Working Group 8 – ISP Network Protection Practices

Description: This Working Group will investigate current practices that ISPs use to protect their networks from harms caused by the *logical* connection of computer equipment, as well as desired practices and associated implementation obstacles.[1] The work should address techniques for dynamically identifying computer equipment that is engaging in a malicious cyber attack, notifying the user, and remediating the problem. The Working Group will develop proposed recommendations for CSRIC's consideration for best practices and actions the FCC could take that may help overcome implementation obstacles.

Duration: Twelve months.

---

[1] As used here "computer equipment" includes a wide variety of personal equipment (*e.g.,* servers, PCs, smart phones, home routers, *etc.*) as well as household devices with embedded IP network connectivity. "logical connection" refers to end-user data communications protocol signaling and transmission. Harms result from the ability to degrade the communications infrastructure though malicious protocol exchanges and information transmission.