Coalition for Fair Gaming, LLC

Class II Gaming Systems Risk Analysis Report

November 12, 2017

Prepared by:

Conquest Security, Inc.
267 Kentlands Blvd., #800
Gaithersburg, MD 20878
www.conquestsecurity.com

Confidential

INTRODUCTION

The Indian Gaming Regulatory Act of 1988 (IGRA) established the various classes of gaming. Bingo and similar games were classified under this regulation as "Class II". This included electronic systems that simulate these games. The electronic games are sophisticated and mimic the Las Vegas (Class III) style slot machines while still based on the game of Bingo.

Minimum technical standards entitled "Technical Standards for Electronic, Computer, or Other Technologic Aids Used in the Play of Class II Games" (25 CFR 547) were published by the National Indian Gaming Commission (NIGC) on October 10, 2008. The purpose of this regulatory requirement was to assist tribal governments, tribal gaming regulatory authorities, and operations in ensuring the integrity and security of Class II games and gaming revenue. The Commission understood that existing Class II gaming systems likely did not meet all the requirements of the Technical Standards. To avoid any potentially significant economic and practical consequences of requiring immediate compliance, the Technical Standards implement a five-year "grandfather period" for existing gaming systems. This requirement specifically stipulated that all Class II machines must be compliant or removed by November 10, 2013.

On September 21, 2012, the commission updated it regulatory requirement and published "Minimum Technical Standards for Class II Gaming Systems and Equipment". This revision was critical to tribal gaming regulators as the standards provided much needed updates to the control regulations, which had fallen behind technology, and were intended to ensure the integrity of Indian Gaming is upheld. The grandfather clause was extended for Class II gaming systems manufactured before November 10, 2008 from November 10, 2013, to November 10, 2018.

On September 28, 2017, the NIGC proposed to amend the minimum technical standards for Class II gaming systems and equipment. The proposed rule removes the deadline by which qualified grandfathered machines built prior to November 10, 2008 must be compliant with the full technical standards.

This paper shows that the minimum technical requirements are essential controls for ensuring the integrity and security of Class II gaming systems. The paper explains the risks mitigated for each control defined in 25 CFR 547. Gaming systems that do not comply with these regulatory controls are significantly at risk of attack and compromise due to the absence of controls on obsolete hardware, firmware, operating systems, and software.

THE RISKS AND DANGERS OF OUTDATED TECHNOLOGY

Many of the normal economic forces that drive technology and security updates in the business world do not work as effectively in the Class II gaming industry.

Computer hardware and software have considerably short life cycles. In the business community, workstations, servers, networking equipment, and mobile devices are replaced regularly. Technology upgrades are driven by rapidly increasing business application performance demands. Security requirements also drive technology upgrades. With the exponentially increasing incidents of data breaches, corporate espionage, and other cybercrimes, the business community must have the latest technological advances to protect their critical assets from sophisticated attacks.

Because the business world replaces older technology at such a rapid pace, as hardware and software reach the end of their useful life in the marketplace, the manufacturer will designate the product as "End-of-life" (EOL). When hardware has reached EOL, the manufacturer will discontinue support, services, and the availability of spare parts. With software and operating systems, the vendor will discontinue telephone and email support, the release of bug fixes, and security updates when designated EOL.

However, in the gaming industry the applications are developed for a specific hardware platform, such as a slot machine, which is static and does not change. Gaming applications do not continuously demand greater performance from the hardware. As a result, the gaming industry has not been required to continuously refresh outdated hardware and operating systems. The systems remain stable, functional and profitable for many years, but without as much pressure to continuously update as is present in other industries the hidden dangers of outdated and unsupported technology have been ignored.

The NIGC has recognized the security risks associated with outdated Class II gaming systems and has attempted to impose regulatory security controls. Yielding to pressures from the gaming industry, the NIGC has allowed these highly vulnerable systems to be grandfathered for 10 years. On November 10, 2018, these grandfathered systems must be made compliant with regulatory controls or be removed from the gaming floor. Some in the industry believe the grandfather waiver should be extended even longer for these obsolete and vulnerable systems.

The bottom line is that allowing the outdated technology used in these grandfathered systems to continue to be used is putting the gaming industry at considerable risk of serious cyber-attacks that may lead to a breach of customer trust, financial loses, and data compromise. Furthermore, the vulnerabilities inherent in the grandfathered systems also put newer and compliant systems at risk of compromise.

Security and Outdated Technology

Security risks are the number one danger of older technology. The older the operating system, the longer the hackers have had to find and exploit vulnerabilities. This is especially true when the manufacturer has designated the operating system to be EOL and is no longer actively maintaining support. If the firmware is old and outdated, the risk of a major security incident doubles.

Obsolete systems are exposed to countless and constantly increasing security vulnerabilities. In fact, research shows that over 10,000 new malware threats are discovered each hour. With outdated technology, the risk is constantly increasing at exponential rates.

Older Operating System Risks

Microsoft's Windows XP operating system is designated EOL and unsupported. This is the most common operating system found in the grandfathered Class II gaming systems manufactured before November 10, 2008.

A system running Windows XP is 6x more likely to be infected with malware than a system running Windows 10.

The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information security vulnerabilities and exposures. The National Cybersecurity Federally Funded Research and Development Center, operated by the MITRE Corporation, maintains the system, with funding from the National Cyber Security Division of the United States Department of Homeland Security.

According to the CVE, Windows XP has 729 known vulnerabilities. 129 of these vulnerabilities have been patched by Microsoft when it was still a supported operating system. There are 22 known exploits of Windows XP vulnerabilities. Since Windows XP is EOL and unsupported, 600 known vulnerabilities remain unpatched and exposed to immediate attacks. Even this grim outlook is optimistic, as it assumes that all of the 129 Microsoft patches have been applied. With the grandfathered Class II gaming systems, it is highly unlikely these patches have been installed. Patched or unpatched, Windows XP systems are an easy target for cybercriminals.

2017 has been an especially bad year for the security of Windows XP and other EOL Microsoft operating systems. The National Security Agency (NSA) had developed a classified toolkit that was only known to the agency and used by the agency to exploit Windows vulnerabilities. This toolkit was stolen from the NSA by an underground group of cybercriminals known as Shadow Brokers and released to the public.

While Microsoft reluctantly released an "emergency patch" for unsupported operating systems, it only addressed some of the vulnerabilities that can be exploited by the NSA Toolkit.

The other common Operating System in use by grandfathered games is Linux. The Linux OS available in 2008, of which there were ten varieties, were all designated EOL before 2013. Linux being a free OS also means that it is supported only by the community and does not have official personnel protecting its security. Users come up with answers for security holes and then they release a new distribution. This also means that there are some security issues that are never addressed due to the time constraints faced by volunteer efforts.

Considering that grandfathered Class II gaming systems are unpatched, the threats posed by the NSA Toolkit, other known exploits, and unknown exploits is an indisputable argument for removing grandfathered systems from gaming floors.

Outdated Firmware Vulnerabilities

Firmware is software written to a rewritable chip, such as the BIOS chip, a hard drive controller chip, and so on. Almost every electronic device has a rewritable firmware chip.

Computers rely on fundamental system firmware, commonly known as the system Basic Input/output System (BIOS), to facilitate the hardware initialization process and transition control to the operating system. The BIOS is typically developed by the original equipment manufacturers (OEMs) and independent BIOS vendors and is distributed to end-users by motherboard or computer manufacturers.

Unauthorized modification of BIOS firmware by malicious software constitutes a significant threat because of the BIOS's unique and privileged position within the PC architecture. A malicious BIOS modification could be part of a sophisticated, targeted attack on a system—either a permanent denial of service (if the BIOS is corrupted) or a persistent malware presence (if the BIOS is implanted with malware).

Firmware attacks recur on a regular basis. To combat them, BIOS manufacturers have created more defensible firmware versions, and in 2011, the National Institute of Standards and Technology (NIST) published two firmware protection guidance documents: Special Publication 800-147 (PDF) and Special Publication 800-155 (PDF).

The gold standard of firmware protection is defined in the NIST documents and has culminated in the open BIOS specification called UEFI (Universal Extensible Firmware Interface), considered the first strongly secure boot firmware standard. It requires trusted roots, digital certificates, and digital signatures.

Unfortunately for older systems, UEFI 2 requires different chipsets than pre-UEFI motherboards. Microsoft's Windows Secure Boot technology only began offering UEFI protections with Windows 8- and 2012-certified computers. As a result, grandfathered systems are more vulnerable to firmware attacks that would likely include malware, surveillance, theft.

Outdated Hardware Risks

Old hardware has vulnerabilities that cyber-criminals can take advantage of to breach systems. The longer hardware has been available to the public, the longer criminals have had to find their cyber and physical weaknesses.

Because of this, just as with software manufacturers, hardware manufacturers assume customers will upgrade their assets to cover the latest issues, most of which include enhanced functionality, greater performance and security.

With outdated hardware, the greatest risk is the absence of security features. When hardware is considered obsolete (EOL), most organizations will upgrade the hardware or deploy compensating controls to protect against threats to the system. In the Class II gaming industry, the NIGC's Minimum Technical Standards serve as the compensating controls. This is why it is so important that these controls be implemented across all Class II gaming machines.

The hardware used in the grandfathered gaming systems have been known to the public for 10 years and these systems are exempt from many of the compensating controls offered by the Minimum Technical Standards. As a result, these systems pose a clear risk to the gaming industry.

Risks to Compliant Systems and Gaming Infrastructures

According to BitSight Security Ratings, if half of a network's endpoints are outdated, the chances of the entire network experiencing a breach nearly triples. These findings underscore the seriousness of the risk posed by outdated software, operating systems, firmware, and hardware.

