

## CYBERSECURITY ROADMAP COMMENTS FOR THE FCC.

This roadmap will establish a plan for the FCC: Comments should offer responses to the following questions:

- 1. What are the most vital cybersecurity vulnerabilities for communications networks and users?*

Every IT communications network relies on thousands of different devices and servers. A critical infrastructure server for most large telcos is the mainframe. Most of the attention, budget and human resources within an IT organization, since the advent of the “high risk” internet, have been focused on the distributed network itself and little attention has been paid to making sure that mainframes within the network are secure. A failure by a single mainframe can be a mission critical failure for a network. Mainframes are more vulnerable to attack than generally known, and therefore mainframes are part of the most vital cybersecurity vulnerabilities for communications networks.

- 2. How can these vulnerabilities be addressed?*

The implementation of strong security configuration controls for all IT platforms, including the mainframe, will help ensure that the level of security maintained for these systems is robust enough to withstand attacks (and that the systems can continue to operate while under attack). Increased security training for network providers and users is also critical, cost effective and will help ensure that security throughout the network is properly configured and maintained.

- 3. What role should the Commission play in addressing them?*

The Commission should leverage the work of the National Institute of Standards Technology (NIST), including the security standards and the security configuration controls published by or endorsed by NIST. To the extent that NIST security standards and security configuration controls do not cover relevant parts of the communications networks or users, the Commission should leverage the security standards and security configuration controls of the National Security Agency and the Defense Information Systems Agency.

We recommend that the FCC not try to duplicate the efforts and expend dollars unnecessarily to re-create programs, standards or controls. Many entities within the communications network, and many users, are already subject to the standards and controls published by NIST, NSA and DISA, and if separate, and necessarily

different, standards and controls were to be adopted by the Commission the state of communications security might be negatively impacted.

*4. What steps should the Commission take, if any, to remediate them?*

The Commission could mandate the use of the Security Standards and Configuration controls promulgated by NIST, NSA and DISA be followed by all entities regulated by the Commission. The Commission should work with NIST, NSA and DISA to ensure that the security standards and configuration controls adopted by those agencies cover communications network vulnerabilities to the extent they currently do not.

*5. If the FCC does not play a role in addressing these vulnerabilities and problems, what agency or entity would fulfill that role?*

The FCC does have a role to play in terms of its area of interest, but the security standards and configuration controls should be those adopted by NIST, NSA and DISA.

*6. How should the Commission coordinate its efforts with other agencies of government?*

We recommend the commission work with agencies like NIST, NSA, DISA as well as DHS in utilizing initiatives already in place to ensure the safety of their core infrastructure.

References:

Gartner Inc.: Why Your IBM z/OS Mainframe May Not Be as Secure as You Think It Is and What You Can Do About It by Ant Allen. (Gartner RAS Core Research Note G00172909, January 2010.)

Forbes.com/JargonSpy: The Naked Mainframe by Dan Woods. (Forbes.com/JargonSpy January 2010.)

Fierce GovernmentIT: NIST Promotes common cybersecurity controls by David Perera. (FierceGovernmentIT, The government IT News Briefing, June, 2010.)

Fierce GovernmentIT: NIST encourages agencies to adopt SCAP by Molly Bernhart Walker. (FierceGovernmentIT, The government IT News Briefing, August, 2010.)