



OFFICE OF
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

July 29, 2014

The Honorable Mike Rogers
U.S. House of Representatives
2112 Rayburn House Office Building
Washington, D.C. 20515

Dear Representative Rogers:

Thank you for your leadership on cybersecurity issues and for sharing your views on the importance of communications security to our nation's broader security interests. I appreciate the opportunity to respond to your questions about the FCC's role in these matters.

First, I want to underscore the marketplace-driven and innovation-oriented core principles that drive our cybersecurity efforts at the FCC, particularly as "can't fail" public safety functions such as 911 and emergency alerting transition to Internet Protocol (IP)-based communications. These principles are fundamentally aligned with the views you expressed in your letter and, more generally, with the private sector-driven approach you have promoted on these issues.

Secure communications networks and the public safety functions that rely on them are crucial to our national security. As these networks transition to IP-based technologies, forward-looking market innovation driven by the business interests and expertise of the private sector is indispensable to their security and central to consumer and investor confidence in the communications market. This is the guiding principle of our cybersecurity efforts at the FCC, both in our work with providers to ensure the security of the core communications network infrastructure, and in our efforts to guarantee the integrity and reliability of crucial public safety functions such as 911 and emergency alerting. The strongest posture our nation can have is a capable private sector leading the development and implementation of effective, defensive cybersecurity measures.

In short, I agree with you, and I look forward to working with you to advance these principles in a dynamic, robust, and innovative communications sector. With this common ground in mind, please find below my responses to your specific questions about the FCC's role on these matters.

Upon what basis have you concluded that companies subject to the FCC's jurisdiction are not adequately protecting their networks from cyber attacks?

Unfortunately, we have unequivocal evidence that our communications networks are both the target of, and vulnerable to, cyber attacks. Specifically, in February 2013, an unidentified person gained unauthorized access through the Internet to Emergency Alert System (EAS)

equipment of several broadcast stations and sent an emergency message to the local public that “dead bodies are rising from their graves.” This “zombie alert” was recognized as a hoax that fortunately resulted in no harm to the public, but it reflected the poor readiness within some sectors of the communications industry and the direct linkage to public safety. Since this incident, we have been working with stakeholders in the EAS community to help them better protect their infrastructure from cyber threats.

This episode highlighted the vulnerabilities of public safety functions as our communications networks converge around IP-based communication infrastructure. Emergency alerting capabilities, 911, and other emergency and national security communications capabilities that increasingly ride over IP-based networks are reachable from anywhere on the globe. They are far more susceptible to distant cyber espionage or sabotage than were the locally-based, legacy communication systems of the past. We are working diligently with the stakeholders in the communications sector to ensure that today’s hoaxes and pranks do not become tomorrow’s public safety disasters.

I want to be clear, however, that I have *not* concluded that communications companies are universally unprepared to address cyber threats. Among communications sector companies, there is a wide range of cyber defense capabilities. Effective employment of cyber capabilities varies depending on a number of factors, including company size and scale, reliance on public-facing Internet infrastructure, experience with adversary exploitation attempts, and workforce training, among other factors. However, given the seriousness and sophistication of the threats that these networks face and the accelerating convergence of public safety communications around IP-based networks, I am extremely concerned that the relevant information is simply not yet available for the FCC – or any other entity – to have an informed understanding of the sufficiency of the protections that are in place. Developing a well-informed understanding of accepted cyber risks for our core networks is a threshold issue for our country’s national security interests and for the Commission’s execution of its statutory public safety responsibilities.

Addressing the present lack of situational awareness must begin at the company level, with the owners and operators of the networks. The companies that have built our communications networks must be able to measure cyber risk. If they cannot, and if our networks underpin virtually every critical infrastructure sector, then our communications networks and our national security are subject to uncertain and, I believe, unacceptable risk. That is why the FCC, as our nation’s expert agency regarding commercial communications networks, has challenged communications companies to act to measure and mitigate cyber risk. In doing so, these companies will not only be serving their own interests, but also addressing our broader national security concerns. They will meet this goal by doing what they do best: by rigorously analyzing their businesses’ exposure to specific risks and seeking opportunities for profit and return on investment in light of those identified risks. If they do that, they will have created a foundation for what I have called a “new regulatory paradigm” that is both more dynamic than reactive compliance with rules and more effective than blindly trusting the marketplace. Such an approach allows for responsible transparency and assurances regarding

companies' capabilities to manage risks and fulfills the FCC's statutory responsibility to ensure that the communications sector has an adequate public safety-related risk posture.