As we have established the risk associated with grandfathered systems, it should be noted that these outdated systems also pose a serious threat to compliant systems and the gaming infrastructures as a whole. Grandfathered systems can be easily compromised and used as a pivot point for attacking or compromising other systems on the same internal networks. If even one manufacturer has grandfathered games on a casino floor, every other game on the network, compliant or not, is at risk. This may put casinos in a difficult liability situation given

that they have allowed fully compliant machines owned by others to be put at risk under their supervision by allowing vulnerable machines into the same network.

Casino and Gaming Firm Incidents

Given the volume of financial data and the likelihood of gaming fraud, casinos and gaming firms are an ideal target for cyber-attacks.

Theoretically, gaming floors operate on closed networks. However, there are documented incidents where closed casino networks have been connected to public networks. An example of this is the casino that was compromised due to an internet connected fish tank. With the increased usage of mobile devices, wireless networking technologies, and internet connected devices, the risk of cyber criminals infiltrating gaming floor networks and compromising the extremely vulnerable grandfathered Class II gaming systems is continuously increasing.

CONCLUSION

According to the SANS Institute 2017 Threat Landscape Survey, Endpoint devices (an Internet-capable computer on a TCP/IP network) are on the front lines of the cybersecurity battle. They represent the most significant entry points for attackers obtaining a toehold into the network.

Systems that have not been updated since November 10, 2008 are technologically obsolete and are at higher risk of compromise. As discussed in this report, the vulnerabilities introduced by outdated and unpatched software, operating systems, firmware and hardware provide the perfect target for cybercriminals. These systems are also an entry point that can be used to launch more sophisticated attacks on regulatory compliant systems. By attacking and compromising the highly vulnerable grandfathered system, the cybercriminal can pivot and use these systems to compromise other compliant systems and casino's infrastructure, including point-of-sale (POS) systems, accounting systems, voucher systems, communication devices, network security safeguards, and physical security controls.

This method of pivoting from the soft targets (systems that are easily compromised) to compromise every computer and device on the network is the primary tactic used by sophisticated attackers.

Casinos and the gaming manufacturers are a target for cybercriminals and this industry must improve its cyber security capabilities. The NIGC intent to require obsolete systems

manufactured before November 10, 2008 to comply with the Minimum Technical Standards will significantly improve the cybersecurity of casinos and gaming floor systems.

Appendix A of this report provides an analysis of the Minimal Technical Standards provided in 25 CFR 547. The conclusion of this analysis is that the absence of these controls in grandfathered systems significantly increase the risks to the integrity, confidentiality, accountability, and fairness of play for Class II gaming systems.

APPENDIX A: CONTROLS, RISKS AND EXPOSURE

1. **Control 547.1: What is the purpose of this part?**
   The Indian Gaming Regulatory Act, 25 U.S.C. 2703(7)(A)(i), permits the use of electronic, computer, or other technologic aids in connection with the play of Class II games. This part establishes the minimum technical standards governing the use of such aids.

   Risks Mitigated by Control:

   Defining the "purpose" is essential for standards. Control 547.1 explains that these controls are intended for electronic, computer, or other technologic aids in connection with the play of Class II games. This reduces the risk of misinterpretation whether intentional or unintentional.

   Exposure of Non-Compliant System:

   Non-compliant gaming systems have no basic requirements to ensure the integrity and security of Class II games and gaming revenue.

2. **Control 547.2: What are the definitions for this part?**

   Risks Mitigated by Control:

   By defining the technical terms used in a standard, all stakeholders including manufacturers, testing laboratories, tribal governments, tribal gaming regulatory authorities, and operations all have a common understanding of the terms. Without definitions, the regulatory controls may be misinterpreted and incorrectly implemented exposing the gaming system to integrity and security risks.

   Exposure of Non-Compliant System:

   Non-Compliant systems have no reference of standardized terms. A component in one manufactures system may have different functionality from a component in another manufacturer's system with the name. This can also lead to confusion in operations and expose systems to additional risks.

3. Control 547.3: Who is responsible for implementing these standards?

(a) Minimum standards. These are minimum standards and a TGRA may establish and implement additional technical standards that do not conflict with the standards set out in this part.

Risk Mitigated by Control:

Control 547.3 provides further definition and and clarity to the standard. While these are the minimum (baseline) controls, additional controls may be implemented provided that do not conflict or negate the minimum control.

Exposure of Non-Compliant System:
Non-compliant systems that have employed additional controls but do not meet the baseline or minimum requirements are likely to expose the system to catastrophic security and/or integrity risks. As an analogy, automobiles have a minimum requirement to have airbags. If an automobile was non-compliant but decided to employ additional controls such as forward collision warning, the results would be catastrophic. The automobile would warn of a collision but fail to protect the occupants because the minimum standard was not met.

(b) No limitation of technology. This part should not be interpreted to limit the use of technology or to preclude the use of technology not specifically referenced.

Risk Mitigated by Control:
Additional guidance is provided by defining that there are no limitations of technology.

Exposure of Non-Compliant System:
Without the minimum controls, the greater use of technology will expose the system to more vulnerabilities and risk of attack. The minimum technical standards are designed to provide the basic protection mechanisms to protect the system and thereby does not limit the use of technology.

(c) Only applicable standards apply. Gaming equipment and software must meet all applicable requirements of this part. For example, if a Class II gaming system lacks the ability to print or accept vouchers, then any standards that govern vouchers do not apply. These standards do not apply to associated equipment such as voucher and kiosk systems.

Risk Mitigated by Control:
Part C provides additional clarification and ensures that standards that are not applicable are introduced into the system. If a function does not exist, there is no need to employ a control that is not needed.
Exposure of Non-Compliant System:
Non-compliant systems adhere to no standard. As a result, all functions of the system are vulnerable to the threats the minimum standards mitigate.

(d) State jurisdiction. Nothing in this part should be construed to grant to a state jurisdiction over Class II gaming or to extend a state's jurisdiction over Class III gaming.

Risks Mitigated by Control:
No control required by the minimum technical standards would grant or extend state jurisdiction over the gaming system. This reduces the risk of conflicting regulatory requirements that could reduce the effectiveness and minimum controls.

Exposure of Non-Compliant System:
Non-compliant systems comply with no jurisdiction's regulations. As a result, these systems could violate law that may grant jurisdiction by state governments.

4. **Control 547.4: What are the rules of general application for this part?**
(a) Fairness. No Class II gaming system may cheat or mislead users. All prizes advertised must be available to win during the game. A test laboratory must calculate and/or verify the mathematical expectations of game play, where applicable, in accordance with the manufacturer stated submission. The results must be included in the test laboratory's report to the TGRA. At the request of the TGRA, the manufacturer must also submit the mathematical expectations of the game play to the TGRA.

Risk Mitigated by Control:
This control ensures the game is fair and not misleading or tricking game players. This control mitigates liability

Exposure of Non-Compliant System:
Non-compliant systems have no third party validation and maybe violating the expectations of the game. As a result, non-compliant systems increases the liability of the operator.

(b) Approved gaming equipment and software only. All gaming equipment and software used with Class II gaming systems must be identical in all respects to a prototype reviewed and tested by a testing laboratory and approved for use by the TGRA pursuant to § 547.5(a) through (c).

Risk Mitigated by Control:
This control prevents the possibility of a system being deployed either knowingly or unintentional that has been altered from the configuration that was tested and certified.

Exposure of Non-Compliant System:
Non-compliant systems have no controls to ensure that configurations are not altered from the prototype tested. This increases the risk of systems violating the expectations and fairness of the game.

(c) Proper functioning. All gaming equipment and software used with Class II gaming systems must perform according to the manufacturer's design and operating specifications.

Risks Mitigated by Control:
This control ensures the system's design and operating specifications are accurate and represent the actual system.

Exposure of Non-Compliant System:
Non-compliant systems may operate and function differently than their design and operating specifications. These systems are more vulnerable to security and integrity risks as the system may intentionally or unintentionally be violating the operating behavior intended by the manufacturer.

5. **Control 547.5: How does a tribal government, TGRA, or tribal gaming operation comply with this part?**
(a) Grandfathered gaming systems: Any Class II gaming system manufactured before November 10, 2008, that is not already certified pursuant to this sub-section or compliant with paragraph (c) of this section may be made available for use at any tribal gaming operation if:

(1) The TGRA submits the Class II gaming system software that affects the play of the Class II game, together with the signature verification required by § 547.8(f) to a testing laboratory recognized pursuant to paragraph (f) of this section within 120 days after October 22, 2012;

(2) The testing laboratory tests the submission to the standards established by § 547.8(b), § 547.8(f), § 547.14, and any additional technical standards adopted by the TGRA;

(3) The testing laboratory provides the TGRA with a formal written report setting forth and certifying to the findings and conclusions of the test;

(4) The TGRA makes a finding, in the form of a certificate provided to the supplier or manufacturer of the Class II gaming system, that the Class II gaming system qualifies for grandfather status under the provisions of this section. A TGRA may make such a finding only upon receipt of a testing laboratory's report that the Class II gaming system is compliant with § 547.8(b), § 547.8(f), § 547.14, and any other technical standards adopted by the TGRA. If the TGRA does not issue the certificate, or if the testing laboratory finds that the Class II gaming system is not compliant with § 547.8(b), § 547.8(f), § 547.14, or any other technical standards adopted by the TGRA, then the gaming system must immediately be removed from play and not be utilized.

