

This is a preliminary transcript of a Committee hearing. It has not yet been subject to a review process to ensure that the statements within are appropriately attributed to the witness or member of Congress who made them, to determine whether there are any inconsistencies between the statement within and what was actually said at the proceeding, or to make any other corrections to ensure the accuracy of the record.

1 {York Stenographic Services, Inc.}

2 RPTS MEYERS

3 HIF067.160

4 CYBERSECURITY: THE PIVOTAL ROLE OF COMMUNICATIONS NETWORKS

5 WEDNESDAY, MARCH 7, 2012

6 House of Representatives,

7 Subcommittee on Communications and Technology

8 Committee on Energy and Commerce

9 Washington, D.C.

10 The Subcommittee met, pursuant to call, at 10:04 a.m.,
11 in Room 2123 of the Rayburn House Office Building, Hon. Greg
12 Walden [Chairman of the Subcommittee] presiding.

13 Members present: Representatives Walden, Terry,
14 Stearns, Shimkus, Bono Mack, Rogers, Blackburn, Bilbray,
15 Bass, Gingrey, Scalise, Latta, Guthrie, Kinzinger, Eshoo,
16 Doyle, Matsui, Barrow, Christensen, DeGette, Dingell and
17 Waxman (ex officio).

18 Staff present: Ray Baum, Senior Policy Advisor/Director

19 of Coalitions; Nicholas Degani, FCC Detailee; Neil Fried,
20 Chief Counsel, Communications and Technology; Debbie Keller,
21 Press Secretary; Katie Novaria, Legislative Clerk; Andrew
22 Powaleny, Deputy Press Secretary; David Redl, Counsel,
23 Telecom; Roger Sherman, Democratic Chief Counsel,
24 Communications and Technology; Jeff Cohen, FCC Detailee;
25 Shawn Chang, Democratic Senior Counsel; Hadass Kogan, Legal
26 Fellow; and Kara van Stralen, Democratic Special Assistant.

|
27 Mr. {Walden.} We will call to order the Subcommittee on
28 Communications and Technology for a hearing on
29 ``Cybersecurity: the Pivotal Role of Communications
30 Networks.'' I want to thank our witnesses for being here
31 this morning. We look forward to your testimony and are very
32 appreciative of your taking the time to be here to help
33 educate us so we can do the right thing in terms of assisting
34 you all, particularly the security networks or the cyber
35 networks.

36 Back in October, the House Republican Cybersecurity Task
37 Force appointed by the Speaker recommended that the
38 committees of jurisdiction review cybersecurity issues. This
39 Subcommittee has embarked on a series of hearings to heed
40 that call and to get a complete picture of the cybersecurity
41 challenges that our Nation faces.

42 In our February 8 hearing, we examined threats to
43 communications networks and the concerns of the private
44 sector security firms helping to secure those communications
45 networks. That hearing provided us with valuable information
46 and even some potential solutions.

47 This hearing continues our Subcommittee's review of
48 cybersecurity issues with a focus on the steps that network
49 operators have taken to secure their networks and any

50 recommendations that you all might have on how Congress can
51 help, actually help in those efforts.

52 As we heard in the February 8 hearing, threats to
53 communications networks have come a long way in a very short
54 period of time. Before coming to Congress, I spent 22 years
55 as a radio broadcaster, and as a small businessperson, I had
56 to worry about securing our own communications network, but
57 those were simpler times. In modern communications networks
58 of all types, cybersecurity has become a pressing concern.
59 In our February 8 hearing, we had a dizzying array of new
60 cybersecurity threats discussed like supply chain
61 vulnerabilities, botnets and Domain Name System spoofing.

62 On the brighter side, we were also told during that
63 hearing about several potential solutions to make
64 communications networks more secure. This is why I have
65 asked a number of my colleagues to serve as the
66 Communications and Technology Cybersecurity Working Group.
67 The working group is a bipartisan team of six subcommittee
68 members, led by Subcommittee Vice Chair Lee Terry and
69 Subcommittee Ranking Member Anna Eshoo, that will look into
70 some of these potential solutions and the legal and
71 regulatory impediments to securing communications networks
72 against cyber threats. With an eye toward incentive-based
73 approaches, the working group looks to facilitate

74 communication among private sector companies and the public
75 sector on a variety of topics, including DNSSEC adoption,
76 supply chain risk management, and a voluntary code of conduct
77 and best practices for network operators.

78 Now, in this hearing, we are privileged to have five
79 witnesses that represent parts of the commercial network to
80 guide us through the complex cybersecurity issues that you
81 each face. Network operators own, maintain and operate most
82 of the infrastructure that makes up our communications
83 networks. Their management of the wires, the towers, the
84 base stations, the servers and the wireless handsets that are
85 integral parts of communications networks put these companies
86 on the front lines of cybersecurity. I want to know what
87 cybersecurity services and educational initiatives are being
88 aimed at your consumers, what steps are being taken to secure
89 the core components that make up our communications networks,
90 and what affirmative steps network operators have taken to
91 secure the supply chain and to prevent cyber attacks.

92 I would also expect to hear what you think the
93 appropriate role of the Federal Government is to combat cyber
94 threats. Are federal laws and regulations helping or
95 hindering information sharing? Are there cybersecurity
96 solutions that your company has identified that would prevent
97 cyber attacks, but would run afoul of existing laws? How can

98 the Federal Government incent network operators and other
99 members of the private sector to invest and innovate in the
100 cybersecurity arena? And coming off of our prior hearing on
101 February 8, how do we make sure that we don't put things in
102 statute that cause misallocation of your capital and make you
103 less nimble in this extraordinary cyber threat environment.
104 So I look forward to your testimony today.

105 [The prepared statement of Mr. Walden follows:]

106 ***** COMMITTEE INSERT *****

|
107 Mr. {Walden.} I would yield time to Ms. Blackburn.

108 Mrs. {Blackburn.} Thank you, Mr. Chairman. Welcome to
109 all of you, and we are deeply appreciative of your time for
110 being here.

111 I think one of the things that--

112 Mr. {Walden.} Could you get a little closer to your
113 microphone?

114 Mrs. {Blackburn.} I certainly can. I am a mother. I
115 can always talk louder. That is right.

116 The GAO report that mentioned we have seen a 650 percent
117 growth in cyber attacks over the past 5 years, I think that
118 that caused a lot of people to, you know, sit up and take
119 note of what might be happening out there, because you look
120 at the attacks, you look at what that equates to an effect on
121 the economy. Chairman Bono Mack and I are working on
122 introducing a bill, the cybersecurity bill here in the House,
123 similar to secure IT from the Senate, and I think the
124 concepts we are viewing are not to be overly prescriptive and
125 to kind of work off the first principle of ``do no harm'' and
126 have a good, broad conversation in this. I would love to
127 hear you all talk a little bit about government networks and
128 the importance you think and responsibility you think
129 government has in securing its own networks and system. I

130 would love to also hear a little bit from you about
131 incentive-based security and how we approach that.

132 With that, I yield back.

133 [The prepared statement of Mrs. Blackburn follows:]

134 ***** COMMITTEE INSERT *****

|
135 Mr. {Walden.} I thank the gentlelady for her comments
136 and now recognize my friend from California, Ms. Eshoo, for
137 an opening statement.

138 Ms. {Eshoo.} Thank you, Mr. Chairman, and welcome to
139 all of the witnesses and thank you for being here today.

140 As the title of today's hearing suggests, our
141 communications networks are part of the backbone of our
142 Nation's critical infrastructure. From electricity
143 generation to financial service and transportation, we depend
144 on our communications networks for nearly all aspects of our
145 daily lives. Yet as was highlighted during our first
146 cybersecurity hearing, our networks remain vulnerable to
147 attack.

148 In particular, there are three areas I would like to
149 hear more about from our witnesses today. First, as we
150 discussed in last month's hearing, the FCC chairman is
151 currently proposing a voluntary ISP code of conduct as a way
152 to alert consumers when a botnet or other malware infection
153 is discovered. So today's witnesses will be on the front
154 line in ensuring such best practices are effectively
155 implemented and obviously I think that you are going to talk
156 about that, and I look forward to it.

157 Second, I would like to hear more about your views on

158 the supply chain security. I continue to have really grave
159 concerns stemming from my 8 years that I just recently
160 completed at the House Intelligence Committee about the
161 implications of foreign-controlled telecommunications
162 infrastructure companies providing equipment to the U.S.
163 market. In 2010, I wrote to the FCC chairman asking for a
164 better understanding of the FCC's authority to address these
165 challenges and what kind of transparency requirements should
166 be placed on companies seeking to sell telecommunications
167 infrastructure equipment to U.S. network providers.

168 Third, I would like to learn more about any unique
169 challenges in securing mobile networks. As more data is
170 transmitted wirelessly, we need to look closely at how these
171 networks are secured to ensure they don't become the entryway
172 to the broader network.

173 So today's hearing is an important aspect of our
174 Subcommittee's work on cybersecurity. Again, I want to thank
175 each one of our witnesses for being willing to testify today
176 to be instructive to us, and I want to thank the chairman for
177 the spirit of cooperation around this issue. Usually there
178 are some Democratic witnesses that are called and Republican
179 witnesses. That is not the case today. So this is something
180 that rises above that, and I look forward to working with the
181 entire Committee so that we not only better understand the

182 cybersecurity challenges facing communications networks but
183 what steps we can take to secure them and thereby strengthen
184 the country.

185 [The prepared statement of Ms. Eshoo follows:]

186 ***** COMMITTEE INSERT *****

|
187 Ms. {Eshoo.} I would like to yield my remaining time to
188 Representative Matsui.

189 Ms. {Matsui.} Thank you, Ranking Member Eshoo, for
190 yielding me time. Mr. Chairman, thank you for holding
191 today's hearing, and I want to thank the witnesses for being
192 here today.

193 There is no doubt that cyber attacks are real and
194 continue to pose significant threats to several aspects of
195 our economy, and Mr. Chairman, I am pleased that you and
196 Ranking Member Eshoo formed a bipartisan cyber working group
197 so that we can appropriately explore our Subcommittee's
198 interest to enhance our Nation's efforts against a cyber
199 attack.

200 There are a variety of issues that we may explore.
201 Communications networks are one of the many areas that our
202 Nation must protect and ensure safety and soundness.
203 Advancing IP-based technologies and public safety
204 communications heighten the concerns for cybersecurity. It
205 would be important that data is protected from a PC or a cell
206 phone in transit to cloud storage, particularly as more and
207 more Americans send personal information to the cloud.

208 I also believe that our Subcommittee will have the
209 ability to further promote information sharing on cyber

210 threats. Securing the supply chain will be of high
211 importance so that tech components remain secure through
212 their manufacturing and distribution processes. Among
213 others, I believe that R&D incentives could encourage
214 industry to explore ways to better address and defend against
215 malware and botnets.

216 Again, I thank the Chairman for holding today's hearing.
217 I look forward to working with my colleagues on ways that
218 this Subcommittee can encourage greater protection against
219 cyber threats. I thank the witnesses for appearing today.

220 I yield back the remainder of my time.

221 [The prepared statement of Ms. Matsui follows:]

222 ***** COMMITTEE INSERT *****

|
223 Mr. {Walden.} I thank the gentlelady for her comments.

224 I will now recognize the Vice Chairman of the Committee,
225 Mr. Terry, for opening comments.

226 Mr. {Terry.} Thank you, Chairman, and let me start by
227 saying that I believe that most of my colleagues on this
228 Committee share my optimism that a collaborative, active
229 cyber defense capability is actually achievable. There might
230 be a few differences in opinion on what needs to be done to
231 reach this goal, but through the bipartisan conversations
232 like those taking place in the working group and public
233 hearings like this, we are getting closer.

234 In reading through the written testimony provided by
235 today's witnesses, I noticed a common threat throughout. As
236 Mr. Amoroso eloquently says, ``Quite simply, innovation is
237 inconsistent with standardization.'' I agree wholeheartedly
238 with our witness, and in my opinion, I find this to be the
239 most vital guiding principle in considering how to enhance
240 our Nation's cybersecurity. In fact, as I continue to dig
241 deeper on this issue, I become more convinced that any sort
242 of legislative effort to provide overbroad regulation or
243 certification regimes will surely come with unintended
244 consequences. Instead, ISPs should have the flexibility to
245 respond to real-time security threats in a manner that

246 minimizes delay and maximizes their ability to innovate as
247 they strive to protect their consumers and their network.

248 A couple of things I believe that we can do to help
249 reach the goal of collaborative active cyber defense
250 capability are, one, remove the current barriers in place
251 that prevent communication networks from sharing cyber
252 threat information with the government agencies and also with
253 the private sector entities. Provide adequate liability
254 protection in order for the sharing of cyber threat
255 information is second.

256 Again, I thank our witnesses for joining us today, and
257 shall I yield to Mr. Stearns?

258 [The prepared statement of Mr. Terry follows:]

259 ***** COMMITTEE INSERT *****

|
260 Mr. {Stearns.} I thank my colleague.

261 My colleagues, I think the consistent message from our
262 witnesses today is that the private sector has very strong
263 commercial incentives to invest in and maintain robust
264 cybersecurity. In fact, each of our witnesses today has
265 described unique and thorough approaches to protecting their
266 own networks. These examples demonstrate that one-size-fits-
267 all legislation is not the appropriate solution to
268 cybersecurity threats. Moreover, because these threats
269 change every day, industry must be provided the flexibility
270 to respond quickly to an attack.

271 Therefore, I believe that prescriptive top-down
272 government mandates are not only unnecessary but they simply
273 will not work. Instead, government should seek to improve
274 information sharing and consumer education. We also should
275 work to eliminate outdated regulations that have created
276 unintentional barriers toward ensuring the security of our
277 networks.

278 So I look forward to our witnesses today and I thank
279 you, Mr. Chairman, for this great hearing.

280 [The prepared statement of Mr. Stearns follows:]

281 ***** COMMITTEE INSERT *****

|
282 Mr. {Walden.} Are there any other member seeking time
283 on our side? If not, the gentleman yields back his time and
284 I recognized the gentleman from California, Mr. Waxman, for
285 an opening statement.

286 Mr. {Waxman.} Thank you very much, Mr. Chairman, and I
287 welcome our witnesses as well.

288 I am pleased that that the Subcommittee is looking at
289 this issue of cybersecurity. This is our second hearing.
290 Every week we learn of a new cyber breach or vulnerability,
291 so it is vital that we are paying attention to this question.

292 Like the smart grid, which was the topic of our last
293 hearing by the Subcommittee on Oversight and Investigations,
294 communications networks are highly vulnerable to cyber
295 attack. The potential for severe disruptions are high
296 because communications networks are the common thread to all
297 critical infrastructure sectors.

298 In fact, the public safety legislation that was just
299 signed into law exemplifies these concerns. Under the new
300 law, first responders will be relying on broadband
301 communications networks to secure the safety of life and
302 property. That will strengthen their ability to protect the
303 public, but only if the networks are protected from cyber
304 attacks.

305 Today, I look forward to continuing our discussion of
306 the security threats faced by mobile devices and the proper
307 role for this Subcommittee in ensuring cybersecurity. Our
308 witnesses today represent a broad cross-section of Internet
309 service providers, as well as a handset manufacturer. This
310 should further help our understanding of what risks threaten
311 communications networks, what companies are doing to mitigate
312 these risks, and what the subcommittee might do to assist you
313 in these efforts.