Tackling our nation's cybersecurity challenges will be a collaborative effort. We believe the companies that make up the communications sector recognize their special role and the value proposition in leading the way, and we look forward to continuing to work with these stakeholders, such as through the Communications Security, Reliability, and Interoperability Council (CSRIC), an industry-led FCC advisory group, which has a working group tasked with developing and recommending implementation details for the NIST Cybersecurity Framework in the communications sector.

What are the “other options” you are referring to when you state that you “will rely on industry and the market first while preserving other options if that approach is unsuccessful.”

We are asking private sector companies to establish an approach to cybersecurity in which they generate the sufficiency thresholds for their internal cybersecurity controls and then – as a substitute for traditional regulation – hold themselves accountable to their own internal controls. This approach would be the opposite of traditional, prescriptive, checklist-oriented regulation. We believe that CSRIC's efforts to implement the NIST Cybersecurity Framework will provide a constructive process in which the companies themselves voluntarily and proactively take real ownership of successful cyber risk management on their own and throughout the communications sector. And we are confident the communications sector will rise to meet this challenge so that prescriptive regulation is not necessary. It is in their core business interest to do so.

At this point, it would be premature to speculate on what other options might exist or might be needed, as neither the FCC nor the communications providers themselves have sufficient data or information on which to base such determinations. However, so long as I am Chairman, I will seek to lead the FCC's cybersecurity efforts based on the principle that cybersecurity must start with proactive, marketplace-driven risk management at the network operator level. Therefore, if the promising CSRIC approach does not advance to the extent that we all expect, the options that we will consider will be grounded in that same principle and based on the expertise and innovation of the network owners and operators themselves.

What would constitute a lack of success by the industry and the market that would trigger your pursuit of these “other options”?

We tasked CSRIC with establishing cybersecurity risk management processes to implement the NIST Cybersecurity Framework. Over 100 subject matter experts are working urgently to meet this challenge by March of 2015, the end of the term of the CSRIC. While we do not direct CSRIC's response to our questions, we are working in close constructive partnership on these issues, and we are all learning how best to work together to secure these

networks. Everyone involved in this effort is working toward the same goal: a business-driven approach to measuring, managing, and communicating cyber risk.

I do not wish to prejudge this important industry-led effort, and it would be premature to comment on where the effort may conclude. We all want this effort to succeed, and the FCC will work diligently with communications providers and other stakeholders to make it so.

How would prescriptive regulations enhance cybersecurity and encourage companies to create innovative cybersecurity strategies?

I completely agree with your assessment that “even well-meaning regulation cannot keep pace with evolving cyber threats.” Prescriptive regulation is not the best answer to our cybersecurity challenges. In my recent speech at the American Enterprise Institute calling on communications providers to create a “new paradigm” of proactive, measurable, accountable, market-driven cyber risk management, I put it this way: “The pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking.”

Do you believe the FCC has statutory authority to impose regulation related to cybersecurity practices? If so, what specific statutory provisions provide the FCC with such authority? Please explain.

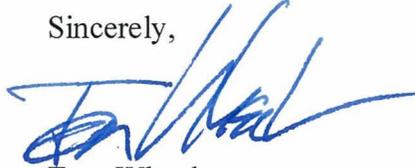
The FCC’s responsibility to promote public safety and network security is fundamental. This mandate is codified in the Communications Act, which states that the FCC was established for the purpose of, among other things, promoting the national defense and the safety of life and property. Congress wisely gave the FCC the agility to face new circumstances developing from the rapidly changing technical landscape such as those the communications sector is going through now in the transition to IP-based communications. The statute speaks in terms of effects, and this effects-based orientation, along with various statutory amendments since 1934, provides the FCC the necessary flexibility to fulfill our fundamental public safety and network security responsibilities even as communications technologies change.

In the years ahead, the FCC’s challenge will be to safeguard the national security and public safety effects mandate as the networks that enable those effects evolve. Further developments in the transition to IP-based networks, as well as additional information we gain from our experience of the CSRIC processes and other marketplace-driven initiatives, will further broadband deployment, technology transition, and inform us on both the challenges and opportunities ahead. My core belief is that the FCC cannot abdicate its statutory responsibilities for the communications sector simply because threats to national security and life and safety have begun to arrive via new communications technologies. The FCC has unique, indispensable expertise and responsibilities when it comes to communications security and reliability, and so long as I am Chairman, we will work diligently and strategically with all stakeholders to leverage that expertise and fulfill these responsibilities.

Page 5—The Honorable Mike Rogers

Thank you again reaching me on this important matter, which has benefitted greatly from your strong leadership. I look forward to working with you toward our mutual goal of protecting our nation's communications networks from the growing threats they face.

Sincerely,

A handwritten signature in blue ink, appearing to read "Tom Wheeler", with a long horizontal flourish extending to the right.