(5) The TGRA retains a copy of any testing laboratory's report so long as the Class II gaming system that is the subject of the report remains available to the public for play; and

(6) The TGRA retains a copy of any certificate of grandfather status so long as the Class II gaming system that is the subject of the certificate remains available to the public for play.

(b) Grandfather provisions. All Class II gaming systems manufactured on or before November 10, 2008, that have been certified pursuant to paragraph (a) of this section, are grandfathered Class II gaming systems for which the following provisions apply:

(1) Grandfathered Class II gaming systems may continue in operation for a period of ten years from November 10, 2008.

(2) Grandfathered Class II gaming systems may only be used as approved by the TGRA. The TGRA must transmit its notice of that approval, identifying the grandfathered Class II gaming system and its components, to the Commission.

(3) Remote communications may only be allowed if authorized by the TGRA.

(4) As permitted by the TGRA, individual hardware or software components of a grandfathered Class II gaming system may be repaired or replaced to ensure proper functioning, security, or integrity of the grandfathered Class II gaming system.

(5) All modifications that affect the play of a grandfathered Class II gaming system must be approved pursuant to paragraph (c) of this section, except for the following:

(i) Any software modifications that the TGRA finds will maintain or advance the Class II gaming system's overall compliance with this part or any applicable provisions of part 543 of this chapter, after receiving a new testing laboratory report that the modifications are compliant with the standards established by § 547.4(a), § 547.8(b), § 547.14, and any other standards adopted by the TGRA;

(ii) Any hardware modifications that the TGRA finds will maintain or advance the Class II gaming system's overall compliance with this part or any applicable provisions of part 543 of this chapter; and

(iii) Any other modification to the software of a grandfathered Class II gaming system that the TGRA finds will not detract from, compromise or prejudice:

(A) The proper functioning, security, or integrity of the Class II gaming system, and

(B) The gaming system's overall compliance with the requirements of this part or any applicable provisions of part 543 of this chapter.

(iv) No such modification may be implemented without the approval of the TGRA. The TGRA must maintain a record of the modification so long as the Class II gaming system that is the subject of the modification remains available to the public for play and must make the record available to the Commission upon request. The Commission will only make available for public review records or portions of records subject to release under the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act of 1974, 5 U.S.C. 552a; or the Indian Gaming Regulatory Act, 25 U.S.C. 2716(a).

(6) The player interface must exhibit information consistent with § 547.7(d) and any other information required by the TGRA.

(7) If a grandfathered Class II gaming system is approved pursuant to paragraph (c) of this section, it ceases to be a grandfathered system and the restrictions of paragraph (a) and (b) of this section no longer apply.

(c) Submission, testing, and approval—generally. Except as provided in paragraphs (b) and (d) of this section, a TGRA may not permit the use of any Class II gaming system, or any associated cashless system or voucher system or any modification thereto, in a tribal gaming operation unless:

(1) The Class II gaming system, cashless system, voucher system, or modification thereto has been submitted to a testing laboratory;

(2) The testing laboratory tests the submission to the standards established by:

(i) This part;

(ii) Any applicable provisions of part 543 of this chapter that are testable by the testing laboratory; and

(iii) The TGRA;

(3) The testing laboratory provides a formal written report to the party making the submission, setting forth and certifying its findings and conclusions, and noting compliance with any standard established by the TGRA pursuant to paragraph (c)(2)(iii) of this section;

(4) The testing laboratory's written report confirms that the operation of a player interface prototype has been certified that it will not be compromised or affected by electrostatic discharge, liquid spills, electromagnetic interference, radio frequency interference, or any other tests required by the TGRA;

(5) Following receipt of the testing laboratory's report, the TGRA makes a finding that the Class II gaming system, cashless system, or voucher system conforms to the standards established by:

(i) This part;

(ii) Any applicable provisions of part 543 of this chapter that are testable by the testing laboratory; and

(iii) The TGRA.

(6) The TGRA retains a copy of the testing laboratory's report required by paragraph (c) of this section for as long as the Class II gaming system, cashless system, voucher system, or modification thereto that is the subject of the report remains available to the public for play in its tribal gaming operation.

(d) Emergency hardware and software modifications. (1) A TGRA, in its discretion, may permit the modification of previously approved hardware or software to be made available for play without prior laboratory testing or review if the modified hardware or software is:

(i) Necessary to correct a problem affecting the fairness, security, or integrity of a game

or accounting system or any cashless system, or voucher system; or

(ii) Unrelated to game play, an accounting system, a cashless system, or a voucher system.

(2) If a TGRA authorizes modified software or hardware to be made available for play or use without prior testing laboratory review, the TGRA must thereafter require the hardware or software manufacturer to:

(i) Immediately advise other users of the same hardware or software of the importance and availability of the update;

(ii) Immediately submit the new or modified hardware or software to a testing laboratory for testing and verification of compliance with this part and any applicable provisions of part 543 of this chapter that are testable by the testing laboratory; and

(iii) Immediately provide the TGRA with a software signature verification tool meeting the requirements of § 547.8(f) for any new or modified software.

(3) If a TGRA authorizes a software or hardware modification under this paragraph, it must maintain a record of the modification and a copy of the testing laboratory report so long as the Class II gaming system that is the subject of the modification remains available to the public for play and must make the record available to the Commission upon request. The Commission will only make available for public review records or portions of records subject to release under the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act of 1974, 5 U.S.C. 552a; or the Indian Gaming Regulatory Act, 25 U.S.C. 2716(a).

(e) Compliance by charitable gaming operations. This part does not apply to charitable gaming operations, provided that:

(1) The tribal government determines that the organization sponsoring the gaming operation is a charitable organization;

(2) All proceeds of the charitable gaming operation are for the benefit of the charitable organization;

(3) The TGRA permits the charitable organization to be exempt from this part;

(4) The charitable gaming operation is operated wholly by the charitable organization's employees or volunteers; and

(5) The annual gross gaming revenue of the charitable gaming operation does not exceed $1,000,000.

(f) Testing laboratories. (1) A testing laboratory may provide the examination, testing, evaluating and reporting functions required by this section provided that:

(i) It demonstrates its integrity, independence and financial stability to the TGRA.

(ii) It demonstrates its technical skill and capability to the TGRA.

(iii) If the testing laboratory is owned or operated by, or affiliated with, a tribe, it must be independent from the manufacturer and gaming operator for whom it is providing the testing, evaluating, and reporting functions required by this section.

(iv) The TGRA:

(A) Makes a suitability determination of the testing laboratory based upon standards no less stringent than those set out in § 533.6(b)(1)(ii) through (v) of this chapter and based upon no less information than that required by § 537.1 of this chapter, or

(B) Accepts, in its discretion, a determination of suitability for the testing laboratory made by any other gaming regulatory authority in the United States.

(v) After reviewing the suitability determination and the information provided by the testing laboratory, the TGRA determines that the testing laboratory is qualified to test and evaluate Class II gaming systems.

(2) The TGRA must:

(i) Maintain a record of all determinations made pursuant to paragraphs (f)(1)(iii) and (f)(1)(iv) of this section for a minimum of three years and must make the records available to the Commission upon request. The Commission will only make available for public review records or portions of records subject to release under the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act of 1974, 5 U.S.C. 552a; or the Indian Gaming Regulatory Act, 25 U.S.C. 2716(a).

(ii) Place the testing laboratory under a continuing obligation to notify it of any adverse regulatory action in any jurisdiction where the testing laboratory conducts business.

(iii) Require the testing laboratory to provide notice of any material changes to the

information provided to the TGRA.

Risk Mitigated by Control:
547.5 describes the conditions in which a grandfathered system may operate. This does not mitigate any risks and the ten year old grandfather rights exposes aging technology to greater risks without the protections of the minimum technical standards.

Exposure of Non-Compliant System:
Since grandfathered system do not employ the minimal technical standards, their exposure to security vulnerabilities and operational accuracy is compromised. The integrity of the hardware, software, operating parameters, and fairness of play is questionable due to the lack of baseline regulatory controls.

6. **Control 547.6: What are the minimum technical standards for enrolling and enabling Class II gaming system components?**

(a) General requirements. Class II gaming systems must provide a method to:

(1) Enroll and unenroll Class II gaming system components;

(2) Enable and disable specific Class II gaming system components.

Risk Mitigated by Control:

This control ensures that there is a defined method by which a Class II gaming system identifies and establishes communications with an additional system component to allow for live gaming activity to take place on that component. This control reduces the risk of unauthorized communications between system components. This control ensures a proper process for disabling system components.

Exposure of Non-Compliant System:

Non-compliant systems may not have a defined method for identifying system components and establishing communications. Errors in identifying, establishing communications and disabling system components can expose the system to integrity and security risks.

(b) Specific requirements. Class II gaming systems must:

(1) Ensure that only enrolled and enabled Class II gaming system components participate in gaming; and

(2) Ensure that the default condition for components must be unenrolled and disabled.

Risks Mitigated by Control:
The purpose of this control is to limit unauthorized requests to the server for any component that is not previously registered or enrolled. The control also requires a provision that requires the remote unenrollment or disabling of remote component. While we emphasize server, since it's the common type of attack, the control also applies to components within the game device itself.

Exposure of Non-Compliant System:
A malicious intruder could connect a rogue device into the network or connect a form of hardware sniffer into the device to learn system behavior or tamper with it. Non-compliant systems are vulnerable to a variety of rogue and unauthorized component attacks.

7. **Control 547.7: What are the minimum technical hardware standards applicable to Class II gaming systems?**

(a) Printed circuit boards.

(1) Printed circuit boards that have the potential to affect the outcome or integrity of the game, and are specially manufactured or proprietary and not off-the-shelf, must display a unique identifier such as a part number and/or revision number, which must be updated to reflect new revisions or modifications of the board.