314 I believe the Federal Government has an important role
315 to play in ensuring the cybersecurity of the Nation's
316 communications networks. One important federal role is
317 developing practices that will keep the Internet safe. The
318 FCC's upcoming release of its cyber best practices report,
319 developed by the well-regarded Communications Security,
320 Reliability and Interoperability Council, such a long name
321 that is reduced to CSRIC, will provide valuable guidance to
322 industry and our Subcommittee.

323 I understand the Chairman is planning a third hearing
324 with government agencies. I commend him for this series of
325 hearings and look forward to what our witnesses have to tell
326 us.

327 And finally, I want to join in thanking you, Mr.
328 Chairman, for organizing a bipartisan working group to study

329 cyber threats and inform the Subcommittee of its findings.
330 This is a good opportunity for Subcommittee members and staff
331 to work together on an issue of common concern. I look
332 forward to hearing back from the working group and exploring
333 with the subcommittee potential further actions.

334 Thank you for the hearing. I thank all the witnesses
335 for being here. I look forward to the testimony. Yield
336 back.

337 [The prepared statement of Mr. Waxman follows:]

338 ***** COMMITTEE INSERT *****

|
339 Mr. {Walden.} The gentleman yields back his time. I
340 thank you for your comments. We have a lot of big brains on
341 this Committee and we are going to need them all to protect
342 America, so thank you to the members who have agreed to serve
343 on that working group.

344 Gentlemen, we are delighted to have you here today. We
345 will start with Mr. Livingood. We appreciate your being
346 here, Vice President, Internet Systems Engineering from
347 Comcast Corporation. Thank you for being here. Just a
348 friendly reminder, being an old radio guy, pull these
349 microphones very close and make sure the button is lit and
350 you will be good to go.

|
351 ^STATEMENTS OF JASON LIVINGOOD, VICE PRESIDENT, INTERNET
352 SYSTEMS ENGINEERING, COMCAST CORPORATION; EDWARD AMOROSO,
353 CHIEF SECURITY OFFICER, AT&T SERVICES, INC.; DAVID MAHON,
354 CHIEF SECURITY OFFICER, CENTURYLINK; JOHN OLSEN, SENIOR VICE
355 PRESIDENT AND CHIEF SECURITY OFFICER, METROPCS COMMUNICATIONS
356 INC.; AND SCOTT TOTZKE, SENIOR VICE PRESIDENT, BLACKBERRY
357 SECURITY GROUP, RESEARCH IN MOTION

|
358 ^STATEMENT OF JASON LIVINGOOD

359 } Mr. {Livingood.} Okay. Thank you very much, Mr.
360 Chairman, Ranking Member Eshoo and members of the
361 Subcommittee for inviting me to discuss some of the work that
362 Comcast is doing to protect consumers and cyberspace. We
363 appreciate the Subcommittee's interest in this issue and its
364 willingness to hear the perspective of someone like me, an
365 engineer working in cybersecurity and other technical
366 Internet issues every day.

367 I serve as Vice President of Internet Systems
368 Engineering at Comcast, and I am the Engineering Leader in
369 charge of our residential high-speed Internet service. I
370 currently serve on an FCC CSRIC working group, on ICANN's
371 Security and Stability Advisory Committee, on the Broadband

372 Internet Technical Advisory Group, and am a member of the
373 board of trustees of the Internet Society. I am also an
374 active contributor of the Internet Engineering Task Force, or
375 IETF.

376 At Comcast, we take cybersecurity issues seriously, and
377 we know that our customers are very concerned about security.
378 We strive to provide them with the best, fastest and most
379 secure Internet service possible, and our engineering team
380 devotes significant time, energy and investment to constantly
381 update and refine our cybersecurity efforts.

382 One such threat that we focused on comes from malicious
383 software called a bot. Bots run on an end user's computer
384 without their knowledge and are controlled remotely. Bots
385 are used to conduct identity and credit card theft, denial of
386 service attacks, steal user names and passwords, and send
387 spam. It is important to understand that a person need not
388 consciously do something like downloading an app to become
389 infected. Sometimes they can be infected just by visiting a
390 website.

391 To counter bots, we developed a system called Constant
392 Guard. This customer-facing system first detects botnet
393 traffic, notifies end users of infection such as sending them
394 alerts in their web browser, and provides them with tools to
395 remove those infections.

396 Another area of threat is to the Domain Name System,
397 which is a foundational and extraordinarily important and
398 critical part of the Internet. The Domain Name System, or
399 DNS for short, is responsible for basically translating names
400 like Comcast.com into IP addresses, which are the addresses
401 used to connect and route traffic across the Internet. So it
402 is extremely important. But a vulnerability in the DNS can
403 permit an attacker to inject a fake answer into the DNS. An
404 attacker, for example, can then direct traffic destined to a
405 site such as a banking website to computers that they
406 control, perhaps to collect login and financial information,
407 but the address in the user's web browser still appears
408 correct.

409 The long-term fix is to implement DNS security
410 extensions, or DNSSEC for short. This involves someone doing
411 two things. First, cryptographically signing the domain
412 names that they own and then Internet service providers
413 validating those signatures before connecting a user to that
414 site. This is basically akin to your bank keeping your
415 signature on file and checking the signature on your check
416 against that before cashing your check.

417 It is important to note that DNSSEC was developed via an
418 international multi-stakeholder process at the IETF and will
419 require adoption across the entire ecosystem such as by

420 banks, web browsers, software companies and cloud services,
421 not just ISPs. I am pleased to report as part of Constant
422 Guard, Comcast was the first ISP in the United States to
423 fully deploy DNSSEC in January.

424 But it is important to understand that no open and
425 massively interconnected network can ever be completely and
426 totally secure. While there is no perfect solution to
427 security, that does not mean that there are no good
428 solutions, so our focus has been quite simply to roll up our
429 sleeves and get to work chipping away at the security threats
430 day in and day out, quickly learning and adapting. We are
431 working within the industry and on a global basis to combat
432 the key threats and to protect our customers the best that we
433 can and also to help them protect themselves. There are
434 powerful incentives to take strong and effective measures to
435 ensure network security and safety. Our consumers want
436 assurance that the networks that they are using are safe and
437 secure, and we have strong reasons therefore to invest
438 capital and resources into cybersecurity safeguards. The
439 same is of course true for other network providers. We all
440 have powerful incentives to take actions necessary to secure
441 our substantial investments in our networks.

442 Policymakers can help these efforts by removing legal
443 uncertainties that can inhibit collaboration while preserving

444 and strengthening this flexibility that providers have to
445 develop the best solutions for each of our networks. As one
446 of the members said a moment ago, there is no one-size-fits-
447 all solution, so flexibility is key, and it is important
448 because the threats change as rapidly as they do.

449 Flexibility will help to ensure that we can continue to focus
450 on security and innovation rather than compliance and
451 regulation.

452 Thank you.

453 [The prepared statement of Mr. Livingood follows:]

454 ***** INSERT 1 *****

|
455 Mr. {Walden.} Thank you, sir. We appreciate your
456 comments and we will back to you with some questions on the
457 specifics of what those uncertainties are in the law.

458 We now are delighted to have Dr. Edward Amoroso with us.
459 He is the Chief Security Officer for AT&T Services, Inc.
460 Doctor, we are glad to have you here. We look forward to
461 your comments.

|
462 ^STATEMENT OF EDWARD AMOROSO

463 } Mr. {Amoroso.} Great. Thanks. Hi, everybody. I am Ed
464 Amoroso. I have spent my entire adult life in cybersecurity.
465 In fact, even as a teenager, my dad was a computer scientist
466 so I was logging onto ARPAnet when I was a little kid. So I
467 have been in and around this forever. I started work at Bell
468 Laboratories and found that I was actually a pretty good
469 hacker, and have been doing ever since and now I am the Chief
470 Security Officer, so I kind of come at this with very
471 practical perspective on threat.

472 There are three things I want to share with you that I
473 think are observations that might help you as you develop
474 legislation, and they are based on empirical day-to-day, you
475 know, dealings with security issues with our mobility network
476 and our wireline network and the entire Fortune 1000 and lots
477 of different countries we deal with, so I do that all day
478 long and I wanted to share.

479 And the first one is about innovation. We are being
480 out-innovated by our adversaries is basically the case. I
481 mean, I don't know if you have ever bought a piece of
482 furniture and taken it home and admired the handiwork in the
483 future. That is what we do with malware that is being

484 developed by adversaries. It is so good and so well crafted
485 that we marvel at how far the adversary has come. These are
486 not script kiddies doing dopey things. And these are pretty
487 good. I don't know if any of you watch 60 Minutes, if you
488 saw the Stuxnet piece. That is an incredible piece of
489 computer science, that worm. So I think we need to recognize
490 that whatever we do collectively as a Nation, we need to
491 figure out a way to incent companies and universities and
492 government agencies to innovate in this area. If we don't,
493 we are going to be in trouble because I will tell you, and I
494 bet everybody on the panel here would agree with me, the best
495 state-of-the-art security protections that any one of us can
496 put in place will not stop a determined adversary in 2012.
497 That is a fact, so we need to do something to get ahead of
498 that, and the way you do something is, you innovate. We need
499 to do something to get ahead of it, and part of the problem
500 with sort of prescribing an answer to everyone, hey, we are
501 all going to do the following, is it would be like every NBA
502 team publishing their defense and saying this is what we are
503 going to do. Guess what? You think the adversaries don't
504 read your legislation? You think they don't look and see
505 what we are all going to do? I mean, you lay it out and you
506 say okay, I will step around these things that you are doing.
507 I mean, that is just a practical issue in cybersecurity.

508 This is not, you know, the kind of thing where, you know, we
509 can all kind of do commonsense stuff and it will fix it.
510 There is a million things in our lives where if we all go
511 back to the basics and do a set of commonsense things that
512 will make things better. We all live our lives that way.
513 Cybersecurity doesn't work that way. We are dealing with an
514 adversary. So the first issue is innovation.

515 The second is infrastructure, and I think everybody also
516 at this table would agree that complexity in infrastructure
517 is the biggest problem for cybersecurity. When things get
518 way to complicated, we can't keep track of it. It becomes
519 almost impossible to protect something that has become so big
520 and complicated that you can't get your arms around it, and
521 part of the problem with things like DNSSEC and others, which
522 clearly have benefit--I mean, I certainly agree with a lot of
523 the points that were made--but they add complexity. Like the
524 way to think of DNSSEC is, you know when you do a commercial
525 and at the end you say I am such-and-such and I approved this
526 commercial, that is DNSSEC. I mean, it is essentially the
527 server attesting to the fact that here is a signature that I
528 am who I am, but if somebody is breaking in to and owns that
529 server, the signature is meaningless. It doesn't do any
530 good. And I would say empirically, I see a lot more break-
531 ins to DNS servers than forged, you know, different types of

532 protocol responses and so on. So I think what we need to
533 keep in mind as we develop legislation that when we add
534 complexity, when you add things that we need to keep track
535 of, do this, do that, overlay this, add this new thing, add
536 that new thing, the complexity can be very stifling. You
537 know when DNSSEC was first proposed? Decades ago. Right.
538 This is not something that was dreamed up last week. We have
539 been working on adding cryptography to Internet protocols
540 forever, and the reason we don't have them today is because
541 they are unbelievably complicated to run. They do add some
542 benefit but they have side effects. It would be like
543 bringing a senior citizen to the doctor with five ailments
544 and the doctor says well, I am going to give you medicine for
545 one of them but it has side effects. That is DNSSEC. It
546 does have benefit, it has side effects, it doesn't fix
547 everything, so that is the second.

548 The third and last issue I want to raise is software.
549 At the root of every cyber attack, every problem I have ever
550 dealt with in my entire career is bad software, and I think
551 that it needs to be addressed. The discipline of software
552 engineering, the profession of writing software is one that
553 is a complete mess right now. And I am a professor at the
554 Stevens Institute of Technology. I have been teaching in the
555 computer science department there for 22 years. I teach

556 software engineering, teach computer security, that kind of
557 thing, so maybe blame me, but the bottom line is that
558 youngsters and even professionals today cannot write a non-
559 trivial piece of software that is bug-free and those bugs are
560 the way our adversaries get into our companies. We open up
561 websites because we have no choice. Are we going to close
562 the website down? It is there and the software powering that
563 has vulnerabilities we don't know about. I bought it, I
564 install it, I test it, everything is great, but some
565 adversary finds an open door that I don't know about, that
566 the manufacturer doesn't know about, and they dance right in.
567 Bad software is a fundamental problem here, and I think it
568 needs to be addressed, probably through the educational
569 system. Thanks.

570 [The prepared statement of Mr. Amoroso follows:]

571 ***** INSERT 2 *****

|
572 Mr. {Walden.} Thank you. We appreciate your comments
573 and we will back to you with questions as well.

574 Now we are joined by Mr. David Mahon, Chief Security
575 Officer for CenturyLink. Thank you for being here. We look
576 forward to your comments.

|
577 ^STATEMENT OF DAVID MAHON

578 } Mr. {Mahon.} Chairman Walden, Ranking Member Eshoo and
579 members of the Subcommittee, thank you for the opportunity to
580 testify on this important topic.

581 CenturyLink, a tier one backbone provider, provides
582 communication services to over--

583 Mr. {Walden.} We are having trouble hearing you. Is
584 that light lit up there, and you really have to get really
585 close.

586 Mr. {Mahon.} Chairman Walden, Ranking Member Eshoo and
587 members of the Subcommittee, thank you for the opportunity to
588 testify today on this important topic.

589 CenturyLink, a tier one backbone provider, provides
590 communication services to over 14 million homes and
591 businesses in more than 37 States and around the world. Our
592 services include voice, broadband, video entertainment and
593 data, as well as fiber backhaul, cloud computing and managed
594 security solutions. Our customers range from the most basic
595 voice and Internet customers to the largest Fortune 500
596 companies and large government agencies. As Vice President
597 and Chief Security Officer for CenturyLink, I am responsible
598 for all corporate security functions including information

599 security.

600 Before joining CenturyLink, I worked for over 30 years
601 with the FBI and was responsible for investigative teams and
602 programs related to target attacks on the Internet, computer
603 systems and networks exploited by terrorist organizations,
604 criminal and intelligence operations of foreign governments,
605 white-collar crime investigations, and crisis management.

606 The cyber threat is real and serious. Our networks and
607 those of our customers are the targets of thousands of
608 cybersecurity events daily from simple port scans probing
609 network defenses to sophisticated attacks. CenturyLink and
610 our customers invest significant resources in ongoing efforts
611 to keep those assets secure. CenturyLink uses an overarching
612 governance, risk and compliance framework to ensure
613 cybersecurity threats are addressed enterprise-wide. As
614 stewards of the Internet infrastructure, CenturyLink's
615 programs on cybersecurity fall into several general
616 categories: protecting the customer, protecting our core
617 networks and providing managed cybersecurity and secure
618 communication services.

619 We have worked extensively with our industry peers,
620 partners in government and other stakeholders to strengthen
621 our collective defenses against cyber attacks. From our
622 CEO's participation on the President's National Security

623 Telecommunications Advisory Committee to my security team's
624 participation in key organizations such as DHS's
625 Communication Sector Coordinating Counsel and the FBI's
626 Domestic Security Alliance Council, we conduct risk
627 assessments, information sharing, incident response planning
628 and participate in government-sponsored cybersecurity
629 exercises.