Tom Wheeler



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

July 29, 2014

The Honorable Mike Pompeo
U.S. House of Representatives
107 Cannon House Office Building
Washington, D.C. 20515

Dear Representative Pompeo:

Thank you for your leadership on cybersecurity issues and for sharing your views on the importance of communications security to our nation's broader security interests. I appreciate the opportunity to respond to your questions about the FCC's role in these matters.

First, I want to underscore the marketplace-driven and innovation-oriented core principles that drive our cybersecurity efforts at the FCC, particularly as "can't fail" public safety functions such as 911 and emergency alerting transition to Internet Protocol (IP)-based communications. These principles are fundamentally aligned with the views you expressed in your letter and, more generally, with the private sector-driven approach you have promoted on these issues.

Secure communications networks and the public safety functions that rely on them are crucial to our national security. As these networks transition to IP-based technologies, forward-looking market innovation driven by the business interests and expertise of the private sector is indispensable to their security and central to consumer and investor confidence in the communications market. This is the guiding principle of our cybersecurity efforts at the FCC, both in our work with providers to ensure the security of the core communications network infrastructure, and in our efforts to guarantee the integrity and reliability of crucial public safety functions such as 911 and emergency alerting. The strongest posture our nation can have is a capable private sector leading the development and implementation of effective, defensive cybersecurity measures.

In short, I agree with you, and I look forward to working with you to advance these principles in a dynamic, robust, and innovative communications sector. With this common ground in mind, please find below my responses to your specific questions about the FCC's role on these matters.

Upon what basis have you concluded that companies subject to the FCC's jurisdiction are not adequately protecting their networks from cyber attacks?

Unfortunately, we have unequivocal evidence that our communications networks are both the target of, and vulnerable to, cyber attacks. Specifically, in February 2013, an unidentified person gained unauthorized access through the Internet to Emergency Alert System (EAS)

equipment of several broadcast stations and sent an emergency message to the local public that “dead bodies are rising from their graves.” This “zombie alert” was recognized as a hoax that fortunately resulted in no harm to the public, but it reflected the poor readiness within some sectors of the communications industry and the direct linkage to public safety. Since this incident, we have been working with stakeholders in the EAS community to help them better protect their infrastructure from cyber threats.

This episode highlighted the vulnerabilities of public safety functions as our communications networks converge around IP-based communication infrastructure. Emergency alerting capabilities, 911, and other emergency and national security communications capabilities that increasingly ride over IP-based networks are reachable from anywhere on the globe. They are far more susceptible to distant cyber espionage or sabotage than were the locally-based, legacy communication systems of the past. We are working diligently with the stakeholders in the communications sector to ensure that today’s hoaxes and pranks do not become tomorrow’s public safety disasters.

I want to be clear, however, that I have *not* concluded that communications companies are universally unprepared to address cyber threats. Among communications sector companies, there is a wide range of cyber defense capabilities. Effective employment of cyber capabilities varies depending on a number of factors, including company size and scale, reliance on public-facing Internet infrastructure, experience with adversary exploitation attempts, and workforce training, among other factors. However, given the seriousness and sophistication of the threats that these networks face and the accelerating convergence of public safety communications around IP-based networks, I am extremely concerned that the relevant information is simply not yet available for the FCC – or any other entity – to have an informed understanding of the sufficiency of the protections that are in place. Developing a well-informed understanding of accepted cyber risks for our core networks is a threshold issue for our country’s national security interests and for the Commission’s execution of its statutory public safety responsibilities.

Addressing the present lack of situational awareness must begin at the company level, with the owners and operators of the networks. The companies that have built our communications networks must be able to measure cyber risk. If they cannot, and if our networks underpin virtually every critical infrastructure sector, then our communications networks and our national security are subject to uncertain and, I believe, unacceptable risk. That is why the FCC, as our nation’s expert agency regarding commercial communications networks, has challenged communications companies to act to measure and mitigate cyber risk. In doing so, these companies will not only be serving their own interests, but also addressing our broader national security concerns. They will meet this goal by doing what they do best: by rigorously analyzing their businesses’ exposure to specific risks and seeking opportunities for profit and return on investment in light of those identified risks. If they do that, they will have created a foundation for what I have called a “new regulatory paradigm” that is both more dynamic than reactive compliance with rules and more effective than blindly trusting the marketplace. Such an approach allows for responsible transparency and assurances regarding

companies' capabilities to manage risks and fulfills the FCC's statutory responsibility to ensure that the communications sector has an adequate public safety-related risk posture.

