FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

November 16, 2009

The Honorable John D. Rockefeller
Chairman
Committee on Commerce, Science and Transportation
United States Senate
508 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Rockefeller:

Thank you for your letter regarding the cybersecurity preparedness of the Federal Communications Commission, and the effectiveness of the Commission's incident response capability. I concur with your view that this is an issue that requires constant vigilance.

As you know, on June 30, 2009, as one of my first actions as FCC Chairman, I directed the FCC's Public Safety and Homeland Security Bureau to conduct a 30-day, top-to-bottom review of the agency's state of readiness. This review included a thorough self-assessment of the Commission's ability to detect, respond to, and mitigate cyber attacks, both to the agency's own networks and IT systems, as well to the nation's communications infrastructure, which the Commission is statutorily bound to protect. Enclosed with this response is a copy of the report, which was released on September 8, 2009. The report addresses the issues raised in your letter. My response summarizes those portions of the report particularly relevant to the five questions that you ask in your letter.

1. What plans or procedures does the FCC have in place to respond to and mitigate cybersecurity incidents?

   With respect to its own network and IT systems, the Commission applies Department of Homeland Security (DHS) Computer Emergency Readiness Team (US-CERT) Concept of Operations (CONOPS) guidance for responding to potential cybersecurity incidents affecting FCC major application systems. The Commission's cybersecurity incident team monitors both United States government and open-source information technology security sources for potential threats that could introduce security risks to the Commission's computing environment. This situational awareness helps the team triage whether application system vulnerabilities can be exploited by potential threats. Furthermore, if a breach of personally identifiable information (PII) were to occur, the Senior Agency Official for Privacy (SAOP) will lead the Commission's response efforts to mitigate the situation. Finally, in cases involving law enforcement, the cybersecurity incident team coordinates cybersecurity incident responses with the Commission's Office of the Inspector General.

With respect to cyber security issues that occur in the public communications networks, the FCC is much more limited in its ability to detect, monitor, and analyze cyber attacks outside the FCC. The FCC currently has no mechanism to collect – on a mandatory basis – data on the functioning of IP-based networks to monitor, detect, and analyze cyber attacks. It relies instead on a variety of U.S. Government and open sources of data. With regard to mitigation, the FCC has a series of responses that it is prepared to provide to affected industry members. For example, the FCC may grant special temporary authorizations to reconstruct infrastructure or to operate in an alternative mode while infrastructure is being replaced. However, where an attack is purely cyber-based, such as denial of service (DoS) attacks or attacks on the Internet routing infrastructure, the FCC does not currently have procedures regarding response.

2. How often does the FCC test and exercise its emergency recovery and continuity of operations plans?

   The Commission follows Federal Continuity of Operations Directives that require key personnel to engage in at least one continuity of operations (COOP) exercise each year. In addition to an ongoing program of internal testing, the Commission has participated in at least one National Level Exercise each year since 2005 (e.g., TOPOFF3, Pinnacle, Forward Challenge, and Eagle Horizon). The Commission participates in CLASSIFIED exercise programs as well. The Commission's Information Technology Center also conducts periodic failover testing of mission essential capabilities from its headquarters location to its alternate COOP facility.

3. How often does the FCC probe its own systems for vulnerabilities in order to take corrective action before they can be exploited?

   The Commission implements a risk management approach for protecting its mission critical application systems that takes into consideration the threat, vulnerabilities, countermeasures required to mitigate those vulnerabilities, and impact from exploitation of those vulnerabilities.

   Following a forward looking, proactive, defense-in-depth philosophy the Commission performs continuous scanning for vulnerabilities of mission critical application systems. Using criteria developed by the National Institutes of Standards and Technology (NIST) as well as other sources, the Commission ranks its vulnerabilities and addresses those vulnerabilities through configuration management-based remediation.

4. Do contractors or service providers have the specific cybersecurity-related service level agreements that provide assurance that attackers cannot use them as backdoor points of entry?

The Commission integrates information technology security metrics in its performance-based contract vehicles to enforce cybersecurity protections for its mission critical information systems. In addition, interconnection security agreements and memoranda of understanding are used to formalize the Commission's service level agreements with Federal agencies and businesses with whom the Commission's systems interconnect.

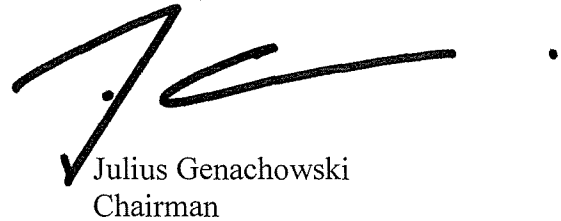
5. Does the FCC have the necessary resources (staff, expertise, or financial) to properly prepare for and effectively respond to major cybersecurity incidents?

As threats from cybersecurity increase, it will be important that Commission resources reflect needs in this area over time. The Commission currently is in the process of staffing a vacancy for its Chief Information Security Officer position. However, we continue to maintain our security focus through the efforts of existing staff and contract resources. Specifically, an independent contract team, under the direction of the Commission's Acting Chief Information Security Officer oversees compliance with Federal mandates, and establishes policy to reflect these mandates at the Commission level. A separate contract team is chartered with day-to-day enforcement of information technology security policy, network security operations, situational awareness, and incident prevention and response.

Where the public networks are concerned, the *30-Day Report* recommends that the FCC expand its cyber security expertise and cyber security role in general. We have created a new working group to help us make an informed determination of what the appropriate role for the Commission would be, and what resources the Commission would need to perform that role. This working group currently is reviewing the FCC's cyber security expertise and assets, identifying gaps and vulnerabilities, and assessing the Commission's needs and requirements for cyber security expertise. The working group will provide me with a report by the end of this year.

I appreciate your interest in these important matters. Please do not hesitate to contact me if you wish to discuss this response or if I can be of any further assistance.

Sincerely,



Julius Genachowski
Chairman

Enclosure