630 In addition, CenturyLink's CEO, Glen Post, chairs the
631 FCC's Communications Security, Reliability and
632 Interoperability Council, which is working on voluntary best
633 practices for botnet remediation, Domain Name System
634 Security, Internet route hijacking, and other emerging issues
635 unique to the communications industry.

636 More can and should be done but carefully. Public-
637 private partnerships have yielded significant progress in the
638 last few years by building a framework of collective defense
639 and cooperation and helping us understand the cyber threat.
640 As many of you have pointed out, we are entering into a new
641 era of cybersecurity threats where our adversaries have
642 become more sophisticated and determined, and the need to
643 collectively step up our game is more acute.

644 We are particularly encouraged by legislation like H.R.
645 3523, the Cyber Intelligence Sharing and Protection Act, and
646 similar provisions in Senate bills that could clarify and

647 enhance cyber-related public-private information sharing.

648 As communication providers, we see a number of areas
649 where Congressional action can make valuable improvements to
650 our Nation's cybersecurity process such as improving
651 information sharing, market-based incentives and gap
652 analysis, improving the Federal Government's cybersecurity
653 posture, and expanded research and development.

654 Shifting to a mandated-based approach would be
655 counterproductive. We strongly caution against the
656 traditional regulatory approach based on government mandates
657 or performance requirements. Because our network is the one
658 central asset of our business, CenturyLink and our industry
659 peers already have the strongest commercial incentives to
660 invest in and maintain robust cybersecurity. There is
661 neither a lack of will nor a lack of commitment to do this
662 among the major communications providers.

663 At its best, cybersecurity is a dynamic, constantly
664 evolving challenge best done in a collaborative partnership.
665 At its worst, cybersecurity can devolve into a checklist
666 exercise and diverts resources away from effective
667 protections into expensive compliance measures that may be
668 already outdated by the time they are implemented. We have
669 the most knowledge of our network systems and databases, and
670 we understand the most effective and efficient ways to

671 protect these assets.

672 We commend the members of the Energy and Commerce
673 Committee for their interest in improving the Nation's
674 cybersecurity and for the deliberate process the committee is
675 undertaking to find the right mix of incentives and
676 elimination of legal barriers. CenturyLink has strived to be
677 a constructive partner in this effort, and we will continue
678 to do so. Thank you.

679 [The prepared statement of Mr. Mahon follows:]

680 ***** INSERT 3 *****

|
681 Mr. {Walden.} Thank you, sir. We appreciate your
682 testimony, and now we will move to Mr. John Olsen, Senior
683 Vice President and Chief Security Officer for MetroPCS
684 Communications. Welcome, and we look forward to your
685 comments.

|
686 ^STATEMENT OF JOHN OLSEN

687 } Mr. {Olsen.} Thank you, Chairman Walden and Ranking
688 Member Eshoo. It is an honor to appear before you and your
689 colleagues today. I am the Senior Vice President and Chief
690 Information Officer for MetroPCS Communications. I have
691 nearly 30 years of IT experience, and I am responsible for
692 our IT networks.

693 MetroPCS is a leading provider of unlimited wireless
694 communication services for a flat rate with no annual
695 contract. We sell our services through our own retail stores
696 and independent MetroPCS dealers to retail consumers. We do
697 not sell through business-to-business sales channels or to
698 the government.

699 Our communications networks use four well-known and
700 established network vendors: Alcatel-Lucent, Ericsson, Cisco
701 and Samsung. We also purchase handsets from well-known and
702 established vendors. These vendors are not our primary
703 network vendors, which mitigates the risk that an embedded
704 handset threat is able to exploit vulnerabilities in our
705 network.

706 Our communications networks utilize security measures
707 similar to other carriers. We have also adopted measures

708 both physical and logical to protect these networks. We have
709 four IT networks which are critically important to our
710 business. As we will discuss in more detail, we have
711 voluntarily undertaken a number of cybersecurity measures to
712 protect our IT networks, both physical and logical.

713 Security of these critical networks is very important to
714 MetroPCS. We maintain a comprehensive, holistic, risk-based
715 information security program built on industry best practices
716 covering people, process and technology. We use a
717 combination of hardware and software services. Our security
718 program directives are driven by a formal governance function
719 and include, among other things, centralized policy
720 management, security awareness, training, and internal and
721 third-party monitoring, physical protection, threat
722 identification and vulnerability management as well as
723 intrusion prevention.

724 We are particularly focused on security at the perimeter
725 of our IT networks and use multi-level security technologies
726 to prevent unauthorized access to our IT networks from both
727 inside and outside our company. We conduct and we have
728 third-party vendors conduct regular network security audits
729 and penetration tests and have standardized on a single
730 provider for all network equipment. Further, our IT networks
731 are broken up into segments with firewalls between critical

732 segments. Our 24/7 monitoring efforts, which are augmented
733 by our cybersecurity partners, can generate hundreds of
734 thousands of potential cyber threat alerts a day but result
735 in just a handful of real threats, which we address
736 immediately. While we cannot say definitely we have never
737 had a cyber intrusion, we are not aware of any significant
738 cyber intrusions or cyber attacks that have been successful
739 at disrupting our IT or communication networks.

740 In addition, we have also adopted a number of other
741 measures to protect our customer information such as
742 encrypting hard drives, installing virus and malware
743 software, and for a mode access requiring two factor
744 authentication. We also conduct background checks, segregate
745 duties of personnel and log all access and changes to
746 critical systems. MetroPCS has also implemented numerous
747 physical security measures such as card key and biometric
748 access.

749 Our staff also maintains vendor-specific and industry-
750 recognized certifications and regularly participates in
751 vendor-sponsored symposiums, industry summits and
752 conferences. We are involved in these groups, not because we
753 are required to but because they are a valuable source of
754 information and best practices.

755 MetroPCS does not believe that regulation is required or

756 warranted at this time, particularly for carriers that do not
757 provide services to government or local public safety
758 organizations. Carriers are already well incented to protect
759 their networks, and this is particularly true for month-to-
760 month service providers like MetroPCS. If we do not provide
761 the level of protection our customers want or demand, they
762 can terminate service without penalty and can active service
763 with a competitor. Governmental regulations and private
764 sector certifications such as PCI also force providers to
765 invest in the appropriate tools and practices to detect and
766 deter cyber threats.

767 Market forces are better suited to respond to constantly
768 changing cyber threats. If regulations are considered,
769 MetroPCS urges that these requirements be flexible and
770 tailored to the threat. Regulatory compliance can be
771 particularly burdensome for carriers who compete by providing
772 an affordably priced differentiated service for consumers.

773 Unfortunately, even voluntary obligations can evolve
774 into a mandate on industry. We support voluntary industry
775 efforts, industry standard bodies, enhanced governmental
776 consumer education and the FCC's cybersecurity stakeholder
777 efforts along with government sharing of cyber threat
778 intelligence including a natural central clearinghouse.
779 Finally, no carrier should be liable for using such

780 information.

781 Thank you again for the opportunity to testify and I

782 look forward to any questions that you may have.

783 [The prepared statement of Mr. Olsen follows:]

784 ***** INSERT 4 *****

|
785 Mr. {Walden.} Thank you, Mr. Olsen. We appreciate your
786 comments today and we will back to you with questions as
787 well.

788 Now we will turn to our final witness on the panel this
789 morning, Mr. Scott Tetzke, Senior Vice President, BlackBerry
790 Security Group, Research in Motion, RIM. Thank you for being
791 here and we look forward to your comments.

|
792 ^STATEMENT OF SCOTT TOTZKE

793 } Mr. {Totzke.} Chairman Walden, Ranking Member Eshoo,
794 members of the Subcommittee. Thank you very much. My name
795 is Scott Totzke. I am the Senior Vice President of
796 BlackBerry Security at Research in Motion, and I am pleased
797 to be here to talk to you on the topic of cybersecurity.

798 RIM revolutionized the mobile industry when we
799 introduced the BlackBerry in 1999, and today our products and
800 services are used by millions of customers around the world.
801 There are more than 630 carriers and distribution partners in
802 175 countries that offer BlackBerry products and services to
803 our customers. More than 90 percent of the Fortune 500
804 customers are BlackBerry customers today, and we have a
805 longstanding relationship with the U.S. Federal Government
806 including Congress, the Department of Defense and the
807 Department of Homeland Security.

808 Mobile communications face similar security risks as
809 non-mobile communications. Several of the same types of
810 threats and attacks that have existed in traditional
811 computing platforms can impact smart users today, and as the
812 power, ubiquity and computing capabilities of smartphones
813 have increased over the last few years, the threat matrix

814 continues to evolve exponentially. Most users have yet to
815 realize the applicability of both the existing and emerging
816 threats to what is essentially a smaller and more mobile
817 computing platform that they already have at their home or
818 office.

819 An effective and comprehensive mobile security solution
820 must therefore provide protection by providing unauthorized
821 access to the smartphone and its data, to protect the data in
822 transit over the wireless network and to protect the
823 corporate network using features that are built into the
824 platform. While technology vendors can provide components of
825 these solutions, it is equally important that as a mobile
826 technology industry, we help government, enterprises and
827 consumers better understand the risks involved with all types
828 of online activities.

829 For our part, RIM focuses on designing secure and
830 efficient solutions for enterprises and consumers. RIM has a
831 history of integrating security features into its products
832 and firmly believes that security technologies are an
833 important foundation for a digital economy. RIM has built
834 security features in that allow for data to be encrypted and
835 protected from unauthorized access, to limit and control
836 access to information on the smartphone by third-party
837 applications, and to remotely erase sensitive information in

838 a case where a phone is lost or stolen. These controls can
839 all be centrally managed by the BlackBerry Enterprise
840 Solution, which is designed to give large and small
841 organizations the ability to balance individual and
842 enterprise use of BlackBerry smartphones while protecting the
843 privacy of their corporate and employee information.

844 RIM also believes that there needs to be more focus on
845 security testing and certification that establishes a
846 baseline for technology vendors. Without an established
847 baseline to properly gauge the security of a product or a
848 network, it is difficult to make informed decisions. Vendors
849 that work to certify their mobile solutions through trusted
850 validation programs provide assurances to governments and
851 consumers who would otherwise be unable to verify the
852 security of the claims being made by the vendor.

853 BlackBerry products and solutions have already received
854 more security accreditations globally than any other wireless
855 solutions, and our consumers value this level of transparency
856 when it comes to protecting their information. We feel that
857 greater adherence to security standards like FIPS would help
858 customers better understand their personal and professional
859 investments in protecting their information.

860 Lastly, this panel has raised a number of concerns
861 regarding two extremely important points related to the

862 evolution of security and technology in the mobile industry
863 that I would like to address. The first concern is related
864 to information sharing. While there is increased competition
865 between vendors, there is also an increasing degree of
866 commonality in the components used by many desktop and mobile
867 platforms. This directly translates into an evolving risk of
868 cross-platform vulnerabilities, creating a level of shared
869 risk that increases the need for vendors to work together to
870 responsively disclose and address these concerns. This also
871 means that programs such as RIM's information sharing program
872 need to fully engage with public sector entities such as the
873 US-CERT to ensure timely and bidirectional flow of security
874 information.

875 The second issue raised here is related to supply chain
876 security and the impact it can have on the security and
877 availability of networks. A product that has been modified
878 or created in an authorized manner could pose security risks
879 to the customer's information and to the overall posture of
880 RIM's network, our carriers' networks or our customers'
881 networks. RIM has been working for several years to embed
882 network security elements directly into the silicon of our
883 products and in all aspects of our manufacturing process to
884 ensure that only authentic products are allowed to obtain
885 network services. We believe that this combination of

886 hardware security, operational security and manufacturing,
887 facility security, software security, network security work
888 together to mitigate many of the concerns about knockoff
889 products or products that have otherwise been tampered with,
890 impacting the security of our customers' information. We
891 support the Subcommittee's efforts to raise awareness of this
892 wide-reaching impact in respect to supply chain-related
893 security issues.

894 Chairman Walden and members of the Subcommittee, I would
895 like to thank you again for the opportunity to provide RIM's
896 perspective on these critical issues.

897 [The prepared statement of Mr. Totzke follows:]

898 ***** INSERT 5 *****

|
899 Mr. {Walden.} Mr. Totzke, thank you very much for your
900 testimony. All of you, thank you very much. We appreciate
901 your being here.

902 I am going to lead off with questions. So Dr. Amoroso
903 and Mr. Olsen, you say in your testimony that you routinely
904 track threats to your networks. I assume you all do that.
905 How can we facilitate information sharing among network
906 providers of such information while protecting consumers'
907 privacy and companies' competitively sensitive data?

908 Mr. {Amoroso.} I think the big debate has been between
909 government and industry, right, that has been the big issue.
910 Like if I go to a security conference and some hacker
911 whispers to me that there is a signature that I should be
912 looking at, then I scribble it down, run back to my op center
913 and put it in place. If a government individual does that,
914 then I can't put that in the network because we would be
915 operating as a branch or an agent of the government or
916 something like that. So that seems to me a little silly,
917 like that is something that probably ought to be addressed.

918 Mr. {Walden.} That is the kind of specific issue we are
919 trying to drill down to here. Can you give us something more
920 specific? Where does that show up? Do you know statutorily?

921 Mr. {Amoroso.} Oh, yeah. I mean, like the United

922 States intelligence agencies and law enforcement agencies
923 regularly see different types of signatures that we don't
924 look for. We are not in law enforcement. We are providing
925 service to customers. We don't chase that sort of thing
926 down. We chase it to the point where we can stop it, and
927 that is it, but like intelligence groups will really dig down
928 deep and see something that we don't. For them to share
929 that, particularly if it is classified or something is
930 awkward and it is stilted. And I know in my own company
931 whenever I get involved in something like that, there is more
932 lawyers involved in the discussion than there are people in
933 this room right now. So, you know, it is almost like we are
934 disincented to even bother. So I don't think it is so much
935 whether, you know, between different groups we share because,
936 frankly, we kind of do. The Internet wouldn't work if we
937 weren't sharing constantly.

938 Mr. {Walden.} But are there any prohibitions? If you
939 spot something, if you go to that conference and a hacker
940 says look for this signature, is that something that Mr.
941 Olsen, Mr. Mahon and others should be looking for as well on
942 their networks?

943 Mr. {Amoroso.} I am sure they do.

944 Mr. {Walden.} And then is there a way you can share
945 that information with them or are there impediments to that

946 kind of sharing?

947 Mr. {Amoroso.} I mean, we all buy services from a lot
948 of the same companies that do that. You know, we pick
949 companies that do a really great job of that. I buy from
950 three or four different companies that provide about the same
951 intelligence everybody else is going to get. You know, it is
952 pretty good, you know, and they are incented to make sure it
953 is pretty useful because I pay them every month for it.

954 Mr. {Walden.} And do the customers. And so I guess the
955 question then is, there is not a problem sharing information
956 back and forth?