(2) Switches or jumpers on all circuit boards that have the potential to affect the outcome or integrity of any game, progressive award, financial instrument, cashless transaction, voucher transaction, or accounting records must be capable of being sealed.

Risk Mitigated by Control:
Off-the-shelf printed circuit boards may be vulnerable to common and well-known attack vectors. This control requires proprietary boards with unique identifiers. The risks of off-the-shelf attacks are reduced. The unique identifier indicates the proprietary manufacturer and version of the board. Security measure to prevent tampering with switches and jumpers are required.

Exposure of Non-Compliant System:
Non-compliant systems may deploy common off-the-shelf printed circuit boards that are vulnerable to well known attack vectors. The lack of unique identifiers on the board introduces accountability issues and reduces confidence in the system and the ability to identify the manufacturer and revision of the board. Furthermore, without compliance

to the tamper-proof requirement, a threat actor with physical access to the system could compromise the integrity of the game by tampering with switches and jumpers.

(b) Electrostatic discharge. Class II gaming system components accessible to the public must be constructed so that they exhibit immunity to human body electrostatic discharges on areas exposed to contact. Static discharges of ±15 kV for air discharges and ±7.5 kV for contact discharges must not cause damage or inhibit operation or integrity of the Class II gaming system.

Risk Mitigated by Control:
This control ensures that systems components that are accessible to the public are immune immunity to human body electrostatic discharges. Electrostatic discharge can damage system components or affect the integrity of the game by introducing electronic error.

Exposure of Non-Compliant System:
Non-compliant system are vulnerable to damage, errors, and integrity threats due to electrostatic discharge.

(c) Physical enclosures. Physical enclosures must be of a robust construction designed to resist determined illegal entry. All protuberances and attachments such as buttons, identification plates, and labels must be sufficiently robust to avoid unauthorized removal.

Risk Mitigated by Control:
This control mitigates risks associated with physical intrusion to system components. Systems compliant with this minimum technical standard are tamper resistant.

Exposure of Non-Compliant System:
Non compliant systems could be tampered with physically through a breach of the enclosure or attachments and buttons. WIthout robust labeling, system identifications and other labeling could be altered.

(d) Player interface. The player interface must exhibit a serial number and date of manufacture and include a method or means to:

(1) Display information to a player; and

(2) Allow the player to interact with the Class II gaming system.

Risk Mitigated by Control:

This control identifies the system to the player and improves the trustworthiness, accountability and fairness of play.

Exposure of Non-Compliant System:
Non-compliant systems can reduce player trust in the system due the lack of accountability information. Non-compliance with this control may prevent a player from interacting with the system.

(e) Account access components. A Class II gaming system component that reads account access media must be located within a secure and locked area, cabinet, or housing that is of a robust construction designed to resist determined illegal entry and to protect internal components. In addition, the account access component:

(1) Must be constructed so that physical tampering leaves evidence of such tampering; and

(2) Must provide a method to enable the Class II gaming system to interpret and act upon valid or invalid input or error condition.

Risk Mitigated by Control:
These controls prevent a system from being physically tampered with when account access media is used. Any attempt to tamper with the system is physically evident. These controls also ensure that the input from account access media are valid without error.

Exposure of Non-Compliant System:
Non-Compliant systems can be tampered with physically and there will be no physical evidence of tampering. Inputs can also be invalid without controls to ensure the validity and that the input is error-free.

(f) Financial instrument storage components. Any financial instrument storage components managed by Class II gaming system software must be located within a secure and locked area, cabinet, or housing that is of a robust construction designed to resist determined illegal entry and to protect internal components.

Risk Mitigated by Control:
This controls ensures that system components that store tangible item of value (bills, coins, vouchers and coupons) are tamper resistant. Both the content and components of the storage component are physically protected by this control.

Exposure of Non-Compliant System:

Tangible items of value can be stolen from non-compliant systems. Additionally, storage system component can be physically damaged.

(g) Financial instrument acceptors. (1) Any Class II gaming system components that handle financial instruments and that are not operated under the direct control of an agent must:

(i) Be located within a secure and locked area, cabinet, or housing that is of a robust construction designed to resist determined illegal entry and to protect internal components;

(ii) Be able to detect the entry of valid or invalid financial instruments and to provide a method to enable the Class II gaming system to interpret and act upon valid or invalid input or error condition; and

(iii) Be constructed to permit communication with the Class II gaming system of the accounting information required by § 547.9(a) and by applicable provisions of any Commission and TGRA regulations governing minimum internal control standards.

(2) Prior to completion of a valid financial instrument transaction by the Class II gaming system, no monetary amount related to that instrument may be available for play. For example, credits may not be available for play until a financial instrument inserted into an acceptor is secured in the storage component.

(3) The monetary amount related to all valid financial instrument transactions by the Class II gaming system must be recorded as required by § 547.9(a) and the applicable provisions of any Commission and TGRA regulations governing minimum internal control standards.

Risk Mitigated by Control:
This control ensures that the system is protected from physical tampering of the Financial instrument acceptors and that the financial instrument is valid. The control also protects the system from timing attacks because no credit for play are provided until the financial instrument is validated and secured in the system storage compartment.

Exposure of Non-Compliant System:
Non compliant systems are vulnerable to physical tampering, invalid acceptance of fraudulent financial instruments, and timing attacks. A timing attack would cause the system to provide a game play before the financial instrument is validated and securely stored.

(h) Financial instrument dispensers. (1) Any Class II gaming system components that dispense financial instruments and that are not operated under the direct control of a tribal gaming operation agent must:

(i) Be located within a secure, locked and tamper-evident area or in a locked cabinet or housing that is of a robust construction designed to resist determined illegal entry and to protect internal components;

(ii) Provide a method to enable the Class II gaming system to interpret and act upon valid or invalid input or error condition; and

(iii) Be constructed to permit communication with the Class II gaming system of the accounting information required by § 547.9(a) and by applicable provisions of any Commission and TGRA regulations governing minimum internal control standards.

(2) The monetary amount related to all valid financial instrument transactions by the Class II gaming system must be recorded as required by § 547.9(a), the applicable provisions of part 543 of this chapter, and any TGRA regulations governing minimum internal control standards.

(i) Game Outcome Determination Components. Any Class II gaming system logic components that affect the game outcome and that are not operated under the direct control of a tribal gaming operation agent must be located within a secure, locked and tamper-evident area or in a locked cabinet or housing that is of a robust construction designed to resist determined illegal entry and to protect internal components. DIP switches or jumpers that can affect the integrity of the Class II gaming system must be capable of being sealed by the TGRA.

Risk Mitigated by Control:
This control ensures that financial instrument dispensers are both tamper resistant and tamper evident. The system must have controls to detect valid, invalid, and error conditions and communicate with financial components. These controls protect the dispenser and the logic components

Exposure of Non-Compliant System:
A non-complaint system is vulnerable to physical tampering of the financial instrument dispenser. Without this control, the system may dispense financial instruments without the ability to detect invalid transactions and errors. The lack of this control can lead to financial loses.

(j) Door access detection. All components of the Class II gaming system that are locked in order to meet the requirements of this part must include a sensor or other methods to monitor an open door. A door open sensor, and its components or cables, must be secure against attempts to disable them or interfere with their normal mode of operation.

Risk Mitigated by Control:
This control protects the system from physical access and tampering through door access.

Exposure of Non-Compliant System:
Non-compliant system are vulnerable to physical tampering and sabotage due to the lack of sensors on door access and potentially vulnerable components and cables.

(k) Separation of functions/no limitations on technology. Nothing herein prohibits the account access component, financial instrument storage component, financial instrument acceptor, and financial instrument dispenser from being included within the same component or being separated into individual components.

Risk Mitigated by Control:
This standard allows system functions to be included into a single component or separated into individual components. No risks are mitigated by this requirement.

Exposure of Non-Compliant System:
This standard requirement does not introduce additional vulnerabilities to non-compliant as this standard allows functions to be integrated into a single component or distributed components.

8. **Control 547.8: What are the minimum technical software standards applicable to Class II gaming systems?**

(a) Player interface displays.

(1) If not otherwise provided to the player, the player interface must display the following:

(i) The purchase or wager amount;
(ii) Game results; and
(iii) Any player credit balance.

(2) Between plays of any game and until the start of the next play, or until the player selects a new game option such as purchase or wager amount or card

selection, whichever is earlier, if not otherwise provided to the player, the player interface must display:

(i) The total purchase or wager amount and all prizes and total credits won for the last game played;
(ii) The final results for the last game played; and
(iii) Any default purchase or wager amount for the next play.

Risk Mitigated by Control:
This control mitigates the risk of incorrect information about the game and player status from being displayed on the player interface. This could be due to faulty or tampered software or hardware malfunction.

Exposure of Non-Compliant System:
Non-compliant systems are to faulty software, tampering, and hardware malfunctions. Without this control, the player interface can fail to display the required information.

(b) Game initiation and play.

(1) Each game played on the Class II gaming system must follow and not deviate from a constant set of rules for each game provided to players pursuant to § 547.16. There must be no undisclosed changes of rules.

(2) The Class II gaming system may not alter or allow to be altered the card permutations used for play of a Class II game unless specifically chosen by the player prior to commitment to participate in the game. No duplicate cards may be sold for any common draw.

(3) No game play may commence, and no financial instrument or credit may be accepted on the affected player interface, in the presence of any fault condition that affects the outcome of the game, or while in test, audit, or lock-up mode.

(4) Each player must initiate his or her participation in the play of a game.

