

February 10, 2022


Mr. E. Sequoyah Simermeyer, Chairperson  
National Indian Gaming Commission  
1849 C. Street NW  
Mail Stop # 1621  
Washington, D.C. 20240

Re: Tribal Comments to the NIGC's Consultation Series C

Dear Chair Simermeyer & Vice-Chair Hovland:

The Seneca-Cayuga Nation Office of the Gaming Commissioner is pleased to offer these comments on the National Indian Gaming Commission's Series C topics that were discussed and presented via video conference on January 11-12, 18, and 25, 2022. We appreciate the NIGC's efforts to solicit and consider tribal input on these important matters, which will have a tangible effect on the regulation of gaming. The opportunity to provide input at this early stage is consistent with the principles of a strong government-to-government relationship, and we believe will produce better, more fully considered rules.

Sincerely,

  
\_\_\_\_\_  
Danielle Brashear, Commissioner  
Seneca-Cayuga Office of the Gaming Commissioner

Enclosure.

**COMMENTS OF THE SENECA-CAYUGA NATION OFFICE OF THE GAMING COMMISSIONER ON THE NATIONAL INDIAN GAMING COMMISSIONS SERIES C CONSULTATION TOPICS**

**I. Introduction.**

These comments are made in response to the Series C topics published by the NIGC on its website and discussed via Zoom on January 11-12, 18, and 25, 2022. We are pleased to provide input on these potential regulatory changes. The Seneca-Cayuga Nation Office of the Gaming Commissioner (“SCOGC”) therefore submits the following comments, which are included under the pertinent text of the consultation questions below.

**II. Comments.**

**1. Technological Enhancements and Technology Threats**

- a. *Should the NIGC consider other tools to promote awareness and strengthen cyber security practices?*

Yes, the SCOGC does believe that the NIGC should consider additional tools to promote awareness and strengthen cybersecurity practices. However, instead of promulgating additional regulations on cybersecurity-related issues, the SCOGC believes that the NIGC should increase educational opportunities and provide particularized technical assistance to Tribal governments, gaming operation employees, and associated IT departments upon request.

By increasing educational opportunities, training, and technical assistance regarding cybersecurity-related issues, the NIGC can better promote tribal self-sufficiency and strong tribal governments without any risk of going beyond the scope of its congressional mandate set forth in IGRA. As the primary regulators of tribal gaming, TGRAs are better positioned to understand a gaming operation’s unique IT infrastructure and, accordingly, are better equipped to develop their own particularized internal controls on these matters. Different gaming operations face different cybersecurity-related challenges, and the on-the-ground regulators have a stronger likelihood of appreciating the specific risks related to a particular gaming operation’s cybersecurity infrastructure.

The SCOGC does support the current efforts of the NIGC to provide education and training on cybersecurity-related issues, but we believe that more can be accomplished in this area. The first thing we recommend is creating an easily accessible library on the NIGC’s website that contains past and future trainings on these issues. Because the NIGC’s Tribal Cybersecurity Readiness document outlines common types of cyberattacks, it can help raise awareness for those without a high degree of threat awareness. However, we believe this could be a much more effective and useful tool if the Commission were to provide more sophisticated on-demand training modules. Currently, the NIGC hosts a limited number of trainings over Zoom on the subject, but there are limits on the efficacy of these efforts. If an interested party wishes to see a particular session, it must go through the specific process to request such recordings. An on-demand library, on the other hand, would allow interested parties to watch these recordings at convenient times on their

own. Further, if the NIGC does not employ enough subject matter experts on cybersecurity to aid tribal governments at the high levels that may be needed in the wake of a major breach, we recommend that the NIGC look to coordinate with the Cybersecurity & Infrastructure Security Agency (CISA), which has recently begun an outreach effort to tribal governments.

Next, the SCOGC believes that the NIGC should encourage communication between tribal governments and the NIGC regarding cyber threats. If the NIGC were to take a prescriptive regulatory approach with issues related to cybersecurity, this necessarily entails the threat of punitive enforcement measures. Instead, we urge an approach consistent with IGRA's purposes, particularly those aimed at strengthening the capacity of tribal governments to protect their assets. As discussed further below, we do not believe that tribal governments must be forced to address cybersecurity concerns, and we certainly object to the idea that a data breach would warrant a closure order or civil fine assessment. By finding ways to increase communications between tribal governments and the NIGC, it will further support the NIGC's efforts to disseminate necessary information on pressing matters as soon as the need arises.

