

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 ALDINGER

3 HIF039.160

4 ``CYBERSECURITY: THREATS TO COMMUNICATIONS NETWORKS AND

5 PRIVATE SECTOR RESPONSES''

6 WEDNESDAY, FEBRUARY 8, 2012

7 House of Representatives,

8 Subcommittee on Communications and Technology

9 Committee on Energy and Commerce

10 Washington, D.C.

11 The Subcommittee met, pursuant to call, at 9:39 a.m., in

12 Room 2322 of the Rayburn House Office Building, Hon. Greg

13 Walden [Chairman of the Subcommittee] presiding.

14 Members present: Representatives Walden, Terry,

15 Stearns, Shimkus, Rogers, Bilbray, Bass, Blackburn, Gingrey,

16 Latta, Guthrie, Kinzinger, Barton, Eshoo, Markey, Doyle,

17 Matsui, Barrow, Christensen and Waxman (ex officio).

18 Staff present: Carl Anderson, Counsel, Oversight; Gary

19 Andres, Staff Director; Ray Baum, Senior Policy
20 Advisor/Director of Coalitions; Nicholas Degani, Detailee,
21 FCC; Neil Fried, Chief Counsel, Communications and
22 Technology; Debbie Keller, Press Secretary; Katie Novaria,
23 Legislative Clerk; David Redl, Counsel, Telecom; Shannon
24 Weinberg, Counsel, Communication and Technology; Jeff Cohen,
25 FCC Detailee; Kara Van Stralen, Democratic Special Assistant;
26 Shawn Chang, Democratic Subcommittee Chief Counsel; and Roger
27 Sherman, Democratic Chief Counsel.

|
28 Mr. {Walden.} I am going to call the order the
29 Subcommittee on Communications and Technology. I want to
30 welcome our members and our witnesses for today's hearing on
31 cybersecurity threats to communications networks and private
32 sector responses.

33 Back in October, the House Republican Cybersecurity Task
34 Force recommended that the committees of jurisdiction review
35 cybersecurity issues. So this hearing continues our
36 committee's review of cybersecurity issues with an
37 examination of threats to communications networks and the
38 responses of the private sector. Threats to communications
39 networks have come a long way in a very short time and they
40 are very, very real and serious.

41 Before coming to Congress, I spent about 22 years as a
42 radio broadcaster, and as a small businessman, I had to worry
43 about securing our communications network, and back then, 20
44 years ago, it was relatively straightforward. You had to
45 have a fence around the tower and you couldn't let people get
46 near the transmitter and a few things like that, and every
47 once in a while somebody would come and shoot an insulator
48 out or something and you kind of got grumpy and had to repair
49 that, and every once in a while some idiot would try to cut
50 the guy wires, and those usually spun around and got them.

51 That never happened at my stations but it does happen
52 occasionally. But all of that was sort of security of that
53 wireless age. Not anymore.

54 While physical security remains important, cybersecurity
55 has also become a pressing concern. Now a small business
56 confronts a dizzying array of threats online from the Zeus
57 Trojan horse to Stuxnet, from lulzsec to botnets. These
58 threats are serious. Unless our cyber defenses hold, a bad
59 actor could drain the bank account of a business, crash an
60 online company's website, or launch a barrage of cyber
61 attacks on a company's network. Those are serious
62 consequences for any business, and especially for the small
63 businesses that are at the heart of creating new jobs in this
64 economy. And indeed, in our small business, I don't know, 10
65 years or so when we did create a computer network and put
66 everything up on digital audio, our main server was hacked
67 and taken over, and all of a sudden it started running slower
68 and slower and slower and eventually we determined it had
69 been overtaken.

70 Every month, we learn more about these cyber threats,
71 and what we have learned thus far is of great concern. I am
72 concerned that our communications networks are under siege.
73 I am worried that the devices consumers use to access those
74 networks are vulnerable, and I am concerned that our process

75 for looking at communications supply chain issues lacks
76 coordination. I am also concerned that our cyber defenses
77 are not keeping pace with the cyber threats.

78 Now, in this hearing, we are lucky to have the voices of
79 five private sector witnesses to guide us through the complex
80 issue of cybersecurity. I am hoping that you will tell me
81 that cyberspace is secure and we can all rest easy at night.
82 Unfortunately, I have read your testimony and it is not so.
83 So I expect that you will tell us that the threats to our
84 communications networks are all too real, American businesses
85 are losing dollars, jobs, intellectual property and much,
86 much more because of cyber crime and cyber espionage, and
87 that our national security is potentially at risk as well.

88 I also expect that you will explain what the private
89 sector is doing to fortify our cybersecurity defenses. The
90 private sector owns most of the critical infrastructure--the
91 wires, the servers, the towers and base stations--that make
92 up our communications networks, and they are on the front
93 lines of cybersecurity. So I want to know what cybersecurity
94 services are being offered to consumers, what protections are
95 being deployed in our communications networks, and what
96 affirmative steps the private sector has taken to lock down
97 the supply chain and to combat cyber crime.

98 I also expect to hear what you think the appropriate,

99 and underscore ``appropriate'' the federal role is. Are
100 federal laws and regulations helping or interfering with
101 information sharing? Are federal regulations of
102 cybersecurity practices appropriate, and if so, how? Should
103 the federal government be providing incentives for Internet
104 service providers and other members of the private sector to
105 invest and innovate in the cybersecurity arena? And how
106 should our country's fiscal state shape our discussion of the
107 federal role?

108 These questions and others will form the basis for
109 deciding what cybersecurity legislation, if any, is needed in
110 the near term, and how we can best secure cyberspace in the
111 long run. So I want to thank the panelists today for taking
112 time out of your schedules to be here to help inform this
113 important subcommittee, the Energy and Commerce Committee, on
114 what we should do and how we can be better informed in doing
115 our job.

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

117 ***** COMMITTEE INSERT *****

|
118 Mr. {Walden.} With that, I would recognize the
119 gentlelady from California, the ranking member of the
120 subcommittee, Ms. Eshoo, for an opening statement.

121 Ms. {Eshoo.} Thank you, Mr. Chairman, for convening
122 this morning's important hearing, and I want to welcome the
123 witnesses and I am especially pleased that Juniper Networks
124 and McAfee, two outstanding Silicon Valley companies, are
125 here to talk to us about tackling the challenges of
126 cybersecurity this morning.

127 We all recognize the serious threat to our Nation's
128 communications networks. Since 2006, the number of federal
129 cybersecurity incidents reported to the Department of
130 Homeland Security has increased by 659 percent. That is a
131 whopping number. And the economic impact of these incidents
132 is equally significant. A recent study by the Ponemon
133 Institute estimated that the median annualized cost of cyber
134 crime to a victim organization is \$5.9 million per year, an
135 increase of 56 percent from 2010.

136 The more we rely on the Internet to conduct our
137 business, the more vulnerabilities we create for hackers to
138 exploit. Having served as a member of the House Intelligence
139 Committee for 8 years, I am very well aware of the threat,
140 not just from criminal hackers but also obviously from other

141 countries. But talking about the problem is not enough. We
142 need to act, and that requires the help of both the private
143 sector and the federal government. The private sector really
144 represents 95 percent of this, the federal government the
145 other 5 percent.

146 One of the first steps to tackling this growing threat
147 is, I think, education and training. Whether at home or in
148 the workplace, every American should understand what they can
149 do to protect themselves against a cyber attack. Improved
150 information sharing is also a key aspect of our Nation's
151 response to cybersecurity. If we are going to ask industry
152 to report cybersecurity incidents to the government, then we
153 need to establish a clear process to do so.

154 I am pleased to support our colleague Mike Rogers'
155 effort, the Cyber Intelligence Sharing and Protection Act of
156 2011. That is one of three or four bills in the House.
157 There are least three or four in the Senate as well.

158 It is also important to recognize the timely alerts to
159 consumers and businesses can be the difference between an
160 isolated cybersecurity incident and one that impacts millions
161 of users. A voluntary ISP code of conduct currently being
162 developed by the FCC is one of the proposed ways to alert
163 consumers when a botnet or other malware infection is
164 discovered.

165 Today's hearing is a very important opportunity for us
166 to better understand our subcommittee's role in cybersecurity
167 including what role the FCC and NTIA should play in
168 protecting our Nation's communication networks and how the
169 private sector and other federal agencies should interact
170 with them.

171 So thank you to all of the witnesses, those that come
172 from Silicon Valley to instruct us, and what remaining time I
173 have I would like to yield to Mr. Markey.

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

175 ***** COMMITTEE INSERT *****

|
176 Mr. {Markey.} I thank the gentlelady.

177 Last week, FBI Director Robert Mueller testified that
178 cyber threats will soon surpass terrorism as the number one
179 threat facing the United States. We know from the Department
180 of Homeland Security that there have already been threats to
181 the utility sector. We also know that Russia and China have
182 probed our electricity grid to find vulnerabilities.

183 Our economy hinges on a reliable flow of power with
184 losses that go into the billions of dollars with every major
185 blackout. Our national security also depends upon it since
186 99 percent of the electricity used to power our military
187 facilities including critical strategic command assets comes
188 from the commercially operated grid.

189 Last September, I asked all five commissioners from the
190 Federal Energy Regulatory Commission under our jurisdiction
191 to name the number one threat to electricity reliability.
192 All five commissioners agreed, cyber threats are the number
193 one threat to the grid.

194 In 2009, the full Energy and Commerce Committee
195 unanimously passed the GRID Act, which I authored along with
196 Chairman Upton. That bill gave FERC the authority to quickly
197 issue grid security orders or rules that vulnerabilities or
198 threats have not been adequately addressed by the industry.

199 It was killed in the Senate. All five FERC commissioners
200 also agreed that giving FERC this authority would increase
201 America's ability to secure our electric grid.

202 With cyber threats growing by the day threatening our
203 security and our economy, it is imperative that this
204 committee pass the GRID Act so that we can move it forward
205 and empower the FERC to move quickly to safeguard the
206 electric grid from cyber threats that are not sufficiently
207 addressed by industry. We should listen to FBI Director
208 Mueller, to the FERC and to the warnings coming from Russia
209 and China. We should pass the GRID Act soon.

210 I yield back.

211 [The prepared statement of Mr. Markey follows:]

212 ***** COMMITTEE INSERT *****

|
213 Mr. {Walden.} I thank the gentleman for his comments,
214 and we are now going to recognize the Chairman Emeritus of
215 the Committee, Mr. Barton.

216 Before I do that, I just want to say how important it is
217 to have members who have been so engaged on this, and
218 especially we are blessed to have Anna here, who served on
219 the Intelligence Committee, and Mike Rogers, who chairs it
220 now, and Lee Terry and Mr. Latta and Mr. Murphy, who is not
221 part of the subcommittee but were on the cybersecurity task
222 force the Speaker appointed, so all of that is most helpful
223 is we tackle both of these issues.

224 I now recognized the gentleman from Texas, Mr. Barton.

225 Mr. {Barton.} Thank you, Chairman Walden. I thought
226 Mr. Markey was going to say the experts said the biggest
227 threat to our grid was the EPA, but he went a different way
228 with that.

229 Back in 2006, Subcommittee Chairman Upton held a hearing
230 on this very same issue, and as Full Committee Chairman, he
231 and I sent a letter to the GAO asking them to take a look at
232 this issue. The response that we received then is the
233 response that we are receiving today and that is that it is
234 quite possible that we could have a major attack, a cyber
235 attack, in this country that would dramatically affect our

236 country.

237 According to the Norton cyber crime report for this last
238 year, cyber crime is a \$388 billion industry with 431 million
239 adults experiencing at least one cyber crime in the last
240 year. In another study, research has showed that the median
241 annualized cost of cyber crime for companies is over \$6
242 million a year with the range being between \$1.5 million to
243 \$36 million per year. Now, these are real numbers, real
244 statistics and that is for the year 2011.

245 As we use the Internet more and more every day, it is
246 absolutely imperative, Mr. Chairman and Ranking Member Eshoo,
247 that we really take this seriously, and as you have pointed
248 out and Anna has pointed out, it is good to have the Chairman
249 of the Select Committee on Intelligence on this subcommittee
250 because he has access to information that could be useful if
251 and when we decide to legislate.

252 So thank you, Mr. Chairman, for holding the hearing. As
253 you know, there is an EPA hearing downstairs in the energy
254 subcommittee, so I will be shuttling back and forth.

255 [The prepared statement of Mr. Barton follows:]

256 ***** COMMITTEE INSERT *****

|
257 Mr. {Walden.} Mr. Chairman, if you don't mind yielding
258 to Mr. Terry?

259 Mr. {Barton.} I will yield 2 minutes.

260 Mr. {Terry.} Thank you, Mr. Barton and Mr. Chairman.

261 This is an extremely important hearing and that we have
262 to elevate the level of discussion and potential solutions.

263 There is only one silver bullet that exists to prevent
264 cyber crimes. That is to completely disconnect your computer
265 from any network. Use it as a paperweight. Maybe just play
266 solitaire. That is it. If you are going to engage in any
267 level of commerce using the Internet, you are at risk, and
268 the only thing we can do is to try to minimize it. There is
269 no silver bullet.

270 Why these folks are here today is for us to understand
271 what tools may be available. In the cyber task force, one of
272 the things that we concluded is that the vast majority of
273 everyday hacking can be maybe not prevented but go a long way
274 which is basic security features offered by private sector
275 today or the networks or ISPs. But we have to have people to
276 actually purchase those or use those tools. In fact, there
277 was one incident in Omaha with our entity that controls our
278 facilities that never thought that it was important to have
279 those type of securities, and guess what? They were hacked

280 and all of their information was stolen.

281 But then the next level is where it gets dicey. How do
282 you protect people? How do they protect their data? We
283 can't engage in setting the standards because frankly we set
284 the standards. Before the ink is dry on the bill, the
285 standards have changed.

286 So you are here to help us understand what solutions may
287 be available to minimize and help secure our infrastructure,
288 and I want to thank you all for being here today. Does
289 anybody else want 48 seconds?

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

291 ***** COMMITTEE INSERT *****

|
292 Mr. {Walden.} Mr. Rogers.

293 Mr. {Rogers.} Thank you very much. In the short time
294 that we have, I can't tell you a more important issue.

295 There are a lot of things that can keep you up, as the
296 Chairman of the Intelligence Committee, and this one is one
297 of the main ones. Eighty percent of the attacks that happen
298 every day can be prevented by the operator. It is those
299 other 20 percent that are the devil in the details. Between
300 criminal attacks, economic espionage, disruption or
301 attacking, as we would call it, on cybersecurity, we have a
302 very real and present danger when it comes to cyber threats
303 to our networks.

304 Nobody is more integrated than the United States, and
305 therefore we are more at risk than other countries. I do
306 believe it is unprecedented in history that such a massive
307 and sustained intelligence effort by a government to
308 blatantly steal commercial data and intellectual property to
309 use against the United States is well underway. We don't
310 talk about it a lot because companies are reluctant to talk
311 about it. The real number we think is closer to somewhere
312 between \$300 billion and \$1 trillion in lost intellectual
313 property per year. Countries like China are leading that
314 charge. Russia is not far behind. Iran's capabilities are

315 getting better, and the most concerning are non-nation states
316 who are developing cyber capability to conduct disruption and
317 attack activities against targets like the United States.
318 All are serious problems.

319 I want to thank Anna Eshoo. We did a seminar out at
320 Stanford University on this very issue. I think it was well
321 received. Her support of this bill is incredibly important.
322 I look forward to hearing from the witnesses, and I
323 appreciate you being here so that we can get to that next
324 step and actually do something that helps us have a fighting
325 chance against these cyber threats.

