attacks | AC-20, SA-9 | Use of External Information Systems, External Information System Services | Appendix D 5.1 | Removal of Unnecessary Services and Programs | | | B.1.20, C.11.3 | Proprietary Protocol Visibility, Baseline Configuration |
| ID.AM-5 | Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | Designing a Robust Security Infrastructure for IT and IC Systems: Risk Assessment | CP-2, RA-2, SA-14 | Contingency Plan, Security Categorization, Criticality Analysis | Appendix D 3.5 | Resource Priority | 5.41 | Safety Importance - lays this out | A.3.1.3, B.3.5 | Identification of Critical Digital Assets, Resource Priority |
| ID.AM-6 | Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | Defining Roles and Responsibilities for IT and IC security | CP-2, PS-7, PM-11 | Contingency Plan, Third-Party Personnel Security, Mission/Business Process Definition | Appendix E 8.1 | Contingency Plan | 7.6 | Third party/vendor access control procedure | A.3.1.2, C.5.2 | Cyber Security Team, Third Party/Escorted Access |
| ID.BE-1 | The organization's role in the supply chain is identified and communicated | Using a Design Basis Threat for cyber security | CP-2, SA-12 | Contingency Plan, Supply Chain Protection | | | | | | |
| ID.BE-2 | The organization's place in critical infrastructure and its industry sector is identified and communicated | Using a Design Basis Threat for cyber security | PM-8 | Critical Infrastructure Plan | | | 6.2 | Risk assessment and management (not communicated, identified for purpose of risk assessment) | | |
| ID.BE-3 | Priorities for organizational mission, objectives, and activities are established and communicated | | PM-11, SA-14 | Mission/Business Process Definition, Criticality Analysis | | | | | | |
| ID.BE-4 | Dependencies and critical functions for delivery of critical services are established | Design Principles: Providing defence in depth | CP-8, PE-9, PE-11, PM-8, SA-14 | Telecommunications Services, Power Equipment and Cabling, Emergency Power, Critical Infrastructure Plan, Criticality Analysis | Appendix D 3.2 | Application Partitioning/ Security Function Isolation | 5.3 | Asset Analysis and Management | A.3.1.4 | Reviews and Validation Testing |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established | Designing a Robust Security Infrastructure for IT and IC Systems: Risk Assessment | CP-2, CP-11, SA-14 | Contingency Plan | Appendix D 3.21 | Fail In Known (Safe) State | Section 3 | Business operational requirements | A.3.1.3, B.3.22 | Identification of Critical Digital Assets, Fail in Known State |
| ID.GV-1 | Organizational information security policy is established | Responding to attacks | -1 controls from all families | | Appendix E 1.1, 3.1 | Media Protection Policy and Procedures; System and Information Integrity Policy and Procedures | 5.5.3 | Generic: Policies and practices are defined for each level | Appendix A A.3.1.1 | Security Assessment and Authorization |
| ID.GV-2 | Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | Lifecycle Management | PM-1, PS-7 | Information Security Program Plan, Third-Party Personnel Security | | | | | A.3.1.1, A.3.1.2, C.10.5 | Security Assessment and Authorization, Cyber Security Team, Cross-Functional Cyber Security Team |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ID.GV-3 | Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | Responding to attacks | -1 controls from all families (except PM-1) | | | | Section 3 | Legislative and regulatory compliance | A.1, A.5 | Document Control and Record Retention and Handling |
| ID.GV-4 | Governance and risk management processes address cybersecurity risks | Using a Design Basis Threat for cyber security | PM-9, PM-11 | Risk Management Strategy, Mission/Business Process Definition | | | 7.3 | Demand for additional connectivity and related consequences | | |
| ID.RA-1 | Asset vulnerabilities are identified and documented | Design Principles: Integrating Physical and Cyber Security | CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 | Security Assessments, Continuous Monitoring, Penetration Testing, Risk Assessment, Vulnerability Scanning, Information System Documentation, Developer Security Testing and Evaluation, Flaw Remediation, Information System Monitoring, Security Alerts, Advisories, and Directives | Appendix E 3.2, 12 | Flaw Remediation, Evaluate and Manage Cyber Risk | 6.2 | Risk assessment and management | A.3.1.3, C.13.1 | Identification of Critical Digital Assets, Threat and Vulnerability Management |
| ID.RA-2 | Threat and vulnerability information is received from information sharing forums and sources | Cyber DBTs | PM-15, PM-16, SI-5 | Contacts with Security Groups and Associations, Threat Awareness Program, Security Alerts, Advisories, and Directives | Appendix E 3.5 | Security Alerts and Advisories | | | C.3.4, C.3.5, C.10.9 | Monitoring Tools and Techniques, Security Alerts and Advisories, Contacts with Security Groups and Associations |
| ID.RA-3 | Threats, both internal and external, are identified and documented | Using a Design Basis Threat for cyber security, Designing a Robust Security Infrastructure for IT and IC Systems: Risk Assessment | RA-3, SI-5, PM-12, PM-16 | Risk Assessment; Security Alerts, Advisories, and Directives; Insider Threat Program; Threat Awareness Program | Appendix E 7.4 | Incident Handling | 6.3.2 | Attacker profiles | | |
| ID.RA-4 | Potential business impacts and likelihoods are identified | Build a business case for security | RA-2, RA-3, PM-9, PM-11, SA-14 | Security Categorization; Risk Assessment; Risk Management Strategy; Mission/Business Process Definition; Criticality Analysis | | | | | A.3.1.2 | Cyber Security Team |
| ID.RA-5 | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | Designing a Robust Security Infrastructure for IT and IC Systems: Risk Assessment | RA-2, RA-3, PM-16 | Security Categorization; Risk Assessment; Threat Awareness Program | Appendix E 10.5 | Security Impact Analysis | 6.4 | Simplified outcomes of risk assessment | A.4.2.2, C.3.2 | Security Impact Analysis of Changes and Environment, Flaw Remediation |
| ID.RA-6 | Risk responses are identified and prioritized | Responding to attacks | PM-4, PM-9 | Plan of Action and Milestones Process; Risk Management Strategy | Appendix E 7.1 | Incident Response Policy and Procedures | | | A.4.2.2, B.1.20, C.3.11 | Security Impact Analysis of Changes and Environment, Proprietary Protocol Visibility, Anticipated Failure Response |
| ID.RM-1 | Risk management processes are established, managed, and agreed to by organizational stakeholders | Designing a Robust Security Infrastructure for IT and IC Systems: Risk Assessment | PM-9 | Risk Management Strategy | | | 6.2 | Risk assessment and management | A.4.1.2, C.8.8 | Effectiveness Analysis, Cyber Incident Response Plan |
| ID.RM-2 | Organizational risk tolerance is determined and clearly expressed | Designing a Robust Security Infrastructure for IT and IC Systems: Risk Assessment | PM-9 | Risk Management Strategy | Appendix D 4.2 | Cyber Security Controls | | | | |
| ID.RM-3 | The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | Designing a Robust Security Infrastructure for IT and IC Systems: Risk Assessment | PM-8, PM-9, PM-11, SA-14 | Critical Infrastructure Plan; Risk Management Strategy; Mission/Business Process Definition; Criticality Analysis | | | Sec 3 | Formal risk analysis | | already sector specific |
| PR.AC-1 | Identities and credentials are managed for authorized devices and users | Operations | AC-2, IA Family | Account Management; Identification and Authentication | Appendix D 1.1, 4.2, 4.6; Appendix E 5.4 | Access control policy and procedures, User Identification and Authentication, Identifier Management; Physical Access Authorizations | 5.5.3 | Generic: Appropriate access control and user authentication are in place | B.1.1.1, B.4.1, B.4.2, B.4.6 | Access Control Policy and Procedures, Identification and Authentication Policies and Procedures, User Identification and Authentication, Identifier Management |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| PR.AC-2 | Physical access to assets is managed and protected | Design Principles: Zoning & Compartmentalising, Integrating Physical and Cyber Security, Operations | PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 | Physical Access Authorizations; Physical Access Control; Access Control for Transmission Medium; Access Control for Output Devices; Power Equipment and Cabling | Appendix D 3.2, 4.2 | Application Partitioning/ Security Function Isolation, User Identification and Authentication | 5.2.1, 5.5.3 (G) | Physical access; Generic: Physical access to components and systems is restricted according to their function | A.3.1.6, B.1.15, B.5.4, C.5.4, C.5.5, C.5.6 | Application of Security Controls, Network Access Control, Hardware Configuration, Physical Access Authorization, Physical Access Control, Access Control for Transmission Medium |
| PR.AC-3 | Remote access is managed | Design Principles: Integrating Physical and Cyber Security | AC‑17, AC-19, AC-20 | Remote Access; Access Control for Mobile Devices; Use of External Information Systems | 3.10- | Unauthorized Remote Activation of Services | 5.41 | Safety importance | A.3.1.6, B.1.15, B.5.4, C.5.4, C.5.5, C.5.6 | Access Control Policy and Procedures, Unauthorized Remote Activation of Services |
| PR.AC-4 | Access permissions are managed, incorporating the principles of least privilege and separation of duties | Operations | AC-2, AC-3, AC-5, AC-6, AC-16 | Account Management; Access Enforcement; Separation of Duties; Least Privilege; Security Attributes | Appendix D 1.1, 4.2; Appendix E 1.2 | Access control policy and procedures, User Identification and Authentication; Media Access | 5.5.3 | Generic: Staff permitted access to the system must be suitably qualified and experienced and security cleared where necessary | B.1.1, B.1.2, B.1.5, B.1.6 | Access Control Policy and Procedures, Account Management, Separation of Functions, Least Privilege |