Risk Mitigated by Control:
The risk of Game initiation and play is a control to provide protection to the player under fair use. If a malfunction is detected, the game will not proceed.

Exposure of Non-Compliant System:
Non-compliant systems have no controls of Game initiation and play. Systems may malfunction and violate fairness of play regulations.

(c) Audit mode.

(1) If an audit mode is provided, the Class II gaming system must, for those components actively involved in the audit:

(i) Provide all accounting functions required by § 547.9, by applicable provisions of any Commission regulations governing minimum internal control standards, and by any internal controls adopted by the tribe or TGRA;

(ii) Display player interface identification; and

(iii) Display software version or game identification.

(2) Audit mode must be accessible by a secure method such as an agent PIN, key, or other auditable access control.

(3) Accounting function data must be accessible by an agent at any time, except during a payout, during a handpay, or during play.

(4) The Class II gaming system must disable financial instrument acceptance on the affected player interface while in audit mode, except during financial instrument acceptance testing.

Risk Mitigated by Control:
This control assures that systems accounting functions can be audited and that the proper identification information is displayed on the player interface.

Exposure of Non-Compliant System:
Non-compliant systems may not provide the ability to be audited and may not display the appropriate identification information. The lack of this control reduces confidence in the system and its accountability.

(d) Last game recall. The last game recall function must:

(1) Be retrievable at all times, other than when the recall component is involved in the play of a game, upon the operation of an external key-switch, entry of an audit card, or a similar method;

(2) Display the results of recalled games as originally displayed or in text representation so as to enable the TGRA or operator to clearly identify the sequences and results that occurred;

(3) Allow the Class II gaming system component providing game recall, upon return to normal game play mode, to restore any affected display to the positions, forms and values displayed before access to the game recall information; and

(4) Provide the following information for the current and previous four games played and must display:

(i) Play start time, end time, and date;
(ii) The total number of credits at the start of play;
(iii) The purchase or wager amount;
(iv) The total number of credits at the end of play;
(v) The total number of credits won as a result of the game recalled, and the value in dollars and cents for progressive prizes, if different;
(vi) For bingo games and games similar to bingo, also display:

(A) The card(s) used by the player;
(B) The identifier of the bingo game played;
(C) The numbers or other designations drawn, in the order that they were drawn;
(D) The numbers or other designations and prize patterns covered on each card;
(E) All prizes won by the player, including winning patterns, if any; and
(F) The unique identifier of the card on which prizes were won;
(vii) For pull-tab games only, also display:

(A) The result(s) of each pull-tab, displayed in the same pattern as on the tangible pull-tab;
(B) All prizes won by the player;
(C) The unique identifier of each pull tab; and
(D) Any other information necessary to fully reconstruct the current and four previous plays.

Risk Mitigated by Control:
This control ensures that an investigation can be conducted using the last game recall function.

Exposure of Non-Compliant System:
Non-compliant systems are at risk of not being able to recall the "Last game recall" function at any given time is that the system has being tampered with to hide payouts or odd results that could be obvious to an investigation. The lack of "Last game recall" controls may lead to financial losses.

(e) Voucher and credit transfer recall. Notwithstanding the requirements of any other section in this part, a Class II gaming system must have the capacity to:

(1) Display the information specified in § 547.11(b)(5)(ii) through (vi) for the last five vouchers or coupons printed and the last five vouchers or coupons accepted; and

(2) Display a complete transaction history for the last five cashless transactions made and the last five cashless transactions accepted.

Risk Mitigated by Control:
This control ensures that an investigation can be conducted using the "Voucher and credit transfer recall" function.

Exposure of Non-Compliant System:
Non-compliant systems are at risk of not being able to recall the "Voucher and credit transfer recall" function at any given time is that the system has being tampered with to hide voucher and credit results that could be obvious to an investigation.

(f) Software signature verification. The manufacturer or developer of the Class II gaming system must provide to the testing laboratory and to the TGRA an industry-standard methodology, acceptable to the TGRA, for verifying the Class II gaming system game software. For example, for game software stored on rewritable media, such methodologies include signature algorithms and hashing formulas such as SHA-1.

Risk Mitigated by Control:
This control ensures through digital signatures (Authenticity and Integrity) or hashing algorithms (Integrity) that the manufacturers software truly originated from the developer and that is has not been modified intentionally or unintentionally.

Exposure of Non-Compliant System:

Non-compliant systems are vulnerable to fraudulent or imposter software submissions and software that may have been modified intentionally or by error.

(g) Test, diagnostic, and demonstration modes. If test, diagnostic, and/or demonstration modes are provided, the Class II gaming system must, for those components actively involved in the test, diagnostic, or demonstration mode:

(1) Clearly indicate when that component is in the test, diagnostic, or demonstration mode;

(2) Not alter financial data on that component other than temporary data;

(3) Only be available after entering a specific mode;

(4) Disable credit acceptance and payment unless credit acceptance or payment is being tested; and

(5) Terminate all mode-specific functions upon exiting a mode.

Risk Mitigated by Control:
The control for the Test, diagnostic, and demonstration modes (if provided) specifies that no payment can be accepted and the display should indicate the mode. This control prevents the alternation of financial data while in test, diagnostic, and demonstration modes.

Exposure of Non-Compliant System:
Non-compliant systems are vulnerable to financial fraud as they do not have controls to prevent manipulation of financial data while in test, diagnostic, and demonstration modes.

(h) Multigame. If multiple games are offered for player selection at the player interface, the player interface must:

(1) Provide a display of available games;
(2) Provide the means of selecting among them;
(3) Display the full amount of the player's credit balance;
(4) Identify the game selected or being played; and
(5) Not force the play of a game after its selection.

Risk Mitigated by Control:
The Multigame control relates to player protection, to make sure that their balance is carried over from game to game.

Exposure of Non-Compliant System:
Non-compliant systems may violate player protection rules losing player information and balance information in multi game mode.

(i) Program interruption and resumption. The Class II gaming system software must be designed so that upon resumption following any interruption, the system:

(1) Is able to return to a known state;
(2) Must check for any fault condition;
(3) Must verify the integrity of data stored in critical memory;
(4) Must return the purchase or wager amount to the player in accordance with the rules of the game; and
(5) Must detect any change or corruption in the Class II gaming system software.

Risk Mitigated by Control:
This control ensures that the system fails and recovers in a safe and predictable manner.

Exposure of Non-Compliant System:
Non-compliant systems may fail to an unknown state, fail to detect failure conditions and produce financial accounting errors.

(j) Class II gaming system components acting as progressive controllers. This paragraph applies to progressive controllers and components acting as progressive controllers in Class II gaming systems.

(1) Modification of progressive parameters must be conducted in a secure manner approved by the TGRA. Such parameters may include:
(i) Increment value;
(ii) Secondary pool increment(s);
(iii) Reset amount(s);
(iv) Maximum value(s); and
(v) Identity of participating player interfaces.

(2) The Class II gaming system component or other progressive controller must provide a means of creating a progressive balancing report for each progressive link it controls. At a minimum, that report must provide balancing of the changes of the progressive amount, including progressive prizes won, for all participating player interfaces versus

current progressive amount(s), plus progressive prizes. In addition, the report must account for, and not be made inaccurate by, unusual events such as:

(i) Class II gaming system critical memory clears;
(ii) Modification, alteration, or deletion of progressive prizes;
(iii) Offline equipment; or
(iv) Multiple site progressive prizes.

Risk Mitigated by Control:
This control related Class II gaming system components acting as progressive controllers indicates that the rules for these complex games are very strict and the reporting module must account for this complex progressive mode to avoid missing any tampering or software defect.

Exposure of Non-Compliant System:
Non-compliant systems may prevent the auditing of progressive transactions. These systems are at risk of tampering and violating fairness of play.

(k) Critical memory. (1) Critical memory may be located anywhere within the Class II gaming system. Critical memory is any memory that maintains any of the following data:

(i) Accounting data;
(ii) Current credits;
(iii) Configuration data;
(iv) Last game play recall information required by paragraph (d) of this section;
(v) Game play recall information for the current game play, if incomplete;
(vi) Software state (the last normal state software was in before interruption);
(vii) RNG seed(s), if necessary for maintaining integrity;
(viii) Encryption keys, if necessary for maintaining integrity;
(ix) Progressive prize parameters and current values;
(x) The five most recent financial instruments accepted by type, excluding coins and tokens;
(xi) The five most recent financial instruments dispensed by type, excluding coins and tokens; and
(xii) The five most recent cashless transactions paid and the five most recent cashless transactions accepted.

(2) Critical memory must be maintained using a methodology that enables errors to be identified and acted upon. All accounting and recall functions must be verified as necessary to ensure their ongoing integrity.

(3) The validity of affected data stored in critical memory must be checked after each of the following events:

(i) Every restart;
(ii) Each attendant paid win;
(iii) Each attendant paid progressive win;
(iv) Each sensored door closure; and
(v) Every reconfiguration, download, or change of prize schedule or denomination requiring operator intervention or action.

Risk Mitigated by Control:
This control ensures the validity and integrity of system transactions and data in critical memory.

Exposure of Non-Compliant System:
Non-compliant systems are vulnerable to critical memory errors: storing faulty data, losing stored data or corrupted memory system, or retrieving incorrect data. All these could occur due to hardware or software malfunction, or due to malicious software tampering.

(l) Secured access. Class II gaming systems that use a logon or other means of secured access must include a user account lockout after a predetermined number of consecutive failed attempts to access the Class II gaming system.

Risk Mitigated by Control:
This access control is to minimize the risk of potential intruders trying to brute force the logon account by trying many combinations to guess the password. This control sets a clipping level that after a number of invalid tries, will lockout the account.