957 Mr. {Amoroso.} Sometimes there is, right?

958 Mr. {Walden.} Is that a problem we should address? We
959 are looking for barriers.

960 Mr. {Amoroso.} I mean, here is the classic example.
961 AT&T had an exclusive on the iPhone for some period of time,
962 so I put a bunch of people down in New York City, PhDs right
963 out of school and I told them find ways to filter attacks
964 being aimed at iPhones, that will really help our customers,
965 and they worked real hard and we came up with some, and once
966 other carriers got access to the iPhone, do you really think
967 I would want to give them, you know, the fruits of the work
968 that we are doing? Their incentive is to do it as well and,
969 you know, compete with us, and I would like my customers to

970 say hey, I am going to stay with AT&T because they are really
971 investing in doing protection and our competitors say the
972 same thing, and we innovate that way. That is kind of--that
973 is a case where, you know, it is not necessary for me to
974 share. The market is going to force our competitors to want
975 to catch up or for me to catch up to somebody else. That is
976 the right balance between, I believe, all of us. But between
977 government and industry, I think the information sharing
978 should be more free.

979 Mr. {Walden.} Thank you, Doctor.

980 Mr. Olsen, do you want to comment on that?

981 Mr. {Olsen.} Thank you, Mr. Chairman. At MetroPCS,
982 besides our internal controls and our internal systems, we
983 also have cybersecurity partners, so securing monitoring
984 firms that we use to monitor our network and our systems 24
985 hours a day. Those firms do share information between them,
986 but if I believe I understand your question, there is not a
987 central clearinghouse for that information for the folks that
988 are outside of those security companies to easily share
989 information. So if Mr. Amoroso recognizes a threat or is
990 told about a threat in his network, there isn't a central
991 place where he could notify other companies or other carriers
992 even in the same industry that this threat is out there and
993 we should respond to it.

994 Mr. {Walden.} And is there an incentive? Because I
995 almost a disincentive to do that. If you have done the
996 research, you identify the threat, you protect your
997 customers, why do you tell other iPhone--

998 Mr. {Amoroso.} I don't know that it is a disincentive.
999 Keep in mind that when we advertise or broadcast that there
1000 is a threat we are worried about, you are telling the bad
1001 guys too, right? I mean, so it is a little--it would be a
1002 little weird to be too open about what you are concerned
1003 with. So I kind of like the existing model. I mean, I think
1004 that there are companies that do this. We evaluate them, and
1005 when the intelligence looks pretty good, we buy it.

1006 Mr. {Walden.} All right. My time is expired.

1007 We will turn now to the gentlelady from California, Ms
1008 Eshoo.

1009 Ms. {Eshoo.} Thank you to all of the witnesses.
1010 Excellent testimony.

1011 First to Mr. Livingood, I think it is really terrific
1012 that you are the first ISP in North America to fully
1013 implement the DNSSEC as you noted in your testimony. How do
1014 we encourage other ISPs to follow your lead? What would be--
1015 just quickly. I have a whole series of questions.

1016 Mr. {Livingood.} So I think on that question regarding
1017 DNSSEC adoption by other providers, I think it is important

1018 to keep in mind one thing, which is, it is not just about
1019 network operators, it is about banking sites, it is about
1020 other websites, software developers. A lot of people have to
1021 implement DNSSEC to make it work in the ecosystem. But
1022 specific to network operators, I would say that there is
1023 actually already a lot of that interaction going on already.
1024 You know, one of the beautiful things about the way that the
1025 Internet has worked and is successful is, there is a lot of
1026 these multi-stakeholder consensus-based organizations that
1027 groups get involved in. One of them in fact happens to be
1028 one of the CSRIC working groups that I am on, and they will
1029 be coming out with a recommendation soon, and a number of our
1030 companies participate--

1031 Ms. {Eshoo.} When will that be?

1032 Mr. {Livingood.} I think that it is due today, the
1033 recommendations.

1034 Ms. {Eshoo.} Oh, good. You never know on government
1035 time. Congress has an extensive network to ensure the
1036 security of our mobile devices and the network that they run
1037 on. I experienced this firsthand last year when I traveled
1038 abroad as part of a Congressional delegation, and my device
1039 became infected during the trip, and the device never left
1040 me. I mean, I practically slept with the thing under my
1041 pillow. It never was out of my purse. It was never left in

1042 the hotel. But nonetheless it was infected. The good news
1043 is, because of the proactive measures in place, the threat
1044 was detected prior to being reactivated in the House network.
1045 So as a company, what steps do you take to ensure that your
1046 customers, particularly those in smaller organizations,
1047 adhere to the same proactive security measures? And I guess
1048 my question is to Mr. Tetzke, to Dr. Amoroso--I love your
1049 name, Amoroso--and Mr. Olsen.

1050 Mr. {Tetzke.} Thank you, Congresswoman. I will go
1051 first. I mean, we provide a comprehensive list of guidelines
1052 for configuration of the device so our administrators have
1053 white papers and information they can access on the website,
1054 and our goal is to make sure that your administrator, your IT
1055 organization that looks after your device if it is a
1056 BlackBerry device has full control over that device at all
1057 times, so there is a comprehensive set of policies, more than
1058 500 of them, than administrator can send to control all
1059 aspects of the platform including preventing access to
1060 information or disallowing you the installation of software
1061 on the device. So we try and do that. As I think will be a
1062 common thread here, there is a lot of education in this
1063 industry. Security is a complex set of decision-making
1064 things that we have to do on a daily basis and a lot of risk
1065 that is really difficult for people to understand. We are

1066 trying to offer as much transparency and help to our
1067 customers through publication of standards and best practices
1068 and forums like this.

1069 Ms. {Eshoo.} As I understand, one way to prevent
1070 potential botnet activity is to isolate and block IP
1071 addresses that pose a threat. Do you all have the technology
1072 to do this today, and if so, has it been effective?

1073 Mr. {Amoroso.} I can comment. I mean, we have the
1074 technology to block but it doesn't work, so, you know, we can
1075 certainly--we do try. We try real hard. Botnets all of your
1076 PCs being infected. That is what it is. Like we have made
1077 the mistake in computing of turning every person in this room
1078 into a Windows system administrator. That is what you do
1079 part time when you are not legislating. So that model is
1080 wrong, and most of you don't do a very good job of it, nor do
1081 I. I bet people at this table, we would shrug and say we
1082 probably don't do it well either. So we have distributed the
1083 responsibility massively and that risk--

1084 Ms. {Eshoo.} Is that what causes the complexity that
1085 you just discussed?

1086 Mr. {Amoroso.} Well, it is billions of people around
1087 planet Earth with PCs that are improperly protected, so it is
1088 a piece of cake to built a botnet. We watch botnets, you
1089 know, new ones every day, ones that are 50,000, 100,000

1090 botnets we don't even bother naming. We just say oh, there
1091 is another one. We track them and just try to contain it.
1092 So it is not a matter of blocking the IP addresses, because
1093 we would be blocking you. You probably wouldn't like that.
1094 ``Sorry, you can't get on the Internet today. Why? It looks
1095 like you have a botnet.'' We would just shut the whole
1096 Internet down if we did that.

1097 Ms. {Eshoo.} In my opening statement, I mentioned the
1098 issue of supply chain and the security that I think really
1099 needs to be brought to that. First of all, do you share
1100 these concerns about the supply chain, and if so, what do you
1101 think would be the appropriate role for us to play in
1102 addressing it? I think it is a serious issue. Our
1103 telecommunications network that we came to more fully
1104 appreciate after our country was attacked was the system that
1105 we relied on. If we didn't have that, I don't know what we
1106 would have done. So I think that--and there are constant
1107 things that keep coming up relative to the supply chain. So
1108 I welcome any comments on that.

1109 Mr. {Tetzke.} So I will answer that from a device
1110 manufacturer's standpoint. You know, this has been a concern
1111 for RIM for the decade-plus that I have been there. We have
1112 to understand where we get our components from, where we
1113 manufacture the devices, and when we started, it was real

1114 easy because we just made everything in our factory and it
1115 was all under our control and you grow into a global entity,
1116 you deal with outsourced manufacturing and kind of
1117 distributing that capability around the world with different
1118 partners. So it brings into question, you know, are you
1119 actually manufacturing the product you think you are making
1120 or are you getting something that is whole and intact. We
1121 have really focused on understanding what we can do to secure
1122 our products in the manufacturing process as well as the
1123 parts that come in. So for some of our strategic vendors, we
1124 are actually doing serialization and embedding kind of
1125 cryptographic elements in their silicon before it gets to us,
1126 and then our manufacturing process goes through a
1127 verification of every tool along the line, checking with RIM
1128 head office to say are you allowed to actually perform this
1129 operation, and the combination of hardware and software, so
1130 the embedded certificate is in the silicon. The hardware
1131 checking that the software hasn't been tampered with is used
1132 to authenticate the device to get BlackBerry services. So we
1133 know that a device hasn't been tampered with and it has been
1134 manufactured by RIM and it is intact when you first turn it
1135 on, and that authentication protects our network, our carrier
1136 partners' network and your networks, and is that hardware,
1137 software and network layer all working together to ensure the

1138 integrity of the BlackBerry services that we provide to our
1139 customers.

1140 Ms. {Eshoo.} Thank you.

1141 Mr. {Walden.} Thank you.

1142 We will now turn to the vice chair of the committee, Mr.
1143 Terry, for questions.

1144 Mr. {Terry.} Thank you, and with my 5 minutes and five
1145 people, I want to ask you all the same question, and that is
1146 in regard to the fact that you are the interface. If I want
1147 to have an Internet experience, I have to hire one of you.
1148 So what are you doing to provide me services that will
1149 protect at least to some extent from botnets and viruses or
1150 attacks to my information and my computer? And we will start
1151 from left to right, my left to right, Mr. Livingood.

1152 Mr. {Livingood.} Sure. Thank you. So I think we all
1153 have somewhat similar, you know, capabilities. It is a
1154 multilayered approach. There is not any one thing that is
1155 going to solve it. So it is sort of, you know, like an
1156 onion. There is lots of layers, and it is everything from
1157 intrusion protection that is at the edge of a network to
1158 things that provide denial-of-service attack, you know,
1159 mitigation when you see those things to botnet intelligence
1160 systems that detect botnets and start to notify customers--I
1161 mentioned that in my opening statement--and then to notify

1162 customers, and there are also a number of things that we all
1163 do and we do in particular to educate customers, to help them
1164 understand what things they need to secure in their network,
1165 the software they need to manage, gets them the software that
1166 they need to secure their network and their computers. So it
1167 is a multilayered approach.

1168 Mr. {Terry.} Mr. Amoroso?

1169 Mr. {Amoroso.} That was exactly what we do, same thing.
1170 There are a lot of different products and product names. I
1171 mean, I will you the one thing we don't do, and that is, we
1172 didn't sell you the computer, we didn't sell you the
1173 operating system that runs on the computer and we didn't help
1174 you select what type of software to put on there, and
1175 increasingly the ISPs are getting dragged into that, and it
1176 is a difficult situation because, you know, a lot of times
1177 people will say ISP, you know, I got something wrong with my
1178 PCs, you guys are sitting off in a cloud somewhere watching,
1179 you should figure out how to fix my PC, and that is something
1180 all of us struggle with.

1181 Mr. {Mahon.} We do all a number of very similar things,
1182 I think, in the ISP world, you know, to protect particularly
1183 residential customers. I think you have heard the spyware,
1184 the anti-virus, parental controls. We all have education and
1185 awareness, you know, places on our website, our home page

1186 where you can go to. We have a botnet notification program.
1187 In fact, if your computer does become a bot on a botnet, we
1188 have a method to notify you and then facilitate you cleaning
1189 up your home device.

1190 Mr. {Terry.} Mr. Olsen?

1191 Mr. {Olsen.} I think there is a lot of commonality in
1192 the approaches that we are all taking. One of the
1193 distinctions that I made in my opening comments regarding our
1194 cybersecurity partners I think is really important. These
1195 are people that are focused, that their full-time job is
1196 cybersecurity. They are looking for threats all the time and
1197 they have hundreds, if not thousands, of customers that are
1198 feeding them information and they are seeing real-time
1199 threats go through many companies. So a threat that might
1200 hit one company, they are aware of before many of us would
1201 see that. So I think that information sharing in that
1202 cybersecurity industry is really critical and it is something
1203 that we value.

1204 Mr. {Terry.} All right. Mr. Totzke, you may have
1205 already answered this question when you were talking to Ms.
1206 Eshoo.

1207 Mr. {Totzke.} Yes. So certainly the embedded security
1208 elements are part of that but beyond that, you know, we have
1209 user- and administrator-controlled security that lets our

1210 users dictate what level of protection they want to put into
1211 the platform, and we do have services available to consumers
1212 and enterprises that allow for on-device encryption of data,
1213 remote backup, remote restore, the ability to remotely lock
1214 and wipe the device so you can deal with this eventuality as
1215 a mobile device that is going to be lost or stolen or left in
1216 a taxicab, so we give you the capability out of the box to
1217 deal with any of those eventualities.

1218 Mr. {Terry.} Good. I appreciate that. I guess the
1219 last 47 seconds I am going to give to Mr. Amoroso. Should
1220 the responsibility be on the ISP providers to have a system
1221 to detect viruses as they enter into your network before they
1222 get to my computer?

1223 Mr. {Amoroso.} If we knew how to do that reliably, I
1224 would have been trying to sell you that years ago. It is a
1225 very difficult thing to detect viruses and malware.
1226 Sometimes we can kind of pick it up, and we do notify, just
1227 like the rest of them. I call 100 to 1,000 people very week.
1228 The problem is, if I really knew what to tell them, knew
1229 exactly how to fix their PC, I would call everybody. Why
1230 just restrict it to the ones that happen to notice active
1231 malware? We would tell everyone. The problem is, there
1232 isn't a person in this room that can tell you how to clean
1233 malware off your PC other than reimage your computer. You

1234 know, that is the best we can do.

1235 Mr. {Terry.} Can't we just tell you to stop it?

1236 Mr. {Amoroso.} I wish I knew what--you know, here is
1237 the reason we can't stop it. I don't know if you are
1238 familiar with the concept of an encrypted tunnel, but when
1239 you visit a website and see https, that means there is
1240 cryptography between you and the website and everybody says
1241 oh, that is really secure, you should look for that. The
1242 reality is, every hacker in the world knows to make sure they
1243 are pushing their malware through that encrypted tunnel
1244 because none of us can see it. So we can sort of block the
1245 website but they hide the malware in places we can't see.
1246 That is where anybody would go.

1247 Mr. {Terry.} Well, it is such a fun issue to deal with.

1248 Mr. {Amoroso.} Here is what--when we pick up malware,
1249 it is the equivalent to somebody falling over and having a
1250 heart attack on the table, and we all go, that is rapid
1251 response to preventive care. You fell over, you had a heart
1252 attack, I picked that up. That is easy. It is picking up
1253 the stuff that isn't easy, and that is why it is difficult
1254 for us to build reliable services that will detect malware
1255 because it is hidden. Any hacker would do it that way.

1256 Mr. {Walden.} Thanks.

1257 Mr. Doyle, you are up next.

1258 Mr. {Doyle.} I think we ought to just call him Dr.
1259 Sunshine.

1260 Mr. Tetzke, I want to ask you about federal workers. As
1261 you might know, the White House is currently working on a
1262 national mobility strategy to determine how the employees of
1263 the Federal Government are using their mobile devices, and
1264 they are going to decide, for example, whether all agencies
1265 can bring their own devices to work much like many private
1266 sector employees do. Now, we don't of course advocate to
1267 prescribe one particular type of phone for everyone to use in
1268 the Federal Government but what security issues do you
1269 foresee that might come up as a result of this if we allow
1270 all federal workers to use their own mobile devices and how
1271 do you think device manufacturers can make sure that the data
1272 that is on the phone of federal workers, especially in
1273 sensitive agencies, remains secure?