| PR.AC-5 | Network integrity is protected, incorporating network segregation where appropriate | Design Principles: Zoning & Compartmentalising, Implementing detection and monitoring capability | AC-4, SC-7 | Information Flow Enforcement; Boundary Protection | Appendix D 1.15 | Network Access Control | 5.5.3 | Level 1: Measures to ensure the integrity and availability of the systems are typically explained as a part of the safety cases | B.3.2, B.3.6, C.6 | Application Partitioning and Security Function Isolation, Transmission Integrity, Defensive Strategy |
| PR.AT-1 | All users are informed and trained | Raising the need for cyber security and developing a comprehensive security culture; Developing Skills and Competencies | AT-2, PM-13 | Security Awareness Training; Information Security Workforce | Appendix E 9.1 | Cyber Security Awareness and Training | 5.5.3 | Generic: Security operating procedures are written for and read by all users | A.3.1.3, C.9.4, C.10.1 | Identification of Critical Digital Assets, Contingency Plan Training, Cyber Security Awareness and Training |
| PR.AT-2 | Privileged users understand roles & responsibilities | Defining Roles and Responsibilities for IT and IC Security: Operations, Information Technology; Developing Skills and Competencies | AT-3, PM-13 | Role-Based Security Training, Information Security Workforce | Appendix E 9.2 | Technical Training | Section 3 | Competency requirements for key persons | A.3.1.2, C.10.1, C.10.3 | Cyber Security Team, Cyber Security Awareness and Training, Technical Training |
| PR.AT-3 | Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities | Defining Roles and Responsibilities for IT and IC Security: Maintenance, Vendors & Contractors, Lifecycle Management; Raising the need for cyber security and developing a comprehensive security culture | PS-7, SA-9 | Third-Party Personnel Security, External Information System Services | Appendix E 5.1, 9.2 | Physical and Operational Environment Protection Policies and Procedures, Awareness Training | 7.5, 7.6 | Secure Design and Specifications for Computer Systems: Formalization of security requirements should be done as part of contractual negotiation with suppliers (ISO 15408); Third party/vendor access control procedure | A.3.1.3, B.1.22, C.5.2, C.10.1 | Identification of Critical Digital Assets, Use of External Systems, Third Party/Escorted Access, Cyber Security Awareness and Training |
| PR.AT-4 | Senior executives understand roles & responsibilities | Defining Roles and Responsibilities for IT and IC Security | AT-3, PM-13 | Role-Based Security Training, Information Security Workforce | | | Section 3 | Competency requirements for key persons | C.10.1 | Cyber Security Awareness and Training |
| PR.AT-5 | Physical and information security personnel understand roles & responsibilities | Defining Roles and Responsibilities for IT and IC Security, Raising the need for cyber security and developing a comprehensive security culture | AT-3, PM-13 | Role-Based Security Training, Information Security Workforce | Appendix D 1.5; Appendix E 5.1, 5.2, 7.4, 9.4 | Separation of Functions: Establishes and documents divisions of responsiiblity and separates functions; Physical and Operational Environment Protection Policies and Procedures, Third Party/Escorted Access, Incident Handling, Specialized Cyber Security Training | 5.2.1 | Physical security | A.3.1.2, A.3.2, C.5.1, C.10.4 | Cyber Security Team, Incorporating the Cyber Security Program into the Physical Protection Program, Physical and Environmental Protection Policies and Procedures, Specialized Cyber Security Technical Training |
| PR.DS-1 | Data-at-rest is protected | | SC-28 | Protection of Information at Rest | Appendix D 3.19 | Confidentiality of Information at Rest | | | B.3.20 | Confidentiality of Information at Rest |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| PR.DS-2 | Data-in-transit is protected | | SC-8 | Transmission Confidentiality and Integrity | Appendix E 1.5 | Media Transport | | | B.3.6, B.3.7 | Transmission Integrity, Transmission Confidentiality |
| PR.DS-3 | Assets are formally managed throughout removal, transfers, and disposition | Lifecycle Management | CM-8, MP-6, PE-16 | Information System Component Inventory; Media Sanitization; Delivery and Removal | | | | | A.4 | Maintaining the Cyber Security Program |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | | AU-4, CP-2, SC-5 | Audit Storage Capacity; Contingency Plan; Denial of Service Protection | Appendix D 3.4 | Denial of Service Protection | 5.5.3 | Level 1: Measures to ensure the integrity and availability of the systems are typically explained as part of the safety cases | B.3.4, C.9.2 | Denial of Service Protection, Contingency Plan |
| PR.DS-5 | Protections against data leaks are implemented | Defining Roles and Responsibilities for IT and IC Security: Vendors & Contractors, Risk Assessment | AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 | Information Flow Enforcement; Separation of Duties; Least Privilege; Boundary Protection; Trasmission Confidentiality and Integrity; Cryptographic Protection; Covert Channel Analysis; Information System Monitoring | Appendix D 1.23, 3.7; Appendix E 3.10, 5.7 | Public Access Access Protections, Transmission Confidentiality; Information Output Handling and Retention, Access Control for Display Medium | | | B.1.23, B.3.7, C.1.1, C.3.9, C.3.10 | Publicly Accessible Content, Transmission Confidentiality, Media Protection Policy and Procedures, Error Handling, Information Output Handling and Retention |
| PR.DS-6 | Integrity checking mechanisms are used to verify software, firmware, and information integrity | Design Principles: Implementing detection and monitoring capability,Lifecycle Management; Detecting attacks: Maintenance ports | SI-7 | Software, Firmware, and Information Integrity | Appendix D 3.6; Appendix E 3.7 | Transmission Integrity; Software and Information Integrity (every 92 days) | 5.5.3 | Level 1: Measures to ensure the integrity and availability of the systems are typically explained as part of the safety cases | C.3.1, C.3.7 | System and Information Integrity Policy and Procedures, Software and Information Integrity |
| PR.DS-7 | The development and testing environment(s) are separate from the production environment | Perform penetration testing | CM-2 | Baseline Configuration | | | | | A.4.1.3, C.11.3 | Vulnerability Assessments and Scans, Baseline Configuration |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained | Detecting attacks | CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 | Baseline Configuration; Configuration Change Control; Security Impact Analysis; Access Restrictions for Change; Configuration Settings; Least Functionality; Configuration Management Plan; Developer Configuration Management | Appendix E 10.3 | Baseline Configuration | Section 3 | Configuration management | C.11.3, C.11.7 | Baseline Configuration, Configuration Settings |
| PR.IP-2 | A System Development Life Cycle to manage systems is implemented | Lifecycle Management | SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8 | System Development Life Cycle; Acquisition Process; Security Engineering Principles; Developer Configuration Management; Developer Security Testing and Evaluation; Supply Chain Protection; Development Process, Standards, and Tools; Developer Security Architecture and Design; Information Security Architecture | | | | | C.3 | Establishing and Implementing a Cyber Security Program |
| PR.IP-3 | Configuration change control processes are in place | Operations | CM-3, CM-4, SA-10 | Configuration Change Control; Security Impact Analysis; Developer Configuration Management | Appendix E 10.4 | Configuration Change Control | Section 3 | Configuration management | A.4.2.1, B.5.3, C.11.1, C.11.2, C.11.4 | Configuration Management, Changes to File System and Operating System Permissions, Configuration Management, Configuration Management Policy and Procedures, Configuration Change Control |
| PR.IP-4 | Backups of information are conducted, maintained, and tested periodically | Defining Roles and Responsibilities for IT and IC Security: Maintenance, Design Principles: Resiliency and Reliability | CP-4, CP-6, CP-9 | Contingency Plan Testing; Alternate Storage Site; Information System Backup | Appendix E 8.5 | CDA Backups | 5.5.3 | Generic: Appropriate backup/recovery procedures are in place | C.8.1, C.9.6 | Incident Response Policy and Procedures, CDA Backups |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| PR.IP-5 | Policy and regulations regarding the physical operating envrionment for organizational assets are met | Responding to attacks | PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 | Emergency Shutoff; Emergency Lighting; Fire Protection; Temperature and Humidity Controls; Water Damage Protection; Location of Information System Components | Appendix E 5.3 | Physical and Environmental Protection | Section 3 | Legislative and regulatory compliance | C.5.1, C.5.3 | Physical and Environmental Protection Policies and Procedures, Physical and Environmental Protection |
| PR.IP-6 | Data is destroyed according to policy | Lifecycle Management | MP-6 | Media Sanitization | Appendix E 3.10 | Information Output Handling and Retention | | | B.2.2, C.1.6 | Auditable Events, Media Sanitation and Disposal |
| PR.IP-7 | Protection processes are continuously improved | | CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 | Security Assessments; Continuous Monitoring; Contingency Plan; Incident Response Plan; System Security Plan; Information Security Measures of Performance | | | Section 3 | Amendment and approval of computer security measures | A.3.1.2 | Cyber Security Team |
| PR.IP-8 | Effectiveness of protection technologies is shared with appropriate parties | | AC-21, CA-7, SI-4 | Information Sharing; Continuous Monitoring; Information System Monitoring | Appendix E 3.6 | Security Functionality Verification | | | A.4.1.3, A.4.3, B.2.1, C.3.3 | Vulnerability Assessments and Scans, Cyber Security Program Review, Audit and Accountability Policy and Procedures, Malicious Code Protection |