326 I yield back, Mr. Chairman.

327 [The prepared statement of Mr. Roger follows:]

328 ***** COMMITTEE INSERT *****

|
329 Mr. {Walden.} The chair recognizes the gentlelady from
330 California, Ms. Matsui, who is going to control Mr. Waxman's
331 time.

332 Ms. {Matsui.} Thank you very much, Mr. Chairman, for
333 holding today's hearing, and I would also like to welcome our
334 witnesses here today and look forward to your testimony.

335 There is no doubt that cyber attacks are real and
336 continue to pose significant threats to several aspects of
337 our economy. Communications networks are one of many areas
338 that our Nation must protect and assure safety and soundness,
339 particularly as we consider deploying an advanced nationwide
340 broadband network for public safety. Advanced IP-based
341 technologies and public safety communications heighten the
342 concerns for cybersecurity. This new network, however, will
343 share many of the same cyber concerns as any other network.
344 This is something we have to take seriously and must protect.

345 Moreover, our economy continues to experience ever-
346 evolving ingenuity and innovation in the American technology
347 industry. One of those technologies which will continue to
348 play a prominent role in our economy, both in the public and
349 private sector, is cloud computing. We are also seeing
350 consumer cloud applications like the iCloud. As I see it,
351 one of the key issues is the challenge of cybersecurity

352 relating to the cloud.

353 The challenge is to find the critical balance of
354 continuing to foster American innovation and growth while
355 combating cyber attacks. For the most part, the private
356 sector will need to be up to the challenge of managing itself
357 and its networks from potential cyber attacks. That said, I
358 do believe that some balance may be appropriate where the
359 government must work together in partnership with the private
360 sector on enhancing our Nation's cybersecurity preparedness.
361 Simply put, one cannot do it without the other.

362 Small businesses, many of whom rely on the broadband
363 economy, are also very susceptible to cyber attacks. In many
364 instances, small businesses cannot fend off such attacks
365 because they do not have a plan or lack the resources. Such
366 an attack, though, would be very costly to their businesses.
367 During this economic recovery, the last thing small business
368 owners in my district and across the country need to worry
369 about is a cyber attack that will hinder their business.

370 I am pleased that the FCC recently launched a public-
371 private partnership, the Small Biz Cyber Planner, which is an
372 online tool that will allow small businesses to create
373 customized cybersecurity plans. It is important that we
374 continue to educate small businesses and the public in
375 general about the risks that cybersecurity poses to small

376 businesses, the government and to our economy as a whole. I
377 also believe a strong public-private partnership is critical
378 to protect against cyber attacks. It is my hope that
379 partnership continues to foster moving forward.

380 I look forward to exploring appropriate jurisdiction of
381 this committee, given the communications and technology
382 relevance of cybersecurity. I look forward to hearing from
383 the witnesses today and hope that we will have future
384 hearings in this subcommittee so that we can also hear more
385 about the government's efforts to combat cyber attacks.

386 Again, I thank the Chairman for holding today's
387 hearings, and I would be happy to yield to anyone on our side
388 if they would like to. Okay. I yield back the balance of my
389 time.

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

391 ***** COMMITTEE INSERT *****

|
392 Mr. {Walden.} The gentlelady yields back the balance of
393 her time.

394 We will now proceed to the witnesses. We have a very
395 distinguished panel. We thank you again for being here today
396 to share the information you have in your testimony, and we
397 are going to start with Mr. Bill Conner, who is the President
398 and Chief Executive Officer of Entrust. Mr. Conner, thanks
399 for your testimony and we look forward to your comments.

|
400 ^STATEMENTS OF BILL CONNER, PRESIDENT AND CHIEF EXECUTIVE
401 OFFICER, ENTRUST; ROBERT DIX, VICE PRESIDENT OF GOVERNMENT
402 AFFAIRS AND CRITICAL INFRASTRUCTURE PROTECTION, JUNIPER
403 NETWORKS; JAMES A. LEWIS, DIRECTOR AND SENIOR FELLOW,
404 TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC
405 AND INTERNATIONAL STUDIES; LARRY CLINTON, PRESIDENT AND CHIEF
406 EXECUTIVE OFFICER, INTERNET SECURITY ALLIANCE; AND PHYLLIS
407 SCHNECK, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER,

|
408 ^STATEMENT OF BILL CONNER

409 } Mr. {Conner.} Good morning, Mr. Chairman and
410 distinguished members of the subcommittee. It is a privilege
411 and honor to spend a morning here with you out of the cyber
412 warfare game to discuss and educate what is happening below
413 the screen.

414 I would like to focus my early comments on the arms race
415 on one particular vector of security, and it is called man in
416 the browser. Now, that vector of security is probably the
417 leading cyber stealer in the world today, and it has been
418 around a while and certainly impacts the small and medium
419 business and it is certainly impacting the change and nature
420 of stealing IP and money both at a country state and at an

421 organized-crime state.

422 Specifically, it is known as Zeus. It is commonly now
423 combined with SpyEye. For those of you don't know, Zeus was
424 the original man in the browser software. It started out of
425 the Ukraine and Russia. It went under its own merger and
426 acquisition by its lead competitor in the underground world
427 called SpyEye. Their tools and technology were next
428 generation. They merged in the fall of 2010 behind the
429 scenes. As law enforcement started to attack it, the guy
430 took his money and ran, combined it. In February of last
431 year, that new code is out on the market. You can buy it off
432 the Internet and buy it with 24/7 support. So no longer do
433 you have to be intelligent to write the code. You buy it,
434 you pay for the support, and they will help you design your
435 attack vector on which banks, which geographics you want to
436 do.

437 How does this technology work? It is real simple. It
438 is very complicated. You cannot find it with the traditional
439 software that you have on our desktop whether it is an
440 antivirus or the operating systems looking for it. It is
441 cloaked software that is really targeted at small and medium
442 business because it is targeted for money. This is a for-
443 money game for that. What it basically does, it targets a
444 small or medium business that probably doesn't have the

445 technology or banking understanding with its supplier to
446 understand how to deal with it. How does it work? I am a
447 treasurer at a small business. I go online to my financial
448 institution. I say I want to move \$1,000 or \$10,000, let us
449 say \$10,000, to a supplier. I have an agreement with my
450 local bank to have online bill pay. I type that in. The
451 bank sees that but before the bank sees it, this software
452 wakes up in the browser and changes the payees from one
453 supplier to, let us say, six mules. It changes the dollar
454 amount from \$10,000 to \$100,000, so what the bank sees is
455 \$100,000 going to six people. That bank says guess what,
456 we've got good security, you had to use a password, it is on
457 your IP address in your network and your location, I am going
458 to send it back because I want a one-time passcode, 30-year-
459 old technology that we are trying to apply to the digital
460 world. It sends it back to the controller of your business
461 and says please confirm by putting your passcode that is
462 going to expire in 30 seconds that you authorized this
463 transaction. That software wakes back up, converts that
464 \$100,000 back to \$10,000, six payers back to one. You type
465 in your passcode, hit enter to send it back, and guess what?
466 That \$100,000 is now gone from the bank. You lose it, the
467 bank loses it. Six mules that are going to feed that money
468 back into organized crime around the world are off and

469 running.

470 Unlike the personal side where I am protected by FDIC,
471 my friends, you are protected as a small or medium business
472 by nothing, the contract you have written, and if you look
473 around this wonderful country of ours, there is no clear case
474 law. There is case law on both sides of this because the
475 banks said I did nothing. We have had cases overturned that
476 even though a business had only done four transactions in the
477 last year and 20 transactions happened in six hours totaling
478 \$2 million when online was only \$500,000, that is what is
479 happening.

480 The good thing is, the technology exists to deal with
481 that today. The banks aren't doing it and small businesses
482 don't know what to do. So our belief is very
483 straightforward. Much like quality, there wasn't a lexicon.
484 To deal with cybersecurity, we need a lexicon. Much like
485 quality, it isn't a one time like year 2000. We need to do
486 it over time. That is why education is critical.

487 The second thing you must do is have public-private
488 partnership. I co-chair the DHS piece. I can tell you, the
489 legislative laws around this do not work for anybody, and I
490 think you have got to break public-private at different
491 levels from intelligence to the people like me that try to
492 secure the U.S. government and others to energy grids where

493 Department of Energy works with those types of organizations.

494 And finally, we must take a unified effort in public and
495 private to defend because it is an arms race and it is a pace
496 as we mentioned earlier. Thank you.

497 [The prepared statement of Mr. Conner follows:]

498 ***** INSERT 1 *****

|
499 Mr. {Walden.} Mr. Connor, thank you. Excellent
500 testimony. I think we are going to have to recess so we can
501 all go deal with our own campaign accounts, and we will back
502 in about an hour. We really appreciate it and we look
503 forward to getting into questions with you and exploring it
504 further.

505 We are now going to go to Mr. Robert Dix, who is Vice
506 President of Government Affairs and Critical Infrastructure
507 Protection for Juniper Networks, which I believe is from your
508 district.

509 Mr. {Dix.} Proudly.

510 Mr. {Walden.} We are delighted to have you here.
511 Thanks for coming the distance to share your wisdom with us,
512 and please proceed.

|
513 ^STATEMENT OF ROBERT DIX

514 } Mr. {Dix.} Thank you, Chairman Walden, Ranking Member
515 Eshoo and members of the subcommittee. Good morning. Thank
516 you very much for inviting me to testify about cybersecurity.

517 Juniper Networks is a publicly held private corporation,
518 hardware and software manufacturer, headquartered in
519 Sunnyvale, California, with offices and operations around the
520 world. Information technology and communications networks
521 are embedded in all manner of the Nation's critical
522 infrastructure including power plants and the electrical
523 grid, water filtration systems, financial systems and
524 transportation networks, just to name a few.

525 While sectorwide risk assessments conducted or being
526 conducted in the IT and communications sectors validate that
527 networks are resilient, it is important to acknowledge that
528 the risk continues to grow and change and our efforts to
529 protect and prevent must be sustained and agile. In
530 recognition of this reality, the private sector is working
531 every day to protect against cyber threats through self-
532 driven research and innovation, industry collaboration and
533 partnerships with government.

534 Let me share just a few examples. In 2007, a group of

535 private sector companies came together to address the issue
536 of software assurance and improving the development process
537 integrity of software and hardware products. SAFECode, the
538 Software Assurance Forum for Excellence in Code, is a group
539 of companies and subject-matter experts that has set aside
540 their competitive interest to gather and share industry best
541 practices through a series of written deliverables that are
542 available not just to the participating companies but to the
543 industry at large.

544 Additionally, in 2008, a group of private sector
545 companies came together to address the need for
546 collaborative, global incident response by forming ICASI, the
547 Internet Consortium for Advancement of Security on the
548 Internet. Once again, the participating companies who
549 compete vigorously in the marketplace routinely share
550 information in an effort to mitigate anomalous and abnormal
551 network activity globally because the cause is greater than
552 any one company.

553 Across the 18 critical infrastructure sectors, we have
554 organizations such as ISACs, Information Sharing and Analysis
555 Centers, since 1988 working on the operational issues.
556 Additionally, we have sector coordinating councils that were
557 derived as a result of the National Infrastructure Protection
558 Plan in 2006.

559 The Partnership for Critical Infrastructure Security is
560 the cross-sector coordinating council representing all 18
561 critical infrastructure sectors and working with the Federal
562 Senior Leadership Council under the NIPP partnership
563 framework to advance the mission of critical infrastructure
564 protection and cybersecurity. In fact, we are currently
565 working with the Administration on the implementation around
566 Presidential Policy Directive #8 for national preparedness
567 and the review and update of HSPD-7 regarding an all-hazards
568 approach to critical infrastructure protection and
569 cybersecurity.

570 Mr. Chairman, the number of users connecting to the
571 Internet and other networks will continue to growth. Global
572 Internet traffic is increasing at a rate of 40 to 50 percent
573 a year and is expected to grow to 4 billion users in 2013.
574 The explosion in the use of smartphones and tablets and the
575 advent and growth in the use of social media is rapidly
576 changing the workplace and how we communicate--example, an
577 average of 10,000 tweets per second the last 3 minutes on the
578 Super Bowl on Sunday evening--while introducing cyber risks
579 in a way that few of us could have imagined only a short time
580 ago. This is the essence of technology. It enables us to do
581 what we never could have imagined, and that includes those
582 with nefarious motives. The convenience of the technology

583 has changed banking, purchasing and sharing of personal
584 financial information.

585 So it is only reasonable to expect that the conversation
586 about cybersecurity must include a discussion about economics
587 but there are two sides to this coin. If we focus only on
588 technology and technology development, we are likely to miss
589 the opportunity to examine the challenges and impediments to
590 technology and solution adoption. The market is delivering
591 innovation at an unprecedented pace in history. However, the
592 evidence would suggest that adoption of available solutions
593 has not kept pace and should be a topic of further
594 examination and discussion. Many low-cost and no-cost
595 solutions are available to improve end users' protection
596 profile. Accordingly, there are many things we can do
597 together. It is reported by reliable sources that some 80
598 percent of the exploited vulnerabilities are the result of
599 poor or no cyber hygiene. For me, this is basic blocking and
600 tackling. If we can raise the bar of protection, it makes it
601 more difficult and more costly for the bad guys to do harm.

602 When our Nation was confronted a couple of years ago
603 with the threat of the H1N1 virus, we mobilized as a Nation
604 to warn and advise folks how to protect themselves from the
605 risks of infection. We have the opportunity to use that same
606 model for a sustained awareness program to help educate

607 citizens, small business, students, nonprofits and other
608 stakeholders how to protect themselves from the risks of
609 malware, phishing and other forms of infection in cyberspace.

610 Chairman Walden, Ranking Member Eshoo and members of the
611 subcommittee, we must move beyond just thinking about the
612 challenges of today to thinking about the risk profile of
613 tomorrow. Today's cyber attacks are more complex and often
614 difficult to detect and can target classes of users, even
615 specific users, gaining access to valuable data and causing
616 significant harm. With a commitment to working together in a
617 collaborative manner, the United States will lead the effort
618 to the protection, preparedness and resilience of critical
619 infrastructure and cybersecurity.

620 On behalf of my colleagues across the industry and the
621 proud employees of Juniper Networks, I thank you again for
622 the opportunity to testify before you this morning. The
623 threat is real, the vulnerabilities are extensive, and the
624 time for action is now. The American people are counting on
625 us to get this right and the private sector looks forward to
626 continuing the collaborative relationship between Congress,
627 the Administration and private industry on this important
628 issue. Thank you.

629 [The prepared statement of Mr. Dix follows:]

630 ***** INSERT 2 *****

|
631 Mr. {Walden.} Mr. Dix, thank you very much for sharing
632 those comments with us.

633 We now go to Dr. James A. Lewis, Director and Senior
634 Fellow, Technology and Public Policy Programs, Center for
635 Strategic and International Studies. Dr. Lewis, thank you
636 for being with us. We look forward to your testimony as
637 well.

|
638 ^STATEMENT OF JAMES A. LEWIS

639 } Mr. {Lewis.} Thank you, Mr. Chairman, and I would like
640 to thank the committee for this opportunity to testify.

641 One thing that military and intelligence experts would
642 agree on is that the cybersecurity problem is getting worse,
643 not better. There is straightforward evidence that what we
644 are doing now isn't working. Most of these experts also
645 believe that we will not change our laws and policies until
646 there is a crisis. I hope they are wrong.

647 We all recognize the growing dependence of our economy
648 on cyberspace and the risk this creates. Director of
649 National Intelligence Clapper testified last week about how
650 Iran, which is eagerly developing cyber attack capabilities,
651 is losing its reluctance to attack the American homeland.
652 FBI Director Mueller testified, as you heard, that the threat
653 we face now comes from terrorism but in a few years the
654 bigger threat will come from cyber attack.