b. *Do existing NIGC requirements create any unintended limits on tribes' ability to implement, regulate, or review new technologies?*

Yes and no. Current regulations are reviewed whenever any new technology is considered and sometimes it is not clear whether a particular control standard would be violated if the technology is deployed. In these circumstances, TGRAs and operations must work together to establish or update a control standard. Generally, the NIGC's current regulations do not create insurmountable limitations on new technologies. However, we are concerned that promulgating additional regulations to address emerging technologies could well produce such harms.

c. *What approaches are tribal law makers taking with regard to cloud-based storage investments and external vendor services?*

While the SCOGC is hesitant to support any regulatory changes concerning cloud-based storage solutions and external vendor services, we can predict certain issues arising with tribal gaming operations that are considering these as options for data storage. Most importantly, ownership of the data stored on these cloud-based storage platforms could become an issue in contract negotiations between gaming operations and vendors. Additionally, a vendor's use of and access to such information, both before and after the expiration of a contract, will be a major concern in drafting acceptable service contracts. The SCOGC would support the NIGC in the publishing of a guidance document akin to what it has published regarding sports book agreements, loan documents and financing agreements, and other contracts between gaming operations and vendors.

d. *What changes should the NIGC consider to strengthen cybersecurity for Indian gaming operations?*

As provided in the first framing question to this consultation topic, the SCOGC believes that the NIGC should find ways to increase communication between the Commission and tribal governments regarding actual or attempted cyberattacks without the implied threat of sanctions

against a Tribal government that has already been victimized by a real or attempted cyberattack. Further, the SCOGC believes that increased training and education will enhance the capacity of TGRAs to understand both common and novel threats to a gaming operation's cybersecurity infrastructure.

## **2. Extending Protection of Environment, Public Health, and Safety to Include Issues Related to Cybersecurity**

- a. *Should the agency look to update the EPHS interpretative rule to include the potentially harmful and life altering results of a data privacy breach?*

No, the SCOGC is generally opposed to the NIGC taking regulatory actions concerning data breaches. As alluded to in the first framing question, we are of opinion that the phrase "environment and the public health and safety" as used in the statutory text of IGRA does not extend to issues related to cybersecurity. When questions arose as to the meaning of the EPHS phrase in 2002, the NIGC published an interpretative rule giving the Commission a narrow role and recognizing the superior governmental interest of tribal governments in the EPHS arena. Pursuant to the 2002 EPHS interpretative rule, the NIGC only has the authority thereunder to review plans prepared by tribal governments in relation to emergency preparedness, food and water, and construction and maintenance. The SCOGC does not believe that data breaches and the potential results thereof fall within any of these categories. Neither does the plain language of the phrase "environment, public health, and safety" call to mind the subject of data privacy. Thus, the SCOGC is concerned that any update to the interpretative rule in this regard would exceed the NIGC's regulatory authority under IGRA.

As discussed in the first framing question, the SCOGC believes that the best path forward is for the NIGC to utilize its resources to provide trainings to assist tribal governments in remaining vigilant and knowledgeable of the evolving threats to data privacy. These trainings could include suggestions, recommendations, and best practices for preventing and responding to data privacy breaches.

- b. *What should the agency's role be in promulgating standards and requirements for cybersecurity, and does that intersect with the agency's existing role of ensuring public health and safety?*

The SCOGC does not see any regulatory role within the authority granted the NIGC pursuant to IGRA pertaining to cybersecurity. Expanding the term "public health and safety" to include cybersecurity does not appear to be a reasonable interpretation of that phrase as used in IGRA, and we expect that there would be legal challenges under the *Chevron* doctrine to any such regulations. While the NIGC's concerns about cybersecurity are understandable, agencies must remain dedicated to their core regulatory missions and not exceed the authority granted to it by Congress. We encourage the NIGC to refrain from efforts to expand its authority into areas not contemplated by IGRA or its legislative history, such as cybersecurity.

- c. *What existing cybersecurity considerations are informing tribal lawmakers' decisions in this area?*

Like many other industries, tribal gaming has become increasingly interconnected with electronic and internet-based technologies, and accordingly, TGRAs have had to become more adept in following these developments. To do this, TGRAs and their associated IT departments must regularly monitor and respond to the latest cybersecurity threats, including viruses and other forms of malware that could lead to a security breach. However, in our experience, it is of central importance for tribal gaming regulators to be aware of and protect against vulnerabilities on internal systems, such as weak passwords, phishing attempts, and accessible shared files that individuals with low threat awareness may not fully appreciate.