| PR.IP-9 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | Responding to attacks | CP-2, IR-8 | Contingency Plan; Incident Response Plan | Appendix E 7.1 | Incident Response Policy and Procedures | 5.5.3 | Generic: Appropriate backup/recovery procedures are in place | C.8.1, C.8.3, C.8.8 | Incident Response Policy and Procedures, Incident Handling, Cyber Incident Response Plan |
| PR.IP-10 | Response and recovery plans are tested | Responding to attacks | CP-4, IR-3, PM-14 | Contingency Plan Testing; Incident Response Handling; Testing, Training, and Monitoring | Appendix E 7.1, 7.2 | Incident Response Policy and Procedures, Incident Response Training | | | C.8.1, C.8.3 | Incident Response Policy and Procedures, Incident Response Testing and Drills |
| PR.IP-11 | Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | Defining Roles and Responsibilities for IT and IC Security: Vendors & Contractors; Developing Skills and Competencies | PS Family | Personnel Security | Appendix D 3.2; Appendix E 2.1 | Application Partitioning/ Security Function Isolation; Personnel Security Policy and Procedures | 5.2.2 | Personnel security | C.2.1 | Personnel Security Policy and Procedures |
| PR.IP-12 | A vulnerability management plan is developed and implemented | | RA-3, RA-5, SI-2 | Risk Assessment; Vulnerability Scanning; Flaw Remediation | Appendix E 3.2 | Flaw Remediation | | | C.3.2 | Flaw Remediation |
| PR.MA-1 | Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | Defining Roles and Responsibilities for IT and IC Security: Maintenance, Operations; Detecting attacks: Maintenance ports | MA-2, MA-3, MA-5 | Controlled Maintenance; Maintenance Tools; Maintenance Personnel | Appendix E 4.1 | System Maintenance Policy and Procedures | 5.5.3, 7.1 | Level 1: Strict organizational and administrative procedures apply to any modifications, including hardware maintenance, updates and software modifications; Facility Lifetime Phases and Modes of Operation | B.51, B.5.3, B.5.5, C.3.2, C.4.1, C.4.2, C.11.5 | Removal of Unnecessary Services and Programs, Changes to File System and Operating System Permissions, Installing Operating Systems, Applications, and Third-Party Software Updates, Flaw Remediation, System Maintenance Policy and Procedures, Maintenance Tools, Security Impact Analysis of Changes and Environment |
| PR.MA-2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | Design Principles: Integrating Physical and Cyber Security, Lifecycle Management | MA-4 | Nonlocal Maintenance | | | 5.5.3 | Level 1: No remote maintenance access is allowed; Level 2: Remote maintenance access may be allowed on a case by case basis, must be protected with strong measures and users must respect a defined security policy | B.5.5 | Installing Operating systems, Applications, and Third-Party Software Updates |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | Perform internal and exterenal audits | AU Family | Audit and Accountability | Appendix D 2.1; Appendix E 7.4 | Audit and Accountability Policy and Procedures; Incident Handling | Section 3 | Regular reviews of implemented security measures (audits) by internal and external parties | A.4.2.4, A.4.3, B.2.1, B.2.3 | Updating Cyber Security Strategies, Cyber Security Program Review, Audit and Accountability Policy and Procedures, Content of Audit Records |
| PR.PT-2 | Removable media is protected and its use restricted according to policy | Design Principles: Integrating Physical and Cyber Security; Detecting attacks: USB ports and other user interfaces | MP-2, MP-4, MP-5, MP-7 | Media Access; Media Storage; Media Transport; Media Use | Appendix E 3.3 | Malicious Code Protection | 5.5.3 | Generic: Removable media must be controlled in accordance with security operating procedures | C.1.2, C.3.3 | Media Access, Malicious Code Protection |
| PR.PT-3 | Access to systems and assets is controlled, incorporating the principle of least functionality | Lifecycle Management, Operations | AC-3, CM-7 | Access Enforcement; Least Functionality | Appendix E 10.8 | Least Functionality | 5.5.3 | Generic: Users are given access only to those functions on the systems that they requirefor carrying out their jobs | C.11.8 | Least Functionality |
| PR.PT-4 | Communications and control networks are protected | | AC-4, AC-17, AC-18, CP-8, SC-7 | Information Flow Enforcement; Remote Access; Wireless Access; Telecommunications Services; Boundary Protection | Appendix D 3.8; Appendix E 7.4 | Trusted Path; Incident Handling | 7.3 | | B.1.17, B.3.1, B.3.18 | Wireless Access Restrictions, Critical Digital Asset and Communications Protection Policy and Procedures, Session Authenticity |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | Design Principles: Implementing detection and monitoring capability, Detecting attacks: Network gateways | AC-4, CA-3, CM-2, SI-4 | Information Flow Enforcement; System Interconnections; Baseline Configuration; Information System Monitoring | Appendix D 5.2, 9.5 | Host Intrusion Detection System, Situation Awareness | | | | |
| DE.AE-2 | Detected events are analyzed to understand attack targets and methods | | AU-6, CA-7, IR-4, SI-4 | Audit Review, Analysis, and Reporting; Continuous Monitoring; Incident Handling; Information System Monitoring | Appendix E 3.4 | Monitoring Tools and Techniques | Section 3 | Immediate analysis of computer security incidents and | | |
| DE.AE-3 | Event data are aggregated and correlated from multiple sources and sensors | | AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 | Audit Review, Analysis, and Reporting; Continuous Monitoring; Incident Handling; Incident Monitoring; Incident Response Plan; Information System Monitoring | Appendix D 2.12; Appendix E 3.1 | Audit Generation; System and Information Integrity Policy and Procedures | 5.5.3 | Generic: Computer and network security components are strictly logged and monitored | C.3.1, C.7 | System and Information Integrity Policy and Procedures, Defense-in-Depth |
| DE.AE-4 | Impact of events is determined | Responding to attacks | CP-2, IR-4, RA-3, SI -4 | Contingency Plan; Incident Handling; Risk Assessment; Information System Monitoring | Appendix D 2.3; Appendix E 3.3, 9.2 | Content of Audit Records; Malicious Code Protection, Awareness Training | | | | |
| DE-AE-5 | Incident alert thresholds are established | Design Principles: Implementing detection and monitoring capability; Responding to attacks | IR-4, IR-5, IR-8 | Incident Handling; Incident Monitoring; Incident Response Plan | Appendix E 7.1 | Incident Response Policy and Procedures | | | B.2.2, C.8.4 | Auditable Events, Incident Handling |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events | Design Principles: Implementing detection and monitoring capability, Detecting attacks: Network gateways | AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 | Account Management; Audit Generation; Continuous Monitoring; Configuration Change Control; Denial of Service Protection; Boundary Protection; Information System Monitoring | Appendix D 1.4, 5.2; Appendix E 3.4 | Information Flow Enforcement, Host Intrusion Detection System; Monitoring Tools and Techniques | 5.5.3 | Generic: Anomaly detection systems or procedures are in place | A.4.1, A.4.2.2, B.1.4, B.1.17, B.3.6 | Continuous Monitoring and Assessment, Security Impact Analysis of Changes and Environment, Information Flow Enforcement, Wireless Access Restrictions, Transmission Integrity |
| DE.CM-2 | The physical environment is monitored to detect potential cybersecurity events | Design Principles: Implementing detection and monitoring capability | CA-7, PE-3, PE-6, PE-20 | Continuous Monitoring; Physical Access Control; Monitoring Physical Access; Asset Monitoring and Tracking | Appendix D 3.2; Appendix E 5.3 | Application Partitioning/ Security Function Isolation; Physical & Environmental Protection | 5.2.1 | Physical security | B.1.15, C.5.3 | Network Access Control, Physical and Environmental Protection |
| DE.CM-3 | Personnel activity is monitored to detect potential cybersecurity events | | AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 | Account Management; Audit Generation; Monitoring for Information Disclosure; Continuous Monitoring; Software Usage Restrictions; User-Installed Software | Appendix D 1.11 | Supervision and Review - Access Control | 5.5.3 | Generic: Anomaly detection systems or procedures are in place | B.1.1, B.1.3, B.5.2 | Access Control Policy and Procedures, Access Enforcement, Host Intrustion Detection System |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| DE.CM-4 | Malicious code is detected | Design Principles: Implementing detection and monitoring capability | SI-3 | Malicious Code Protection | Appendix E 3.3 | Malicious Code Protection | | | B.5.2, C.3.3 | Host Intrustion Detection System, Malicious Code Protection |
| DE.CM-5 | Unauthorized mobile code is detected | | SC-18, SI-4. SC-44 | Mobile Code; Information System Monitoring; Detonation Chambers | Appendix D 3.13 | Mobile Code | | | B.3.14 | Mobile Code |