1274 Mr. {Tetzke.} So as you move to more of a heterogeneous
1275 environment where you bring your own device for what we call
1276 personal liable, individual liable devices, one of the
1277 challenges you face is that the security of platforms is
1278 going to vary based on the vendor and the posture and the
1279 features that they built into that. So getting a consistent
1280 view of security and how you are protecting your information
1281 is probably one of the issues. There are, you know, kind of

1282 liability and discovery issues in more of a corporate
1283 context--who owns the information, who owns the intellectual
1284 property if you have to go through any kind of a litigation,
1285 maybe not so much in the case of a Federal Government
1286 employee, and then how do you protect the information on the
1287 device, which I think is probably one of the more important
1288 ones. You know, there is a level of encryption built into
1289 BlackBerry to encrypt of that data at rest, whether that is
1290 personal data or government data, and that is one of those
1291 that can be enforced remotely. But as we look at how we go
1292 into a bring-your-own device scenario, you know, the biggest
1293 concern that I have is this lack of a standard bar for
1294 protecting information, and what I would be most concerned
1295 about is sort of a race to the lowest common denominator so
1296 we have three or four competing platforms, so in order to
1297 allow everything we are going to reduce our security
1298 requirements to the bare minimum, which I think is the wrong
1299 thing, especially at the government level.

1300 Mr. {Doyle.} Thank you.

1301 Mr. Livingood, given the concerns outlined by Dr.
1302 Sunshine about implementing the DNSSEC, can you outline for
1303 us why Comcast made the decision to begin using DNSSEC and
1304 whether you think it has had the intended benefits that you
1305 hoped it would have?

1306 Mr. {Livingood.} Sure. Well, you know, the intended
1307 benefits, it is a long-term game there. I think one of the
1308 challenges with DNSSEC adoption was that you needed some
1309 critical mass for people to start signing their names, for
1310 people to build software to do that, and we felt like we
1311 could play a role in leading the industry in creating that
1312 critical mass. So, you know, that is part of the reason that
1313 we did it. I think the reason, you know, at root why we did
1314 that is, when the Kaminsky vulnerability came out in 2008, it
1315 fundamentally scared the heck of us. If our customers
1316 couldn't be sure that when they went to BankofAmerica.com it
1317 was that website, that scared us because then, you know, they
1318 are less likely to use the Internet, they are not going to
1319 care as much about higher-speed services and so on, and that
1320 is incredibly important to us. So to have a way--we all
1321 certainly had a short-term fix to that but to have a long-
1322 term fix to that we thought was incredibly important, and
1323 DNSSEC appears to be that one, and we are pleased to help
1324 lead the way and create that critical mass to help adoption.

1325 Mr. {Doyle.} Thank you.

1326 And just in closing, Dr. Amoroso, I have enjoyed your
1327 testimony and it makes us all realize how much work we all
1328 have to do together to face this problem that certainly there
1329 is no easy answer to. But I want to thank all the panelists

1330 for your testimony today. It has been very enlightening.

1331 I will yield back, Mr. Chairman.

1332 Mr. {Walden.} Mr. Doyle, thank you very much, and we
1333 will go now to Mr. Shimkus for 5 minutes.

1334 Mr. {Shimkus.} Thank you.

1335 I kind of want to build a little bit on what my friend
1336 Mike Doyle mentioned, but I want a different perspective,
1337 because it popped in my mind when he talked about federal
1338 workers. Where are you finding your cyber warriors today
1339 from? In other words, where are they coming out of? Are
1340 they coming from private universities? Are they coming out
1341 of the military? Briefly, the cutting-edge new people who
1342 are helping you do this stuff, where are they coming from?

1343 Mr. {Livingood.} So I will start. I think it is a
1344 variety of places, and I would say, you know, there is a need
1345 for more educational focus not just in cybersecurity but ICT
1346 generally, but we find people in a variety of ways. Some are
1347 former military service members, former law enforcement.
1348 Others are just Linux system administrators that are
1349 interested in security. Others are, you know, former
1350 childhood hackers or something like this, and they are
1351 interested in it. So it is a variety of things.

1352 Mr. {Shimkus.} But is there a college path? I mean,
1353 can you get IT training in the business schools or computer

1354 science classes?

1355 Mr. {Amoroso.} I would like to comment. So I have been
1356 teaching at Stevens for 22 years. I teach this semester. If
1357 you looked at my class in 1990, you would see something that
1358 would look like a typical college class. I went to
1359 Dickinson, Pennsylvania, so pretty--a mix of kids. My class
1360 today at Stevens is about 98 percent foreign nationals, and I
1361 have got about 65 in the classroom, and almost all of them
1362 have the intention of leaving the country when they complete
1363 their master's or PhD because they see bigger opportunities
1364 elsewhere.

1365 Mr. {Shimkus.} Well, and that kind of segues, and if
1366 you all want to jump in, you can real quick, but I don't want
1367 to forget the aspect of compensation for people entering the
1368 private sector versus the government sector. There is this
1369 debate on salary compensation. I don't know where it is. I
1370 mean, we have the same issues about bringing in the best and
1371 the brightest, but if we are not compensating them for what
1372 the private market bears, then there is another thing. Does
1373 anyone want to jump in?

1374 Mr. {Totzke.} Just on where we source. So there is
1375 certainly out of the education system, out of the military
1376 and intelligence, we find some people kind of moving into
1377 private industry. The most talented guy on my team is a high

1378 school dropout, and so I think using the education system as
1379 a bar doesn't really help identify the best talent. He would
1380 one of the top recognized kind of hackers and researchers in
1381 the world. So it varies, and I don't think you can actually
1382 teach somebody to be a hacker. There is sort of if you want
1383 to be a researcher in that area, there is an ingrained
1384 mentality you are either born with or not, so it is not like
1385 I am teaching somebody a trade like programming and getting
1386 to a level of sophistication in developing software. Being
1387 an attacker is a much different mindset.

1388 Mr. {Shimkus.} Right. Thanks.

1389 You know, the debate on the Senate side, and this is how
1390 you provide is, what happens if the Federal Government
1391 requires you to follow a new government security standard?
1392 What happens to you? That is the debate on the Senate side
1393 legislatively. One has a government-imposed standard. One
1394 is really, I think, letting you guys fight the battle
1395 yourselves. So does anyone want to jump in?

1396 Mr. {Amoroso.} I will offer just a brief point. My
1397 guess is, anything you can write down that you can think of
1398 as kind of a best practice is already being done here, and
1399 the things that we are back at the shop worrying about now
1400 are things that are not on your list, like as an example, we
1401 talked about botnets. You know when I saw the first botnet?

1402 Remember Y2K? We were building the Y2K White House
1403 communications fusion center, and we were worried that we
1404 were going to get DDoS'd for one day. That would be really
1405 bad if you are knocked out one day and miss the millennium
1406 change. You can't really move that date, right? So we were
1407 completely freaked out by botnets then and we have built--a
1408 lot of people in this room, we have built ways to steer
1409 traffic around and fix it and now we have a service and we
1410 moved on to the next thing.

1411 Mr. {Shimkus.} Yes, and let me put a final challenge
1412 out because I do agree, how do we incent innovation in this
1413 area, which is part of the opening statements. Incentivizing
1414 usually means government money here or government tax
1415 credits. You know, that is all kind of persona non grata
1416 right now in this new world in which we live in, so I would
1417 ask you to help us wrap around about this, and maybe it is
1418 easing regulatory burdens. Maybe there are things we can do
1419 that are not a dollar-cents component but tax credits, things
1420 like that. It is very difficult to do in today's
1421 environment. I will just throw that out.

1422 Thank you, Mr. Chairman. I yield back.

1423 Mr. {Walden.} I thank the gentleman.

1424 And with the Committee's indulgence, Doctor, could you
1425 just explain DDoS?

1426 Mr. {Amoroso.} I am sorry. That stands for distributed
1427 denial of service. Here is how it works. When my voice
1428 talks to all of your ears, it is one thing to many years and
1429 it works great if you are all quiet and you listen, your ears
1430 work. But if you could bounce my voice off your ears to him,
1431 it would sound like you are all shouting at him, right? My
1432 voice to all of your ears and then you reflect it back, that
1433 is a denial-of-service attack. We hit all your PCs and then
1434 tell all your PCs to shout this way, and boom, it all comes
1435 and it sounds like this big attack and it clogs the pipes and
1436 knocks them out. That is how it works.

1437 Mr. {Walden.} All right. Thank you, Doctor.

1438 Now we go to Ms. Matsui.

1439 Ms. {Matsui.} Thank you, Mr. Chairman, and this is all
1440 challenging and frightening at the same time here, and I do
1441 appreciate all of your testimony.

1442 I want to go into another area here. As we look into
1443 developing industry best practices standards for ISPs, should
1444 ISPs' own cloud services be included as well as other cloud
1445 providers or do you think because that technology is newer,
1446 it could be better for cloud providers to consider forming
1447 their own best practices to secure data in the cloud? I
1448 would like Mr. Mahon and Dr. Amoroso to answer that, please.

1449 Mr. {Mahon.} Well, first of all, we are already talking

1450 to the cloud providers, and some of us in fact are cloud
1451 providers. So I do think that the conversation is well
1452 underway. We are very familiar with the challenges, and if
1453 you really think about it, the term ``cloud'' is a rather
1454 generic term that is probably misunderstood. It can mean a
1455 number of different things for a different type of customer,
1456 and so therefore I would say we continue to include them in
1457 the conversation as we have everyone else, so to speak, at
1458 the table as partners and the solutions that you are looking
1459 for are really going to have to be integrated across a very
1460 wide platform. So therefore I would say that you would want
1461 to keep them in the conversation.

1462 Ms. {Matsui.} Okay. Thank you.

1463 Mr. {Amoroso.} So my mother has a PC at home that at
1464 this instant I am sure is like attacking China or something.
1465 It is not administered properly and she has got, you know, a
1466 big tower with Verizon FIOS, the whole thing. She doesn't
1467 need that. She would be better much served to have a cloud
1468 provider just take care of all of that for her, and she
1469 should just be using, you know, some appliance to hit the
1470 Internet. The reason she doesn't is because there is
1471 software on the PC that she wants to be able to use that
1472 hasn't been put in the cloud. So in general that concept is
1473 a more secure concept than my mom trying to do it

1474 administration. So I think cloud in general is a more secure
1475 model than the one we have now.

1476 Ms. {Matsui.} Oh, okay. That is good to know.

1477 Dr. Amoroso, given your expertise in this area, what are
1478 the differences between securing wired and wireless
1479 communications networks and how can these differences be
1480 accounted for in any type of cybersecurity initiatives?

1481 Mr. {Amoroso.} Well, they are pretty big, right? The
1482 differences are significant. You know, if we had 3 hours, I
1483 could take you through the whole thing, but I will give you
1484 one example. Remember when--I am guessing most of you
1485 remember when computer security was just don't put an
1486 infected floppy in your computer. Remember that?

1487 Ms. {Matsui.} Yes.

1488 Mr. {Amoroso.} And it was like don't put software on
1489 your machine that you don't know where it came from. It
1490 seemed like perfectly good common sense, right? What do we
1491 do every single day on app stores? You know, we are
1492 downloading stuff, I don't know who wrote that, I don't know
1493 where it came from but boy, it sure looks pretty cool, I
1494 think I will download it to my device. That is something we
1495 are going to have to address from a security perspective.
1496 That is the big difference between wired and wireline.

1497 Ms. {Matsui.} Okay. I am also thinking that so much of

1498 what we do is wireless, so much we do within our homes is
1499 wireless, and yet it is just so easy to do it that most
1500 people don't think about it at all, and I am concerned that
1501 we are not thinking as broadly as we should be thinking as
1502 far as some of the personal use, and I think it came about
1503 here with Mr. Doyle's too and the government area too. But
1504 it is so easy to be carrying tablets and different cell
1505 phones around, and for me, the part that is really to me
1506 quite frightening is that nobody knows what they don't know,
1507 and we are looking at you and you are saying too that there
1508 is a lot of things you don't know too, and we look upon you
1509 as experts, and I am hoping that we can build in some
1510 incentives here with sort of a sharing of information that
1511 goes beyond some of your commercial type of concerns.
1512 Because I am looking ahead, this is even getting more and
1513 more complicated as we develop more tablets and smartphones
1514 and whatever that we are losing control of the cybersecurity
1515 aspect of it, and the software aspect, I think you brought
1516 up, Dr. Amoroso, is really important, the education facet of
1517 that, and actually kind of building our principles and
1518 standards into that too.

1519 So that is just a comment, and I really do appreciate
1520 your being here, and I think I am learning more and more
1521 every time one of you opens your mouth, so thank you very

1522 much for being here.

1523 Mr. {Walden.} Thank you for your comments.

1524 We will go now to Ms. Blackburn for 5 minutes.

1525 Mrs. {Blackburn.} Thank you all so much, and I tell you
1526 what I think I am going to do is just ask my question, then
1527 if you all want to respond or respond in writing, that would
1528 be wonderful.

1529 First of all, going back to something that Mr. Shimkus
1530 said, I would like to hear from each of you, and you can say
1531 it now or send it to me, what you are seeing as the
1532 disturbing trends and what is kind of the next thing out
1533 there. I would like to know that. I would like to get an
1534 idea of how much of your cost of doing business is beginning
1535 to center around the cybersecurity issues.

1536 In your testimony, several of you have mentioned in one
1537 way or another either in response to the questions or
1538 testimony fear that the Federal Government could end up being
1539 more of an impediment than a facilitator in bolstering some
1540 of the cybersecurity efforts. I would like for you to speak
1541 to what you are concerned that we might do and then what we
1542 are not doing that we should be doing and hear from you in
1543 that vein with your consumers, I would appreciate knowing
1544 what you are doing to educate them. I think that one of the
1545 things that helps us as we work through the process is being

1546 certain that consumers are educated, so if I could get that
1547 bit of information.

1548 And then when we look at the hacker attacks that are out
1549 there, some of the anonymous attacks, some of those, there is
1550 one in the news today, I think there are five people that
1551 they are bringing forward on charges. What kind of
1552 government-imposed performance requirements would help keep
1553 pace with some of the technological evolution that you are
1554 seeing in these cyber attacks? And if we were to do a
1555 government top-down sort of structure to try to deal with
1556 cyber enemies, would that be giving a signal to that cyber
1557 enemies? Is that kind of too much information for them to be
1558 able to work around?

1559 So those are the questions that I would love to hear
1560 from you on--the trends, the costs, what we are doing, what
1561 we are not doing, dealing with consumers, how you are
1562 educating them and then looking at the attacks, the cautions
1563 you would give to us there, and with that, anyone that wants
1564 to respond?

1565 Mr. {Livingood.} Sure, I can go first, and I will try
1566 to be quick so that others can answer. In terms of the
1567 positive things that government can do, I think making
1568 information sharing easier, there are a number of things
1569 there to help. I think that government has a role to play in

1570 education, whether that is PSAs or other kinds of education
1571 for, you know, end users, for citizens. I think there is
1572 also an opportunity to help incent or fund additional R&D. I
1573 know that NIST and other groups try to do research and
1574 security and other Internet futures. I think there is more
1575 than can be done there that is important.