As discussed throughout these comments, tribal governments are the appropriate bodies to address cybersecurity concerns. Tribal governments are empowered under law to promulgate policies, procedures, and regulations best suited to that tribal government's unique regulatory needs and to enforce all such controls. Thus, we believe that the NIGC's role in this space is best served in an advisory capacity. Accordingly, we recommend that the NIGC explore methods by which it could disseminate information on and recommend safeguards against trending and emerging threats on which it has received intelligence.

Moreover, we recommend that the NIGC increase the availability of and access to educational resources that could be utilized by TGRAs as teaching tools for their staffs. It would be especially helpful to have access to such guidance on a wide variety of topics, including: 1) personal computer security; 2) methods of monitoring electronic systems for evidence of breach or attempted breach; 3) strategies for protecting patron data and promoting public confidence in data security; 4) effective responses to suspected or confirmed data security breaches; and 5) conducting IT audits.

### **3. Chair's Issuance of a Temporary Closure Order for Misuse of Net Gaming Revenue**

- a. *Given IGRA's intent and requirement that the Tribe be the primary beneficiary of its gaming operation, do you view misuses of net gaming revenue as warranting a TCO? Are there circumstances or a level of misuse that you think would warrant a closure order for misuse of net gaming revenue?*

The SCOGC strongly opposes the inclusion of "misuse of gaming revenue" to the list of actions in 25 C.F.R. § 573.4 (a) that would authorize the Chair, in his or her sole discretion, to issue a temporary closure order (TCO) to a tribal gaming operation. The term is simply too broad to provide any meaningful standard for establishing appropriate parameters for the exercise of the NIGC's enforcement authority.

From our observations, most reported misuses of gaming revenues have been caused by a small number of identifiable wrongdoers, whose victims include the tribal government and its members. Those who profit from the conversion, theft, fraud, or misappropriation of tribal

gaming funds or assets should be prosecuted under IGRA's criminal provisions. However, to file a TCO against a tribal government and issue a civil fine assessment for the unlawful acts of a small number of individuals only serves to re-victimize the victims. Such actions could effect irreparable harms to the relationships between the NIGC and such tribal governments, as well as directly to the tribal governments and its members.

One of the other enumerated purposes of IGRA is to provide a statutory basis for the operation of gaming by Indian tribes as a means of promoting tribal economic development, self-sufficiency, and strong tribal governments.<sup>1</sup> This proposal creates the potential for an NIGC Chair to deprive tribal governments and their citizens of revenues that are crucial to fund so many different governmental functions, including, housing, healthcare, law enforcement, education, and elder services. This is in addition to the loss of funds already realized due to a small number of bad actors. Further, during a TCO, gaming facilities may have to cease operations entirely for an indeterminate amount of time which will hinder tribal governments' ability to pay ongoing debt obligations. Considering that the NIGC is only currently comprised of the Chair and Vice-Chair, any appeals of a TCO brought under Parts 573, 584, and 585 would largely be performative as it takes a majority vote of the Commission to overturn the Chair's initial decision.

Lastly, the SCOGC believes that the Letter of Concern and Notice of Violation processes in Part 573 are better avenues to resolve any issues related to the misuse of gaming revenues. These processes more properly respect the sovereignty of tribal governments as it allows for TGRAs or other Tribal entities with the opportunity to remedy problems through their own internal processes before the NIGC Chair could choose to temporarily close a gaming facility at his or her discretion. Moreover, the list of substantial violations included in 573.4 (a) already authorizes the Chair to issue a TCO should a tribal government fail to correct violations within the timeframe outlined in an NOV. Accordingly, the SCOGC strongly opposes this potential regulatory revision as it is unnecessary and overly-punitive.

- b. *There are currently 13 substantial violations for which the Chair may issue a TCO. What would be the impact of adding misuse of net gaming revenue to the list of substantial violations?*

As discussed in the previous response, the SCOGC does not believe that "misuse of gaming revenue" should be included in the list of violations that could warrant a TCO as handling these issues in the current Notice of Violation process is more aligned with the NIGC's goals to ensure compliance with IGRA. The unlawful conversion of net gaming revenue or other criminal acts that would fall under the umbrella of "misuse of net gaming revenue" are best handled by those entities with criminal jurisdiction over such matters. The NIGC's powers under IGRA are civil in nature, and accordingly, the NIGC's regulatory goal is not to punish, but to effect compliance.