655 The ability to launch damaging attacks is spreading from
656 a few advanced nations to many countries and many hostile
657 groups. There is disagreement among when hackers will
658 disrupt critical services in the United States but most
659 estimates put it at sometime in the next couple of years.

660 Cyber crime and espionage are rampant now, costing American
661 jobs and damaging American economic competitiveness and
662 national security.

663 This morning, I was trying to think of what I could say
664 that would be a little different, and I remembered that I
665 attended as a back bencher for the Director of Central
666 Intelligence some of the first meetings in the Clinton
667 Administration on commercializing the Internet. Back then,
668 we thought that it would be used for e-commerce, that it
669 would be eBay and Amazon. We didn't expect a global network
670 that would become the premier vehicle for espionage and a
671 potential avenue for attack. We thought that if we made
672 tools and information available, if we freed up encryption,
673 companies and people would voluntarily secure the networks.
674 I am a little embarrassed sometimes when I see a paper I
675 wrote for the White House in 1996 that said that because I
676 was wrong. We made the same mistakes in our approach to
677 critical infrastructure protection.

678 There were three big errors. The incentives for
679 cybersecurity vary from company to company and sector to
680 sector, and usually they are insufficient. There are legal
681 obstacles that limit the ability of governments and companies
682 to cooperate and to share information. And in any case, we
683 need a coordinated defense, not a grab bag of individual

684 actions. Finally, we did not expect to face world-class
685 opponents, as you heard from some of the earlier testimony,
686 even midrange opponents with access to world-class tools. We
687 overestimated incentives and underestimated threats and legal
688 obstacles, and I would like to point out that Congressman
689 Rogers' bill would be very useful if we could it passed in
690 removing some of the legal obstacles that hamper our ability
691 to provide an adequate cyber defense. A serious defense
692 requires coordination and mandatory action. The big telecom
693 companies are pretty good at securing themselves and don't
694 need more regulation but the other sectors are in bad shape.
695 Some people say regulation is burdensome, but if we do not
696 hold critical infrastructure to mandatory standards, we
697 guarantee a successful attack. Nor does regulation damage
698 innovation. An unregulated Internet is not a substitute for
699 a business-friendly environment that innovation really needs.

700 Partnership and cooperation must become more than an
701 exchange of slogans. Australia has a good model, we heard
702 about that, where the government encouraged Internet service
703 providers to develop a code of conduct to deal with malware.
704 That appears to be working. We are considering in the United
705 States similar options.

706 Finding ways to expand the use of DNSSEC. DNSSEC is a
707 good story. This is a fundamental rule set, the addressing

708 framework for the Internet. We identified problems with it
709 20 years ago. We identified fixes for it 12 years ago. We
710 have not implemented these fixes. This is one where finding
711 some new approach to get people to move faster would be
712 really crucial. The Defense Industrial-Based Initiative,
713 which shares classified threat information, is another good
714 example of how to do real cooperation.

715 There are many opportunities to improve cybersecurity
716 but taking advantage of them will require a new approach. I
717 think one thing I can say is everyone wants to make things
718 better. We all realize the scope of the problem, and
719 everyone wants to do stuff. Hearings like this provide an
720 opportunity to find that new approach that will truly serve
721 national security.

722 I thank the committee for the opportunity and look
723 forward to your questions.

724 [The prepared statement of Mr. Lewis follows:]

725 ***** INSERT 3 *****

|
726 Mr. {Walden.} Dr. Lewis, thank you. We appreciate your
727 testimony, and we will have a few questions for you,
728 especially on the Australia model.

729 We are going to go now to Mr. Larry Clinton, President
730 and Chief Executive Officer of Internet Security Alliance.
731 Mr. Clinton, thank you for being here today. We look forward
732 to your comments.

|

733 ^STATEMENT OF LARRY CLINTON

734 } Mr. {Clinton.} Good morning, Mr. Chairman, members of
735 the committee.

736 There has been a dramatic change in the cyber threat
737 picture in the last 18 to 24 months. Our main concern is not
738 hackers are kids in basements. The fact that a cyber system
739 has been breached is no longer the metric which determines
740 whether or not an attack has been successful. Cyber attacks
741 have grown increasingly sophisticated using what is commonly
742 referred to now as the advanced persistent threat, or the
743 APT. APT attackers are pros. They are highly organized,
744 well-funded, often state-supported, expert attacks who use
745 coordinated sets of attacking methods both technical and
746 personal. Perhaps most indicative of these attacks is if
747 they target a system, they will almost invariably compromise
748 or breach it. Unfortunately, conventional information
749 security defenses don't work against the APT. Attackers are
750 successfully evading all antivirus intrusion and traditional
751 best practices, remaining inside the target's network while
752 the target believes they have been eradicated.

753 This doesn't mean that we have no defense. It means
754 that we need to modernize our notion of what constitutes

755 cyber defense. Traditional approaches including federal
756 regulation will not solve the problem because they are going
757 to be largely reactive and will not stay ahead of the
758 changing threat nature. Worse, bad regulation could be
759 counterproductive, leading companies to expend their limited
760 resources on building in-house efforts to meet regulatory
761 demands rather than focusing on security.

762 The fundamental of stopping the advanced threat is to
763 understand our biggest problems are not technological, they
764 are economic. Independent research has consistently shown
765 that the single biggest barrier to combating the cyber threat
766 is cost. President Obama's Cyberspace Policy Review said
767 many technical and management solutions that would greatly
768 enhance our security already exist in the marketplace but are
769 not being used because of cost and complexity. Just last
770 week, Bloomberg released an extensive study that found that
771 to reach an acceptable, not ideal, acceptable level of
772 security in critical infrastructure would require a 91
773 percent increase in spending.

774 The private sector has been extremely responsive to
775 combating the cyber threat. Average spending on
776 cybersecurity in the telecommunications industry is \$67
777 million a year with governance, by the way, including
778 regulatory compliance, being the single biggest thought.

779 Despite the fact that our critical infrastructure is
780 under constant attack, we have never had an instance of
781 serious breakdown, mass deaths, evacuations, economic
782 catastrophe, similar to what we have seen in the
783 environmental area. This success is due in large part to the
784 flexibility generated by the current system, which relies on
785 voluntary partnerships where an industry understands and can
786 manage the systems best and use their intimate knowledge to
787 respond rapidly to emerging threats in a fashion they believe
788 can best protect the system rather than being driven by a
789 preset government directive. Nevertheless, there is a great
790 deal that Congress can do and the Commerce Committee can do
791 to improve our cybersecurity right now.

792 First of all, we need to get the government's house in
793 order. The National Academy of Sciences, the GAO, and just
794 last week the DOE Inspector General have all documented
795 systemic problems in managing government cyberspace. These
796 need to be addressed immediately.

797 Second, we need to provide the right mix of incentives
798 and regulation. For industries where the economies of the
799 industry are tied directly to a regulatory format such as
800 electric utilities, water, transportation, etc. the current
801 regulatory structure can be used to motivate and fund needed
802 cyber advancements. For industries where the economics are

803 not inherent to a regulatory structure, adding a new
804 regulatory structure will impede innovation and investment,
805 making us less secure. In these sectors, we need to motivate
806 by providing appropriate market incentives to spur greater
807 security and investment. An excellent example of this
808 approach is Mr. Rogers' bill, which passed the Intelligence
809 Committee a couple of weeks ago, which uses liability reforms
810 to stimulate additional information sharing. However,
811 liability reform is only one of many incentives that need to
812 be unleashed to help us secure our cyber networks. Other
813 incentives include better use of government procurement,
814 streamlining regulation in return for demonstrated security
815 improvements, greater use of private insurance, streamlined
816 permitting and licensing. This incentive-based approach was
817 spelled out in some detail in the ISA cybersecurity social
818 contract in 2008 and was also endorsed by President Obama in
819 the Cyberspace Policy Review in 2009, but the multi-trade
820 Association and Civil Liberties Coalition white paper on
821 cybersecurity in 2010, and the House Task Force report in
822 2011.

823 A great deal of work needs to be done to fill out how
824 these incentive models can be used in the various sectors.
825 In the meantime, Congress ought to enact FSMA reform or to do
826 the Rogers information sharing bill and should do a good deal

827 to better coordinate amongst themselves. Passing that
828 package of cybersecurity reforms would be a historic and
829 politically achievable goal.

830 Ladies and gentlemen of the Commerce Committee, you are
831 dealing with the invention of gunpowder. Mandating thicker
832 armor is not going to work any more than building deeper
833 moats was going to stop the horders and the invaders who
834 invented catapults or the Maginot Line was able to stop the
835 Germans in World War II. We need a different approach. We
836 need a contemporary and creative approach that engages the
837 private sector with government, not having the government
838 control what the private sector does.

839 We really look forward to continuing to work with you.

840 [The prepared statement of Mr. Clinton follows:]

841 ***** INSERT 4 *****

|
842 Mr. {Walden.} Mr. Clinton, thank you very much for your
843 testimony. We appreciate it.

844 Our next and final witness today is Phyllis Schneck, who
845 is Vice President and Chief Technology Officer of the Global
846 Public Sector, McAfee Incorporated. Dr. Schneck, thank you
847 for being here today. We look forward to your comments.

|
848 ^STATEMENT OF PHYLLIS SCHNECK

849 } Ms. {Schneck.} Good morning, Chairman Walden and
850 Ranking Member Eshoo and other members of the subcommittee.
851 Thank you very much for the opportunity to be here this
852 morning, and thank you for your interest in cybersecurity as
853 it applies to the telecom sector.

854 My testimony will focus this morning on four areas: the
855 threat landscape, the communications sector's unique role in
856 cybersecurity, private sector technologies and policy
857 recommendations to enable greater cross-sector cyber
858 resilience.

859 First, just a bit of background. My technical
860 background is high-performance computing and cryptography. I
861 was raised in this back to the days of the radio tower. My
862 father was one of the first in supercomputing in this country
863 and taught me to write code. I know how to exploit code, but
864 I was taught the responsibility of that and the
865 responsibility of the computing power that we have and I am
866 confused on and passionate about protecting that and
867 protecting good science. I am also focused on partnership.
868 Outside of McAfee as a volunteer, I ran the private sector
869 side of the FBI's InfraGard program, about which Director

870 Mueller testified several times. I ran that for 8 years and
871 grew that program from 2,000 subject-matter experts across
872 the critical infrastructure sectors to 33,000, and today
873 chair the national board of directors for the National Cyber
874 Forensics and Training Alliance, which brings together the
875 top fraud analysts from the banking sector, telecom,
876 pharmaceuticals and others with the FBI under the same roof
877 and other organizations and governments, do analytics that
878 helped to arrest 400 cyber criminals worldwide in the past 2
879 years.

880 A little bit about McAfee. We are based in Santa Clara.
881 We are the world's largest dedicated security company. We
882 protect business, governments and consumers all over the
883 world from the full spectrum of cybersecurity attacks. We
884 are a trusted partner and adviser on cybersecurity throughout
885 the world, and as a wholly owned subsidiary of the Intel
886 Corporation enjoy driving that innovation that goes directly
887 to the hardware. The buck stops at the hardware, so the
888 adversaries can get in in several different ways, but when a
889 piece of hardware knows not to execute a malicious
890 instruction, that is when we have the enemy.

891 As you have heard this morning, the cyber threat
892 landscape has evolved. Obviously it is not a dorm-room
893 activity anymore. It is more a mass espionage. There are

894 two kinds of companies and agencies across the world, public
895 sector and private, those who know they are owned and those
896 who don't. We are looking at the mass movement of money
897 markets and jobs between countries and companies and we are
898 looking at the threat of destruction should they desire.
899 This enemy is faster and smarter than we are at times. They
900 are certainly faster. They have no intellectual property
901 boundaries, no legal boundaries, no policy boundaries, and in
902 many cases, they have plenty of money. They have absolutely
903 no obstacles to execute on our infrastructure.

904 Which leads us to the role of the Internet service
905 providers. In the days when I sent my first packets between
906 my sister's room and mine, there was nothing in that route
907 except one address on the other. Now we have an unknown set
908 of routes but we have an ability and a great infrastructure
909 run by the ISPs that deliver our traffic and that if the
910 adversary very reliably. So the enemy has now used our great
911 cyber infrastructures that we built as the good guys over the
912 world as a mass executive transport system for malware. They
913 haul packets at high speed. They do a great job. They are
914 fairly secure, as was mentioned earlier, but the current
915 Internet architecture allows everything to get delivered to
916 the grid, to the banks, to the rest of the critical
917 infrastructure.

918 ISPs can play a key role in better cybersecurity. They
919 are already doing some of this but they have some challenges.
920 One thing they can do is help detect this traffic in the
921 network fabric and use some global threat intelligence to do
922 that, and I will explain that in just a moment, but imagine
923 if our network fabric was smart enough not to route the
924 traffic of an adversary and only to route good traffic.
925 Secondly, demand more secure technologies and equipment from
926 the market. Demand that those technologies are armed with
927 proactive technologies and not let a malicious instruction
928 run. And third, ISPs can't carry the burden alone. As was
929 said earlier, it is up to every system to be hardened, up to
930 every company and user to harden their enterprise, and good
931 cyber hygiene plays a role in that.

932 What are the challenges that the ISPs face today? Just
933 to name a couple, you have things such as Stored
934 Communications Act of 1986, a little while ago. That was
935 before I sent my first packet. It prevents sharing
936 information outside of the telecoms, so imagine the
937 difficulty in enabling the global threat picture that the
938 enemies use. We can't make that rule because legally we
939 can't combine our information together. Secondly, it costs a
940 lot of money. Clean bandwidth costs money and users aren't
941 willing to pay that difference, so we need some help leading

942 to some policy recommendations and some proactive
943 technologies.

944 First and foremost, we can put threat intelligence
945 together and map a global cyber radar map of where the enemy
946 is at any time. At McAfee, across 160 million endpoints, we
947 see a risk profile in every IP address on the Internet.
948 Other companies do this. Telecoms do this. Governments can
949 do this if we can share that information together and make a
950 global threat picture and prevent those malicious
951 instructions from running, whether it is application listing
952 or working with the hardware, keep the enemy out.

953 So for the policy recommendations, we support the
954 recommendations in Representative Thornberry's work,
955 certainly with information sharing, insurance reforms and tax
956 credits, and certainly in the bill of Representative Rogers
957 and Representative Ruppertsberger enabling the government to
958 finally facilitate the good information sharing, to put that
959 information together to not only provide liability
960 protections, protections for privacy and for civil liberties
961 but to balance out the advantage that the adversaries had
962 over us until now. Let the government facilitate that
963 collaboration so we can build that global threat picture,
964 feed it back into the network fabric and have it grow as a
965 living, breathing system to feed us the information in

966 return. ISPs play a central role in the global digital
967 infrastructure. They can help us. We can help them. We
968 have to work on this legal and policy framework for global
969 information sharing.

970 Thank you very much for requesting McAfee's views on
971 these issues. I look forward to answering any questions.

972 [The prepared statement of Ms. Schneck follows:]

973 ***** INSERT 5 *****

|
974 Mr. {Walden.} Very impressive testimony. Thank you.
975 Thanks for all the work you do to try to keep us secure.

976 We will now go into our question phase, and I wonder,
977 Mr. Clinton, you talked about incentives and were fairly
978 specific. Can you dive down a little deeper in terms of what
979 that means in terms of more specifics on the incentives that
980 would make a difference here?

