



Dear Data Integrity Advocate:

Over the last several months, GreenTec-USA has been working closely with the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) on a [cybersecurity project on data integrity](#).

The NCCoE is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. I'm excited to share that the NCCoE has just released a draft practice guide, titled [NIST SP 1800-11, Data Integrity: Recovering from Ransomware and Other Destructive Events](#).

The guide explores methods that organizations can use to effectively recover from a data corruption event in various Information Technology (IT) enterprise environments. The guide also maps security characteristics to standards, guidance, and best practices from NIST, and other standards organizations.

To complete this guide, NCCoE also collaborated with technology vendors including: GreenTec-USA; HPE; IBM; Tripwire; Veeam.

The [draft is available for download](#) on the NCCoE website. Please share your thoughts on this step-by-step guide with NCCoE to help make it better.

This practice guide can help businesses recover from a detected cybersecurity event by showing how commercially available technologies, like WORMdisks™ and CYBERdisks™,* can be integrated with your existing tools and IT system infrastructure. The NCCoE and we think the guide helps meet a critical cybersecurity need, but we'd like to hear from you.

[Download the guide](#) and [provide your thoughts on the NCCoE website](#).

Please let us know how we can help with your cyber-defense and data integrity needs.

Thank you,

Steve Petruzzo
President and CEO



22375 Broderick Dr., Suite 155, Sterling, VA 20166
(703) 283-3052 (cell) (703) 880-8332 (land line)
www.GreenTec-USA.com

*While the example implementation uses certain products, including GreenTec WORMdisks™ and CYBERdisks™, NIST and the NCCoE do not endorse these products. The guide presents the characteristics and capabilities of those products, which an organization's security experts can use to identify similar standards-based products that will fit within with their organization's existing tools and infrastructure.