Tackling our nation's cybersecurity challenges will be a collaborative effort. We believe the companies that make up the communications sector recognize their special role and the value proposition in leading the way, and we look forward to continuing to work with these stakeholders, such as through the Communications Security, Reliability, and Interoperability Council (CSRIC), an industry-led FCC advisory group, which has a working group tasked with developing and recommending implementation details for the NIST Cybersecurity Framework in the communications sector.

What are the “other options” you are referring to when you state that you “will rely on industry and the market first while preserving other options if that approach is unsuccessful.”

We are asking private sector companies to establish an approach to cybersecurity in which they generate the sufficiency thresholds for their internal cybersecurity controls and then – as a substitute for traditional regulation – hold themselves accountable to their own internal controls. This approach would be the opposite of traditional, prescriptive, checklist-oriented regulation. We believe that CSRIC's efforts to implement the NIST Cybersecurity Framework will provide a constructive process in which the companies themselves voluntarily and proactively take real ownership of successful cyber risk management on their own and throughout the communications sector. And we are confident the communications sector will rise to meet this challenge so that prescriptive regulation is not necessary. It is in their core business interest to do so.

At this point, it would be premature to speculate on what other options might exist or might be needed, as neither the FCC nor the communications providers themselves have sufficient data or information on which to base such determinations. However, so long as I am Chairman, I will seek to lead the FCC's cybersecurity efforts based on the principle that cybersecurity must start with proactive, marketplace-driven risk management at the network operator level. Therefore, if the promising CSRIC approach does not advance to the extent that we all expect, the options that we will consider will be grounded in that same principle and based on the expertise and innovation of the network owners and operators themselves.

What would constitute a lack of success by the industry and the market that would trigger your pursuit of these “other options”?

We tasked CSRIC with establishing cybersecurity risk management processes to implement the NIST Cybersecurity Framework. Over 100 subject matter experts are working urgently to meet this challenge by March of 2015, the end of the term of the CSRIC. While we do not direct CSRIC's response to our questions, we are working in close constructive partnership on these issues, and we are all learning how best to work together to secure these

networks. Everyone involved in this effort is working toward the same goal: a business-driven approach to measuring, managing, and communicating cyber risk.

I do not wish to prejudge this important industry-led effort, and it would be premature to comment on where the effort may conclude. We all want this effort to succeed, and the FCC will work diligently with communications providers and other stakeholders to make it so.

How would prescriptive regulations enhance cybersecurity and encourage companies to create innovative cybersecurity strategies?

I completely agree with your assessment that “even well-meaning regulation cannot keep pace with evolving cyber threats.” Prescriptive regulation is not the best answer to our cybersecurity challenges. In my recent speech at the American Enterprise Institute calling on communications providers to create a “new paradigm” of proactive, measurable, accountable, market-driven cyber risk management, I put it this way: “The pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking.”

Do you believe the FCC has statutory authority to impose regulation related to cybersecurity practices? If so, what specific statutory provisions provide the FCC with such authority? Please explain.

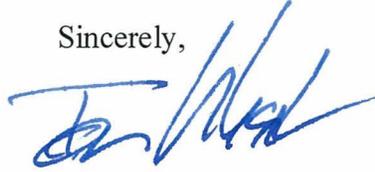
The FCC’s responsibility to promote public safety and network security is fundamental. This mandate is codified in the Communications Act, which states that the FCC was established for the purpose of, among other things, promoting the national defense and the safety of life and property. Congress wisely gave the FCC the agility to face new circumstances developing from the rapidly changing technical landscape such as those the communications sector is going through now in the transition to IP-based communications. The statute speaks in terms of effects, and this effects-based orientation, along with various statutory amendments since 1934, provides the FCC the necessary flexibility to fulfill our fundamental public safety and network security responsibilities even as communications technologies change.

In the years ahead, the FCC’s challenge will be to safeguard the national security and public safety effects mandate as the networks that enable those effects evolve. Further developments in the transition to IP-based networks, as well as additional information we gain from our experience of the CSRIC processes and other marketplace-driven initiatives, will further broadband deployment, technology transition, and inform us on both the challenges and opportunities ahead. My core belief is that the FCC cannot abdicate its statutory responsibilities for the communications sector simply because threats to national security and life and safety have begun to arrive via new communications technologies. The FCC has unique, indispensable expertise and responsibilities when it comes to communications security and reliability, and so long as I am Chairman, we will work diligently and strategically with all stakeholders to leverage that expertise and fulfill these responsibilities.

Page 5—The Honorable Mike Pompeo

Thank you again reaching me on this important matter, which has benefitted greatly from your strong leadership. I look forward to working with you toward our mutual goal of protecting our nation's communications networks from the growing threats they face.

Sincerely,

A handwritten signature in blue ink, appearing to read "Tom Wheeler", with a stylized flourish extending to the right.

Tom Wheeler