981 Mr. {Clinton.} Certainly, sir. Thank you. We are
982 supportive of the approach that was articulated in the House
983 Task Force report which suggests that a menu of incentives
984 needs to be developed because different industries are
985 responsive to different things. The defense industrial base
986 may be attracted by a procurement incentive, the banking
987 industry maybe by an insurance incentive, the utilities
988 perhaps by getting rid some of the outdated regulation that
989 is based in an analog form rather than digitalized. So you
990 need to have a set of incentives.

991 On the other hand, you need to have some agreement as to
992 what needs to be incentivized, and for that, what we have
993 suggested and is in the multi-trade association paper that I
994 spoke of before is that we need to have some independent
995 entity which does not create the standards or practices but
996 simply evaluates the standards and practices, an underwriters

997 laboratory for cybersecurity, if you will, and then
998 organizations would choose to elect a higher or lower level
999 of adoption based on their business plan and their business
1000 plan would be improved because they would have access to
1001 lower liability costs, lower insurance, better chance to get
1002 a federal contract, et cetera. So we are saying that we need
1003 a new system, not a government mandate system but a system
1004 where there are government roles such as providing the
1005 incentives and there are independent roles, something like
1006 this underwriters laboratory, and then responsibility for the
1007 owners and operators.

1008 Now, in those sectors of the economy where the economics
1009 is already built into a regulatory model, then you can use
1010 that regulatory model. You don't need a new regulatory
1011 model. You can use it. For example, if you are dealing with
1012 the utilities, they have generally a fairly detailed
1013 regulatory structure. The problem that they are having is
1014 that they get mandates at one level and the funding comes at
1015 another level so there is going to have to be a correlation
1016 done on the government side. But basically we think you need
1017 an independent set of entities indicating what needs to be
1018 incentivized. That can be done on a continuing basis.
1019 Government needs to provide the incentives and industry needs
1020 to implement them.

1021 Mr. {Walden.} All right. Very helpful. Thank you.

1022 Dr. Schneck, so when you and your sister were trading
1023 packets when you should have been sleeping, obviously, doing
1024 your homework, turn out the lights, that was when this threat
1025 was really computer to computer. Now we understand it to be
1026 bigger than that, broader than that and whole networks that
1027 can be taken down. So can you describe what those threats
1028 look like and what should happen there?

1029 Ms. {Schneck.} Absolutely. We did that over a 1200-
1030 baud modem over a phone line.

1031 Mr. {Walden.} I remember a 300-baud modem where you put
1032 the phone in the little coupler.

1033 Ms. {Schneck.} Right. So the threat really looks at an
1034 instruction that executes off the site of memory, not the
1035 piece of memory in your computer that holds some word-
1036 processing program but it is where your computer grabs the
1037 next instruction, what do I do next. At the root of every
1038 exploit or attack, it is, I am controlling my will on your
1039 machine, whether I am telling your machine to send out a lot
1040 of traffic or adjust something that might change the settings
1041 on something that controls circuit relays on an industrial
1042 system. I am allowing--my will is being changed on your
1043 machine; I am executing on your machine. So as was pointed
1044 out earlier, you can buy these exploits on the Net. You can

1045 even unleash botnets together in a screen that looks like it
1046 came off of Quicken. It is a spreadsheet, and you can choose
1047 addresses to which to send it. You are simply relying on
1048 someone else's construction of a piece of code, and we see in
1049 McAfee labs 66,000 new variants of these pieces of code every
1050 day called malware that allow my will to be instructed on
1051 your machine.

1052 So the idea is, well, it is twofold. One is to catch
1053 the IP addresses that are spreading it across the Internet
1054 and that goes to that threat position, sharing that global
1055 threat picture. I can't forecast the weather without the
1056 weather from all the different States or countries, and that
1057 comes from enabling the information sharing, but also the
1058 ability to detect an instruction that is doing something it
1059 shouldn't do. Resilience means, I can run even if the enemy
1060 gets in so the enemy will get in. The biological analogy is
1061 the disease is in your body but it will never hurt you. So
1062 we have to let many instructions get in because they will and
1063 simply be resilient to that, and that is the ability to work
1064 at the operating system level instead of having to judge
1065 every instruction, are you good or bad, because we have shown
1066 that is not effective, just know what is good and don't let
1067 anything else run. That is known as application white
1068 listing in the community. And then down at the hardware

1069 level, understand what an instruction should be accessing or
1070 shouldn't and just block it, and we can do that.

1071 Mr. {Walden.} I am glad you are on our side.

1072 Ms. {Schneck.} Thank you.

1073 Mr. {Walden.} Mr. Conner, you were talking about Zeus
1074 merging with SpyEye. Some of us wondered maybe that should
1075 have gone through like an FCC approval process for a merger
1076 and it would never have happened. All right. Now we will
1077 get serious.

1078 I am going to turn to my friend and colleague from
1079 California, who brings so much to this discussion and debate,
1080 Ms. Eshoo, for 5 minutes for questions.

1081 Ms. {Eshoo.} Well, I want to thank each one of you for
1082 your understanding testimony. I think that this is one of
1083 the best panels that has been assembled on a given subject
1084 matter and it is highly instructive.

1085 I can't help but feel that this is like trying to get
1086 socks on an octopus, though. I mean, it is massive. And I
1087 think that we all have a pretty good sense of what the threat
1088 it. I don't think that we have a clear picture of really
1089 what to do with it. There are so many agencies. There was a
1090 mention of a 1986 law that I want to hear more about. We
1091 have talked about public-private partnerships. We know that
1092 95 percent of this is in the private sector, 5 percent in the

1093 government. Where do we begin with this? What are the legal
1094 roadblocks as any of you see them right now that are holding
1095 us back to do what my next question would be, what is the new
1096 paradigm? And if we have very good pieces in place right
1097 now, what do we keep, what should we get rid of? And to Dr.
1098 Schneck, do you agree with this notion of Mr. Clinton's of an
1099 underwriters lab? That sounds very interesting to me.

1100 So I don't know who wants to begin with what, maybe with
1101 legal roadblocks that you know of. I think it was Dr.
1102 Schneck, were you the one that mentioned the 1986 law? I am
1103 not familiar with that and what it is blocking.

1104 Ms. {Schneck.} So I am not a lawyer.

1105 Ms. {Eshoo.} Neither am I.

1106 Ms. {Schneck.} But the overall premise and the reason I
1107 mentioned that is because the adversary has the ability to
1108 act on us very quickly because they have no roadblocks. We
1109 have the ultimate weapon, and that is, we own the
1110 infrastructure that works at the speed of light, and if we
1111 can put the instructions together and the intelligence
1112 together to work as your body does, it attacks a virus that
1113 comes in because it knows it doesn't belong there, it doesn't
1114 need to have a meeting to do so. We need the Internet to
1115 work the same way so the routers and the machines that route
1116 our traffic, they need to understand that something is bad,

1117 and to do that, we have to replace the chemical and biology
1118 with the intelligence from data and that means getting data
1119 from all sides of the equation that we control from the
1120 private sector. We have to be able to combine that with data
1121 in the government sector, not even in the classified realm.
1122 That would help, but this is all un-class. And then some of
1123 those laws actually prevent the ISPs from combining that data
1124 together. I don't have the answer legally on how to make
1125 that work while also preserving the civil liberties and
1126 privacy, which are crucial. But we have to find a way to put
1127 together at the indicator level this address, this location
1128 could hurt you and make that accessible to a router at
1129 several hundred gigabits per second.

1130 Ms. {Eshoo.} Now, what you just described, would that
1131 fit in with Mr. Clinton's idea of an underwriters lab, or
1132 not?

1133 Ms. {Schneck.} I think it is different.

1134 Ms. {Eshoo.} It is different. Okay. Did anyone ever
1135 tell you that you look like David Gergen? I was looking at
1136 you and I thought, I know he reminds me of someone.

1137 Mr. {Clinton.} Well, I am pretty flattered. I hear
1138 David is upset when the comparison is made.

1139 I agree with Phyllis. I think that it is a--we are
1140 talking about kind of different things. First of all, with

1141 respect to the legal issues, after he got elected, President
1142 Obama appointed Melissa Hathaway to do a 60-day cyber review
1143 on the National Security Council staff and the largest
1144 portion of that is appendix A, which is a thick document
1145 going through all of the legal barriers that need to be
1146 reviewed, so that is a place to start.

1147 Essentially what we have here is, we have a whole bunch
1148 of laws that were written for an analog world and we are now
1149 in a digital world. I mean, we have still laws on the books
1150 dealing with how you manage your videotapes. I haven't had a
1151 videotape in quite a while. So there is a lot that can be
1152 done to work out that legal underbrush and modernize things.
1153 We have suggested some of those things are regulatory and
1154 could be offered as incentives, you know, to get away from
1155 some of these burdens. Some of them, for example, are
1156 duplicative auditing requirements. We are all for auditing
1157 but we should have one unified cybersecurity audit and you
1158 pass that audit and you don't have to do the rest of the
1159 audits but there are multiple State, local, federal,
1160 different agencies that are involved in this, so
1161 organizations are spending a lot of their time and money
1162 doing redundant things. We should strip away a whole bunch
1163 of those sorts of things.

1164 The last thing on where you start, I would strongly

1165 suggest that Congress start by cleaning up the federal
1166 government's roles and responsibilities. That is a much more
1167 limited system. You can make a lot of progress really
1168 quickly while we are continuing to work with a public-private
1169 partnership model that we currently have.

1170 Ms. {Eshoo.} Thank you. I am out of time.

1171 Mr. {Walden.} I will yield to the gentleman from
1172 Nebraska, Mr. Terry. Before I do so, it strikes me, we ought
1173 to get this appendix A and maybe have a task force of this
1174 subcommittee that really gets into the weeds and that more
1175 deeply, and we have got people who have great experience
1176 here.

1177 Mr. {Terry.} So where do we start, Mr. Clinton?

1178 Mr. {Clinton.} Well, as I said, I would start first of
1179 all at the federal level. We need to straighten out roles
1180 and responsibilities of the federal government and between
1181 governments at the federal, local and State levels. So, for
1182 example, I mentioned the problem that we have in the utility
1183 sector where we have mandates that exist at one level, the
1184 funding comes at another level, and what we have to do is
1185 realize that solving some of the cybersecurity problem is
1186 going to cost us some money. Unfortunately, when you have
1187 State public utility commissioners, they are resistant to
1188 increasing the rate base, and this is understandable, but we

1189 have to find some way to get a pass-through on some of these
1190 things.

1191 So I think a good review and scrubbing of the
1192 governmental issues is one place to start. Simultaneously,
1193 we have a lot of activity already going through the public-
1194 private partnership that can use a number of these things.
1195 Mr. Rogers' bill is a good example. And then I think we need
1196 a really concentrated effort on working on these other
1197 incentive programs, exactly what do we need to do with the
1198 insurance industry to get them to be bigger players, exactly
1199 what--

1200 Mr. {Terry.} In what way?

1201 Mr. {Clinton.} Well, you know, private insurance is one
1202 of the most effective pro-social motivators we have. People
1203 drive better, they give up smoking, et cetera.

1204 Mr. {Terry.} So cyber insurance?

1205 Mr. {Clinton.} Cyber insurance, sure, so that if there
1206 is--the problem that we have in insurance, there is a couple
1207 of problems. One of the problems is, we don't have enough
1208 actuarial data because the data is being held.

1209 Mr. {Terry.} Doesn't Google have all of that?

1210 Mr. {Clinton.} Pardon me?

1211 Mr. {Terry.} I am sorry.

1212 Mr. {Clinton.} A lot of the insurance guys would like--

1213 Mr. {Terry.} You guys were good at humor. I tried it.

1214 Mr. {Clinton.} A lot of the insurance guys would like
1215 to share data but this runs into antitrust problems, okay,
1216 because to be sharing data for rates, but actually if we
1217 could get them to share that, perhaps in a public-private
1218 partnership, we would get a more realistic view of what the
1219 threat is. Right now they set everything at maximum, but if
1220 we share data, we could get a more realistic view of what the
1221 threat is. We think this would bring down insurance rates.
1222 When you bring down insurance rates, more people will buy the
1223 insurance. When more people are buying the insurance, more
1224 insurance companies will get in, and we get a virtuous cycle
1225 going on and we can use insurance to motivate better
1226 cybersecurity investment.

1227 Mr. {Terry.} All right. Mr. Dix, one question for you,
1228 and you can add on wherever you want, but you mentioned that,
1229 you know, for everyday users, small businesses, it is a just
1230 a matter of cyber hygiene, so I say, okay, you pull out your
1231 soap and you wash. What does that really mean and what can
1232 you do? What can we do as small business people or whatever?

1233 Mr. {Dix.} So again, as I mentioned, I think we need a
1234 comprehensive and sustained national education and awareness
1235 campaign that tells the user constituencies how better to
1236 protect themselves from the infection in cyberspace.

1237 Leveraging the resources of the federal government such as
1238 the Small Business Administration, the Internal Revenue
1239 Service, the U.S. Postal Service and other agencies that
1240 interact with citizens and businesses every day would be a
1241 place to help message that, creating and leveraging a model
1242 like we did with H1N1 where we have a sustained plan of
1243 public service announcements that drive people to a place
1244 where they can get information. It might even be nice if
1245 every Member of Congress had a link on their constituent web
1246 page that directed folks to the National Cybersecurity
1247 Alliance or the Internet Security Alliance as a place to
1248 learn basic best practices, low-cost or no-cost things that
1249 they can do to protect themselves.

1250 If I might add, another piece of the fundamental
1251 blocking and tackling is to ensure an operational capability
1252 that presents something like a National Weather Service or a
1253 CDC capability where we have a picture into what is going on
1254 in the networks at all times in steady states and in points
1255 of escalation. I raise that because many of us work together
1256 through the National Security Telecommunications Advisory
1257 Committee and delivered a report to the President in May of
1258 2009 that recommended the creation of a joint coordination
1259 center, a joint public-private integrated 24/7 operational
1260 capability to improve detection, prevention and mitigation.

1261 We have got to get in front of this. Most of our time now is
1262 spent in response and recovery. Part of the problem we ran
1263 into, legal barriers. Once we got into trying to integrate,
1264 we developed a model in the private sector. Once we began to
1265 try and integrate that capability with the government, the
1266 lawyers told us they couldn't talk because they couldn't
1267 share this information. Hopefully Representative Rogers'
1268 bill will help break down some of those barriers, but we
1269 should have an operational capability that has a picture as
1270 to what is going on in the network at all times and we have
1271 those kinds of data feeds available. Organizing them and
1272 having a National Weather Service or CDC type of capability
1273 is long overdue.

1274 Mr. {Terry.} Thank you.

1275 Mr. {Walden.} The gentleman's time has expired.

1276 I believe Mr. Waxman is next for 5 minutes for
1277 questions.

1278 Mr. {Waxman.} Thank you very much, Mr. Chairman.

1279 Dr. Schneck, and anybody else who wants to respond to
1280 this question, what special considerations do the growing use
1281 of smartphones and tablets present?

1282 Ms. {Schneck.} Thank you. There are several.
1283 Smartphones and tablets are just small computers. They have
1284 the exact same vulnerabilities that all the other machines

1285 have that you are used to, and they have tens of thousands
1286 times of memory in them that the guidance systems do that
1287 took our first Apollo rockets to the moon. So when you think
1288 about the power that is in your hands, you now have the
1289 ability twofold. One is that it enables the enemy to, if it
1290 is not secured appropriately, it enables an adversary to use
1291 it as a platform to get into your enterprise network. In the
1292 interest of time, I am going to simplify this a lot, but
1293 people are wanting to use the home device at work, and what
1294 happens is, once the adversaries discover they can use that
1295 unprotected home device that happily houses Angry Birds and
1296 launch an attack into the enterprise network because
1297 companies are letting folks use the small devices.