In short, to include "misuse of gaming revenue" to 25 C.F.R. § 573.4 (a) would grant the NIGC chair nearly untethered authority to enforce an overly-broad standard that will likely be subject to allegations of arbitrary and capricious decision-making, further punish the actual victims of the misuse of gaming revenue and weaken Tribal sovereignty as it deprives a tribal government the ability to handle its own internal matters within a reasonable amount of time.

---

<sup>1</sup> 25 U.S.C. § 2702 (1).

#### **4. Modifying NIGC Regulations to Provide More Transparency, Accountability, and Efficiency in its Contract Reviews**

- a. *What regulatory updates would provide additional transparency, accountability, and efficiency in the NIGC Chair's contract review and background investigation process?*

The SCOGC encourages the NIGC to dedicate its resources to increasing transparency and accountability with regard to existing regulatory structures without actually promulgating additional regulations. Instead, the SCOGC believes that tribal governments would more directly benefit from trainings and non-binding guidance on issues of importance in these areas.

Specifically, the SCOGC believes that this approach would be effective in response to contracts concerning emerging areas of gaming, such as cloud-based storage solutions as addressed above. Since the particulars of novel forms of gaming have yet to be fully developed, we believe that promulgating extensive regulation would be premature and risk stunting the growth of evolving technologies and innovation by creating standards that may not serve the best interests of tribal governments for the long term. However, by identifying best practices in other jurisdictions, or highlighting factors that the NIGC identifies as particularly problematic when backgrounding individuals or entities providing products or services related to emerging technologies, tribal governments' regulation over these matters can evolve side-by-side with such technologies. As opposed to the lengthy and burdensome development and review processes of promulgating regulations, the NIGC could quickly publish or update non-binding guidance documents in light of new information.

If the NIGC determines it necessary to promulgate additional regulations that will provide transparency, accountability, and efficiency in the Chair's contract review and background process, we encourage the NIGC to focus on promulgating standards that provide certainty to tribal governments regarding the length of time these review processes may require. For example, under 25 C.F.R. § 537.4, the Chair is required to "promptly" notify a tribal government if the Chair cannot or will not approve a management contract based on background findings. By setting definitive deadlines for such determinations and communications, tribal governments could rely on a set timeline for moving forward with an agreement or pursuant other opportunities.

- b. *How might technology provide more efficiency and lower cost in this process?*

In conjunction with our previous response, the SCOGC believes that technology could be best utilized to facilitate communications, especially about best practices in negotiating management contracts and facilitating background checks required under 25 C.F.R. Part 537. While the NIGC's consultation series has been an adequate avenue to discuss proposed regulatory amendments and other developments with the NIGC, we believe that more can be done to facilitate communications between tribal governments. Accordingly, we would support the use of technology to facilitate round table discussions that could serve as a forum between tribal officials on these issues. These round table discussions could allow tribal leaders and regulators

to discuss these issues while the NIGC could provide insight on questions regarding its view on contract provisions and investigation techniques. Following these roundtable discussions, the NIGC could provide a summary of the findings and conclusions that would be made available to interested tribal governments.

Like the on-demand trainings that could prove to be extremely beneficial in matters related to cybersecurity, the SCOGC further encourages the NIGC to make available on-demand trainings on contracting best-practices and backgrounding strategies. Publishing these trainings in a manner that is easy to locate, fully captioned, and accompanied by training modules or other downloadable content would not only better ensure that TGRAs and employees are aware of their duties under IGRA, but could eliminate unnecessary compliance issues down the road.

Utilizing technology in this way may bring about cost savings since addressing compliance issues before they are encountered increases tribal regulatory efficiency, both functionally and monetarily. Currently, the SCOGC perceives that the NIGC has mainly used its authority in a reactive manner, rather than a proactive manner. We believe that by becoming proactive and focusing on preempting negative circumstances by establishing clear guidelines is also more aligned with the NIGC's purpose to ensure compliance with IGRA. By enhancing educational opportunities, the NIGC can better allow tribal lawmakers and regulators to achieve their goals more efficiently, which will further the tenets of self-governance outlined in IGRA.

### **III. Conclusion.**

The SCOGC appreciates the opportunity to offer our comments to the NIGC by providing the comments herein, and we are grateful for the NIGC's consideration of our comments, as well as those of other Tribal governments. The SCOGC further looks forward to continuing to engage in meaningful consultation with the NIGC on these matters throughout the revision process. We are confident that such collaboration results in better regulation beneficial to the tribal gaming industry and Indian Country as a whole.