UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards **Docket No. AD19-18-000**

Comments on Transparency/Further Recommendations

Submitted to FERC on October 28, 2019

Dr. George Kondos, a private citizen with over 40 years of experience in systems development and cyber security including many years working on telecommunications systems, submits the following comments on FERC Docket No. AD19-18-000, Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards.

BACKGROUND

I am considered to be an expert on computer and network systems cybersecurity with over 40 years of experience in systems, network, and telecommunications design, development, and security analysis and implementation. I was a founding member of the Computer Security Institute (1974) and have worked on security issues for many Fortune 100 companies including Digital Equipment Corporation, MCI, Siemens and FedEx. I have also worked on analysis, monitoring and security issues for the FBI (as a GS-15) and on DoD projects for NORAD, the US Space Command, and the Missile Defense Agency in senior technical/subject matter expert and team lead positions. I have also worked with senior level personnel from the CIA, NSA, NRO, and ODNI. I have written multiple guides for systems monitoring (mostly classified).

My education includes Masters and Doctoral degrees in Computer Science with studies in security and cryptography. I am a member of ISC2, ISSA, and InfraGard and have held a CISSP certification for many years. Additional studies include extensive coursework in security, systems penetration (hacking), network security and design, security management and much more.

COMMENTS on TRANSPARENCY

Having been involved in analyzing and testing systems for functionality and security, and having been trained in hacking/penetration testing I am well aware of the need to keep some information that could be used for attacking systems confidential. On the other hand, I have seen how transparency can help insure that both companies and government agencies are held accountable for their actions. It is possible to ensure that the release of information that is useful to hackers is mitigated, while still providing the public with adequate information to hold utilities accountable for their actions to protect the electric grid from cyber and other attacks. I have seen too many organizations trivialize, hide, or otherwise fail to adequately address issues where transparency has been lacking. Transparency is one of the reasons why Sarbanes-Oxley was devised and there is substantial evidence that this has positively influenced security for the affected public corporations. Without adequate transparency, how do we hold organizations accountable? How can we even know if they are adequately addressing critical risks and vulnerabilities?

Having read some of the commentaries on this docket, I find that I agree with comments on transparency such as those submitted by Michael Mabee and others, and I fully concur with the comments by Joseph Weiss on acknowledging cyber incidents and setting appropriate Supply Chain requirements. I have seen issues with questionable components while working on DoD projects and I know that the DoD takes supply chain issues seriously.

Overall, it is my opinion that adequate transparency is necessary for true security. I hope that FERC/NERC will ensure that an adequate level of transparency is required to help ensure that our electric grid is adequately protected.

George Kondos

Dr. George Kondos, DCS, CISSP

Document Content(s)

FERC Submitta3.PDF...1-2