1298 So there are technologies to lock that down. We do a
1299 lot of that. We manage that worldwide. But you are looking
1300 at a massive explosion of small devices. The lady mentioned
1301 the cloud. These devices leverage the cloud because they
1302 don't have as much processing power as the big machine. So
1303 most of your processing is done in the cloud. You have to
1304 pay extra attention to the security on that motion data at
1305 rest and shared resources where your data are when they are
1306 not on the phone. Your personal information most likely is
1307 all over that phone, pictures of your friends and family,
1308 locations. If you lose it, you want to make sure you have a

1309 remote capability to destroy that. It is a wonderful device
1310 but it accessed to again all the critical infrastructure. If
1311 you are working on one and it is talking to your network, it
1312 has access now to your personal information.

1313 So I think it brings a wonderful new--I spoke about this
1314 at the consumer electronics show. It brings a wonderful new
1315 sense of fun to computing and it also brings new dangers that
1316 we need, to quote my colleagues here, to get out in front of
1317 before this is yet another massive vector because mobility is
1318 multiplying.

1319 Mr. {Lewis.} Just real quickly, every once in a while I
1320 talk to hackers just to see what they are up to, and recently
1321 one of them told me that the price for a toolkit to hack an
1322 iPhone is about \$200,000 on the black market, and he said for
1323 other phones it is only \$10,000. So, you know, I don't know.
1324 What this is going to do, though, it is going to force us to
1325 pay more attention to the service providers, to the big
1326 telcos, to the ISPs to the cable companies. Responsibility
1327 is going to shift away from the edge, away from the consumer
1328 to the service provider.

1329 You don't patch your cell phone. You know, you don't
1330 program it. You depend on its computing becoming a service,
1331 and that will change the contours of security and change the
1332 requirements for regulation.

1333 Mr. {Conner.} With all due respect, I disagree with
1334 that. If you look at Metcalfe's law and if you look at just
1335 what happened with Apple and AT&T, the value has shifted. It
1336 shifted from the carriers to the endpoints, and this is about
1337 identity, and I will give you a good example. The threat I
1338 talked about going out of band or using a mobile network and
1339 a device is a surefire way to stop that kind of transaction
1340 today, and it is safe and it is protected. It uses digital
1341 signature through a wireless carrier network and on a mobile
1342 device with digital signature which is probably why to try to
1343 hack the device costs a heck of a lot more on an iPhone or
1344 iPad than a normal phone. And if you use that, the
1345 probability on that attack factor, you don't break it.

1346 So I think there are good pieces and I think my personal
1347 experience, the minute you think you are going to stop all
1348 this in the network, the ID and IP address is no longer the
1349 identity. The number one people fake is who you are, what
1350 you are and the application of who are you, and that is the
1351 hardest thing to combat in terms of good guys versus bad
1352 guys. The threat I showed you is not the identity of the
1353 person that is doing it. He has faked your identity, and no
1354 perimeter technology, no network can deal with that until
1355 they deal with the endpoint itself.

1356 Mr. {Lewis.} I don't think we are disagreeing, though.

1357 I think that you are going to see that the authentication
1358 technologies you are talking about will depend ultimately on
1359 the service provider.

1360 Mr. {Waxman.} Well, let me ask one question, and I know
1361 I don't have much time, but many of you mentioned in your
1362 testimony how communications networks are central to most
1363 other critical infrastructure sectors. How does this then
1364 relate to the importance of this committee in addressing
1365 cybersecurity of communications networks? Anybody want to
1366 respond to that?

1367 Mr. {Lewis.} Well, I think that in the opening remarks,
1368 a few of you mentioned some of the things that are going on
1369 at NTIA and FCC that could reduce risk, right, and one of the
1370 examples we have heard about is of course this measure to get
1371 the Internet service providers to adopt a voluntary code of
1372 conduct for dealing with malware. It is a good thing to do.
1373 It is sort of basic-level stuff. The FCC has an effort to
1374 promote the use of DNS security, DNSSEC, and this is--not to
1375 get too complicated, but this is a growing vulnerability. It
1376 is relatively easy to fix. Other countries have moved faster
1377 than the United States. It is something that we can probably
1378 do on a collaborative basis.

1379 The third thing to look at is some of the
1380 responsibilities for other activities, other protocols. This

1381 is a place where you don't want the government creating
1382 technology, right. It is not for this kind of level of
1383 technology. But you do want it maybe coordinating a
1384 response, and so when you look at FCC, when you look at NTIA,
1385 the DNSSEC, the ISP efforts, some of the other measures,
1386 Commerce is doing similar things, this is where you can play
1387 a big role.

1388 Mr. {Waxman.} Thank you, Mr. Chairman.

1389 Mr. {Walden.} With the committee's indulgence, we were
1390 all going to ask you about the Australia model, and then we
1391 all forgot. Without objection, would you mind addressing the
1392 Australia model?

1393 Mr. {Lewis.} Well, Phyllis talked about this as well.
1394 Your ISP probably has a pretty good idea of what is going on
1395 on your computer at home, right, and right now they don't
1396 really do much about it, and I think Bob talked about this as
1397 well. You know, there is basic hygiene things that most
1398 people don't do. Your ISP has fairly good knowledge when you
1399 are running malware, when you are part of a botnet, not
1400 perfect knowledge but good knowledge. What actions can they
1401 take to stop that? And in Australia, Australia is not the
1402 only country that does this anymore, at one point they
1403 thought the attorney general will come in and tell the ISPs
1404 what to do, because the ISPs were not doing anything. This

1405 was a failure of incentives, right. And there was a tussle,
1406 a political tussle. At the end of the day, the ISPs--and
1407 Australia is a little easier because it is a smaller country.
1408 They said how about if we come up with a voluntary code of
1409 conduct that will let us deal with the malware threat, and
1410 with a little guidance and help and involvement from the
1411 attorney general and the Australian federal police, which is
1412 roughly equivalent to some of our federal agencies, they came
1413 up with a pretty good system that works pretty well.

1414 This will not deal with the advanced threat but it will
1415 deal with--you know, quick, name a country in the world that
1416 is the biggest supplier of botnets used in cyber crime. It
1417 is the United States, and it is not because we are cyber
1418 criminals, it is because we are incompetent in our defenses.
1419 The Australian model changes that. We are number one, hey,
1420 great.

1421 There are some issues, and I will just do them quickly.
1422 Other countries that do this--Germany. Germans have a
1423 lighter approach. What happens in Germany is, you get a
1424 little popup on your screen that says basically we notice you
1425 are infected, call this number if you want help. Australians
1426 and some of the other countries that do this say click here
1427 and we will clean your computer for you. A few other places
1428 that don't go public, they just intervene without your

1429 knowledge. You have a privacy issue. You have to be careful
1430 about that. One of the things that comes up over and over
1431 again is, should we isolated infected computers. Should we
1432 cut infected users off from the Internet. Some companies are
1433 beginning to do this. You are putting such a burden on me
1434 that I am just going to cut you off. A big issue. If you
1435 look at the places where we have data, there is an amazing
1436 drop in the rate of infection. So this works, and it would
1437 be useful if we followed the Australians, the Germans, the
1438 Japanese, the Turks, any number of countries.

1439 Mr. {Conner.} I will give you two other points on
1440 Australia that are, I think, relevant to this group.
1441 Australia is also looking at their energy grid, and granted,
1442 their energy grid is a little different architecture than the
1443 United States, more like Ireland and others, but in the
1444 process that we are working with them, they are starting with
1445 the infrastructure part and the actual production side, the
1446 energy creation, one, to lock down the authentication of the
1447 systems within the creation of the power and starting there,
1448 and then going to the export of that power through the grid
1449 as it extends through the different carriers all the way to
1450 the endpoint in terms of that. We are involved with other
1451 companies here in the United States helping them do that.

1452 The other piece is, as they look at health care, they

1453 think that is a critical area in terms of being able to have
1454 health care cards, a novel idea when you get to privacy
1455 concerns here, but as I say, you can't have privacy without
1456 security and policy.

1457 Mr. {Walden.} Thank you, and thanks for the indulgence
1458 of the committee. I am going to go to--oh, Dr. Schneck. I
1459 am sorry. Go ahead.

1460 Ms. {Schneck.} One point, if that is okay.

1461 Mr. {Walden.} Yes, sure.

1462 Ms. {Schneck.} So I think that the example in Australia
1463 is a beautiful example of this need for information sharing.
1464 I would challenge the wording a little bit from Dr. Lewis,
1465 and I don't think he meant it this way, but the ISPs don't
1466 know what is going on in your computer. They are not
1467 watching your banking. They are not watching you work. They
1468 see because they own that block of addresses. They see the
1469 behavior from that block of addresses as a footprint as it
1470 tries to send traffic, which the ISPs are able to track to
1471 protect you from malware. They see that footprint, just like
1472 McAfee sees it, reflect on things they own, and from that
1473 they can see where traffic has come in, for example, a
1474 ridiculously large volume in a short period of time from a
1475 certain set of machines and they can look at those machines
1476 and say these are infected with certain code, and they can

1477 then, in the Australian model, let you know, and so the
1478 question becomes, how do they let you know. I think it is a
1479 great example of the use of that intelligence picture. It
1480 shows how with Representative Rogers' work, we could actually
1481 get a larger intelligence picture. That is what makes for
1482 the humans that the pretty weather map picture that Mr. Dix
1483 recommends. But also, you have the ability now to look at
1484 who is infected where and start looking at these incentives.
1485 How do we incentivize the general public to do this hygiene?
1486 Most people with a computer don't know what it does all night
1487 when they are sleeping. If they knew, they would clean it
1488 up. It is not that hard. So I think this is a really neat
1489 exercise on the information sharing and the incentives.

1490 Mr. {Walden.} I appreciate that, and I appreciate the
1491 committee's indulgence in just trying to get some more
1492 information out there.

1493 Mr. Rogers, thank you.

1494 Mr. {Rogers.} Thank you very much. I know we are short
1495 on time.

1496 Mr. Conner, are you familiar with the company DigiNotar
1497 or what used to be the company DigiNotar?

1498 Mr. {Conner.} Very much so.

1499 Mr. {Rogers.} And signatures and attribution is very,
1500 very difficult, although I think we are getting better. It

1501 is pretty difficult. Can you briefly--I think it would be
1502 good for the committee to hear the story of DigiNotar and how
1503 a viable company went away in about a month after being
1504 hacked and what it does, quickly, and what happened and why
1505 this is important to move forward.

1506 Mr. {Conner.} So if you look at the Internet when it
1507 was created, the little yellow lock, everyone sees the little
1508 yellow lock on their browser and on their PC and they think
1509 they are safe. Very few people know what that little yellow
1510 lock means, and what it is supposed to mean is the
1511 communication path is secure between you and the website that
1512 you are communicating with and who is on each end of that.
1513 The problem is in the SSL world, which is kind of the
1514 security level of that, the identify on each side of that may
1515 or may not be who is reported to be. We co-chaired along
1516 with Verisign a new standard on that extended validation
1517 because if you go to your Super Bowl last week, you will see
1518 people advertising, hosting and selling that little yellow
1519 lock for \$19 for your business website. The only problem is,
1520 the verification of who on the end of that is, is pretty lax.
1521 And they just look at the server and go well, that must be
1522 you.

1523 So the issue was, this one company that provides the
1524 little yellow lock, in this case, predominantly in the

1525 Netherlands, was breached, and they were breached from Iran
1526 just many other security vendors have been breached. We get
1527 a target every day from country states, our little 350-person
1528 company with no help to the U.S. government, thank you very
1529 much, to defend that. Well, this little company got attacked
1530 just like Kimodo did, just like others did, and they breached
1531 that little yellow lock that said who they were and they
1532 began to take down the government security because that
1533 government used the little yellow lock for all its online
1534 capabilities, and the people in Iran, guess what, used that
1535 little yellow lock to say they were Google and other people.
1536 So anyone in Iran that was googling content in that country
1537 was able to give up to the Iranian government whatever they
1538 were looking at, whatever they were doing, and one government
1539 was basically shut down for at least 60 days, and
1540 unfortunately, to those of us in the security world, we found
1541 out about it through the browser forum and actually Entrust
1542 was a partner to that group, and it ended our relationship
1543 with them prior to that, and even we weren't notified. So
1544 that talks about to your question of the legal framework of
1545 what is going on here and the disclosure requirements.

1546 Mr. {Rogers.} Thank you. And I just think that was a
1547 great example of a nation-state using its intelligence
1548 services to co-opt something like that. And by the way,

1549 DigiNotar is no longer a company, so if you want--

1550 Mr. {Conner.} Yes, it is our of business.

1551 Mr. {Rogers.} --to talk about the cost, there is a hack
1552 that took this company and is now out of business, so--

1553 Mr. {Conner.} Well, be careful. It was a subsidiary of
1554 a public business that still exists that acts like it didn't
1555 happen.

1556 Mr. {Rogers.} But the contracts that it has in the
1557 Netherlands no longer exist?

1558 Mr. {Conner.} No, that is correct.

1559 Mr. {Rogers.} Okay.

1560 Mr. {Conner.} That is exactly correct.

1561 Mr. {Rogers.} It is an American company that actually
1562 owned it?

1563 Mr. {Conner.} That is right. And I think the point
1564 that you are on, Congressman, is an important one. There are
1565 ways--we have been attempted to be hacked by the same group.
1566 We have watched them try that over the last 12 months. Two
1567 of the people that own the yellow locks in the United States
1568 and abroad have been taken down relative to Iran being able
1569 to break in and impersonate those pieces. So it is happening
1570 every day.

1571 Mr. {Rogers.} I thought it was important for the
1572 committee to hear that particular case because it shows how

1573 sophisticated and how dangerous it can be if somebody has a
1574 nefarious purpose other than criminal. Criminal is bad
1575 enough. This was other than criminal. And I see my time is
1576 almost up so I am going to ask two questions and close up.

1577 Mr. Lewis, I would like you to talk about, we have been
1578 through a long time. It has been very difficult to get to a
1579 place where we have a very narrow focus on how to move to the
1580 next step. Just talk about the challenges of why we think it
1581 has been difficult to even get a very narrow change in the
1582 law.

1583 And lastly, Dr. Schneck and maybe Mr. Dix can talk about
1584 this, you talked about hardware. There is much concern about
1585 hardware entering our system that may be malicious and very
1586 difficult for us to understand exactly what that hardware is
1587 doing in our systems, and I am hoping you can talk about that
1588 and what we might be able to do from a regulatory and/or
1589 cautionary position on behalf of the United States Government
1590 to make sure that those type of hardware systems don't enter
1591 our system and some of our hardware systems are not exposed
1592 when they leave this country to manipulation by foreign
1593 nation-states.

1594 Mr. {Lewis.} Thank you, because those are hard
1595 questions. They are great questions but I am glad Phyllis
1596 got one of them. So, you know, the neutral answer is to say

1597 when you look at a new technology, it usually takes the
1598 United States somewhere between 20 and 50 years to figure out
1599 to get it an order. So you look at airplanes, steamboats,
1600 railroads, electricity, cars. We are in year 18 for the
1601 Internet. So we are not doing too bad, I guess. I mean, we
1602 have a couple years to sort this out.

1603 A little more pointed answer. We have so many old
1604 ideas. They have not gone away. If it was in PDD-63, which
1605 was the Clinton Administration policy, and we are still
1606 trying it, it doesn't work. Give it up. And the second
1607 thing is, as you have heard, we have old laws that are real
1608 obstacles. You of course are trying to fix this but if it is
1609 the Electronic Communication Privacy Act designed for dial
1610 telephones, you have serious issues here. You have business
1611 issues, you have privacy issues. So it is a hard problem and
1612 it will take time to work out, but the prevalence of the old
1613 thinking and the difficult legal environment we have has
1614 really slowed us down and put us at risk.

