



Date: October 19, 2022

RE: Indian Gaming Association (IGA) Cyber Security Training

Today I had the opportunity to present NIGC's perspective on cyber security at the Indian Gaming Association's cyber security training in Las Vegas. I'm grateful to Rebecca Fisher for including the Agency in the dialogue on this very important topic. IGA's dedication to matters related to cyber security is an important part of Indian gaming's response and effective preparation for cybersecurity events.

Through an agency-wide focus on regulatory **preparedness**, my presentation outlined how four factors have played a significant role in shaping NIGC's approach to cyber security:

- NIGC's own experience with addressing and re-investing in the Agency's technology and data infrastructure needs.
- The increase in the sophistication of ransomware attacks and the significance of the threats the attacks pose to tribal governments' continuity of operations and their ability to regulate and protect gaming operation assets.
- The rise in attention at federal leadership levels to support the implementation of strong cybersecurity practices at all federal agency operations by establishing CISA and announcing various Executive Orders.
- NIGC's regulatory trajectory over the last 10 years that has increased the Agency's focus on risk-based assessments informed by local level conditions and threats.

You can download the presentation [HERE](#).

I also highlighted NIGC's virtual cyber summit - [The Federal Perspective on Cyber Security](#), November 15 and 16.

###

Visit www.NIGC.gov to learn more about the NIGC 3 For 35 Project— a year-long project emphasizing the importance of conversations among the tribal gaming regulatory community about workforce preparedness.