Exposure of Non-Compliant System:
Non-compliant systems are vulnerable to brute force login attacks.

9. **Control 547.9: What are the minimum technical standards for Class II gaming system accounting functions?**

(a) Required accounting data. The following minimum accounting data, however named, must be maintained by the Class II gaming system:

(1) Amount In: The total value of all financial instruments and cashless transactions accepted by the Class II gaming system. Each type of financial instrument accepted by the Class II gaming system must be tracked independently per financial instrument

acceptor, and as required by applicable requirements of TGRA regulations that meet or exceed the minimum internal control standards at 25 CFR part 543.

(2) Amount Out: The total value of all financial instruments and cashless transactions paid by the Class II gaming system, plus the total value of attendant pay. Each type of financial instrument paid by the Class II Gaming System must be tracked independently per financial instrument dispenser, and as required by applicable requirements of TGRA regulations that meet or exceed the minimum internal control standards at 25 CFR part 543.

Risk Mitigated by Control:
This control is both an accounting and audit control to monitor system financial transactions.

Exposure of Non-Compliant System:
Non-compliant systems are vulnerable to financial fraud due to the lack of accounting audit capabilities.

(b) Accounting data storage. If the Class II gaming system electronically maintains accounting data:

(1) Accounting data must be stored with at least eight decimal digits.

(2) Credit balances must have sufficient digits to accommodate the design of the game.

(3) Accounting data displayed to the player may be incremented or decremented using visual effects, but the internal storage of this data must be immediately updated in full.

(4) Accounting data must be updated upon the occurrence of the relevant accounting event.

(5) Modifications to accounting data must be recorded, including the identity of the person(s) making the modifications, and be reportable by the Class II gaming system.

Risk Mitigated by Control:
This control ensures proper accounting transaction, precision of the data and accounting systems.

Exposure of Non-Compliant System:
Non-compliant systems cannot ensure that accounting data is properly stored, the precision of the data, the logging of persons modifying accounting data, and ensuring

the transactions are recorded upon a relevant event.

(c) Rollover. Accounting data that rolls over to zero must not corrupt data.

Risk Mitigated by Control:
This control ensures when data rolls over to zero no data corruption occurs.

Exposure of Non-Compliant System:
Non-compliant systems are at risk of corrupting data.

(d) Credit balance display and function. (1) Any credit balance maintained at the player interface must be prominently displayed at all times except:

(i) In audit, configuration, recall and test modes; or

(ii) Temporarily, during entertaining displays of game results.

(2) Progressive prizes may be added to the player's credit balance provided that:

(i) The player credit balance is maintained in dollars and cents;

(ii) The progressive accounting data is incremented in number of credits; or

(iii) The prize in dollars and cents is converted to player credits or transferred to the player's credit balance in a manner that does not mislead the player or cause accounting imbalances.

(3) If the player credit balance displays in credits, but the actual balance includes fractional credits, the Class II gaming system must display the fractional credit when the player credit balance drops below one credit.

Risk Mitigated by Control:
This control ensures that any credit balance maintained at the player interface must be prominently displayed.

Exposure of Non-Compliant System:
Non-compliant systems may violate fairness of play by not properly displaying credit balance at the required precision.

10. Control 547.10: What are the minimum standards for Class II gaming system critical events?

(a) Fault events. (1) The following are fault events that must be capable of being recorded by the Class II gaming system:

(i) Component fault

Reported when a fault on a component is detected. When possible, this event message should indicate what the nature of the fault is.

(ii) Financial storage component full
Reported when a financial instrument acceptor or dispenser includes storage, and it becomes full. This event message must indicate what financial storage component is full.
(iii) Financial output component empty Reported when a financial instrument dispenser is empty. The event message must indicate which financial output component is affected, and whether it is empty.
(iv) Financial component fault
Reported when an occurrence on a financial component results in a known fault state.

(v) Critical memory error
Some critical memory error has occurred. When a non-correctable critical memory error has occurred, the data on the Class II gaming system component can no longer be considered reliable. Accordingly, any game play on the affected component must cease immediately, and an appropriate message must be displayed, if possible.

(vi) Progressive communication fault
If applicable; when communications with a progressive controller component is in a known fault state.

(vii) Program storage medium fault
The software has failed its own internal security check or the medium itself has some fault. Any game play on the affected component must cease immediately, and an appropriate message must be displayed, if possible.

(2) The occurrence of any event identified in paragraph (a)(1) of this section must be recorded.

(3) Upon clearing any event identified in paragraph (a)(1) of this section, the Class II gaming system must:

(i) Record that the fault condition has been cleared;

(ii) Ensure the integrity of all related accounting data; and

(iii) In the case of a malfunction, return a player's purchase or wager according to the rules of the game.

Risk Mitigated by Control:
This control is critical to ensuring the integrity of the systems by detecting and logging fault events.

Exposure of Non-Compliant System:
Non-compliant systems may be unable to record fault events. This violates the security, integrity and accounting reliability of the system.

(b)Door open/close events.

(1) In addition to the requirements of paragraph (a)(1) of this section, the Class II gaming system must perform the following for any component affected by any sensored door open event:
(i) Indicate that the state of a sensored door changes from closed to open or opened to closed;
(ii) Disable all financial instrument acceptance, unless a test mode is entered;
(iii) Disable game play on the affected player interface;
(iv) Disable player inputs on the affected player interface, unless test mode is entered; and
(v) Disable all financial instrument disbursement, unless a test mode is entered.
(2) The Class II gaming system may return the component to a ready to play state when all sensored doors are closed.

Risk Mitigated by Control:
This control ensures that the system will halt play and financial transactions when a door sensor is active.

Exposure of Non-Compliant System:
Non-compliant systems may not detect a door open sensor and allow play and financial transactions to continue. The lack of this control may allow fraudulent play and financial transactions while the system is in a physical insecure state.

(c) Non-fault events. The following non-fault events are to be acted upon as described below, if applicable:

Event Definition
(1) Player interface off during play Indicates power has been lost during game play. This condition must be reported by the affected component(s).
(2) Player interface power on Indicates the player interface has been turned on. This condition must be reported by the affected component(s).

(3) Financial instrument storage component container/stacker removed Indicates that a financial instrument storage container has been removed. The event message must indicate which storage container was removed.

Risk Mitigated by Control:
This control ensures that non-fault events are properly reported and the components affected are indicated.

Exposure of Non-Compliant System:
Non-compliant systems may not report non-fault events. The lack of this control reduces the integrity of the system by not reporting non-fault events.

11. Control 547.11: What are the minimum technical standards for money and credit handling?

(a) Credit acceptance, generally. (1) Upon any credit acceptance, the Class II gaming system must register the correct number of credits on the player's credit balance.
(2) The Class II gaming system must reject financial instruments deemed invalid.

Risk Mitigated by Control:
This control ensures the system correctly registers valid player credits and rejects financial instruments deemed invalid.

Exposure of Non-Compliant System:
Non-compliant systems are at risk of accepting invalid financial instruments and not properly registering player credits.

(b) Credit redemption, generally. (1) For cashable credits on a player interface, players must be allowed to cash out and/or redeem those credits at the player interface except when that player interface is:

(i) Involved in the play of a game;
(ii) In audit mode, recall mode or any test mode;
(iii) Detecting any sensored door open condition;
(iv) Updating the player credit balance or total win accounting data; or
(v) Displaying a fault condition that would prevent cash-out or credit redemption. In this case a fault indication must be displayed.

(2) For cashable credits not on a player interface, the player must be allowed to cash out and/or redeem those credits at any time.

(3) A Class II gaming system must not automatically pay an award subject to mandatory tax reporting or withholding.

(4) Credit redemption by voucher or coupon must conform to the following:
(i) A Class II gaming system may redeem credits by issuing a voucher or coupon when it communicates with a voucher system that validates the voucher or coupon.
(ii) A Class II gaming system that redeems credits by issuing vouchers and coupons must either:

(A) Maintain an electronic record of all information required by paragraphs (b)(5)(ii) through (vi) of this section; or

(B) Generate two identical copies of each voucher or coupon issued, one to be provided to the player and the other to be retained within the electronic player interface for audit purposes.

(5) Valid vouchers and coupons from a voucher system must contain the following:

(i) Tribal gaming operation name and location;

(ii) The identification number of the Class II gaming system component or the player interface number, as applicable;

(iii) Date and time of issuance;

(iv) Alpha and numeric dollar amount;

(v) A sequence number;

(vi) A validation number that:

(A) Is produced by a means specifically designed to prevent repetition of validation numbers; and

(B) Has some form of checkcode or other form of information redundancy to prevent prediction of subsequent validation numbers without knowledge of the checkcode algorithm and parameters;

(vii) For machine-readable vouchers and coupons, a bar code or other form of machine readable representation of the validation number, which must have enough redundancy

and error checking to ensure that 99.9% of all misreads are flagged as errors;

(viii) Transaction type or other method of differentiating voucher and coupon types; and

(ix) Expiration period or date.

(6) Transfers from an account may not exceed the balance of that account.

(7) For Class II gaming systems not using dollars and cents accounting and not having odd cents accounting, the Class II gaming system must reject any transfers from voucher systems or cashless systems that are not even multiples of the Class II gaming system denomination.

(8) Voucher systems must include the ability to report redemptions per redemption location or user.

Risk Mitigated by Control:
This control ensures rules and conditions are follow for cashable credit and vouchers.

Exposure of Non-Compliant System:
Non-compliant systems are vulnerable to invalid cashable payments, fraudulent vouchers and accounting errors due to their lack of rules based controls.