1615 Mr. {Rogers.} Mr. Dix or Dr. Schneck?

1616 Mr. {Dix.} First of all, I would like the record to
1617 reflect that Mr. Lewis and I agree on that last point. Thank
1618 you. First of all, let me just touch on the hardware issue
1619 because the whole supply risk management issue, you know, it
1620 is interesting to me, the last count, there is 155 different

1621 supply chain risk management initiatives in the government
1622 today. We need to coordinate those issues. And quite
1623 frankly, organizations like ours, we invest heavily in what
1624 we call our brand integrity program because our reputation is
1625 how we grow our business. So we invest from concept to
1626 delivery in our products, in our hardware and software
1627 products.

1628 To make this short, one of the things that I think that
1629 this body could help with, as we sit here today and we deal
1630 with this supply chain risk management problem, the federal
1631 government still continues to buy from untrusted sources.
1632 There is a cultural cost to government of cost and schedule
1633 across the departments and agencies where in order to save 5
1634 cents on a widget, we are buying from low cost, low bid. As
1635 a result of that, we end up in the gray market and then we
1636 wonder why we have counterfeit or malicious products in our
1637 government supply chain. We should be buying from trusted
1638 sources. If there is some reason why we are not going to buy
1639 from trusted sources, there should be a justification, it
1640 should be public, and the liability from that should accrue
1641 to whoever the acquirer is.

1642 Mr. {Rogers.} Dr. Schneck, can you just comment on that
1643 as well?

1644 Ms. {Schneck.} I do agree. I will also add that we

1645 look at supply chain again as an issue of your product
1646 integrity. We do rigorous testing, both the manufacturing
1647 and acquisition. We would also believe in leveraging some of
1648 the existing standards to really focus on a product integrity
1649 issue, because what you want to know is, did that widget that
1650 you bought, is it exactly what you think you bought. That is
1651 the heart of the issue. So it is rigorous testing and
1652 expanding some of the existing standards.

1653 Mr. {Rogers.} Just to clarify for the record, Mr.
1654 Chairman, so we are at risk if we integrate into the U.S.
1655 system non-trusted sources of product? I want to make sure I
1656 am clear on that.

1657 Mr. {Dix.} I certainly think it increases the risk.

1658 Mr. {Rogers.} Thank you.

1659 Mr. {Lewis.} I used to do the supply chain stuff when I
1660 was in the government sort of on both sides of the table, and
1661 a couple points on that. First, right now it so easy to
1662 hack, you know, that you have to assume that our Chinese and
1663 Russian friends are taking the low-cost approach to
1664 espionage. Why should they not do it? The second one is, it
1665 is very hard to push this out to a global supply chain. We
1666 are not going to be able to get out of that. So this is an
1667 exceptionally difficult issue that will probably force us to
1668 think about how we are going to work with foreign suppliers.

1669 And there is not really a choice here. So what I do think
1670 will happen--I will just say this real quick--right now
1671 hacking is so easy, why bother. If we ever manage to improve
1672 our defenses, they will switch to supply chain.

1673 Mr. {Walden.} I appreciate that. Here is the problem.

1674 I am 5 minutes over his time and I think members are--

1675 Mr. {Rogers.} But this is a Clinton we can all agree
1676 with right here.

1677 Mr. {Walden.} The gentleman's time has long ago
1678 expired, and I appreciate the patience of the committee
1679 members who haven't had a chance to ask a question yet, so we
1680 will try to get back on schedule. Mr. Doyle.

1681 Mr. {Doyle.} Thank you, Mr. Chairman. Thank you for
1682 putting this hearing together, and to the panelists, your
1683 testimony and your answers to the questions have been very
1684 informative.

1685 I want to follow up on a line of questioning that Mr.
1686 Waxman had to Dr. Schneck. Dr. Schneck, I know in your
1687 testimony, McAfee labs predicts an increase in attacks on
1688 smartphones and mobile devices in the future, and it is my
1689 understanding, your company had partnered with a research
1690 facility at Carnegie Mellon University sci lab, which is in
1691 Pittsburgh, the district I represent, about how businesses
1692 and employees handle mobile device security, and apparently

1693 this study showed that most of lost and stolen mobile devices
1694 create some of the biggest concern for businesses. About 40
1695 percent of the organizations surveyed have had lost or stolen
1696 devices and half of those devices contained business-critical
1697 data. Further, about 50 percent of mobile users that were
1698 studied, we found out they store their passwords and their
1699 PIN numbers and credit card information on their mobile
1700 devices, which I am completely guilty of. I am going to
1701 erase them as soon as this hearing is over.

1702 It seems to me that one way to tackle this is to make
1703 sure that the devices that employees are using are secure in
1704 the first place so that if an employee uses them, that the
1705 data remains secure or you could remove that data from a
1706 remote source, and to follow up with what Mr. Waxman asked
1707 you, to your knowledge, could you elaborate on what is being
1708 done by device manufacturers and app developers to secure
1709 their products for commercial use?

1710 Ms. {Schneck.} So we look at protecting them once they
1711 are received so from what we have worked with, there are a
1712 couple of vectors on what they are doing before delivery.
1713 You know, one is--I will take the application side first.
1714 When people download an application, they rarely think about
1715 is this application secure. One of the biggest dangers we
1716 see is not did I catch a virus, it is did I go and purposely

1717 download something with a big smiley face on it and a great
1718 app that did something neat for me, but what it is actually
1719 is, it is a pretty picture and delivery of malware. One of
1720 those instructions will get to be a platform to enter your
1721 network corporate or to start shipping back your personal
1722 information for sale in the Russian underground. So that is
1723 one risk. And the app developers, so some companies are very
1724 careful in the app markets and only approved or back to the
1725 trusted source point, the only approved apps are there for
1726 sale. Other companies are more open about it and it is up to
1727 the user to be very careful about what you download.

1728 Mr. {Doyle.} Mr. Conner, do you have some thoughts on
1729 that?

1730 Mr. {Conner.} Yes. We work with all of them, so from
1731 the droid operating system to IOS to the Microsoft, the first
1732 thing we are working with each of them on is, how do you
1733 identify the device itself securely and authenticate that
1734 back to your company, because if you don't know it is
1735 connected to your company, you have got your first issue and
1736 kind of the consumerization and the enterprise.

1737 The second theme becomes, how do you then work with the
1738 applications that go into that phone, and each one of those
1739 ecosystems do that differently. Some have sandboxing where
1740 they then can use our security or others to make sure they

1741 know who is coming in to put that there. They all three have
1742 very different testing mechanisms to test those apps in terms
1743 of that sandbox and how they communicate that back and forth.
1744 And then the third thing we are working with each of them on
1745 is how you secure email and content and communication,
1746 whether it is mobile, no different than we did with laptops
1747 and desktops before.

1748 Mr. {Doyle.} Mr. Dix?

1749 Mr. {Dix.} Yes, and good old U.S.-based innovation has
1750 delivered today. Available in the market today, a capability
1751 to lock, locate and wipe those devices on demand.

1752 Mr. {Lewis.} We are getting close to maybe having a
1753 solution to authentication. It has been the holy grail for
1754 about 20 years.

1755 Just a quick story to help put this in perspective.
1756 There used to be just one government-approved private company
1757 in North Korea. Do you know what they made? They made
1758 mobile phone apps. I see a pattern.

1759 Mr. {Doyle.} And just another general question for the
1760 panel. Do you think the FCC has any role to increase mobile
1761 device security, and what should that be? Mr. Conner?

1762 Mr. {Conner.} Absolutely. In fact, you look at the
1763 FCC, the critical infrastructure there. I mean, I spent 10
1764 years at AT&T and another 10 putting electronics and systems

1765 into those type of companies. It starts with that. I mean,
1766 I said you can look at the mobile networks as either good or
1767 bad. It can stop the crime I talked about today if used
1768 correctly with technology that cannot be broken today. So I
1769 think that if you think of one governing body trying to own
1770 each of these pieces, it is folly. I think DOE needs to work
1771 with the public partnership and private partnership for its
1772 domain. I think Commerce and Treasury needs to work it, and
1773 I think FCC needs to own that infrastructure around that
1774 ecosystem because to think that the attack vectors that the
1775 bad guys are taking against us are one size fits all is just
1776 ludicrous.

1777 Mr. {Doyle.} Very good. Mr. Chairman, thank you.

1778 Mr. {Walden.} Thank you, Mr. Doyle.

1779 We will now go, I think Mr. Gingrey is next in order.

1780 Dr. {Gingrey.} Mr. Chairman, thank you.

1781 This question is for the entire panel. Maybe we will
1782 start with Mr. Conner. Some have argued that before we enter
1783 the cybersecurity debate, we should heed the Hippocratic oath
1784 and make sure that in the first place we do no harm. If
1785 there were one caution that you could offer us before
1786 legislating, what would that be? Mr. Conner, why don't we
1787 start with you?

1788 Mr. {Conner.} Well, I think the way I would start as a

1789 government is the bully pulpit, frankly. I spend a lot of my
1790 personal time with this team and others, spend a lot of time
1791 educating, and I think quality is a great example that this
1792 government got right. They didn't need equality. They just
1793 got on the bully pulpit and said quality is important. And
1794 when I think of security, the lexicon was not here. It still
1795 isn't here the way it was. If someone started quality saying
1796 I am going to get to six sigma, they wouldn't know what it
1797 meant when quality started before the book. You heard cost
1798 equality. I hear cost of security. We are focused on what
1799 cost. Are you focused on the total cost of security or just
1800 the cost to implement something? So I would start with
1801 education and your bully pulpit.

1802 The second thing I would start on is the inability of
1803 businesses to talk to governments or to themselves because of
1804 antitrust and the patchwork legislation in the States. I am
1805 tired of it being it a one-way communication street to
1806 intelligence and nothing in return, and I understand they
1807 legally can't do it, but as the company that is tasked with
1808 protecting our government and governments and enterprises and
1809 citizens, it is pretty folly to me. I can only give you
1810 information; you cannot give me any.

1811 Dr. {Gingrey.} Mr. Conner, thank you.

1812 We will go to Mr. Dix and move rapidly.

1813 Mr. {Dix.} Thank you very much. Two quick things. One
1814 is, continue to inspire and drive an environment that
1815 supports innovation and investment, and secondly, be
1816 cognizant of the fact that the bad guys move fast. We need
1817 to have speed, nimbleness and agility in our ability to
1818 respond. Attempting to comply with a compliance model that
1819 takes a long time to build and implement slows us down and
1820 imposes impediments to our ability to have speed, nimbleness
1821 and agility.

1822 Mr. {Lewis.} In 2007, we had an intelligence disaster--

1823 Mr. {Walden.} I don't believe your microphone is on.

1824 Mr. {Lewis.} In 2007, we had an intelligence disaster
1825 in this country. The details are still largely classified.
1826 In 2008, DOD's Supernet was hacked. We were unable to get
1827 the opponent off for about a week. In 2010, we saw Google
1828 and about 80 other companies get whacked, lose intellectual
1829 property. Most of them have not reported it but this will
1830 show up in Chinese products in about 5 years. Last year we
1831 saw Stuxnet, which was the ability to destroy physical
1832 infrastructure using cyber attack, and we have a list at CSIS
1833 of major cyber events, mainly because I got tired of people
1834 asking me when we would have a cyber Pearl Harbor. The list
1835 is up to 90.

1836 So I think what we need now is, we need to stop saying

1837 do no harm. We need to move out. We need to do a
1838 coordinated defense.

1839 Dr. {Gingrey.} Dr. Lewis, so you think we definitely
1840 need legislation?

1841 Mr. {Lewis.} I do, and I think there are things--one
1842 thing that we can say now that we couldn't have said 5 years
1843 ago, we now have a pretty good idea of how to do this between
1844 the experts up here, some of the other places. There are
1845 agencies that have done a particularly good job. We now have
1846 a good idea of how to reduce risk and we need to implement
1847 that.

1848 Dr. {Gingrey.} Mr. Clinton?

1849 Mr. {Clinton.} I agree that we do need legislation.
1850 The question is, what is the legislation that we need. I do
1851 subscribe to the ``do no harm'' theory. I think the one
1852 thing that I would tell the committee is to understand that
1853 this is not a technology issue. It is an enterprise-wide
1854 risk management issue. The problem we have is that in the
1855 cybersecurity world, all the incentives favor the bad guys.
1856 Attacks are cheap. They are easy. They are really
1857 profitable. It is a terrific business model. Defense is
1858 hard. We are following the attackers around. It is really
1859 hard to show return on investment to what you prevent, and
1860 criminal prosecution is virtually nonexistent. So I would go

1861 back to the last thing I said before I finished my oral
1862 statement. Understand that you are dealing with the
1863 invention of gunpowder. This is an entirely different thing.
1864 You can't just take 20th century models and plug it in here
1865 because you can pass legislation that will do harm, that will
1866 take away needed resources from where they need to be. We
1867 need a creative 21st century approach, and a lot of what we
1868 are seeing in the public policy world is not that.

1869 Dr. {Gingrey.} Mr. Clinton, thank you.

1870 In the last 12 seconds, last but not least, Dr. Schneck.

1871 Ms. {Schneck.} Let us take this is an opportunity,
1872 unleash the power of the private sector. We built this
1873 thing. We didn't build it with security. Now we understand
1874 this adversary. Let us take the information we have, the
1875 data we have, the ISPs, see all the mobile phone activity.
1876 They can see that. They can protect that. Incentivize us so
1877 that we can still eat when we get done doing it but let us
1878 make sure that we build business models around building
1879 security in from the hardware up, and I think you will see
1880 this world change in a few worlds.

1881 Dr. {Gingrey.} I thank the panel for their excellent
1882 responses, and Mr. Chairman, I yield back.

1883 Mr. {Walden.} Thank you, Dr. Gingrey.

1884 Ms. Eshoo and I were talking about, we are going to lock

1885 the doors and not let you out until you give us all the ideas
1886 that we need to do here, and we will let you out today. But
1887 seriously, in terms of helping us understand how to get this
1888 right. You have a lot of them but in your testimony but if
1889 you could help us drill down very specifically, at least
1890 within the jurisdiction we have, we would really appreciate
1891 very specific suggestions back.

1892 We are going to go now to Ms. Matsui from California.
1893 Thank you for participating.

1894 Ms. {Matsui.} Thank you, Mr. Chairman, and I have to
1895 say, this is probably the most interesting and scary
1896 testimony I have ever heard. But I think that quite frankly,
1897 our country doesn't realize what risk we have, and I think
1898 the things we hear about over the news are things--talk about
1899 hacking but they are at a level, a personal level that people
1900 understand. This is far beyond that. It really affects
1901 every sector of our economy, our country, the way we live.
1902 So I truly believe that this education process is going to be
1903 very, very important. And I also believe that people like
1904 you have to step up to talk about it in ways that the public
1905 could understand. Cybersecurity, everybody sort of
1906 understands it but doesn't understand it. So I think with
1907 every advance in technology, we open ourselves up, and our
1908 daily lives can be impacted so much.

1909 I wanted to follow up a little bit more on the cloud-
1910 based services. Businesses and governments are now going
1911 into the cloud, and what are the unique challenges facing the
1912 cloud with respect to cybersecurity and are we prepared, are
1913 we thinking ahead, knowing what we know now about how we
1914 address these challenges, and why don't we just start over
1915 here with Mr. Conner?