| DE.CM-6 | External service provider activity is monitored to detect potential cybersecurity events | Lifecycle Management | CA-7, PS-7, SA-4, SA-9, SI-4 | Continuous Monitoring; Third-Party Personnel Security; Acquisition Process; External Information System Services; Information System Monitoring | Appendix D 1.11, 1.21; Appendix E 5.2 | Supervision and Review - Access Control, Third Party Products and Controls; Third Party/Escorted Access | 7.6 | Third party/vendor access control procedure | B.1.3, B.5.2 | Access Enforcement, Host Intrustion Detection System |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | Design Principles: Implementing detection and monitoring capability; Detecting attacks: Maintenance ports | AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 | Audit Generation; Continuous Monitoring; Configuration Change Control; Information System Component Inventory; Physical Access Control; Monitoring Physical Access; Asset Moniotring and Tracking; Information System Monitoring | Appendix D 1.17, 1.18, 1.19, 3.2, 4.5; Appendix E 10.9 | Wireless Access Restrictions, Insecure and Rogue Connections, Access Control for Portable and Mobile devices, Application Partitioning/Security Function Isolation, Device Identification and Authentication; Component Inventory | | | A.4.1, B.1.18, B.1.19, B.4.5, C.3.4, C.3.7, C.5.8, C.5.9, C.11.9, C.13.1 | Continuous Monitoring and Assessment, Wireless Access Restrictions, Access Control for Portable and Mobile Devices, Device Identification and Authentication, Monitoring Tools and Techniques, Software and Information Integrity, Monitoring Physical Access, Visitor Control Access Records, Component Inventory, Threat and Vulnerability Management |
| DE.CM-8 | Vulnerability scans are performed | Design Principles: Integrating Physical and Cyber Security | RA-5 | Vulnerability Scanning | Appendix E 3.2, 12 | Flaw Remediation, Evaluate and Manage Cyber Risk | 5.5.3 | Generic: System vulnerability assessments are undertaken periodically | A.4.1.3, C.3.2, C.13.1 | Vulnerability Assessments and Scans, Flaw Remediation, Threat and Vulnerability Management |
| DE.DP-1 | Roles and responsibilities for detection are well defined to ensure accountability | Design Principles: Resiliency and Reliability | CA-2, CA-7, PM-14 | Security Assessments; Continuous Monitoring; Testing, Training, and Monitoring | | | | | C.8.2 | Incident Response Training |
| DE.DP-2 | Detection activities comply with all applicable requirements | | CA-2, CA-7, PM-14, SI-4 | Security Assessments; Continuous Monitoring; Testing, Training, and Monitoring; Information System Monitoring | | | Section 3 | Legislative and regulatory compliance | B.5.2, C.3.4 | Host Intrustion Detection System, Monitoring Tools and Techniques |
| DE.DP-3 | Detection processes are tested | Defining Roles and Responsibilities for IT and IC Security： Security, Design Principles: Integrating Physical and Cyber Security | CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 | Security Assessments; Continuous Monitoring; Physical Access Control; Testing, Training, and Monitoring; Malicious Code Protection; Information System Monitoring | Appendix E 3.4 | Monitoring Tools and Techniques | | | B.5.2, C.3.4 | Host Intrustion Detection System, Monitoring Tools and Techniques |
| DE.DP-4 | Event detection information is communicated to appropriate parties | Responding to attacks | AU-6, CA-2, CA-7, RA-5, SI-4 | Audit Review, Analysis, and Reporting; Security Assessments; Continuous Monitoring; Vulnerability Scanning; Information System Monitoring | Appendix D 1.8, 2.3; Appendix E 3.1, 3.5, 3.9 | System Use Notification, Content of Audit Records; System and Information Integrity Policy and Procedures, Security Alerts and Advisories, Error Handling | | | B.1.8, C.3.1, C.3.4, C.3.5 | System Use Notification, System and Information Integrity Policy and Procedures, Monitoring Tools and Techniques, Security Alerts and Advisories |
| DE.DP-5 | Detection processes are continuously improved | | CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 | Security Assessments; Continuous Monitoring; System Security Plan; Vulnerability Scanning; Information System Monitoring; Testing, Training, and Monitoring | Appendix E 3.3 | Malicious Code Protection | | | B.5.2 | Host Intrustion Detection System |
| RS.RP-1 | Response plan is executed during or after an event | Responding to attacks | CP-2, CP-10, IR-4, IR-8 | Contingency Plan; Information System Recovery and Reconstitution; Incident Handling; Incident Response Plan | Appendix D 1.4; Appendix E 3.5 | Information Flow Enforcement: Implements near-real time capabilities to respond to illegal or unauthorized information flows; Security Alerts and Advisories | | | C.3.1, C.3.3, C.8 | System and Information Integrity Policy and Procedures, Malicious Code Protection, Incident Response Plan |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| RS.CO-1 | Personnel know their roles and order of operations when a response is needed | Defining Roles and Responsibilities for IT and IC Security: Maintenance, Raising the need for cyber security and developing a comprehensive security culture | CP-2, CP-3, IR-3, IR-8 | Contingency Plan; Contingency Training; | Appendix E 7.1 | Incident Response Policy and Procedures | | | C.3.5, C.8.8 | Security Alerts and Advisories, Cyber Incident Response Plan |
| RS.CO-2 | Events are reported consistent with established criteria | Responding to attacks | AU-6, IR-6, IR-8 | Audit Review, Analysis, and Reporting; Incident Reporting; Incident Response Plan | Appendix D 2.3; Appendix E 3.9, 7.5 | Content of Audit Records; Error Handling, Incident Monitoring | Section 3 | Immediate analysis of computer security incidents and appropriate reporting | B.2.5, B.4.8, C.3.1, C.3.5, C.8, C.8.6 | Response to Audit Processing Failures, Authenticator Feedback, System and Information Integrity Policy and Procedures, Security Alerts and Advisories, Incident Response, Incident Reporting |
| RS.CO-3 | Information is shared consistent with response plans | Responding to attacks | CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 | Security Assessments; Continuous Monitoring; Contingency Plan; Incident Handling; Incident Response Plan; Monitoring Physical Access; Vulnerability Scanning; Information System Monitoring | Appendix D 2.3; Appendix E 3.5 | Content of Audit Records; Security Alerts and Advisories | Section 3 | Immediate analysis of computer security incidents and appropriate reporting | C.3.2, C.3.5, C.8 | Flaw Remediation, Security Alerts and Advisories, Incident Response |
| RS.CO-4 | Coordination with stakeholders occurs consistent with response plans | Responding to attacks | CP-2, IR-4, IR-8 | Contingency Plan; Incident Handling; Incident Response Plan | | | | | | |
| RS.CO-5 | Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | | PM-15, SI-5 | Contacts with Security Groups and Associations; Security Alerts, Advisories, and Directives | | | | | | |
| RS.AN-1 | Notifications from detection systems are investigated | Detecting attacks: Network gateways | AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 | Audit Review, Analysis, and Reporting; Continuous Monitoring; Incident Handling; Incident Monitoring; Monitoring Physical Access; Information System Monitoring | Appendix E 7.1 | Incident Response Policy and Procedures | | | C.8, C.8.1 | Incident Response, Incident Response Policy and Procedures |
| RS.AN-2 | The impact of the incident is understood | Responding to attacks | CP-2, IR-4 | Contingency Plan, Incident Handling | Appendix D 2.3 | Content of Audit Records | | | | |
| RS.AN-3 | Forensics are performed | Responding to attacks | AU-7, IR-4 | Audit Reduction and Report Generation, Incident Handling | Appendix D 2.3 | Content of Audit Records | | | C.8 | Incident Response |
| RS.AN-4 | Incidents are categorized consistent with response plans | Responding to attacks | CP-2, IR-4, IR-5, IR-8 | Contingency Plan, Incident Handling | | | | | | |
| RS.MI-1 | Incidents are contained | Responding to attacks | IR-4 | Incident Handling | Appendix E 3.1 | System and Information Integrity Policy and Procedures | | | C.3.1, C.8 | System and Information Integrity Policy and Procedures, Incident Response |
| RS.MI-2 | Incidents are mitigated | Responding to attacks | IR-4 | Incident Handling | Appendix E 3.3 | Malicious Code Protection | | | C.3.1, C.8 | System and Information Integrity Policy and Procedures, Incident Response |
| RS.MI-3 | Newly identified vulnerabilities are mitigated or documented as accepted risks | | CA-7, RA-3, RA-5 | Continuous Monitoring, Risk Assessment, Risk Assessment Update | Appendix E 3.2; 7.1, 12 | Flaw Remediation, Incident Response Policy and Procedures, Evaluate and Manage Cyber Risk | 5.5.3 | Generic: Application and system vulnerabilities are monitored, and appropriate measures are taken | A.4.2.2, B.1.21, C.3.2, C.8.1 | Security Impact Analysis of Changes and Environment, Third Party Products and Controls, Flaw Remediation, Incident Response Policy and Procedures |
| RS.IM-1 | Response plans incorporate lessons learned | | CP-2, IR-4, IR-8 | Contingency Plan, Incident Handling, Incident Response Plan | Appendix E 7.4 | Incident Handling | | | C.8.4 | Incident Handling |
| RS.IM-2 | Response strategies are updated | Responding to attacks | CP-2, IR-4, IR-8 | Contingency Plan, Incident Handling, Incident Response Plan | | | | | A.3.1.2, A.4.2.4, C.8.8 | Cyber Security Team, Updating Cyber Security Practices, Cyber Incident Response Plan |
| RC.RP-1 | Recovery plan is executed during or after an event | Design Principles: Resiliency and Reliability; Responding to attacks | CP-10, IR-4, IR-8 | Information System Recovery and Reconstitution, Incident Handling | | | | | C.8, C.9.1, C.9.7 | Incident Response, Contingency Planning Policy and Procedures, Recovery and Reconstitution |
| RC.IM-1 | Recovery plans incorporate lessons learned | | CP-2, IR-4, IR-8 | Contingency Plan, Incident Handling, Incident Response Plan | Appendix E 7.1 | Incident Response Policy and Procedures | | | | |
| RC.IM-2 | Recovery strategies are updated | | CP-2, IR-4, IR-8 | Contingency Plan, Incident Handling, Incident Response Plan | | | | | A.4.2.4 | Updating Cyber Security Strategies |
| RC.CO-1 | Public relations are managed | Responding to attacks | | | Appendix D 1.23 | Public Access Access Protections | | | | |
| RC.CO-2 | Reputation after an event is repaired | | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| RC.CO-3 | Recovery activities are communicated to internal stakeholders and executive and management teams | Design Principles: Resiliency and Reliability | CP-2, IR-4 | Contingency Plan, Incident Handling | | | | | C.8, C.8.4, C.9.1 | Incident Response, Incident Handling, Contingency Planning Policy and Procedures |