12. Control 547.12: What are the minimum technical standards for downloading on a Class II gaming system?

(a) Downloads. (1) Downloads are an acceptable means of transporting approved content, including, but not limited to software, files, data, and prize schedules.
(2) Downloads must use secure methodologies that will deliver the download data without alteration or modification, in accordance with § 547.15(a).
(3) Downloads conducted during operational periods must be performed in a manner that will not affect game play.
(4) Downloads must not affect the integrity of accounting data.
(5) The Class II gaming system must be capable of providing:

(i) The time and date of the initiation of the download;

(ii) The time and date of the completion of the download;

(iii) The Class II gaming system components to which software was downloaded;

(iv) The version(s) of download package and any software downloaded. Logging of the unique software signature will satisfy this requirement;

(v) The outcome of any software verification following the download (success or failure); and

(vi) The name and identification number, or other unique identifier, of any individual(s) conducting or scheduling a download.

(b)Verifying downloads. Downloaded software on a Class II gaming system must be capable of being verified by the Class II gaming system using a software signature verification method that meets the requirements of § 547.8(f).

Risk Mitigated by Control:
This control requires the secure transmission of software, including creating audit records and verification to ensure no tampering occurred. An audit trail is created tracking the downloads integrity, source, destination, timestamps, and other identifiers.

Exposure of Non-Compliant System:
Non-compliant systems are vulnerable to downloads that may have been altered, modified, or from unreliable sources. The lack of audit tracking could lead to undesirable behavior from malicious downloads in the the non-compliant system.

13. Control 547.13: What are the minimum technical standards for program storage media?

(a) Removable program storage media. All removable program storage media must maintain an internal checksum or signature of its contents. Verification of this checksum or signature is to be performed after every restart. If the verification fails, the affected Class II gaming system component(s) must lock up and enter a fault state.

Risk Mitigated by Control:
This control prevents removable program storage from invalid sources and from the data being intentionally or unintentionally modified or altered. Signature or checksum failures results in a fault state to protect the system from damage.

Exposure of Non-Compliant System:
Non-compliant systems are at risk of being infected by malicious content on removable program storage. This is a critical control to prevent system damage.

(b) Non-rewritable program storage media. (1) All EPROMs and Programmable Logic Devices that have erasure windows must be fitted with covers over their erasure windows.

(2) All unused areas of EPROMs must be written with the inverse of the erased state (zero bits (00 hex) for most EPROMs), random data, or repeats of the program data.

(3) Flash memory storage components intended to have the same logical function as ROM, must be write-protected or otherwise protected from unauthorized modification.

(4) The write cycle must be closed or finished for all CD-ROMs such that it is not possible to write any further data to the CD.

(5) Write protected hard disks are permitted if the hardware means of enabling the write protect is easily viewable and can be sealed in place. Write protected hard disks are permitted using software write protection verifiable by a testing laboratory.

Risk Mitigated by Control:
This control protects non-rewritable program storage media from unauthorized modification or storage of malicious content.

Exposure of Non-Compliant System:
Non-compliant systems are vulnerable to malicious software and/or unauthorized modification of data on non-rewritable program storage media.

(c) Writable and rewritable program storage media. (1) Writable and rewritable program storage, such as hard disk drives, Flash memory, writable CD-ROMs, and writable DVDs, may be used provided that the software stored thereon may be verified using the mechanism provided pursuant to § 547.8(f).

(2) Program storage must be structured so there is a verifiable separation of fixed data (such as program, fixed parameters, DLLs) and variable data.

Risk Mitigated by Control:
This control assures the integrity of writable and rewritable program storage media through the use of signatures and checksum to validate the source and to prevent modification or alteration.

Exposure of Non-Compliant System:
As with other forms of program storage media, non-compliant systems are vulnerable to malicious software and unauthorized modifications of data due to the lack of this control.

(d) Identification of program storage media. All program storage media that is not rewritable in circuit, (EPROM, CD-ROM) must be uniquely identified, displaying:

(1) Manufacturer;
(2) Program identifier;

(3) Program version number(s); and
(4) Location information, if critical (socket position 3 on the printed circuit board).

Risk Mitigated by Control:
This control is used to track and clearly identify the source and content of program storage media.

Exposure of Non-Compliant System:
Non-compliant systems are at risk of using invalid program storage media due to the lack of labeling controls.

14. Control 547.14; What are the minimum technical standards for electronic random number generation?

(a) Properties. All RNGs must produce output having the following properties:
(1) Statistical randomness;
(2) Unpredictability; and
(3) Non-repeatability.

Risk Mitigated by Control:
This control reduces the risks associated with prediction attacks by ensuring sufficiently random numbers are used by the gaming system.

Exposure of Non-Compliant System:
Non-compliant systems are at risk of not producing sufficiently random numbers. An attacker could calculate and predict the next move or play sequence in the game.

(b) Statistical randomness. (1) Numbers or other designations produced by an RNG must be statistically random individually and in the permutations and combinations used in the application under the rules of the game. For example, if a bingo game with 75 objects with numbers or other designations has a progressive winning pattern of the five numbers or other designations on the bottom of the card, and the winning of this prize is defined to be the five numbers or other designations that are matched in the first five objects drawn, the likelihood of each of the 75C5 combinations are to be verified to be statistically equal.

(2) Numbers or other designations produced by an RNG must pass the statistical tests for randomness to a 99% confidence level, which may include:
(i) Chi-square test;
(ii) Runs test (patterns of occurrences must not be recurrent); and
(iii) Serial correlation test potency and degree of serial correlation (outcomes must be

independent from the previous game).
(iv) Equi-distribution (frequency) test;
(v) Gap test;
(vi) Poker test;
(vii) Coupon collector's test;
(viii) Permutation test;
(ix) Spectral test; or
(x) Test on subsequences.

Risk Mitigated by Control:
This control reduces the risk of a weak RNG producing predictable values.

Exposure of Non-Compliant System:
Non-compliant systems may produce predictable RNG values. A threat actor may discover repeatable pattern in a game to exploit it during game play.

(c) Unpredictability. (1) It must not be feasible to predict future outputs of an RNG, even if the algorithm and the past sequence of outputs are known.

(2) Unpredictability must be ensured by reseeding or by continuously cycling the RNG, and by providing a sufficient number of RNG states for the applications supported.

(3) Re-seeding may be used where the re-seeding input is at least as statistically random as, and independent of, the output of the RNG being re-seeded.

Risk Mitigated by Control:
This control reduces the risks associated with future outputs of a RNG.

Exposure of Non-Compliant System:
Non-compliant systems are at risk of predictability in the RNG.

(d) Non-repeatability. The RNG may not be initialized to reproduce the same output stream that it has produced before, nor may any two instances of an RNG produce the same stream as each other. This property must be ensured by initial seeding that comes from:

(1) A source of “true” randomness, such as a hardware random noise generator; or

(2) A combination of timestamps, parameters unique to a Class II gaming system, previous RNG outputs, or other, similar method.

Risk Mitigated by Control:
This controls reduces the probability the RNG will produce a repeatable output. Seeding from a reliable source of randomness is required.

Exposure of Non-Compliant System:
Non-compliant systems are likely to product repeatability in the RNG is these seeding requirements are not met.

(e) General requirements. (1) Software that calls an RNG to derive game outcome events must immediately use the output returned in accordance with the game rules.

(2) The use of multiple RNGs is permitted as long as they operate in accordance with this section.

(3) RNG outputs must not be arbitrarily discarded or selected.

(4) Where a sequence of outputs is required, the whole of the sequence in the order generated must be used in accordance with the game rules.

(5) The Class II gaming system must neither adjust the RNG process or game outcomes based on the history of prizes obtained in previous games nor use any reflexive software or secondary decision that affects the results shown to the player or game outcome.

Risk Mitigated by Control:
This control mandates the usage of RNG outputs to reduce reduce observation attacks based on analysis of historic RNG outputs.

Exposure of Non-Compliant System:
Systems that are not compliant with the RNG general requirements are at risk of an attacker potentially install monitoring software to analyze historical or unused values in order to predict future reults.

(f) Scaling algorithms and scaled numbers. An RNG that provides output scaled to given ranges must:

(1) Be independent and uniform over the range;

(2) Provide numbers scaled to the ranges required by game rules, and notwithstanding the requirements of paragraph (e)(3) of this section, may discard numbers that do not map uniformly onto the required range but must use the first number in sequence that

does map correctly to the range;

(3) Be capable of producing every possible outcome of a game according to its rules; and

(4) Use an unbiased algorithm. A scaling algorithm is considered to be unbiased if the measured bias is no greater than 1 in 50 million.

Risk Mitigated by Control:
This control ensures that scaling algorithms and scaled numbers do not produce predictable patterns.

Exposure of Non-Compliant System:
The risk of non-compliant systems is predictability in the RNG that an attacker could use to calculate and predict the next move or play sequence in the game.

15. **Control 547.15: What are the minimum technical standards for electronic data communications between system components?**

(a) Sensitive data. Communication of sensitive data must be secure from eavesdropping, access, tampering, intrusion or alteration unauthorized by the TGRA. Sensitive data includes, but is not limited to:

(1) RNG seeds and outcomes;
(2) Encryption keys, where the implementation chosen requires transmission of keys;
(3) PINs;
(4) Passwords;
(5) Financial instrument transactions;
(6) Transfers of funds;
(7) Player tracking information;
(8) Download Packages; and
(9) Any information that affects game outcome.

Risk Mitigated by Control:
This control ensures the protection of sensitive data in communication channels. Protection of the confidentiality and integrity of the data in transit.