1916 Mr. {Conner.} It is something that is getting a lot of
1917 attention from everybody, and I think a lot of people are
1918 running before they thought it through. I think it is very
1919 application and business sensitive, depending what you put in
1920 the cloud. Some stuff you put in the cloud, it is user name
1921 and password sensitive, that is fine, but if you are putting
1922 valuable financial information and intellectual property in
1923 the cloud, you have two issues. The security within the
1924 cloud is not what the security was within a mainframe data
1925 center today, and how do you authenticate to the cloud is
1926 still a matter of how you choose to implement that, and I
1927 think that is very naïve.

1928 Ms. {Matsui.} So are we still at a place though where
1929 we could start looking at that and incorporate, you know, how
1930 we integrate some of these things into some of the
1931 information-sharing activities. We are still okay right now,
1932 but right now you talk about the cloud as a very sexy thing

1933 so people are now jumping to it.

1934 I was curious also, Dr. Lewis, that you mentioned that
1935 government should find ways to incentivize companies, and Dr.
1936 Schneck was talking about the same thing. What types of
1937 incentives would be the most effective, in your opinion? And
1938 I would also like to hear from Dr. Schneck too.

1939 Mr. {Lewis.} There are basically four kinds of
1940 incentives. There is regulation, and we are going to need
1941 some of that, not too much, and it varies from sector to
1942 sector. There are tax breaks. I mentioned this to the
1943 Republican task force on cybersecurity. They thought this
1944 was not the best year to go after tax breaks. There are
1945 subsidies, right, and we might need subsidies for research
1946 and development, perhaps some other things. Finally, there
1947 is a coordinating effect, right? Someone has to lead, and
1948 you can find this--maybe a good story from the Australian
1949 example. If you pull industry together and point them in the
1950 right direction, they will come up with some really good
1951 stuff and we can find some examples in the Defense Department
1952 where that has worked pretty well. So regulation, tax
1953 breaks, subsidies, and that might include building something
1954 into the rate structure for some critical infrastructure, and
1955 then coordination.

1956 Ms. {Matsui.} Dr. Schneck, do you agree?

1957 Ms. {Schneck.} Not entirely. I think regulation draws
1958 a box around the technologies that you are forced to adapt.
1959 It puts all your money there. It takes it away from science
1960 innovation, and even worse, it shows the bad guy what we are
1961 not protecting. But I do favor the rest. I favor tax
1962 incentives. You know, we believe in insurance reform.
1963 Anything that allows a company to be creative, invest upfront
1964 in cybersecurity, because the upfront investment is a lot
1965 easier and a lot more fun than the cleanup, and it is a lot
1966 cheaper. I testified earlier a couple months ago about small
1967 businesses and incentives being needed when--we don't realize
1968 the small to medium businesses make up, you know, 99 percent
1969 in some cases in our business fabric, and if you think about
1970 where some of the newest technologies come from, not just
1971 cyber but maybe our jet engine comes out of a startup of a
1972 couple really bright guys out of college, they are not going
1973 to invest a whole lot in cybersecurity necessarily when they
1974 get that huge SBIR grant, but if built into that grant was
1975 some positive incentive or some extra money saving you will
1976 get this money from the government only if you promise to
1977 secure it, and we could be doing that for all levels of
1978 companies.

1979 Ms. {Matsui.} So government does have that type of
1980 role, though, and I think the part that I am looking at is,

1981 who convenes all this way? How do you do this so you all
1982 work together? Because I think you are absolutely right, the
1983 business sector can work together and have the solutions but
1984 how do we get to the next point?

1985 Mr. {Conner.} Well, I think the first thing you have
1986 got to do is relieve the legal obligation when we sit with
1987 CEOs. In my first public-private, all the CEOs agreed until
1988 they went and talked to their legal counsel, and guess what?
1989 Then it went completely dead because no one wants to go
1990 public. For one, you have got an antitrust issue of sharing,
1991 and second is, the minute you go public, you create a
1992 standard to be sued criminally as well as civilly, and that
1993 is the reality as a government person doesn't understand, but
1994 if you are a CEO, class actions mean something and suits mean
1995 something, and the minute I say something, I now put a
1996 different standard to me to be held to.

1997 Ms. {Matsui.} Well, thank you very much. I see my time
1998 has run out. This is very fascinating.

1999 Mr. {Walden.} Thank you.

2000 We now go to Mr. Latta from Ohio. We look forward to
2001 your comments as well.

2002 Mr. {Latta.} Well, thank you, Mr. Chairman. I
2003 appreciate it. And I thank the panel for being here. For
2004 someone who did serve on the cybersecurity task force, I can

2005 tell you, it is like you go home, go to your office, it is
2006 like, do I really want to turn that thing on now or not.

2007 And if I can go back first, Mr. Conner, you know,
2008 talking about the yellow lock that you engaged with Mr.
2009 Rogers in a discussion about. You know, a lot of times they
2010 tell you if the https comes up, you are safe. Are you going
2011 to tell me that is not true now?

2012 Mr. {Conner.} The only thing I would tell you is,
2013 unless that chrome goes green, I wouldn't assume that you are
2014 safe.

2015 Mr. {Latta.} Okay. Because the reason I ask that, you
2016 know, we have to get this message out to our constituents and
2017 the American people, and I know that a lot of folks see that
2018 little yellow lock come up and say I am fine. I hate to say
2019 that my daughters were on some social networking and we had a
2020 problem for about four days before somebody could spend--I
2021 don't want to say how much money it took to get the thing
2022 fixed before we could get back on the computer. But, you
2023 know, I am really very cognizant of the fact now of watching
2024 for that https to come up, because again, it also goes to the
2025 whole point of, you know, again, let us say you do online
2026 banking or people do certain things, we need to be able to
2027 communicate that, so that is one thing.

2028 If I could ask Mr. Dix and Dr. Schneck this question.

2029 You both mentioned in your testimony the idea of creating
2030 trusted relationships online either through authenticated
2031 emails or through white lists. Could you elaborate on these
2032 ideas and explain how they differ from the previous
2033 cybersecurity measures like spam filters and blacklisting?

2034 Mr. {Dix.} Ladies first.

2035 Ms. {Schneck.} So our focus on trusted relationships
2036 are in the macro and a little bigger. I would say that we
2037 all need to work together, and we do. Organizations such as
2038 Bob mentioned, organizations such as the NCFT and the
2039 InfraGard show that government and private work together. I
2040 think we are dealing online today with a world much different
2041 than spam filter. I used to help build a spam appliance many
2042 companies ago, and what we looked at then was only the email
2043 vector. Now you have the web vector, the firewall vector,
2044 the mobile vector. Again, the enemy is faster. So when you
2045 start looking at trusted relationships online, we had at
2046 least 30 different parameters we looked at just at email. It
2047 wasn't just did I trust the sender. It was all kinds of
2048 things and indicators in that note. And now you multiply
2049 that. So you have, from our perspective in protecting
2050 against cybersecurity threats at all the different vectors,
2051 we have over 1,000 different parameters of trust that we look
2052 at, and it is not just an established relationship. It is

2053 what has your behavior been lately as in the last two
2054 milliseconds and the last 15 years.

2055 Mr. {Dix.} Continuing to advance the development and
2056 implementation of the national strategy for trusted
2057 identifies in cyberspace is a step in the right direction,
2058 and that is an example where industry and government working
2059 with NIST have come together to deal with this issue of
2060 identity. Every one of my colleagues here has mentioned the
2061 issue of identity as being a root issue in this entire trust
2062 discussion that we are having here today. So there is an
2063 effort underway. It is collaborative. It is producing
2064 results and moving to implementation for the in stick would
2065 be a step in the right direction.

2066 Mr. {Latta.} Mr. Conner?

2067 Mr. {Conner.} Just the last comment on that is, the
2068 irony of this is, you think of who are the most trusted
2069 identifies we use. They are usually government issued. And
2070 I think this is one area our government needs to get out of
2071 the U.S. think and into the rest-of-the-world think.

2072 Mr. {Latta.} Let me kind of go on with this, because,
2073 you know, again, when you are looking at, you know, people
2074 trusting what they are doing on the Internet and banking, I
2075 don't care what it is, but when we were talking about trust,
2076 this is another discussion that was held a little bit

2077 earlier, you know, talking about not buying from the low
2078 cost, low bid and you need to buy from that trusted source,
2079 but how do you know? How do you know even if you buy from
2080 somebody that is trusted that that stuff is still good
2081 without going--I mean, how do you go through unless you are
2082 testing? Are you testing constantly? I will throw that out
2083 to all of you.

2084 Mr. {Dix.} So since I brought that up, I will take that
2085 first, with your permission, sir. So each of us that are
2086 manufacturers has a network of authorized resellers and
2087 distributors that we utilize in the distribution of our
2088 products into the marketplace. That is a place to start
2089 from, understanding whose those authorized providers are.
2090 There is also a great deal of work that is going on right now
2091 through the Trusted Technology Forum and the Open Group to be
2092 able to create a certification and accreditation process for
2093 suppliers, working collaboratively with the government again
2094 in a standards-based approach to being able to address this
2095 issue. So there is some good work that is going on right
2096 now, but the fundamental piece of it in my mind is cultural.
2097 We are still evaluating people and departments and agencies
2098 on their ability to meet cost and schedule. That drives a
2099 certain behavior because it doesn't have security as a
2100 paramount foundation of that conduct.

2101 Mr. {Latta.} Mr. Chairman, I see my time is expired and
2102 I yield back.

2103 Mr. {Walden.} Thank you very much.

2104 Dr. Christensen, you are now recognized for questions.

2105 Dr. {Christensen.} Thank you, Mr. Chairman, and thank
2106 you to all of the panelists.

2107 This is a general question. The FCC's Communication
2108 Security, Reliability and Interoperability Council has been
2109 formulating recommendations for best practices to ensure
2110 optimal security and reliability of communication systems, so
2111 how do you see this process contributing to improvements in
2112 cybersecurity, or said another way, what is FCC's role in the
2113 coordinated defense that we heard about?

2114 Mr. {Lewis.} I am really glad you said that because I
2115 have been sitting here trying to remember what CSRIC stood
2116 for. I had gotten all but two of the letters.

2117 We have all said, when you talk about cloud, when you
2118 talk about mobile, that we are moving to a world where the
2119 role of the service providers is going to be more important,
2120 and that is where FCC and NTIA are the lead agencies right
2121 now. There are others of course that are involved but FCC
2122 originally looked at this issue and they were afraid that if
2123 they took too active a role, as I understand it, they might
2124 be seen as trying to regulate the Internet, and they wanted

2125 to avoid that. So instead, they have taken on an approach
2126 that works more on coordination with private sector experts,
2127 with developing venues for these private sector experts to
2128 get together and encouraging them to come up with a voluntary
2129 approach, and one of the things I had said to FCC staff a
2130 while ago is, try the voluntary approach, and if it works,
2131 great. If it doesn't work, then we have to think about more
2132 mandatory measures. So far it looks like it is working,
2133 though. So I understand they have some measures they might
2134 roll out in the next few months. Commerce has some other
2135 things they are doing. This is where the service providers
2136 and their regulators will be one of the key elements of
2137 cybersecurity in the future.

2138 Dr. {Christensen.} Anyone else?

2139 Mr. {Dix.} So they are in a position to serve in a key
2140 role in this education and awareness campaign that we talked
2141 about and coordinating that at the national and in a
2142 sustained manner to help deliver messages to constituent
2143 stakeholders whether they are home users all the way up to
2144 large enterprises, working with the carriers and the content
2145 providers to be able to help deliver that message. So I
2146 think there is a key role in that part of it in showing
2147 leadership around how we advise people how to protect
2148 themselves.

2149 Dr. {Christensen.} Ms. Schneck?

2150 Ms. {Schneck.} Just one point in addition, having
2151 worked with them a bit over the past few months, they are
2152 setting a great example. Their house is in order from a
2153 cybersecurity perspective. They have some new leadership and
2154 they are really looking--they are reaching out to the private
2155 sector saying what are the best practices. They are reaching
2156 out from what they tell us to other CIOs and the government.
2157 So when you talk about the need to get the government's house
2158 in order, I think that is an exemplary piece. And in
2159 addition, they have a group of people really looking at these
2160 policies and really looking at these issues. We have never
2161 seen that before. So I think this is a good time for them to
2162 not only build on the awareness they launched, I believe it
2163 was last spring with the SBA to the hygiene program point but
2164 then jump on that for the larger enterprises also as an
2165 example.

2166 Dr. {Christensen.} Well, Mr. Conner, and this is
2167 probably what you are referring to at the SBA, but your
2168 testimony notes that according to the FCC, three out of every
2169 four small and mid-sized businesses report having been
2170 affected by cyber attacks. So what is the role of the FCC in
2171 preventing the attacks or aiding the small business
2172 community?

2173 Mr. {Conner.} Well, I think increasingly the networks
2174 underpin all those attacks so you have got the ISPs, you've
2175 got the carriers themselves and you got the devices attaching
2176 to it. I think one of the areas that we must remember is, is
2177 it not always outside where those attack vectors come from,
2178 and just like organized crime found its way inside
2179 organizations, I think increasingly we are going to have to
2180 look at that as an attack vector, and that should be
2181 something that the FCC takes into consideration as they look
2182 at how to deal with it in addition to the ISP filtering and
2183 the other pieces they use.

2184 But one thing I would caution, I hear a lot of rhetoric
2185 around building separate networks, and having lived in a
2186 world that I am old enough that we had separate networks, I
2187 think the reliability when things like 9/11 and tsunamis
2188 happen, the benefit of having multiple networks and the
2189 Internet outweigh the needs of a protected, isolated network
2190 because I don't believe in today's world that is a real
2191 answer.

2192 Dr. {Christensen.} I don't have any other questions,
2193 Mr. Chairman. I will yield back the balance of my time.

2194 Mr. {Walden.} I thank the gentlelady for yielding.

2195 I believe Ms. Blackburn is next for questions. Then I
2196 will go to Mr. Shimkus next.

2197 Mrs. {Blackburn.} I will skip.

2198 Mr. {Shimkus.} Thank you, Ms. Blackburn, and thank for
2199 the panel. Sorry, we have two competing panels, and I
2200 apologize for not hearing all the testimony.

2201 Let me go to Mr. Lewis. You mentioned in your written
2202 testimony the importance of domain-name system security,
2203 DNSSEC. Could you describe the problem with the current
2204 implementation of domain-name systems and why DNSSEC is
2205 important?

2206 Mr. {Lewis.} Well, I think what you have heard from all
2207 us is when the people who designed the Internet designed it
2208 as a DOD network and then they thought it would grow out a
2209 little bit. They didn't worry about trust. They didn't
2210 worry about authentication. Phyllis knew it was her sister
2211 at the other end, right? When we did this, we didn't have to
2212 worry about this and so the domain-name system, which is the
2213 addressing system, is vulnerable to spoofing. It can be
2214 manipulated, and I think as you have, redirect traffic. So
2215 you think as far as you can tell on your machine you are
2216 going to a legitimate site and it could instead be the
2217 government of Iran or a Russian cyber criminal. You can
2218 spoof it. And DNSSEC uses authentication technologies
2219 largely so that we reduce that ability, really almost
2220 eliminate it, to impersonate another site.

2221 Mr. {Shimkus.} Yes, and I think the challenge with this
2222 committee is, it is so high tech, so--you know, we are
2223 laypeople for the most part. It is just very tough for
2224 laypeople to understand. That is why we have experts like
2225 you come. A lot of us do understand domain, just the basics,
2226 why you have a domain. Now ICANN is exploding domain names,
2227 and with that, should we--and this is one for the whole
2228 panel--should we be working with ICANN to roll out DNSSEC?

