

My name is Alan Paller, and I am the director of research at the SANS Institute (a brief biography is at the end of this note). I am writing to illuminate the arguments for and against the proposal to extend outage reporting requirements to cover broadband Internet service providers, and to urge the FCC to act as quickly as possible to extend that reporting.

This comment is written from the perspective of the SANS Institute, the largest cyber security school in the world, with more than 140,000 alumni in 70 countries. We are a licensed graduate degree granting institution as well as an immersion training organization. Our graduates are responsible for the confidentiality, integrity, and availability of information, computers, and networks in more than 22,000 organizations, including telecommunications and other critical infrastructure, hospitals, colleges, and government agencies ranging from the National Oceanic and Atmospheric Administration to the US Navy and the National Security Agency.

In drafting this comment, I have tried to encapsulate the interests of our alumni and their employers by answering the following question: What FCC action would help to substantially improve the reliability of the Internet that nearly every one of us relies on every day?

The easy answer is that the FCC staff must aggregate outage information on the broadband Internet in much the same way that they have done for landline communications. This action is imperative for three reasons:

1. Because the financial and human loss associated with major Internet disruptions are far greater than the cost or burden of reporting;
2. Because the landline outage reporting works; and
3. Because the landline reporting model applies well to the broadband Internet.

This response, however, does not fully take into account the opposing view that such reporting is unnecessary and ineffective. Those counterarguments contend that:

- The Internet was designed to withstand cable cuts and unplugged routers, so large-scale outages won't happen.
- Even if large-scale outages were to become a concern, the Internet is so different from landline communications that it would be nearly impossible to define an outage or loss of useful availability and Internet connectivity, and even harder to define reliable measures.
- The government's request for this information is unnecessary because, unlike in landline communications, the big Internet service providers are in constant communication with each other and already share the information needed to maintain reliable service. That sharing even encompasses large government network service providers.
- Because regulators do not run broadband networks and do not understand the business or the technology, their review of the data will do more harm than good.

It is difficult to prove that these counterarguments are completely incorrect. For example, even if one maintains that large-scale outages are possible, if that is true, why haven't we seen many such outages? And who among professionals in the field has not attended meetings with people with so little understanding of the technology of cyber security that they slow rather than advance the public interest?

Having acknowledged that, however, a closer look shows that these arguments are less science and more red herrings concocted by those who simply oppose regulation altogether, even though such regulation will help their employers and their employer's customers. In other words, while such counterarguments have their grains of truth, each in its own way is also misleading and none has sufficient merit to halt approval of the extension of the landline-reporting model to broadband Internet service providers.

Here are the counterarguments again and our reasons why they are unpersuasive:

- *The Internet was designed to withstand cable cuts and unplugged or flooded routers, so large-scale outages won't happen.*

Response: The Internet was also designed with the assumption that users are well behaved. Malicious groups are not just local problems. They can simultaneously target hundreds of thousands of links and routers and bring about major outages—as the banks in Estonia can testify. We need all the data we can assemble on small outages because attackers nearly always test their tools before they execute large-scale deployment. We can learn from the tests and put in place defenses that we would never have used had we not had broad outage reporting.

- *Even if large-scale outages were to become a concern, the Internet is so different from landline communications that it would be nearly impossible to define an outage or loss of useful availability and Internet connectivity, and even harder to define reliable measures.*

Response: While it is true that the Internet and landline communications are different, the Internet service providers need, and gather, directly relevant reliability performance metrics to manage their own organizations and to report to larger customers who have demanded quality service guarantees. Specifically, providers can easily report significant latency increases that last specific periods of time, significant packet loss, and the underlying events such as line outages and switch outages. Determining reasonable thresholds will be difficult, but a 30-day test of thresholds will provide reasonable data on which to choose final thresholds.

- *The government's request for this information is unnecessary because, unlike in landline communications, the big Internet service providers are in constant communication with each other and already share the information needed to maintain reliable service. The sharing even encompasses large government network service providers.*

Response: Unfortunately, although such sharing exists and has proven valuable in dealing with large-scale worms, the level of communication is not nearly as open nor as comprehensive as the Internet service provider lobbyists would have us believe. There is good communication among the technical experts when a major event is under way, but it is highly informal, and it is unreliable in the sense that job changes, busy schedules, the illness of an employee, and any number of other human factors result in such communication failing to cover substantial parts of the Internet. Moreover, the sharing often does not include company proprietary information that could be central to practice improvement. Pattern analysis over time is the exception, not the rule.

- *Because regulators do not run broadband networks and do not understand the business or the technology, their review of the data will do more harm than good.*

Response: Again, it is true that regulators are usually not technical experts, though exceptions can be found. However, they can and do bring in experts from industry and consulting firms, and their convening power ensures they can get the right people in the room.

The bottom line is that, given the increasing threat of cyber crime and the increasing power of botnets, the FCC must not delay any longer. **The FCC must act quickly to extend outage reporting to cover broadband Internet service providers.**

* * *

Biography

Alan Paller is founder and research director of the SANS Institute. He oversees the Internet Storm Center, an early warning system for the Internet; NewsBites, the semi-weekly security news summary that goes to 210,000 people; and annual publication of the “Seven Most Dangerous New Attack Vectors.” He also leads a global security innovation program that identifies people and practices that have made a measureable difference in cyber risk reduction, then disseminates those innovations so other security practitioners can take full advantage of them to improve security in their enterprises. He is one of the founders of the U.S. Cyber Challenge. Mr. Paller has testified many times before both the US Senate and House of Representatives. In 2000, President Bill Clinton appointed him to the President’s National Infrastructure Assurance Council. Under President George W. Bush, the US Office of Management and Budget and the Federal CIO Council awarded Mr. Paller the 2005 Azimuth Award. This lifetime achievement award recognizes outstanding service of a nongovernment person to improving federal information technology. In May 2010, the *Washington Post* named Mr. Paller as one of seven people as “worth knowing, or knowing about in cyber security.”

Mr. Paller has degrees are from Cornell University and the Massachusetts Institute of Technology.