1576 And in terms of things to be careful of or be aware of,
1577 I think it is to be aware of mandates and be careful of
1578 mandates. I think we don't want to be focused on checklists
1579 and compliance. We want to be focused on innovation and the
1580 threats of tomorrow, not sort of the threat today.

1581 Mrs. {Blackburn.} Thank you. Anyone else?

1582 Mr. {Olsen.} Well, I could just make two comments.
1583 Several of the questions and comments today mentioned
1584 incentives. I can tell you as an IT professional, we are
1585 heavily incented to make sure that we are protecting not only
1586 our internal resources but all of our partners that are
1587 interconnected with our systems. I think one of the things
1588 that is a little scary so far is, we monitor all of our
1589 customer service channels, our call centers, stores, website,
1590 and we are not seeing a lot of requests from our customers
1591 concerning their own security of their handsets and devices.
1592 So I think education is certainly going to be important. I
1593 think there is just not a general awareness in the consumer

1594 population how big an issue this is.

1595 Mrs. {Blackburn.} Okay.

1596 Mr. {Mahon.} Maybe a comment more around why it is so
1597 difficult to regulate this arena. We have been speaking here
1598 rather generically about mobile devices and cybersecurity
1599 threats, but it is a much broader problem depending on what
1600 category you are looking at and because there are multiple
1601 categories of threat actors trying to be--finding a solution
1602 in a prescriptive way is very difficult. If you think about
1603 who is coming at you and why they are coming at you, could
1604 have a nation-state coming at you for all sorts of reasons.
1605 They could be coming at the Federal Government for military
1606 reasons but that same nation-state could be coming after a
1607 corporation for intellectual property, everything from
1608 understanding that intellectual property is not just a 50,000
1609 corporate environment, it could be in a 50-person law firm
1610 doing your M&A activity for you. So you have that broad
1611 landscape if you are looking at nation-states.

1612 If you are looking at criminal activity, sure, you have
1613 what used to be the script kiddy doing something that was
1614 relatively harmless and maybe at best you have hired them
1615 today as your network administrator if they grew up, but on
1616 the other hand, you have organized crime looking at more
1617 broadly the world and how does it make money. If you look at

1618 the recent FBI investigation of the DNS-changer malware that
1619 infected hundreds of thousands of computers, then you can
1620 take a look at your anonymous and others that are more
1621 hactivists trying to make a point, and then you come down to
1622 your insider threat in your companies that are doing it to
1623 you.

1624 So if you think about that landscape and the data that
1625 they are after, they are after it for sometimes different
1626 reasons. When you try to put a regulatory overlay on that,
1627 it is very difficult to put us in a position to respond to
1628 those kind of four broad categories, and then at the same
1629 time make sure we have our checklist compliance programs
1630 going. Thank you.

1631 Mrs. {Blackburn.} Thank you. Yield back.

1632 Mr. {Walden.} The gentlelady is yielding back and now
1633 recognize the gentlewoman from the Virgin Islands, Dr.
1634 Christensen.

1635 Dr. {Christensen.} Thank you, Mr. Chairman. Good
1636 morning, everyone. Thank you for being here.

1637 I have a couple of questions. Let me begin with Mr.
1638 Amoroso. You suggest in your testimony that Congress define
1639 the roles of the various executive branch agency in
1640 cybersecurity. Where do you see the FCC as an independent
1641 agency playing a role?

1642 Mr. {Amoroso.} Well, I don't--I mean, I don't think
1643 there is an agency right now that is in a good position to
1644 come in and solve a problem that we can't solve ourselves. I
1645 mean, if it really was the case where you could write out
1646 these five things that we should all be doing and for
1647 whatever reason--negligence, ignorance, whatever--we are not
1648 doing it, then you really do need somebody in government to
1649 shake us, you know, into action. The problem is that we
1650 don't know what it is that you should be telling us we should
1651 be doing. That is why we are pointing to innovation as the
1652 key. So it is almost kind of a moot question, whether it
1653 should be DHS or FCC or whomever because I am not really sure
1654 what they should be telling us. That is the problem. And
1655 there are some things, like I said, I am part of the team
1656 trying to make recommendations. I am not--you know, I don't
1657 want to lead you to believe that we are just kind of punting.
1658 It is such a hard problem. But I would just say from an
1659 agency perspective, if there was an obvious set of things
1660 that should be done right now, I am kind of thinking the
1661 groups that are here would be doing it. You know, we are
1662 incented to do that. That is the problem. So I hope that
1663 addresses the question.

1664 Dr. {Christensen.} Okay. Yes, thank you for that
1665 answer.

1666 Mr. Livingood, you mentioned that Comcast is an active
1667 participant on the FCC's Communications Security, Reliability
1668 and Interoperability Council. So could you just describe for
1669 us how you envision the council's contributing to the
1670 improvements in cybersecurity, especially with respect to the
1671 types of attacks that the council is addressing--botnets,
1672 Internet route hijacking, the main name fraud, et cetera?

1673 Mr. {Livingood.} Sure. There are a number of working
1674 groups. I am on one. One of the folks that works for me,
1675 Mike here, is a chair of one of them, and they focus on
1676 things like the security of the routing infrastructure,
1677 DNSSEC and a whole range of other things, and I think that,
1678 you know, that is a process that works pretty well. People
1679 voluntarily get involved and they work together on what they
1680 think the current best practices are, and that is a process
1681 that repeats regularly every year so that it is not static
1682 and it is not sort of--you know, in 2008, we came up with
1683 some best practices and that is what we are still focused on.
1684 It is something that gets renewed and refreshed all the time
1685 and so we can look at every new threat as it comes out, and
1686 that is one of many places that we all work together. You
1687 know, there are lots of others--the North American Network
1688 Operators Group, Message Anti-Abuse Working Group and a whole
1689 range of others, other acronyms that I could go on for

1690 minutes about. But I think groups like that are good because
1691 they are consensus-based, they are voluntary and they are
1692 focused on best practices and really current issues.

1693 Dr. {Christensen.} And while your customers are mainly
1694 using your service for in-home computers, they also use the
1695 WiFi networks and cellular networks to access Comcast email
1696 and other Comcast video products, so how do you continue to
1697 ensure the same cybersecurity protections you develop for
1698 your core services extend to these uses as well?

1699 Mr. {Livingood.} So a number of our security
1700 protections are things that a customer can download and
1701 install on their device like their home computer, but we have
1702 a bunch of things that are on our network like our Constant
1703 Guard system, which is a bot intelligence and other security
1704 threat system, and that is there for customers that might
1705 just be bringing a device into their network, maybe it is a
1706 friend that is visiting their house and they are on their
1707 WiFi network and they happen to talk, say, a botnet, you
1708 know, we will see those kinds of things. And so, you know,
1709 we can alert customers to that. So whether they have
1710 installed software that we have provided on their device or
1711 not, we still have tools in the toolbox to identify that and
1712 help them--you know, tell them about it and help to solve it.

1713 Dr. {Christensen.} Mr. Amoroso, you stress the need to

1714 foster informations sharing, and we have talked about that a
1715 lot here between the government and private industry as well
1716 as among private companies. What protections do you think
1717 are necessary to protect civil liberties and consumer
1718 privacy, and what do you believe would be the reasonable
1719 boundaries to liability protections and antitrust exceptions?

1720 Mr. {Amoroso.} Well, the issues you raised are the
1721 reason we have those impediments now because, I mean, I am an
1722 American, I want civil liberties, I want all those things, so
1723 that is the current state, that we have swung the pendulum in
1724 the direction of making absolutely certain that we are
1725 protecting civil liberties. That is a good thing. So the
1726 question is, how do we somehow preserve those liberties and
1727 also allow all of us, you know, to know if there is some
1728 malware thing. I really think we have to figure that one
1729 out. I am not sure I can give you a real good answer on how
1730 we do it, but I think it has to be a pretty high priority
1731 because the motivation, everybody's shakes and goes yeah, if
1732 there is not malware, there is not really a civil liberties
1733 issue, Comcast should know that blah, blah, blah is a problem
1734 and they can code that into their system.

1735 So somehow we just have to maybe get the lawyers out of
1736 the room and come up with some kind of a commonsense
1737 approach. But that is the reason, all the things you listed.

1738 That is why we can't take those signatures today.

1739 Dr. {Christensen.} Thank you.

1740 Thank you, Mr. Chairman.

1741 Mr. {Walden.} Thank you, Dr. Christensen.

1742 Dr. Amoroso, you should have seen the people shake
1743 behind you when you said get the lawyers out of the room.

1744 Let us go to Mr. Bass from New Hampshire.

1745 Mr. {Bass.} Thank you very much, Mr. Chairman.

1746 I have a couple questions for Mr. Livingood, but before
1747 I ask those questions, can I ask a mobile or smartphone
1748 question for dummies? Is there a difference in cybersecurity
1749 issues between an iPad or a smart device like this and a
1750 laptop or desktop computer? Make it quick, because I want to
1751 ask some other questions. Can anybody answer that question
1752 for me?

1753 Mr. {Amoroso.} Well, there is probably a firewall
1754 between your PC at work or something on a wired land so we
1755 can do more filtering and policy control. With your
1756 wireless, you go direct to us, to the ISP, and we have been
1757 incented and led, you know, particularly in Washington, push
1758 the packets, don't look at them, don't do anything, God
1759 forbid you impose any kind of policy or filtering, so we do
1760 nothing, so your connection from wireless is directly to the
1761 Internet whereas your wired connection probably has some IT

1762 group at work.

1763 Mr. {Bass.} So is this unit here exposed to bots and--
1764 is there a cybersecurity issue associated with my iPad?

1765 Mr. {Amoroso.} I don't know what you are connected to,
1766 but yes.

1767 Mr. {Bass.} Well, let us say I am connected to Comcast,
1768 which is what I am connected to.

1769 Mr. {Livingood.} Yes, there sure are those issues and,
1770 you know, I think those are a new class of device, and a lot
1771 of the hackers and other criminals, they are very focused on
1772 return on investment. They are focused where the biggest
1773 platforms are and so the more that those devices get out
1774 there, the bigger target that makes and so they will see,
1775 okay, I can spend a couple of days developing this and I have
1776 got a few million devices. So you will start to see more and
1777 more of those things, and depending upon the tablet that you
1778 have, some are more vulnerable at the moment than others,
1779 but, you know, that is something that a lot of Americans are
1780 buying and so that will be the next threat. It will be those
1781 type of devices.

1782 Mr. {Bass.} Who is responsible? Is Apple responsible
1783 for this or are you?

1784 Mr. {Livingood.} Well, I think it is a variety, so I
1785 think with that device, Apple plays a role. With the Android

1786 devices, Google plays a role. And then all the software
1787 vendors that make the apps that go on that play a role. But
1788 there is also a component of customer education, and I am
1789 sure over time, you know, just in the same way that we have
1790 software that runs on PCs to provide security, you know, that
1791 is going to start to develop and evolve for tablets and
1792 provide that extra level of security as well. We are at the
1793 early stages of that adoption curve.

1794 Mr. {Bass.} And the same is true for BlackBerry, right?

1795 Mr. {Tetzke.} Well, I mean, all of the tablets are
1796 going to have different risks and different threats, and we
1797 look at it in terms of how we protect our platform. But the
1798 theme that I keep hearing over and over, and I think it is
1799 one that this committee has really highlighted, is the need
1800 for education, right, and when you talk about computer
1801 security, one of the inevitable comparisons is to driving a
1802 car, right? We don't let people drive a car without a
1803 license but we let them get on the computer, connect to the
1804 Internet and download software without really understanding
1805 what those risks are, and that piece of education--I am not
1806 suggesting we license people to use a computer but we do need
1807 a level of sophistication and education in how we inform
1808 people of risks that they have when they connect a device.

1809 Mr. {Bass.} Fair enough. I just want to ask a couple

1810 questions about the Constant Guard Protection Suite. I note
1811 in your testimony, Mr. Livingood, on page 6, it says ``At
1812 Comcast, we understand that securing cyberspace is a complex
1813 task'' and so forth. ''Education, prevention, detection,
1814 remediation and recovery are the core objectives of our anti-
1815 malware efforts.'' Does Comcast require its customers to
1816 download the Constant Guard Protection Suite, and if not, how
1817 is the customer going to know that it exists and how are you
1818 going to notify them that they have a problem?

1819 Mr. {Livingood.} So it is not required that a customer
1820 download that to use our service. You know, they just have
1821 to have normal Internet connectivity to do that. But we do a
1822 lot to make customers aware of that and to incent them to
1823 download it both before they have an issue and after. So
1824 before they have an issue, you know, when they are installed,
1825 they are given a lot of information about the things that are
1826 available for them and they are given links to that and so
1827 on. When they get a welcome email from us when they sign up
1828 for service, we are reiterating that for them. And we do a
1829 lot of things on our website and other places to promote the
1830 fact that these are available. Certainly after they have an
1831 issue and we notice it, we drive them to a remediation
1832 portal, and that is one of the first things that we recommend
1833 that they download is that suite and we take a number of

1834 other steps. So we do a lot of education upfront. We do a
1835 lot when they come on. We call it onboarding when they come
1836 on as a customer. And we do things while they are a customer
1837 to keep reiterating that and then afterwards.

1838 Mr. {Bass.} Real quick. It is limited to Windows
1839 operating system, correct? How long has it been around?

1840 Mr. {Livingood.} That protection suite is pretty
1841 recent. I think that is a little bit more than a year. That
1842 is a supplement to a larger anti-virus and security suite
1843 that we have had for many, many years that is--

1844 Mr. {Bass.} And real quick, because I have run out of
1845 time. What business incentives, if any, did you get or did
1846 you have in developing and offering this service?

1847 Mr. {Livingood.} Well, we view it in two ways. Number
1848 one, there is a competitive incentive if we can be seen as
1849 having more security features or more secure than the next
1850 guy, someone chooses us as their ISP rather than someone
1851 else, but the other thing is that customers when they come on
1852 board as a customer used to tell us that the two reasons were
1853 price and speed, and today, it is price, speed and security.
1854 So customers are very aware increasingly so, not aware as
1855 they need to be but very aware these days about security.
1856 They ask about those things when they call us up to order
1857 service. And so we view it as a competitive feature that we

1858 need to add, and that is why all of the things that we are
1859 doing as part of Constant Guard, DNSSEC and other things, are
1860 important to us.

1861 Mr. {Bass.} Thank you, Mr. Chairman.

1862 Mr. {Walden.} Thank you.

1863 Now we go to Chairman Dingell for 5 minutes.

1864 Mr. {Dingell.} Mr. Chairman, thank you.

1865 Gentlemen, we have much to do in little time, so I am
1866 going to try to ask questions that you will answer yes or no
1867 to starting now with Mr. Livingood. Gentlemen, you all seem
1868 to be in agreement that imposing new federal cybersecurity
1869 regulations on industry would stifle innovation and harm
1870 industry's ability to protect consumers from cyber threats.
1871 Is that correct, yes or no, starting with you, Mr. Livingood.