## C.2. Standards

| NIST CSF 2014 | | ISO 27001 | | ANSI/ISA 62443-2-1-2009 | | ANSI/ISA 62443-3-3: 2013 | | NERC CIPv5 | |
|---|---|---|---|---|---|---|---|---|---|
| *ID* | *Task* | *ID* | | *ID* | *Task* | *ID* | *Task* | *ID* | *Task* |
| ID.AM-1 | Physical devices and systems within the organization are inventoried | A.8.1.1, A.8.1.2 | Inventory of assets | 4.2.3.4 | Identify the industrial automation and control systems | SR 7.8 | Control system component inventory | 003 R2 | Not required for low impact systems |
| ID.AM-2 | Software platforms and applications within the organization are inventoried | A.8.1.1, A.8.1.2 | Inventory of assets, Ownership of assets | 4.2.3.4 | Identify the industrial automation and control systems | SR 7.8 | Control system component inventory | 003 R2 | Not required for low impact systems |
| ID.AM-3 | Organizational communication and data flows are mapped | A.13.2.1 | Information transfer policies and procedures | 4.2.3.4 | Identify the industrial automation and control systems | | | | |
| ID.AM-4 | External information systems are catalogued | A.11.2.6 | Security of equipment and assets off-premises | | | | | 003 R2 | Not required for low impact systems |
| ID.AM-5 | Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | A.8.2.1 | Classification of information | 4.2.3.6 | Prioritize systems | | | 002 R1 | |
| ID.AM-6 | Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | A.6.1.1 | Information security roles and responsibilities | 4.3.2.3.3 | Define the organizational responsibilities | | | 008 R1.3 | Cyber Security Incident Response Plan Specifications |
| ID.BE-1 | The organization's role in the supply chain is identified and communicated | A.15.1.3, A.15.2.1, A.15.2.2 | Information and communication technology supply chain, Monitoring and review of supplier services, Managing changes to supplier services | | | | | | |
| ID.BE-2 | The organization's place in critical infrastructure and its industry sector is identified and communicated | | | | | | | | |
| ID.BE-3 | Priorities for organizational mission, objectives, and activities are established and communicated | | | 4.2.2.1, 4.2.3.6 | Develop a business rationale, Prioritize systems | | | | |
| ID.BE-4 | Dependencies and critical functions for delivery of critical services are established | A.11.2.2, A.11.2.3, A.12.1.3 | Supporting utilities; Cabling Security; Capacity management | | | | | | |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established | A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 | Protecting against external and environmental threats; Planning information security continuity; Implementing information security continuity; Availability of information processing facilities | | | | | | |
| ID.GV-1 | Organizational information security policy is established | A.5.1.1 | Policies for information security | 4.3.2.6 | Prioritize systmes | | | CIP-003-5 (R1) | |
| ID.GV-2 | Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | A.6.1.1, A.7.2.1 | Information security roles and responsibilities; Management responsibilities | 4.3.2.3.3 | Define the organizational responsibilities | | | | |
| ID.GV-3 | Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | A.18.1 | Identification of applicable legislation and contractual requirements; Intellectual property rights; Protection of records; Privacy and protection of personally identifiable information; Regulation of cryptographic controls | 4.4.3.7 | Monitor and evaluate applicable legislation relevant to cyber security | | | | |
| ID.GV-4 | Governance and risk management processes address cybersecurity risks | | | 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 | Select a risk assessment methodology; Conduct a high-level risk assessment; Identify a detailed risk assessment methodology; Conduct a detailed risk assessment; Integrate physical, HSE and cyber security risk assessment results; Provide training for support personnel; Maintain consistency between risk management systems | | | | |
| ID.RA-1 | Asset vulnerabilities are identified and documented | A.12.6.1, A.18.2.3 | Management of technical vulnerabilities; Technical compliance review | 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 | Risk identification, classification, and assessment; Perform a detailed vulnerability assessment; Conduct a detailed risk assessment; Conduct risk assessments throughout the lifecycle of the IACS | | | CIP-003-5 (R2) | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ID.RA-2 | Threat and vulnerability information is received from information sharing forums and sources | A.6.1.4 | Contact with special interest groups | 4.2.3, 4.2.3.9, 4.2.3.12 | Risk identification, classification, and assessment; Conduct a detailed risk assessment; Conduct risk assessments throughout the lifecycle of the IACS | | | 007 R3 | Malicious Code Prevention |
| ID.RA-3 | Threats, both internal and external, are identified and documented | | | 4.2.3, 4.2.3.9, 4.2.3.12 | Risk identification, classification, and assessment; Conduct a detailed risk assessment; Conduct risk assessments throughout the lifecycle of the IACS | | | | |
| ID.RA-4 | Potential business impacts and likelihoods are identified | A.12.6.1 | Information security risk assessment | 4.2.3, 4.2.3.9, 4.2.3.12 | Risk identification, classification, and assessment; Conduct a detailed risk assessment; Conduct risk assessments throughout the lifecycle of the IACS | | | | |
| ID.RA-5 | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | A.12.6.1 | Information security risk assessment | | | | | | |
| ID.RA-6 | Risk responses are identified and prioritized | | | | | | | | |
| ID.RM-1 | Risk management processes are established, managed, and agreed to by organizational stakeholders | | | 4.3.4.2 | Risk management and implementation | | | | |
| ID.RM-2 | Organizational risk tolerance is determined and clearly expressed | | | 4.3.2.6.5 | Determine the organization's tolerance for risk | | | | |
| ID.RM-3 | The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | | | | | | | | |
| PR.AC-1 | Identities and credentials are managed for authorized devices and users | A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 | User registration and de-registration; User access provisioning; Management of secret authentication information of users; Use of secret authentication information; Secure log-on procedures; Password management system | 4.3.3.5.1 | Access accounts implement authorization security policy | SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 | Human user identification and authentication; Software process and device identification and authentication; Account management; Identifier Management; Authenticator management; Strength of password based authentication; PKI certificates; Strength of public key authentication | 007 R5 | System Access Control |
| PR.AC-2 | Physical access to assets is managed and protected | A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 | Physical security perimeter; Physical entry controls; Protecting against external and environmental threats; Delivery and loading areas; Cabling security | 4.3.3.3.2, 4.3.3.3.8 | Establish physical security perimeter(s); Establish procedures for monitoring and alarming | | | 004 B R4, 006 R1 | Access Management Program, Physical Security Plan |
| PR.AC-3 | Remote access is managed | A.6.2.2, A.13.1.1, A.13.2.1 | Teleworking; Network controls; Information transfer policies and procedures | 4.3.3.6.6 | Develop a policy for remote login and connections | SR 1.13, SR 2.6 | Access via untrusted networks; Remote session termination | 004 B R4, 005 R2 | Access Management Program, Interactive Remote Access Management |
| PR.AC-4 | Access permissions are managed, incorporating the principles of least privilege and separation of duties | A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 | Segregation of duties; Access to networks and network services; Management of privileged access rights; Information access restriction; Use of privileged utility programs | 4.3.3.7.3 | Control access to information or systems via role-based access accounts | SR 2.1 | Authorization enforcement | 004 B R4, 007 R5 | Access Management Program (does not mention least privilege), System Access Control (") |
| PR.AC-5 | Network integrity is protected, incorporating network segregation where appropriate | A.13.1.1, A.13.1.3, A.13.2.1 | Network controls; Segregation in networks; Information transfer policies and procedures | 4.3.3.4 | Network segmentation | SR 3.1, SR 3.8 | Communication integrity; Session integrity | 005 R1 | Electronic Security Perimeter |
| PR.AT-1 | All users are informed and trained | A.7.2.2 | Information security awareness, education and training | 4.3.2.4.2 | Provide procedure and facility training | | | 004 B R1 | Security Awareness Program |
| PR.AT-2 | Privileged users understand roles & responsibilities | A.6.1.1, A.7.2.2 | Information security roles and responsibilities; Information security awareness, education and training | 4.3.2.4.2, 4.3.2.4.3 | Provide procedure and facility training; Provide training for support personnel | | | 004 B R2 | Cyber Security Training Program |
| PR.AT-3 | Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities | A.6.1.1, A.7.2.2 | Information security roles and responsibilities; Information security awareness, education and training | 4.3.2.4.2 | Provide procedure and facility training | | | | |
| PR.AT-4 | Senior executives understand roles & responsibilities | A.6.1.1, A.7.2.2 | Information security roles and responsibilities; Information security awareness, education and training | 4.3.2.4.2 | Provide procedure and facility training | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| PR.AT-5 | Physical and information security personnel understand roles & responsibilities | A.6.1.1, A.7.2.2 | Information security roles and responsibilities; Information security awareness, education and training | 4.3.2.4.2 | Provide procedure and facility training | | | 004 B R2 | Cyber Security Training Program |
| PR.DS-1 | Data-at-rest is protected | A.8.2.3 | Handling of assets | | | SR 3.4, SR 4.1 | Software and information integrity; Information confidentiality | | |