Exposure of Non-Compliant System:
Non-compliant systems are at risk of exposing critical data in transit. The confidentiality and integrity of the data is compromised with these controls.

(b) Wireless communications. (1) Wireless access points must not be accessible to the general public.

(2) Open or unsecured wireless communications are prohibited.

(3) Wireless communications must be secured using a methodology that makes eavesdropping, access, tampering, intrusion or alteration impractical. By way of illustration, such methodologies include encryption, frequency hopping, and code division multiplex access (as in cell phone technology).

Risk Mitigated by Control:
This control ensures the secure transmission of data over and monitoring of wireless communications.

Exposure of Non-Compliant System:
Non-compliant systems expose wireless communication to easily perpetrated and well known attacks the compromise the confidentiality and integrity data.

(c) Methodologies must be used that will ensure the reliable transfer of data and provide a reasonable ability to detect and act upon any corruption of the data.

Risk Mitigated by Control:
This control requires ensures the reliable transmission of data with the ability to detect and recover from data transmission corruption weather intentional or unintentional.

Exposure of Non-Compliant System:
Non-compliant systems are at risk of receiving and transmitting data that has been modified by system errors or malicious actors.

(d) Class II gaming systems must record detectable, unauthorized access or intrusion attempts.

Risk Mitigated by Control:
This detective control ensures intrusions will be detected logged..

Exposure of Non-Compliant System:
Non-compliant systems would allow intrusions to go undetected leading to additional system and data breaches.

(e) Remote communications may only be allowed if authorized by the TGRA. Class II gaming systems must have the ability to enable or disable remote access, and the

default state must be set to disabled.

Risk Mitigated by Control:
This control reduces the risk associated with remote communication by providing mechanisms to disable or remove remote access to keep the system protected.

Exposure of Non-Compliant System:
Non-compliant systems are at risk on remote communication not being disabled. Open remote communication channels could be used by a threat actor to gain unauthorized access to gaming consoles or servers.

(f) Failure of data communications must not affect the integrity of critical memory.

Risk Mitigated by Control:
This control ensures that critical memory integrity will be maintained even if there is loss of communications.

Exposure of Non-Compliant System:
Non-compliant systems are at risk of corrupting the integrity of critical memory during a communications failure.

(g) The Class II gaming system must log the establishment, loss, and re-establishment of data communications between sensitive Class II gaming system components.

Risk Mitigated by Control:
This control ensures that all data communications between system components are logged.

Exposure of Non-Compliant System:
Non-compliant systems will not log the establishment, loss, and re-establishment of data communications between system components. This increases the risk of undetected intrusion and unauthorized access.

16. Control 547.16: What are the minimum standards for game artwork, glass, and rules?

(a) Rules, instructions, and prize schedules, generally. The following must at all times be displayed or made readily available to the player upon request:
(1) Game name, rules, and options such as the purchase or wager amount stated clearly and unambiguously;

(2) Denomination;

(3) Instructions for play on, and use of, the player interface, including the functions of all buttons; and

(4) A prize schedule or other explanation, sufficient to allow a player to determine the correctness of all prizes awarded, including:

(i) The range and values obtainable for any variable prize;

(ii) Whether the value of a prize depends on the purchase or wager amount; and

(iii) The means of division of any pari-mutuel prizes; but

(iv) For Class II Gaming Systems, the prize schedule or other explanation need not state that subsets of winning patterns are not awarded as additional prizes (for example, five in a row does not also pay three in a row or four in a row), unless there are exceptions, which must be clearly stated.

Risk Mitigated by Control:
This control ensures fair play and full disclosure to the player.

Exposure of Non-Compliant System:
Non-compliant systems may not disclose information to Players thereby reducing trust and acceptance of the system.

(b) Disclaimers. The Player Interface must continually display:
(1) “Malfunctions void all prizes and plays” or equivalent; and
(2) “Actual Prizes Determined by Bingo (or other applicable Class II game) Play. Other Displays for Entertainment Only” or equivalent.

Risk Mitigated by Control:
This control provides awareness to the player of all disclaimers in the interest of fair play.

Exposure of Non-Compliant System:
Non-compliant systems violates requirements to display disclaimers.

(c) Odds notification. If the odds of winning any advertised top prize exceeds 100 million to one, the Player Interface must display: “Odds of winning the advertised top prize exceeds 100 million to one” or equivalent.

Risk Mitigated by Control:
The only risk is the player not knowing the odds of the game. More like a legal disclaimer to inform the consumer, not a security risk.

Exposure of Non-Compliant System:
The exposure of older systems not complying with this control is higher than in new systems that have this built in functionality installed. In any event, minimal exposure.

17. Control 547.17: How does a TGRA apply to implement an alternate minimum standard to those required by this part?

(a) TGRA approval. (1) A TGRA may approve an alternate standard from those required by this part if it has determined that the alternate standard will achieve a level of security and integrity sufficient to accomplish the purpose of the standard it is to replace. A gaming operation may implement an alternate standard upon TGRA approval subject to the Chair's decision pursuant to paragraph (b) of this section.

(2) For each enumerated standard for which the TGRA approves an alternate standard, it must submit to the Chair within 30 days a detailed report, which must include the following:

(i) An explanation of how the alternate standard achieves a level of security and integrity sufficient to accomplish the purpose of the standard it is to replace; and

(ii) The alternate standard as approved and the record on which the approval is based.

(3) In the event that the TGRA or the tribe's government chooses to submit an alternate standard request directly to the Chair for joint government to government review, the TGRA or tribal government may do so without the approval requirement set forth in paragraph (a)(1) of this section.

Risk Mitigated by Control:
TGRA may submit a new stronger standard than the minimal technical standards.

Exposure of Non-Compliant System:
Non-compliant systems manufactured before November 10, 2008 are at risk of not having the technology required to meet the requirements of alternate standards.

(b) Chair review. (1) The Chair may approve or object to an alternate standard approved by a TGRA.

(2) If the Chair approves the alternate standard, the Tribe may continue to use it as authorized by the TGRA.

(3) If the Chair objects to the alternate standard, the operation may no longer use the alternate standard and must follow the relevant technical standard set forth in this part.

(4) Any objection by the Chair must be in written form with an explanation why the alternate standard as approved by the TGRA does not provide a level of security or integrity sufficient to accomplish the purpose of the standard it is to replace.

(5) If the Chair fails to approve or object in writing within 60 days after the date of receipt of a complete submission, the alternate standard is considered approved by the Chair. The Chair may, upon notification to the TGRA, extend this deadline an additional 60 days.

Risk Mitigated by Control:
This requirement outlines chair approval of alternate standards.

Exposure of Non-Compliant System:
Non-compliant systems are not likely to meet alternate standards.

(c) Appeal of Chair decision. A TGRA may appeal the Chair's decision pursuant to 25 CFR chapter III, subchapter H.

Risk Mitigated by Control:
This requirement addresses chair decision appeal

Exposure of Non-Compliant System:
Not relevant to non-compliant systems.

APPENDIX B: REFERENCES

NIST Information Security Handbook, Special Publication 800-100 (October 2006)
https://csrc.nist.gov/publications/detail/sp/800-100/final

NIST BIOS Protection Guidelines, Special Publication 800-147 (April 2011)
https://csrc.nist.gov/publications/detail/sp/800-147/final

NIST BIOS Integrity Measurement Guidelines Special Publication 800-155 (December 2011)
https://csrc.nist.gov/CSRC/media/Publications/sp/800-155/draft/documents/draft-SP800-155_Dec2011.pdf

SANS - Information Security Resources | Information Security Policy
https://www.sans.org/security-resources/policies

Center for Internet Security CIS Critical Security Controls
https://www.cisecurity.org/

The Importance of Cyber Hygiene in Cyberspace
http://resources.infosecinstitute.com/the-importance-of-cyber-hygiene-in-cyberspace

U.S. Casinos, Regulators Face Growing Cybersecurity Challenge
https://gamblingcompliance.com/premium-content/news_analysis/us-casinos-regulators-face-growing-cybersecurity-challenge

Verizon 2017 Data Breach Investigations Report
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Data Security Breach Articles:

articles that have data and statistics on cybersecurity

http://www.washingtonpost.com/wp-srv/special/investigative/zeroday/cyber-history-timeline/

https://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

https://en.wikipedia.org/wiki/List_of_data_breaches

https://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history

https://www.symantec.com/content/en/us/about/media/securityintelligence/SSR-Timeline.pdf

https://gcn.com/articles/2013/05/30/gcn30-timeline-cybersecurity.aspx

https://csis-prod.s3.amazonaws.com/s3fs-public/171006_Significant_Cyber_Events_List.pdf?Sm9UDh1TitdFtv3BlXO3tkIHRVfanwdE

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150717_Carter_CybersecurityRequirements_Web.pdf

https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23

https://www.securable.io/infosec-news/infosec-update-cyber-security-education-hacking-more-than-just-computers

https://www.upguard.com/blog/casino-data-breaches-and-doubling-down-on-digital-resilience

https://www.csoonline.com/article/3089449/security/hard-rock-las-vegas-suffers-a-second-data-breach.html

http://www.zdnet.com/article/hard-rock-loews-hotels-admit-data-breach/

https://www.securelink.com/securelink-blog/is-your-casino-network-under-attack/

https://www.bankinfosecurity.com/casino-sues-trustwave-over-data-breach-a-8804

https://globalnews.ca/news/3208546/security-experts-call-grey-eagle-casino-security-breach-a-wake-up-call/

https://www.darktrace.com/resources/wp-global-threat-report-2017.pdf

https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEFCON-25-Gus-Frischie-and-Evan-Teitelman-Backdooring-the-Lottery.pdf