1872 Mr. {Livingood.} Yes, I am concerned about that.

1873 Mr. {Dingell.} Mr. Amoroso?

1874 Mr. {Amoroso.} Yes.

1875 Mr. {Dingell.} Sir?

1876 Mr. {Mahon.} Yes.

1877 Mr. {Dingell.} Sir?

1878 Mr. {Olsen.} Yes.

1879 Mr. {Totzke.} Yes.

1880 Mr. {Dingell.} Now, gentlemen, let us assume for a
1881 moment that the Congress will pursue the no-regulation path

1882 in this matter and instead facilitates greater information
1883 sharing about cyber threats between industry and the
1884 government. Would that be your collective preference? Yes
1885 or no.

1886 Mr. {Livingood.} Yes.

1887 Mr. {Dingell.} Sir?

1888 Mr. {Amoroso.} Yes.

1889 Mr. {Mahon.} Yes.

1890 Mr. {Olsen.} Yes.

1891 Mr. {Tetzke.} I would agree.

1892 Mr. {Dingell.} Gentlemen, thank you. In that case,
1893 would the Congress need to consider granting exemptions to
1894 the antitrust laws and the Federal Trade Commission Act in
1895 order to allow the companies to share cybersecurity
1896 information amongst themselves? Yes or no.

1897 Mr. {Livingood.} Yes.

1898 Mr. {Amoroso.} Yes, I think that is correct.

1899 Mr. {Mahon.} Yes.

1900 Mr. {Olsen.} Yes.

1901 Mr. {Tetzke.} I unfortunately can't comment on that.

1902 Mr. {Dingell.} Very good. Now, gentlemen, similarly,
1903 do you believe that a safe harbor provision should be created
1904 in statute to permit companies to share serious cyber threat
1905 information with government agencies without fear of class

1906 action or other lawsuits being brought against them? Yes or
1907 no.

1908 Mr. {Livingood.} Yes.

1909 Mr. {Amoroso.} Yes.

1910 Mr. {Dingell.} The reporter doesn't have a nod button,
1911 sir, so you have to say yes or no.

1912 Mr. {Mahon.} It is a yes.

1913 Mr. {Dingell.} Thank you.

1914 Sir?

1915 Mr. {Olsen.} Yes.

1916 Mr. {Totzke.} I am afraid I can't comment on that. I
1917 don't know.

1918 Mr. {Dingell.} Now, gentlemen, my last several
1919 questions have been premised on a no-regulation scenario
1920 wherein the Congress adopts legislation to promote
1921 information sharing between industry and government. Would
1922 you please submit for the record what enforcement tools you
1923 believe the Federal Government would have in this scenario to
1924 ensure that industry is adequately guarding and being guarded
1925 against cyber threats? I am asking to make a submission
1926 there for the record because of the shortness of time.

1927 Now, gentlemen, let us assume that the government would
1928 have some role in promoting cybersecurity in the private
1929 sector. If the Federal Government were to require the

1930 promulgation of cybersecurity standards, should such
1931 standards preempt State laws? Starting with you, Mr.
1932 Livingood, yes or no?

1933 Mr. {Livingood.} Yes. It is easier to have one
1934 standard.

1935 Mr. {Amoroso.} Yeah, I don't know. I am not sure. I
1936 haven't really thought that one through.

1937 Mr. {Dingell.} And you, sir?

1938 Mr. {Mahon.} Yes.

1939 Mr. {Dingell.} Sir?

1940 Mr. {Olsen.} I will have to agree with Dr. Amoroso. I
1941 haven't really considered that.

1942 Mr. {Totzke.} Yes, and I can't comment on that either.

1943 Mr. {Dingell.} Now, gentlemen, I have read with some
1944 interest in Mr. Olsen's testimony that, and I quote, ``the
1945 ongoing evaluation or MetroPCS's security program is based on
1946 periodic internal and third-party assessments and auditing.``
1947 Would your respective companies object if such audits were
1948 government mandated? Yes or no.

1949 Mr. {Livingood.} No, we already provide all those
1950 things already. We already do that.

1951 Mr. {Amoroso.} I think we would object, yes.

1952 Mr. {Mahon.} We would object.

1953 Mr. {Dingell.} You would object?

1954 Mr. {Totzke.} Yes, we would.

1955 Mr. {Dingell.} All right. And then let me come back
1956 and ask you to explain that, if you please?

1957 Mr. {Totzke.} Yes, we would probably object but we do
1958 this anyway. We always do that.

1959 Mr. {Dingell.} Now, those who have indicated no, would
1960 you please explain briefly?

1961 Mr. {Amoroso.} I can explain. When you write a law, we
1962 do paperwork, so I take people away from doing their day-to-
1963 day work to sit and do work. We have an ops lab, and one of
1964 our favorite things to show people in the ops lab is along
1965 one of the walls, we have got about a mile's worth of ring
1966 binders and they always say there is the government paperwork
1967 followed by a lot of sort of chuckling laughter, but it is
1968 true. You know, we do have a great of paperwork that we fill
1969 out, you know, when we are dealing with different federal
1970 groups or Sarbanes-Oxley or whatever. There is a lot of
1971 paperwork, so I am just suggesting that if we are already
1972 doing it and government comes in and says I need you to fill
1973 out this compliance checklist, you are taking people away
1974 from the work to do paperwork. That is why we would object.

1975 Mr. {Livingood.} Very quickly, if I can just make a
1976 note very quickly. I think this is dangerous sending an
1977 engineer sometimes, but I am told that we might have

1978 objections. We would object and have the same concerns.

1979 Mr. {Dingell.} Gentlemen, thank you.

1980 Mr. Chairman, thank you for your courtesy.

1981 Mr. {Walden.} Mr. Chairman, thank you for your
1982 questions. I think you got to the heart of the matter
1983 quickly.

1984 We now turn to the chairman of the House Intelligence
1985 Committee and a very important member of our Subcommittee,
1986 Mr. Rogers.

1987 Mr. {Rogers.} Thank you, Mr. Chairman. Thanks for
1988 having the hearing. Thanks to the witnesses as well.

1989 I think one of the big problems that we run into in this
1990 is that we haven't really sounded the alarm bell. I think in
1991 all of the circles of people who look at this every day, all
1992 the security shops, the IT security shops across America,
1993 they know what the problem is. Average users don't see it,
1994 and that is why there is no hew and cry, I think, yet about
1995 how we get this fixed. But I appreciate all your comments
1996 today.

1997 You talked, each of you, about the importance of
1998 information sharing and keeping it as clean and simple as you
1999 can. Talk about how that would work. So if we bring the
2000 folks together, we are sharing the government secret sauce
2001 with you all and you are sharing back malicious ware that

2002 maybe the government is not aware of, talk about how fast
2003 this is. There is a lot of talk about civil liberties, and I
2004 think people have this visual that people are reading emails,
2005 some guy named Bob in Cleveland is reading everybody's email
2006 to find this malicious software. It is not how it works. As
2007 a matter of fact, if that happens, it is a miserable failure.
2008 Can you talk just a little bit about how you envision that
2009 that would with the sharing arrangement, real time, no
2010 regulatory, all voluntary? Can you talk about that quickly?

2011 Mr. {Amoroso.} Yes, I would be happy to. First of all,
2012 I want to compliment you on your legislation. I think that
2013 there is some real nice elements in the work you have done.
2014 First of all, real time, absolutely. Independent auditable,
2015 I think is important so that somebody can come in and look a
2016 the way this is done, but it also has to be controlled like
2017 blasting it out, you know, over the Internet would be a
2018 really bad idea but I think you need the balance, right, this
2019 real time but also the ability to come back and look at the
2020 process, make sure it is transparent without, like I said,
2021 exposing it to our adversaries. That is the right way to do
2022 it.

2023 Mr. {Mahon.} There is also different levels of sharing
2024 by industry. I think you have to look at how you do your
2025 risk assessments on each category that I previously described

2026 but there is also right now a very good example out there of
2027 what is working well, and that is the defense industrial base
2028 pilot that is going on, and that particularly is supporting
2029 defense contractors and DOD, but you can expand that to the
2030 financial services industry and other industries.

2031 Mr. {Rogers.} And just for clarification, when we talk
2032 about real time, I have seen numbers as high as 100 million a
2033 second, the packets of information flying around. So if this
2034 is going to work, the malicious source code has to be
2035 compared at an incredibly fast rate. Can you talk about that
2036 from an engineering perspective? Anyone?

2037 Mr. {Livingood.} So I think one of the challenges is
2038 trying to do any kind of pattern matching. A lot of the
2039 malware that we see and have seen for a number of years is
2040 sort of what is called polymorphic where it changes. Every
2041 individual, you know, instance of it is different from the
2042 next so a lot of stuff changes. It is not like it is with
2043 anti-spam where you can match on a few key words or a file
2044 attachment and know, you know, that is it, that the target
2045 and flag it that way. So you need to come up with ways, and
2046 a number of us have systems like this and there are others
2047 that are in development that can do this on a wider basis,
2048 but that is the very challenge that you are getting at, which
2049 is doing that in real time. It is incredibly difficult and

2050 you are at the edge of computer science at that point.

2051 Mr. {Rogers.} Which is why I think many of you have
2052 told us before the legislation was written, be careful about
2053 the regulatory scheme. If we slow you down, if we give you
2054 another row of books down your mile-long hallway there, it
2055 doesn't work. I mean, we already have outdated what you are
2056 trying to accomplish in the room, and this is a value added
2057 not only for you but for the government, is it not? The
2058 government also gets benefit from the protection of all of
2059 your great work in the private sector, correct?

2060 Mr. {Livingood.} That is correct, and there are two
2061 things that I think that raises that are interesting. One
2062 is, by the time that a very prescriptive law would be
2063 written, by the time that ink was dry, the threats would have
2064 moved on and so you have got to be able to be flexible. The
2065 other is that we all need to have, you know, with our
2066 software developers and security specialists, you know, they
2067 need to be hard at work in a room, not with half a room full
2068 of lawyers with them slowing them down and asking questions
2069 about, you know, why are you doing this and that. They need
2070 to be at work every day trying to solve this problem.

2071 Mr. {Rogers.} And I have to say for the record, this
2072 may be my favorite panel of all time since I have been in
2073 Congress. Never so often have a group of engineers belittled

2074 lawyers at the table. You have warmed my heart today. We
2075 have faith that we are moving forward.

2076 I wish we had time to talk about all the issues. I am
2077 very curious about how you would fix the programming issue, a
2078 huge problem for us as we move forward. We didn't talk about
2079 exfiltration, which is very difficult for any of you to
2080 catch, which I would argue right now is the single greatest
2081 threat to our economy moving forward, aside of the things
2082 that we know today.

2083 Mr. {Walden.} Would the gentleman yield?

2084 Mr. {Rogers.} Yes.

2085 Mr. {Walden.} Could you outline exfiltration?

2086 Mr. {Rogers.} Sure. It is--we know that nation-states
2087 today are engaged in getting on to your network lurking.
2088 They will be there for a very long time. You don't know it.
2089 Your system administrators don't know it. These folks can't
2090 catch it. Sometimes the government--a lot of times the
2091 government can't catch it either. And then they will latch
2092 on to that intellectual property that is on everybody's
2093 computer today, all those designs, everything that is of
2094 value to that company, and at the right time at the right
2095 speed, they latch on to it and run like heck through your
2096 network and take it back. And we know a country like China,
2097 who is investing in this as a national strategy to exfiltrate

2098 intellectual property and then directly use that intellectual
2099 property to compete against United States businesses, and
2100 unfortunately, it is happening at a breathtaking pace,
2101 breathtaking pace, and what is concerning is, these folks are
2102 looking for malicious software that is disruptive or theft-
2103 oriented. This is very sophisticated, as sophisticated as
2104 any you will see, and incredibly hard to detect, and they
2105 really don't want to break anything. They want to get in and
2106 steal it without you knowing it, and that is what is so
2107 troubling about it.

2108 Hundreds and hundreds of thousands of jobs are lost
2109 every year for the theft of that intellectual property that
2110 is being reprogrammed commercially against U.S. companies.
2111 This is as big a problem as I have ever seen and it is one of
2112 the many things that keeps me up at night, Mr. Chairman, so
2113 thanks for letting me explain it, and it is something we
2114 didn't really get into today because that is really not the
2115 focus of what they can even watch. So that is why this
2116 information sharing I think is so important. It would help
2117 American businesses by the Federal Government having
2118 information and being able to identify that code, share it
2119 with the right partners. It is amazing what we would be able
2120 to stop.

2121 Mr. {Walden.} With the indulgence of the Committee

2122 members, perhaps given the importance of that topic you could
2123 each if you have anything you want to add on that area, and
2124 then we will go to Mr. Stearns and Mr. Gingrey. Does anybody
2125 want to comment on that?

2126 Mr. {Amoroso.} I will. It is called advanced
2127 persistent threat, and he has got it exactly right. It is
2128 somebody targeting any of you, like we know the folks that
2129 you run around with, we can craft a fake email that looks
2130 pretty realistic, point you to one of these websites that
2131 establishes a tunnel. It drops a remote access tool on your
2132 PC. You know how you log in when you do remote access from
2133 work or from home, wherever you are doing it? This is the
2134 hacker now doing remote access to you. You are now the
2135 server, and once they are on, they can troll around your PC,
2136 your network and so on, and the intellectual property theft
2137 has become significant. It is probably the number one thing
2138 I bet all of us, you know, when we go back, we talk about bot
2139 nets here and we talk about DNS, but that is not what we deal
2140 with when we go back to the office. We are dealing with APT,
2141 which is kind of our point, right? We are head of the
2142 discussions here, things that we have been dealing with in
2143 the past and the things we deal with now are probably things
2144 we will be here testifying about 5 years from now, so that is
2145 an issue.

2146 Mr. {Totzke.} And just to echo Dr. Amoroso, the
2147 advanced persistent threat, I mean, these are remarkably
2148 sophisticated adversaries. They are slow. They are patient.
2149 They will lurk on your network for years. And, you know, I
2150 from our Canadian headquarters. We had a large company go
2151 out of business, Nortel, and part of the attribution of that
2152 is loss of their intellectual property to a foreign state-
2153 level adversary, you know, siphoning secrets right off their
2154 network.

2155 So when you look at that, this is a serious concern. As
2156 Ed mentioned, 5 years from now, you will probably be looking
2157 at that. That is how advanced they are. It is great that
2158 you are looking at it now, Congressman, because the threat is
2159 real, it is persistent today, and as you stated, it is a
2160 threat to jobs and it is an economic threat to the United
2161 States and elsewhere.

2162 Mr. {Walden.} Thank you.

2163 Mr. {Rogers.} Thank you, Mr. Chairman, and just for the
2164 record, I want to thank Mr. Mahon for his 30 years of FBI
2165 service as well. Thank you for all the time you have put on
2166 the target, sir. Thank you.

2167 Mr. {Mahon.} Thank you.

2168 Mr. {Walden.} You would think Rogers was a former FBI
2169 agent himself.

2170 Let us go to Mr. Stearns now.

2171 Mr. {Stearns.} Thank you, Mr. Chairman.

2172 Let me take my questions a little bit along the lines
2173 that my colleague from Michigan talked about when he talked
2174 about advanced persistent threat. Dr. Amoroso, when you did
2175 your opening statement, you were speaking quite eloquently in
2176 talking about malicious software, malware, you talked about,
2177 and you painted this picture that the malware itself you were
2178 impressed how well it was developed, put together, and you
2179 sort of alluded to the fact that it was almost not
2180 unpenetratable but it was to the point you were respectful of
2181 it and were not sure we were keeping up. Is that my
2182 interpretation of what you said?