| PR.DS-2 | Data-in-transit is protected | A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 | Handling of assets; Network controls; Information transfer policies and procedures; Electronic messaging; Securing application services on public networks; Protecting application services transactions | | | SR 3.1, SR 3.8, SR 4.1, SR 4.2 | Communication integrity; Session integrity; Information confidentiality; Information persistence | | |
| PR.DS-3 | Assets are formally managed throughout removal, transfers, and disposition | A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 | Handling of assets; Management of removable media; Disposal of media; Physical media transfer; Secure disposal or re-use of equipment | 4. 4.3.3.3.9, 4.3.4.4.1 | Establish procedures for the addition, removal, and disposal of assets; Develop lifecycle management processes for IACS information | SR 4.2 | Information persistence | | |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | A.12.3.1 | Information backup | | | SR 7.1, SR 7.2 | Denial of service protection; Resource management | | |
| PR.DS-5 | Protections against data leaks are implemented | A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 | Segregation of duties; Screening; Terms and conditions of employment; Termination or change of employment responsibilities; Labelling of information; Handling of assets; Access control policy; Access to networks and network services; Mangement of privileged access rights; Information access restriction; Use of privileged utility programs; Access control to program source code; Segregation in networks; Information transfer policies and procedures; Electronic messaging; Confidentiality or non-disclosure agreements; Securing application services on public networks; Protecting application services transactions | | | SR 5.2 | Zone boundary protection | | |
| PR.DS-6 | Integrity checking mechanisms are used to verify software, firmware, and information integrity | A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 | Controls against malware; Installation of software on operational systems; Securing application services on public networks; Protecting application services transactions | | | SR 3.1, SR 3.3, SR 3.4, SR 3.8 | Communication integrity; Security functionality verification; Software and information integrity; Session integrity | | |
| PR.DS-7 | The development and testing environment(s) are separate from the production environment | A.12.1.4 | Separation of development, testing and operational environments | | | | | | |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained | A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 | Change mangement; Installation of software on operational systems; Restriction on software installation; System change control procedures; Technical review of applications after operating platform changes; Restrictions on changes to software packages | 4.3.4.3.2, 4.3.4.3.3 | Develop and implement a change management system; Assess all the risks of changing the IACS | SR 7.6 | Network and security configuration settings | | |
| PR.IP-2 | A System Development Life Cycle to manage systems is implemented | A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 | Information security in project management; Information security requirements analysis and specification; Secure developemnt policy; Secure system engineering principles | 4.3.4.3.3 | Assess all the risks of changing the IACS | | | | |
| PR.IP-3 | Configuration change control processes are in place | A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 | Change mangement; Installation of software on operational systems; Restriction on software installation; System change control procedures; Technical review of applications after operating platform changes; Restrictions on changes to software packages | 4.3.4.3.2, 4.3.4.3.3 | Develop and implement a change management system; Assess all the risks of changing the IACS | SR 7.6 | Network and security configuration settings | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| PR.IP-4 | Backups of information are conducted, maintained, and tested periodically | A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 | Information backup; Implementing information security continuity; Verify, review and evaluate information security continuity; Protection of records | 4.3.4.3.9 | Establish backup and restoration procedure | SR 7.3, SR 7.4 | Control system backup; Control system recovery and reconsitution | 009 R1.3, R2.2 | Recovery Plan Specifications, Recovery Plan Implementation and Testing |
| PR.IP-5 | Policy and regulations regarding the physical operating envrionment for organizational assets are met | A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 | Protecting against external and environmental threats; Equipment siting and protection; Supporting utilities; Cabling security | 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 | Establish complementary physical and cyber security policies; Establish physical security perimeter(s); Provide entry controls; Require employees to follow security procedures; Protect connections; Maintain equipment needs | | | 003 Guidelines R1.3, 006 R1 | Physical Security of BES Cyber Systems, Physical Security Plan |
| PR.IP-6 | Data is destroyed according to policy | A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 | Handling of assets; Mangement of removable media; Disposal of media; Secure disposal or re-use of equipment | 4.3.4.4.4 | Ensure appropriate records control | SR 4.2 | Information persistence | | |
| PR.IP-7 | Protection processes are continuously improved | | | 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 | Assign an organization to manage and implement changes to the CSMS; Evaluate the CSMS periodically; Establish triggers to evaluate CSMS; Identify and implement corrective and preventive actions; Review risk tolerance; Monitor and evaluate industry CSMS strategies; Monitor and evaluate applicable legislation relevant to cyber security; Request and report employee feedback on security suggestions | | | | |
| PR.IP-8 | Effectiveness of protection technologies is shared with appropriate parties | A.16.1.6 | Learning from information security incidents | | | | | | |
| PR.IP-9 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | A.16.1.1, A.17.1.1, A.17.1.2 | Responsibilities and procedures; Planning information security continuity; Implementing information security continuity | 4.3.2.5.3, 4.3.4.5.1 | Develop and implement business continuity plans; Implement an incident response plan | | | 008 R1.1 | Cyber Security Incident Response Plan Specifications |
| PR.IP-10 | Response and recovery plans are tested | A.17.1.3 | Verify, review and evaluate information security continuity | 4.3.2.5.7, 4.3.4.5.11 | Test and update the business continuity plan; Conduct drills | SR 3.3 | Security functionality verification | 008 R2.1, 009 R2.1 | Cyber Security Incident Response Plan Implementation and Testing, Recovery Plan Implementation and Testing |
| PR.IP-11 | Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | A.7.1.1, A.7.3.1, A.8.1.4 | Screening; Termination or change of employment responsibilities; Return of assets | 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 | Establish a personnel security policy; Screen personnel initially; Screen personnel on an ongoing basis | | | 004 B R3 | Personnel Risk Assessment Program |
| PR.IP-12 | A vulnerability management plan is developed and implemented | A.12.6.1, A.18.2.2 | Management of technical vulnerabilities; Compliance with security policies and standards | | | | | 003 R2, 007 R2.3 | Security Patch Management |
| PR.MA-1 | Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | A.11.1.2, A.11.2.4, A.11.2.5 | Physical entry controls; Equipment maintenance; Removal of assets | 4.3.3.3.7 | Maintain equipment assets | | | 007 R2 | Security Patch Management |
| PR.MA-2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | A.11.2.4, A.15.1.1, A.15.2.1 | Equipment maintenance; Information security policy for supplier relationships; Monitoring and review of supplier services | 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 | Authenticate all users before system use; Develop a policy for remote login and connections; Disable access account after failed remote login attempts; Require re-authentication after remote system inactivity | | | 005 R2 | Interactive Remote Access Management |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 | Event logging; Protection of log information; Administrator and operator logs; Clock synchronisation; Information systems audit controls | 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 | Establish procedures for the addition, removal, and disposal of assets; Audit account administration; Audit the information and document management process | SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 | Auditable events; Audit storage capacity; Response to audit processing failures; Timestamps; Non-repudiation | 003 C1.2, 008 R2.3 | Evidence Retention, Cyber Security Incident Response Plan Implementation and Testing |
| PR.PT-2 | Removable media is protected and its use restricted according to policy | A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 | Labelling of information; Handling of assets; Management of removable media; Physical media transfer; Clear desk and clear screen policy | | | SR 2.3 | Use control for portable and mobile devices | 007 R4.2 | Security Event Monitoring |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| PR.PT-3 | Access to systems and assets is controlled, incorporating the principle of least functionality | A.9.1.2 | Access to networks and network services | 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 | Access accounts implement authorization security policy; Identify individuals; Authorize account access; Record access accounts; Sustend or remove unneeded accounts; Review account permissions; Change default passwords; Audit account administration; Develop an authentitication strategy; Authenticate all users before system use; Require strong authentication methods for system administration and application config; Develop a policy for remote login and connections; Disable access account after failed remote login attempts; Require re-authentication after remote system inactivity; Employ authentication for task-to-task communication; Define an authorization security policy; Establish appropriate logical and physical permission methods to access IACS devices; Control access to information or systems via role-based access account; Employ multiple authorization methods for critical IACS | SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 | Human user identification and authentication; Software process and device identification and authentication; Account management; Identifier Management; Authenticator management; Strength of password based authentication; Wireless access management; PKI certificates; Strength of public key authentication; Authenticator feedback; Unsuccessful login attempts; Access via untrusted networks; Authorization enforcement; Wireless use control; Use control for portable and mobile devices; Mobile code; Session lock; Remote session termination; Concurrent session control | 007 R5 | System Access Control (doesn't mention least functionality) |
