# A Seductive Model of Governance: Protecting Critical Infrastructure through Network Security Agreements

Joshua W. Abbott

While digital technologies have advanced at light-speed in recent years, lawmakers have made almost no updates to laws protecting critical communications infrastructure. We face geometric increases in threats to the physical and data security of our networks. Yet when changing technologies make regulatory rules obsolete almost overnight, agencies can respond only with rulemaking proceedings that may take months or years to complete. Traditional regulation may simply be inadequate for today's ever-accelerating innovation in network technology. A few agencies, though, have found an innovative way around this problem in some areas. The FCC is responsible for considering national security, law enforcement, and other policy concerns when reviewing certain license applications for international or foreign-owned communication networks. Rather than promulgating general rules or developing independent expertise on these issues, the FCC simply decided at some point that it would defer those applications to the Executive Branch. To review these applications, the Executive created "Team Telecom," an ad hoc interagency group made up of representatives from the Departments of Homeland Security, Defense, and Justice, including the FBI. Team Telecom sometimes negotiates a Network Security Agreement (NSA) with the applicant and later reports to the FCC that it has no objection to the FCC granting the license if conditioned on compliance with the NSA. In this way, the government is able to tailor security requirements to specific network technologies on a case-by-case basis—requirements it could never impose or enforce by normal procedures. This paper will explore the network security review process—with its use of voluntary agreements and leveraging of interagency expertise—as a model of governance within regulated industries marked by rapidly changing technologies.