2183 Mr. {Amoroso.} That is exactly right. We are
2184 definitely not keeping up. We are trying. But think of the
2185 dizzying pace of innovation that you see out in Silicon
2186 Valley, right? I mean, new things every day. The hacking
2187 and the malicious adversary community, they are moving at the
2188 same pace so the job we have is, we have got to keep up, and
2189 you would say hey, guys, you better be ahead of them like not
2190 even enough to just kind of keep up, you better be ahead. So
2191 we are always going to be sort of biased.

2192 Mr. {Stearns.} So you are saying you are always
2193 catching up?

2194 Mr. {Amoroso.} Let us go faster. We have to innovate.
2195 We have to go faster.

2196 Mr. {Stearns.} Is that true, you think you are always
2197 catching up then? That is what you implied to me by saying
2198 the respectability you had for this malware.

2199 Mr. {Amoroso.} Yes.

2200 Mr. {Stearns.} Is this true for adware, spyware,
2201 grayware, all these others? Is it also applicable to that
2202 too?

2203 Mr. {Amoroso.} Yes. APTs are the best, right? I mean,
2204 APT, this exfiltration point that the Congressman spoke
2205 about, that is the elite kind of attack vector in 2012.

2206 Mr. {Stearns.} Okay.

2207 Mr. {Amoroso.} Spyware, maybe not so much.

2208 Mr. {Stearns.} Now, with the malware, who are these
2209 people that are doing this specifically? Can you name them?

2210 Mr. {Amoroso.} I can't. I am not law enforcement. You
2211 might--

2212 Mr. {Stearns.} Is there anybody on the panel--when Dr.
2213 Amoroso talked about this malware so respectfully and how
2214 eloquently it is put together, can anybody tell who we are
2215 talking about?

2216 Mr. {Mahon.} I think if you take a look at the most
2217 recent investigation conducted by the FBI on the DNS malware,

2218 you will see that was a group of individuals operating out of
2219 Estonia that basically sent malware to individuals in various
2220 forms in emails, and you clicked on it and it infected your
2221 computer in a way that it directed you when you went out to
2222 do a DNS-type search, you were looking for, I don't know,
2223 Amazon.com or some other company, you really went to their
2224 servers and their own servers were actually embedded in
2225 various locations in the United States.

2226 So these are organized crimes. They have figured out
2227 how to capitalize on the money you can make with the malware.

2228 Mr. {Stearns.} Are these people, for example in
2229 Estonia, are they part of a mafia, underground, an
2230 organization that is larger than just in Estonia, without you
2231 revealing any--

2232 Mr. {Mahon.} These are no longer just individual
2233 hackers. Individual hackers are out there but now they have
2234 actually formed themselves into types of federations to work
2235 together.

2236 Mr. {Stearns.} Across the world?

2237 Mr. {Mahon.} You can do it across the world. There are
2238 a certain hacking groups you can join and be a member from
2239 different countries.

2240 Mr. {Stearns.} So it is like a fraternity? You say I
2241 am a member of the Estonia--

2242 Mr. {Mahon.} Estonia just seems to be a hotbed right
2243 now, I think because of how the economy is run over there.

2244 Mr. {Stearns.} Anyone else?

2245 Mr. {Livingood.} If I could add to that, I think it is
2246 actually pretty interesting. This is a very large and very
2247 well organized underground economy. They are specialized.
2248 They have some people that write tools, other people that
2249 rent access to bot networks so you can rent botnets by the
2250 hour. You can tell them where you want people--where you
2251 want the bots to be, what kind of computers, you know,
2252 payment network mechanisms between these parties. So it is
2253 very sophisticated and, you know, if you think about from a
2254 criminal standpoint, it is a lot easier to get a return on
2255 investment on this type of thing than it is to go out and do
2256 physically oriented sort of crimes, and the scale is so much
2257 larger. These are folks that operate across borders
2258 internationally and there is just an enormous amount of, you
2259 know, economic incentive for them to do it, and it unlike
2260 APT, at least in some respects, this is primarily an economic
2261 crime. APT is focused certainly on economics but more on
2262 intellectual property or embarrassing companies. This is all
2263 about the money.

2264 Mr. {Stearns.} Well, I guess, Mr. Mahon, is there a
2265 possibility that we have terrorists involved with this that

2266 are part of Estonia? The terrorists could go to this group
2267 or this federation across and are using them? Is that--

2268 Mr. {Mahon.} Absolutely. Terrorists use these types of
2269 schemes for funding. Number one, they need funding for their
2270 operations. And number two, they use it just as a
2271 communications system. They know they are being looked at.
2272 So the ways they need to communicate are surreptitiously in a
2273 manner that they can't be intercepted, so they use these
2274 types of technologies to communicate with one another, but
2275 they have to fund their operations.

2276 Mr. {Stearns.} I guess the basic question is, and this
2277 is probably the premise of understanding what this hearing is
2278 all about, what could we as legislators on this subcommittee
2279 or the full committee or Members of Congress, what can we do
2280 to make it easier for you to operate and at the same time
2281 give you the wherewithal to compete and what should we not
2282 do? What should we do and what should we not do? And just
2283 as a closing statement, Mr. Livingood, if we could just go
2284 down the panel and each give what we should do and what we
2285 should not do, that would be helpful.

2286 Mr. {Livingood.} Sure, of course. I think what you
2287 should do is help make information sharing easier, remove
2288 those impediments. I think also there is a role for
2289 government to play in education, whether that is PSAs or

2290 other things, to raise awareness about security issues, and I
2291 think that there R&D types of things through agencies that
2292 you can help fund to focus on this.

2293 I think what you should not do is focus on mandates and
2294 compliance. That enables us to focus instead on innovation.

2295 Mr. {Amoroso.} That sounded good. I would exactly
2296 repeat those comments. I will add one additional, and that
2297 is that you do have some influence around the federal
2298 procurement process, so a lot of times we see procurements
2299 come out and we scratch our heads and say don't you think
2300 there ought to be, you know, like through GSA there is this
2301 MTIPS program, a lot of us are MTIPS vendors. There ought to
2302 be more business. There isn't. So I would recommend that
2303 that procurement process ought to be the most secure process
2304 in the entire world.

2305 Mr. {Mahon.} You know, I would echo what both of them
2306 said and just add the importance of information sharing. We
2307 have limited resources. We conduct risk assessments when we
2308 are trying to decide on impacts and probability of events
2309 based upon the information we have at the time. If a
2310 government agency or another carrier has additional
2311 information and we don't factor that into our analysis, we
2312 are really misaligning our resources and how we develop our
2313 countermeasures.

2314 Mr. {Olsen.} I think there is a lot of commonality
2315 among the panel here on what we would like to see. I think
2316 just add a little bit to the information-sharing area. I
2317 think the Federal Government has access to information
2318 through various agencies that are watching the country's
2319 cyber borders and we have seen in our company the vast
2320 majority of reconnaissance scams and attempts to gain access
2321 are coming from China and Eastern Europe, and I think the
2322 Federal Government would be in a good position to monitor and
2323 provide more information on that.

2324 Mr. {Tetzke.} Going last, I get to say I agree with
2325 everybody else on the panel here, especially I want to hammer
2326 that information sharing from government to industry. The
2327 purview that intelligence agencies have and that you have in
2328 terms of what you see is much different than what we see. So
2329 my team works with Dr. Amoroso's team on areas of commonality
2330 between RIM and AT&T where we think we have issues that need
2331 to be addressed that impact the security of our customers but
2332 we don't necessary get that feedback from the government
2333 about what do you see that we need to be aware of, and if
2334 there is anything I could ask for, it is a more transparent,
2335 more real-time information-sharing mechanism to let industry
2336 know what government knows so we can act to protect out
2337 networks and by extension protect your information.

2338 Mr. {Walden.} Thank you.

2339 Mr. Gingrey, thanks for your patience as we have gone
2340 through the hearing. You are the last--

2341 Dr. {Gingrey.} Mr. Chairman, you took the words right
2342 out of my mouth. I think you are exacting the last measure
2343 of patience out of the last member to ask a question, but I
2344 moved down here early in the hearing, as all of you know,
2345 because I couldn't hear very well, even though the Chairman
2346 said speak right into your microphones, but I am glad I did
2347 move down close because I knew it was going to be interesting
2348 and I know that all five of you are experts who were going to
2349 have a lot of useful information to present to us, and quite
2350 honestly, after 2 hours of this, I am trying to figure out a
2351 way to beat these guys, and the only thing I can think of is
2352 an opportunity to invest in these hacking operations. I
2353 don't guess that would be legal, but if it were, I think that
2354 would probably be one of the best ways for us to win. Thank
2355 you all very much.

2356 Let me ask a couple of specific questions, and maybe
2357 this cuts a little bit to the chase of one of the main
2358 reasons why the Chairman is holding this hearing, and each
2359 one of you, please, starting with Mr. Livingood, answer this
2360 for me. Do you believe the FCC has enough cybersecurity
2361 expertise to allay the concerns that some industry

2362 stakeholders have with the Commission? If they do choose to
2363 impose cybersecurity regulations on you guys, on the network
2364 providers, do you have enough confidence in their expertise
2365 to do that, Mr. Livingood?

2366 Mr. {Livingood.} So I don't know the answer to that.
2367 You know, we work with a lot of folks at the FCC and enjoy
2368 doing that. They have a lot of expertise. Whether they have
2369 enough here, I think that is a tough question. I don't know
2370 the answer.

2371 Mr. {Amoroso.} I have said earlier, I don't think there
2372 is any agency that has the right expertise to do that. If we
2373 knew what the answer was, we would be doing it, so I don't
2374 think it is a knock on any one particular agency. I just
2375 don't think there is any agency that has that capability
2376 right now.

2377 Dr. {Gingrey.} Mr. Mahon?

2378 Mr. {Mahon.} And I would agree with Ed. The answer is
2379 no. But I don't think anyone does, and I think that is the
2380 importance of collaborative relationships. You do need to
2381 bring people in from all sorts, the federal arena as well as
2382 the private industry area to work together due to the
2383 evolving nature of the threats in this arena.

2384 Dr. {Gingrey.} Mr. Olsen?

2385 Mr. {Olsen.} Yes, it is an important question, but I

2386 would have to agree with Mr. Livingood. I don't know whether
2387 they do or not.

2388 Dr. {Gingrey.} Mr. Tetzke?

2389 Mr. {Tetzke.} Yes, I don't actually know either. I
2390 think what you are hearing here, and it is common amongst the
2391 panel, is the defender job, the job that we are trying to do
2392 to protect your information, is exceptionally hard and it is
2393 actually much more difficult than being on the other side.

2394 Dr. {Gingrey.} Yes, speaking of hedge funds.

2395 Let me go back to Mr. Olsen. In your formal testimony
2396 that you gave, you talked about the clearinghouse. I would
2397 like to know a little bit more about that specifically, and
2398 do you think that would be helpful? And maybe you could
2399 elaborate a little bit more on that.

2400 Mr. {Olsen.} I think there is really two aspects to
2401 that. One is where the Federal Government is sharing with
2402 private sector, with industry, what they are seeing as far as
2403 threats, and I mentioned a little while ago about the threats
2404 from outside the United States, so I think that is a critical
2405 component. The other is where companies should share,
2406 private companies could share information on threats that
2407 they are seeing and that clearinghouse would have to be
2408 sponsored by somebody, and I think the Federal Government is
2409 really the right place to do that.

2410 Dr. {Gingrey.} And I think you addressed also in your
2411 testimony the hold-harmless provision that would be necessary
2412 to share that information so that you wouldn't be subject to
2413 lawsuits and that sort of thing.

2414 Mr. {Olsen.} Yes, sir.

2415 Dr. {Gingrey.} I have got a little time left. I have
2416 one more question then. The Internet is currently
2417 transitioning from this Internet provider v4 to v6
2418 addressing. Does that process create any new cybersecurity
2419 issues, and will transitioning alone solve any cybersecurity
2420 issues that currently exist? Does the process of
2421 transitioning present opportunities to resolve existing
2422 cybersecurity issues? We will start with Mr. Livingood and
2423 just go down the line.

2424 Mr. {Livingood.} Sure. I think, you know, we have been
2425 a leader in IPv6. You know, I think that all of those issues
2426 that exist in the current Internet and IPv4 simply carry over
2427 to IPv6. It is just a new form of addressing. You know,
2428 that being said, because it is a new form of addressing a new
2429 technology, you are introducing new things into the
2430 ecosystem. To Dr. Amoroso's point earlier, it is a complex
2431 ecosystem. When you change something, it can have unintended
2432 consequences. And so it is something that you have to keep
2433 an eye on and make sure that you are not introducing any new

2434 vulnerabilities. But I think if there were any, it is simply
2435 because, you know, some security that worked great in IPv4
2436 might not have all the same features.

2437 Dr. {Gingrey.} Dr. Amoroso?

2438 Mr. {Amoroso.} Every device on the planet running v6 in
2439 theory would be addressable, would be routable, and that is a
2440 pretty dangerous situation, so for all of us, we have to
2441 figure out how to architect security protections around that.
2442 So I do have some concerns about the v6 transition.

2443 Dr. {Gingrey.} Mr. Mahon?

2444 Mr. {Mahon.} Yes, the architect and engineering teams
2445 are still working through this, but as they have said, you
2446 have legacy systems being married up with new evolving
2447 technology, and whenever you do that, you are going to have
2448 things evolve as you begin to deploy it.

2449 Dr. {Gingrey.} Mr. Olsen?

2450 Mr. {Olsen.} I think from a protection standpoint, I
2451 think it is a step ahead, but the bag guys are out there
2452 working just as hard as we are to find another way around
2453 that, so as soon as we make an advancement in technology,
2454 they are right out there keeping pace with us.

2455 Dr. {Gingrey.} And finally, Mr. Totzke?

2456 Mr. {Totzke.} And this just, as Ed said, expands the
2457 attack surface and by doing so increases the risk, so we have

2458 new and unknown risks that we are going to have to figure out
2459 how to mitigate.

2460 Dr. {Gingrey.} Mr. Chairman, thank you for your
2461 generosity of those 45 extra seconds, and I will yield back.

2462 Mr. {Walden.} Actually, you got close to 49. Thank
2463 you, Mr. Gingrey, for staying and participating.

2464 I want to thank all of our witnesses and all the folks
2465 behind them who I am sure played some role, but we really
2466 appreciate your insights. It is very helpful in our effort.
2467 Obviously, we are trying to do the right thing and you are
2468 out there fighting the battle every day, and we don't want to
2469 get in your way. And so we may be back to you with our
2470 working group digging a little deeper on some of these issues
2471 and getting as specific as possible. We hope to look out too
2472 at some of the other types of networks and small providers.
2473 I mean, you obviously represent major providers or a
2474 representation of them. We are also wondering about the
2475 weakest link, which might be small ISPs and how do they deal
2476 with this and do they have the same sorts of capabilities to
2477 fight back.

2478 Anyway, I deeply appreciate your willingness to be here
2479 today and share your knowledge with us. We are better for
2480 it.

2481 So with that, the Subcommittee on Communications and

2482 Technology stands adjourned.

2483 [Whereupon, at 12:13 p.m., the Subcommittee was

2484 adjourned.]