| PR.PT-4 | Communications and control networks are protected | A.13.1.1, A.13.2.1 | Network controls; Information transfer policies and procedures | | | SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 | Communication integrity; Input validation; Session integrity; Information confidentiality; Use of cryptography; Network segmentation; Zone boundary protection; General purpose person-to-person communication restrictions; Denial of service protection; Network and secrity configuration settings | 005 R1.5 | Electronic Security Perimeter |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | | | 4.4.3.3 | Establish triggers to evaluate CSMS | | | | |
| DE.AE-2 | Detected events are analyzed to understand attack targets and methods | A.16.1.1, A.16.1.4 | Responsibilities and procedures; Assessment of and decision on information security events | 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 | Identify and respond to incidents; Identify failed and successful cyber security breaches; Document the details of incidents | SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 | Auditable events; Audit storage capacity; Response to audit processing failures; Timestamps; Non-repudiation; Protection of audit information; Audit log accessibility; Continuous monitoring | | |
| DE.AE-3 | Event data are aggregated and correlated from multiple sources and sensors | | | | | SR 6.1 | Audit log accessibility | | |
| DE.AE-4 | Impact of events is determined | | | | | | | | |
| DE-AE-5 | Incident alert thresholds are established | | | 4.2.3.10 | Identify the reassessment frequency and triggering criteria | | | 007 R4, 008 R1.2 | Security Event Monitoring, Cyber Security Incident Response Plan Specifications |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events | | | | | SR 6.2 | Continuous monitoring | 005 R1.5, 007 R3 | Electronic Security Perimeter, Malicious Code Prevention |
| DE.CM-2 | The physical environment is monitored to detect potential cybersecurity events | | | 4.3.3.3.8 | Establish procedures for monitoring and alarming | | | 006 R1.4 | Physical Security Plan |
| DE.CM-3 | Personnel activity is monitored to detect potential cybersecurity events | A.12.4.1 | Event logging | | | SR 6.2 | Continuous monitoring | 007 R5 | System Access Control |
| DE.CM-4 | Malicious code is detected | A.12.2.1 | Controls against malware | 4.3.4.3.8 | Establish and document antivirus/malware management procedure | SR 3.2 | Malicious code protection | 007 R3 | Malicious Code Prevention |
| DE.CM-5 | Unauthorized mobile code is detected | A.12.5.1 | Installation of software on operational systems | | | SR 2.4 | Mobile code | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| DE.CM-6 | External service provider activity is monitored to detect potential cybersecurity events | A.14.2.7, A.15.2.1 | Outsourced development; Monitoring and review of supplier services | | | | | | |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | | | | | | | 006 R1.6 | Physical Security Plan |
| DE.CM-8 | Vulnerability scans are performed | A.12.6.1 | Management of technical vulnerabilities | 4.2.3.1, 4.2.3.7 | Select a risk assessment methodology; Perform a detailed vulnerability assessment | | | 003 R2 | |
| DE.DP-1 | Roles and responsibilities for detection are well defined to ensure accountability | A.6.1.1 | Information security roles and responsibilities | 4.4.3.1 | Assign an organization to manage and implement changes to the CSMS | | | | |
| DE.DP-2 | Detection activities comply with all applicable requirements | A.18.1.4 | Privacy and protection of personally identifiable information | 4.4.3.2 | Evaluate the CSMS periodically | | | 003 C1.3 | Compliance Monitoring and Assessment Processes |
| DE.DP-3 | Detection processes are tested | A.14.2.8 | System security testing | 4.4.3.2 | Evaluate the CSMS periodically | SR 3.3 | Security functionality verification | 006 R3 | Physical Access Control System Maintenance and Testing Program |
| DE.DP-4 | Event detection information is communicated to appropriate parties | A.16.1.2 | Reporting information security events | 4.3.4.5.9 | Communicate the incident details | SR 6.1 | Audit log accessibility | 008 R1.2 | Cyber Security Incident Response Plan Specifications |
| DE.DP-5 | Detection processes are continuously improved | A.16.1.6 | Learning from information security incidents | 4.4.3.4 | Identify and implement corrective and preventive actions | | | | |
| RS.RP-1 | Response plan is executed during or after an event | A.16.1.5 | Response to information security incidents | 4.3.4.5.1 | Implement an incident response plan | | | 006 R1.5, 008 R2.2 | Physical Security Plan, Cyber Security Incident Response Plan Implementation and Testing |
| RS.CO-1 | Personnel know their roles and order of operations when a response is needed | A.6.1.1, A.16.1.1 | Information security roles and responsibilities; Responsibilities and procedures | 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 | Communicate the incident response plan; Establish a reporting procedure for unusal activities and events; Educate employees on reporting cyber security incidents | | | 004 B R2, 008 R3.1.3 | Cyber Security Training Program, Cyber Security Incident Response Plan Review, Update, and Communication |
| RS.CO-2 | Events are reported consistent with established criteria | A.6.1.3, A.16.1.2 | Contact with authorities; Reporting information security events | 4.3.4.5.5 | Report cyber security incidents in a timely manner | | | 003 C1.3, 006 R1.7, 007 R4, 008 R1.2 | Compliance Monitoring and Assessment Processes, Physical Security Plan, Security Event Monitoring, Cyber Security Incident Response Plan Specifications |
| RS.CO-3 | Information is shared consistent with response plans | A.16.1.2 | Reporting information security events | 4.3.4.5.2 | Communicate the incident response plan | | | 006 R1.5, 007 R4, 008 R1.2 | Physical Security Plan, Security Event Monitoring, Cyber Security Incident Response Plan Specifications |
| RS.CO-4 | Coordination with stakeholders occurs consistent with response plans | | | 4.3.4.5.5 | Report cyber security incidents in a timely manner | | | | |
| RS.CO-5 | Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | | | | | | | | |
| RS.AN-1 | Notifications from detection systems are investigated | A.12.4.1, A.12.4.3, A.16.1.5 | Event logging; Administrator and operator logs; Response to information security incidents | 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 | Identify and respond to incidents; Identify failed and successful cyber security breaches; Document the details of incidents | SR 6.1 | Audit log accessibility | 007 R4 | Security Event Monitoring |
| RS.AN-2 | The impact of the incident is understood | A.16.1.6 | Learning from information security incidents | 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 | Identify and respond to incidents; Identify failed and successful cyber security breaches; Document the details of incidents | | | | |
| RS.AN-3 | Forensics are performed | A.16.1.7 | Collection of evidence | | | SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 | Auditable events; Audit storage capacity; Response to audit processing failures; Timestamps; Non-repudiation; Protection of audit information; Audit log accessibility | | |
| RS.AN-4 | Incidents are categorized consistent with response plans | A.16.1.4 | Assessment of and decision on information security events | 4.3.4.5.6 | Identify and respond to incidents | | | | |
| RS.MI-1 | Incidents are contained | A.16.1.4 | Assessment of and decision on information security events | 4.3.4.5.6 | Identify and respond to incidents | SR 5.1, SR 5.2, SR 5.4 | Network segmentation; Zone boundary protection; Application partitioning | 008 R2.2 | Cyber Security Incident Response Plan Implementation and Testing |
| RS.MI-2 | Incidents are mitigated | A.12.2.1, A.16.1.5 | Controls against malware; Response to information security incidents | 4.3.4.5.6, 4.3.4.5.10 | Identify and respond to incidents; Address and correct issues discovered | | | 007 R3, 008 R2.2 | Malicious Code Prevention, Cyber Security Incident Response Plan Implementation and Testing |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| RS.MI-3 | Newly identified vulnerabilities are mitigated or documented as accepted risks | A.12.6.1 | Management of technical vulnerabilities | | | | | 007 R2 | Security Patch Management |
| RS.IM-1 | Response plans incorporate lessons learned | A.16.1.6 | Learning from information security incidents | 4.3.4.5.10, 4.4.3.4 | Address and correct issues discovered; Identify and implement corrective and preventive actions | | | 008 R3.1.2 | Cyber Security Incident Response Plan Review, Update, and Communication |
| RS.IM-2 | Response strategies are updated | | | | | | | 008 R3.1.2 | Cyber Security Incident Response Plan Review, Update, and Communication |
| RC.RP-1 | Recovery plan is executed during or after an event | A.16.1.5 | Response to information security incidents | | | | | 009 R1 | Recovery Plan Specifications |
| RC.IM-1 | Recovery plans incorporate lessons learned | | | | | | | 009 R3.1.2 | Recovery Plan Review, Update and Communication |
| RC.IM-2 | Recovery strategies are updated | | | | | | | 009 R3.1.2 | Recovery Plan Review, Update and Communication |
| RC.CO-1 | Public relations are managed | | | | | | | | |
| RC.CO-2 | Reputation after an event is repaired | | | | | | | | |
| RC.CO-3 | Recovery activities are communicated to internal stakeholders and executive and management teams | | | | | | | | |

# Appendix D

# Questionnaire

Initially IAEA safety guidelines NS-G-1.1, NS-G-1.3 and GS-G-3.1 were included however their focused was on safety and not specifically on cybersecurity; NS-G-1.1 focused only on software so it was deemed too limited in scope to meet the comprehensiveness criteria for being included in this work.

TALLINN UNIVERSITY OF TECHNOLOGY

# EXPERT QUESTIONNAIRE

**This expert questionnaire is a part of a research project focused on determining the comparative value of cybersecurity standards and guidelines for nuclear power plants. You have been selected as an expert who has practical experience working amongst guidelines and regulations for the nuclear industry. The survey is completely anonymous. In the ensuing report, all answers will be grouped together. Only a list of which country you are working in will be included in order to display geographical scope. Please answer as honestly as you feel comfortable with.**

**On a scale of 1-10 (10 being the highest), how familiar are you with the following standards or guidelines for cybersecurity at NPP?**

NIST Cybersecurity Framework (2014) Choose an item.

IAEA Computer Security Guidelines Choose an item.

NEI 08-09 Cyber Security Plan for Nuclea Choose an item.

NRC Regulatory Guide 5.71 Choose an item.

IAEA Safety Standards

- NS-G-1.1 Choose an item.
- NS-G-1.3 Choose an item.
- GS-G-3.1 Choose an item.

IEEE Standards for Nuclear Power Facilities

- 692-2013 Choose an item.
- 336-2010 Choose an item.
- 497-2010 Choose an item.
- 1023-2004 Choose an item.
- 577-2012 Choose an item.
- 583-1982 Choose an item.
- 603-2009 Choose an item.
- 741-2007 Choose an item.
- 758-1979 Choose an item.
- 845-1999 Choose an item.
- 1289-1998 Choose an item.

ISO/IEC 27000 Series Choose an item.

NIST SP800-82 Choose an item.

ANSI/ISA 62443-2-1-2009 Choose an item.

ANSI/ISA 62443-3-3: 2013 Choose an item.

NERC CIPv5 Choose an item.

**Other:** Click here to enter text.

**Please rank the standards or guidelines from most to least comprehensive. You may use each number only once.**

NIST Cybersecurity Framework (2014) Choose an item.

IAEA Computer Security Guidelines Choose an item.

NEI 08-09 Cyber Security Plan for Nuclea Choose an item.

NRC Regulatory Guide 5.71 Choose an item.

IAEA Safety Standards Choose an item.

- NS-G-1.1
- NS-G-1.3
- GS-G-3.1

IEEE Standards Choose an item.

- 692-2013
- 336-2010
- 497-2010
- 1023-2004
- 577-2012
- 583-1982
- 603-2009
- 741-2007
- 758-1979
- 845-1999
- 1289-1998

ISO/IEC 27000 Series Choose an item.

NIST SP800-82 Choose an item.

ANSI/ISA 62443-2-1-2009 Choose an item.

ANSI/ISA 62443-3-3: 2013 Choose an item.

NERC CIPv5 Choose an item.

**Within the nuclear power industry, how well respected are the following standards or guidelines?**

NIST Cybersecurity Framework (2014) Choose an item.

IAEA Computer Security Guidelines Choose an item.

NEI 08-09 Cyber Security Plan Choose an item.

NRC Regulatory Guide 5.71 Choose an item.

IAEA Safety Standards Choose an item.

- NS-G-1.1
- NS-G-1.3
- GS-G-3.1

IEEE Standards Choose an item.

- 692-2013
- 336-2010
- 497-2010

- 1023-2004
- 577-2012
- 583-1982
- 603-2009
- 741-2007
- 758-1979
- 845-1999
- 1289-1998

ISO/IEC 27000 Series Choose an item.

NIST SP800-82 Choose an item.

NERC CIPv5 Choose an item.

Other Choose an item.

Please specify if other: Click here to enter text.

**Does the NPP or regulatory body you are employed by try to comply (or encourage compliance) with any of the following guidelines or standards?**

☐ NIST Cybersecurity Framework
☐ IAEA Computer Security Guidelines
☐ NEI Cyber Security Plan for Nuclear Power Reactors
☐ NRC Regulatory Guide 5.71
☐ IAEA Safety Standards
    ☐ NS-G-1.1
    ☐ NS-G-1.3
    ☐ GS-G-3.1
☐ IEEE Standards
    ☐ 692-2013
    ☐ 336-2010
    ☐ 497-2010
    ☐ 1023-2004
    ☐ 577-2012
    ☐ 583-1982
    ☐ 603-2009
    ☐ 741-2007
    ☐ 758-1979
    ☐ 845-1999
    ☐ 1289-1998
☐ ISO/IEC 27000 Series
☐ NIST SP800-82
☐ NERC CIPv5
☐ Only national regulations
☐ Other: Click here to enter text.
☐ Not Applicable

**On a scale of 1-10 (1 being the lowest), how difficult do you believe implementing the standards or guidelines would be?**

NIST Cybersecurity Framework (2014) Choose an item.

IAEA Computer Security Guidelines Choose an item.

NEI 08-09 Cyber Security Plan for Nuclea Choose an item.

NRC Regulatory Guide 5.71 Choose an item.

IAEA Safety Standards

- NS-G-1.1 Choose an item.
- NS-G-1.3 Choose an item.
- GS-G-3.1 Choose an item.

IEEE Standards for Nuclear Power Facilities

- 692-2013 Choose an item.
- 336-2010 Choose an item.
- 497-2010 Choose an item.
- 1023-2004 Choose an item.
- 577-2012 Choose an item.
- 583-1982 Choose an item.
- 603-2009 Choose an item.
- 741-2007 Choose an item.
- 758-1979 Choose an item.
- 845-1999 Choose an item.
- 1289-1998 Choose an item.

ISO/IEC 27000 Series Choose an item.

NIST SP800-82 Choose an item.

ANSI/ISA 62443-2-1-2009 Choose an item.

ANSI/ISA 62443-3-3: 2013 Choose an item.

NERC CIPv5 Choose an item.

**Other:** Click here to enter text.

**Which of the above mentioned standards or guidelines is the strongest for regulating (or producing) awareness, training and security policy for cybersecurity?**

Choose an item. If other: Click here to enter text.

**Which of the following is the strongest for ensuring access control?**

Choose an item. If other: Click here to enter text.

**Which of the following is the strongest for ensuring data security?**

Choose an item. If other: Click here to enter text.

**Which of the following is the strongest for developing risk management strategies?**

Choose an item. If other: Click here to enter text.

**Which of the following is the strongest for protecting against intrusions or accidents through technical means?**

Choose an item. If other: Click here to enter text.

**Which of the following is the strongest for detecting anomalies and security breaches?**

Choose an item. If other: Click here to enter text.

**Which of the following is the strongest for response planning and risk mitigation?**

Choose an item. If other: Click here to enter text.

**Which of the following provides the most guidance for ensuring recovery capabilities?**

Choose an item. If other: Click here to enter text.

**Do you believe voluntary compliance with standards is more effective than mandated compliance?** (Yes/No)

Explanation: _____

**Could you be doing more to ensure the cybersecurity of the facility you are working at?**

Choose an item.

Explanation: _____

**Are there more standards or guidelines you believe should be considered within the scope of this study?** (Yes/No)

If so, please write here: _____

**Country you work in:** _____