2229 Mr. {Conner.} I think everybody is already working
2230 that. I would tell you be aware of newfangled toys. DNSSEC
2231 has a promise but it also has liabilities today that are
2232 equal to the liabilities we have today. Will it be there in
2233 5 to 10 years? We hope sooner, but it is not there, not even
2234 close. I think we have got to use the capabilities we have
2235 like EBSSL where the chrome turns green and you know you are
2236 safe, and when someone says your identity is who it is, it
2237 is, and I think that is where I put the focus instead of
2238 buying \$19 authenticate technology to take a responsibility
2239 liability for your identity and who that is, and if it costs
2240 you 500, I mean, that is where a bully pulpit starts to make
2241 a difference in our technology.

2242 Mr. {Shimkus.} Mr. Dix, anyone else want to respond?
2243 Anyone else? That is fine, because I want to go to a couple
2244 other things. I also deal with democracy movements in former

2245 captive nations, eastern Europe, whatever you want to call
2246 them, and followed the cyber techs in Estonia years ago, the
2247 meddling by China and Russia and their neighbors and continue
2248 to be very concerned, although the new technological age is
2249 allowing democracy movements to get their word out, to
2250 communicate, and that keeps evolving. But you also see
2251 governments like the government of Belarus try to clamp down
2252 on that and which I have also been very concerned about. So
2253 that is just a statement. I mean, it just an evolving--it is
2254 like a competitive market. People want to get information
2255 but the bad guys want to get around and it moves too fast
2256 that we can really regulate. I have always said that about
2257 this subcommittee and the tech community, there has got to be
2258 a lot of self-interest that gets people to move before they
2259 get caught.

2260 Let me just segue real quickly into, I serve on the
2261 Energy Committee and we go to power plants all the time. I
2262 am a big proponent of nuclear power. And Mr. Terry's opening
2263 statement talked about, well, you could be secure if you just
2264 had a desktop alone and were no longer connected. Now, with
2265 WiFi and stuff, who knows what folks could end up doing. But
2266 the power utility system relies so much on data going to
2267 RTOs, really what they are producing is excitable electrons
2268 to get on the grid, which if that all we had to worry about

2269 and had a closed system, we would be fairly safe, but it is
2270 all the monitoring and calculation of the load. What is the
2271 solution to the utility industry? Does anyone have--

2272 Mr. {Conner.} Two thoughts. One is, as I testified
2273 earlier, that is why you have to start with DOE's elite.
2274 Electrical is very different than nuclear at the source. We
2275 believe you have got to start within the power production
2276 plant itself. We are working with large manufacturers in
2277 terms of how do you authenticate everything in that power
2278 production plant because you want to know what parts, whether
2279 they are original ones or the alternate parts coming in, who
2280 they are and where they are from. And frankly, that doesn't
2281 matter whether they come from good or bad sources, just know
2282 where they come from and that they are there.

2283 The second thing we then focus on is, who is accessing
2284 those systems and sharing that information so only the people
2285 with the right authorization or identity can see it, and then
2286 the third thing we are working with them is, how that data is
2287 shared because data in and of its own, at one location will
2288 not solve a grid by definition.

2289 Mr. {Lewis.} Two other quick points. The idea of a
2290 secure network, a standalone secure network, just doesn't
2291 make any sense. People bring their iPhone to work and they
2292 plug it in to charge, and we have seen that happen twice with

2293 allegedly isolated air gap networks, so forget it.

2294 We need to think about securing the industrial control
2295 systems, the SCADA networks. This is an avenue of attack.
2296 It is a different kind of network technology. Right now, it
2297 is the typical thing. When you buy it, the password is
2298 ``password'' and the user name is ``admin'' and it doesn't
2299 take a lot of activity for foreign opponents to figure that
2300 out. People also need to look at how their critical
2301 infrastructure connects to the Internet. When you talk to
2302 nuclear companies, for example, they will usually tell you we
2303 are not connected. When you do the actual survey, what you
2304 find is, you know, sure, so we need to have some way to bring
2305 the industry--some companies do great. Others need some help
2306 and we need to figure out how to do that.

2307 Ms. {Schneck.} And one point on that, the good news is,
2308 a lot of these industrial control systems are the same across
2309 sectors so if you can get some best practices and some
2310 incentives in one sector, they will multiply across from the
2311 grid to even transportation and nuclear in some cases.
2312 Authentication is one vector. Another is what gets executed.
2313 It goes back to the instruction. It is a malicious
2314 instruction from someone you don't want going to execute on a
2315 system that talks to something that controls physical
2316 infrastructure, and that comes from working at the component

2317 level, making sure that you have technology in those
2318 components that looks at whatever operating system is on that
2319 and says only execute these things. This is actually pretty
2320 simple on these because they only do one job in life. They
2321 are a component on the SCADA system. It is not just--it is
2322 not like they are a big server so you can lock down what they
2323 do.

2324 Mr. {Shimkus.} Thank you, Mr. Chairman. Thank you.

2325 Mr. {Walden.} Thank you.

2326 We will now go to Ms. Blackburn for 5 minutes for
2327 questions.

2328 Mrs. {Blackburn.} Thank you, Mr. Chairman, and thank
2329 you all for being here and for your patience with us.

2330 I want to say just a couple of things. I think it is so
2331 important that the industry lead on this. Anything that we
2332 do, as different members have said today, is going to be
2333 passé before the ink is dry on whatever it is that we do.

2334 Another thing. We have spent some time in this
2335 committee and also in CMT, Commerce, Manufacturing and Trade,
2336 looking at the issue of privacy and the data security issue,
2337 the breach notification issue, which is a component of what
2338 we have here, and quite frankly, I think that most people do
2339 not realize the vulnerability that exists in their home with
2340 the computer that is there, and believe you me, I hear about

2341 it a lot with my district in Tennessee with all the
2342 songwriters and entertainers and the individuals that are in
2343 logistics informatics or financial service informatics or
2344 health care informatics and auto engineers. So the problems
2345 are compounding for this every day. But as we look at the
2346 privacy issue and in my conversations with them, let me ask
2347 you about federal preemption. And as we look at our
2348 standards on breach notification, data security, I wonder if
2349 you all have any thoughts on putting in federal preemption
2350 language and making certain that we are working from one
2351 standard and the importance of that.

2352 Mr. {Clinton.} Ms. Blackburn, if I could, we are
2353 supportive of federal preemptive notification requirement. I
2354 think we have 47 different ones now. For a multi-state
2355 company, it is very, very difficult to work on the similar
2356 themes that I have been hammering on throughout today and
2357 generally is that we have to understand that it is not a
2358 technical problem, it involves cost. If we can find a way to
2359 reduce cost, we can have good standards but we don't have to
2360 have multiple good standards. So we can lower compliance
2361 costs, increase simplification, we will have better
2362 adherence, we will have better security, better privacy and
2363 at lower cost, and I think that that ability to cut through
2364 kind of the government falling all over itself at the various

2365 levels is critical to getting that done, so I am very
2366 supportive of that.

2367 Mrs. {Blackburn.} Okay.

2368 Mr. {Conner.} I would second that. I would tell you
2369 the single largest legislation issue that has brought
2370 security from being in the Stone Age to today is probably
2371 California 1386. Why? Because it said if it happens, you
2372 have a carrot and a stick. If you tried to protect yourself
2373 with encryption, you are safe, and if you haven't, you are
2374 liable for a class-action suit. That is singly the shot that
2375 was heard around the world, at least in the United States.
2376 The problem being, as Larry said, we have got too many State
2377 legislations, a patchwork, so that needs to get dealt with
2378 because it is an inextricable link to cybersecurity in terms
2379 of that.

2380 The second piece I would tell you is the regulation that
2381 just was passed by the FCC about disclosure is going to have
2382 just as profound impact. The problem is, it is only public
2383 companies, and that disclosure is pretty nebulous in terms of
2384 being meaningful for you as a small business person in
2385 Knoxville or Nashville or Memphis in terms of what that means
2386 to you.

2387 Mrs. {Blackburn.} Okay. Thank you. I will yield back.

2388 Mr. {Walden.} The gentlelady yields back, and now I

2389 think our final questioner is Mr. Bilbray from California.

2390 We welcome your comments. You are recognized for 5 minutes.

2391 Mr. {Bilbray.} Thank you, Mr. Chairman.

2392 Mr. Conner, do you believe that law enforcement has the
2393 tools they need to go after cyber criminals as described in
2394 your testimony?

2395 Mr. {Conner.} No, they do not. I have to tell you, if
2396 you look at the attempts that are being made with DHS and
2397 within Justice to have the criminal network geared up, I
2398 mean, part of the problem is, we look at it and there are
2399 one-time uses for critical events. Well, unless you use it
2400 every day, that system is never going to be ready. We
2401 partnered with Interpol to do just that. They have 6,000
2402 agents worldwide, and their issue was--because I certainly
2403 didn't have the money--Interpol is treated like a country now
2404 under passport control. We were able to put their passport
2405 information so it has biometrics. Unfortunately, this
2406 country doesn't deal with that in its passport today. It is
2407 first generation digital. The second thing it has--and this
2408 is all on commercial chips--it has software to do logical
2409 access so those 6,000 agents if they go after a tsunami, they
2410 can go on any network including an Internet café and be
2411 secure in getting access to that information, whether it is
2412 mobile, etc., and last but not least, physical access to

2413 every Interpol office. All that technology resides on this
2414 little card--this is a real one--that those 6,000 agents use
2415 around the world today as they follow crime, hopping
2416 jurisdictions that have three different standards, three
2417 different use cases, that allows them to do their job. Why
2418 is it important? Because it is what he or she has to use
2419 every day. To the extent it is not something you use every
2420 day, it will not be useful at the time of need in some event.

2421 Mr. {Bilbray.} So basically you are saying we are at
2422 place in cyber crime where we were in the 1930s with the bad
2423 guys running around with Thompson submachine guns and the
2424 cops carrying .38 revolvers.

2425 Mr. {Conner.} Well, and worse than that, we are
2426 isolated. We are isolated here in the United States with, as
2427 my colleague said, the most at risk and no ability to
2428 interwork on a global capability with the good guys to defend
2429 that.

2430 Mr. {Bilbray.} It is interesting you bring that up
2431 because I think that most of us here will remember after 9/11
2432 this issue of the technology, security, the biometrics, the
2433 high-tech stuff was one of the top priorities of the 9/11
2434 Commission. We passed a thing called the REAL ID bill and
2435 now everybody has found excuses to keep dragging it on,
2436 dragging it on. In fact, I think we are even giving grants

2437 to States for homeland security and States are refusing to
2438 implement the 9/11 recommendations, so we are giving them
2439 money and they basically say that we want to spend it on
2440 other things rather than the first priorities. Do you think
2441 we may want to revisit that whole situation rather than just
2442 ignoring the fact that--

2443 Mr. {Conner.} Absolutely. I spoke the morning after
2444 Bush addressed both the House and Senate. That morning
2445 after, I was with Mr. Bennett and other legislators that were
2446 leading this effort and spoke at NATO after 9/11 on, we have
2447 learned to defend air, land and sea, the next frontier is
2448 cyber. Unfortunately, in those 10 years, we made a lot of
2449 progress but the bad guys have made more progress and they
2450 can jump across jurisdictions with no legislative legal
2451 barrier.

2452 Mr. {Bilbray.} Mr. Chairman, I have to say that this is
2453 one thing that I think that our committee always referred
2454 over to Homeland Security but here is a point where we may
2455 want to talk. This is a place that both sides of the aisle
2456 should be able to cooperate on. We have got a consensus
2457 there. And frankly, the bad guys in here, the
2458 obstructionists are on both sides of the aisle too. So maybe
2459 this committee can take a look at, you know, how we can go
2460 back and revisit that and address that issue.

2461 And I appreciate the fact that you draw the line about--
2462 I am concerned and I will ask the doctor to jump in here
2463 because the two at the end brought up two interesting things,
2464 that when we develop strategies, how to address this. We
2465 don't want to create a box that gets people to litigate the
2466 private sector but we also don't want to create a box that
2467 allows the bad guys to know how far they have to move outside
2468 to avoid it, and I would solicit both comments. Let us start
2469 with the doctor and then I will go back of how, you know, can
2470 you elaborate again how that us creating arbitrary boxes may
2471 be utilized by the bad guys.

2472 Ms. {Schneck.} I think it was said earlier, and even by
2473 Ranking Member Eshoo, this issue is so vast, this is science,
2474 that if you start saying you will implement these five
2475 things, the adversary is always looking at how to get around
2476 that. They know their target. They know what they want.
2477 They spend many months and people on finding exactly the
2478 intellectual property they want. They find the person and
2479 the company. They know what the person will respond to and
2480 they get it.

2481 It is quite clear that if we say we are going to seal up
2482 these gateways and these ways, these are the best practices
2483 that we must follow when it is a regulation, that is where
2484 the money will go, and after that, the money won't go to

2485 anything new and different and therefore the adversary then
2486 always goes outside that and says well, I can get in this
2487 way. It is like the point to the industrial control system.
2488 They say they are disconnected but true story after true
2489 story finds a little modem out the back so the person can
2490 watch the game while they do the monitoring. There is always
2491 a way out in science, and what we want to do is instead
2492 incentivize. You have a classic problem. We are not
2493 incentivized to do what is good for the greater good. We are
2494 incentivized towards our shareholders. So instead, if you
2495 put that money and that incentive toward innovation, we will
2496 end up building stronger and better technology at many times
2497 the speed that the legislation could even get through do to
2498 the, quote, protection.

2499 Mr. {Conner.} Congressman, I think that is a great
2500 question. I am frankly less concerned about what we say we
2501 are doing. Say anything you want, by the time you say it,
2502 they have already figured that out. They are not waiting for
2503 us to legislate and regulate and figure out the next hole. I
2504 think the model is very clear. It is joint forces and it is
2505 in DOD. We still have strong Army, Air Force, Marines,
2506 Colonel Garlick, and they act on their own. They are highly
2507 integrated with their suppliers. There is what is publicly
2508 available. I served on the Joint Forces Advisory Board as a

2509 private sector person. There is what you do in that that is
2510 public and there is what you do that is not public, and I
2511 think that is how cybersecurity has to be treated. There was
2512 10 percent of the money set aside to deal with cybersecurity,
2513 and no Army, Air Force department could do. They had to get
2514 their best and brightest in on it and they had to share what
2515 is public is public and what is not public is equally or
2516 maybe more important.

2517 Mr. {Bilbray.} Thank you, Mr. Chairman.

2518 Mr. Chairman, they referred to Australia. Being the son
2519 of an Australian war bride, it reminds me of the story of a
2520 notorious Australian bushman, a robber named Ned Kelly. Ned
2521 Kelly was notorious for putting so much armor on so that
2522 nobody could shoot him, and his armor slowed him down so much
2523 that they shot him in the back where he wasn't armored, and I
2524 think that may be very symbolic of the Ned Kelly syndrome,
2525 that we put on so much armor thinking we are defending and
2526 what we do is create an opportunity for the bad guys to get
2527 around it.

2528 Thank you. I yield back.

2529 Mr. {Walden.} I thank the gentleman and I thank all our
2530 committee members for letting us having a more free-wheeling
2531 hearing that sometimes we have, but the value of the content
2532 we got from you all is just unparalleled, and I think my cg,

2533 Ms. Eshoo, and I will be reaching out to each of you to say
2534 come back to us with what really would work. We got a lot of
2535 that today and our staff has got that. We are going to move
2536 forward on this. I think there is an opportunity to look at
2537 device manufacturers, perhaps the phone side, the router
2538 side, there is an issue on the education side, and so we
2539 really appreciate what you are doing out there in this fight
2540 and your input to us so we can try to get it right and solve
2541 this problem.

2542 With that--

2543 Ms. {Eshoo.} I would say bravo and thank you very much.
2544 Every member really drew so much from your testimony and the
2545 answers to our questions have been most, most helpful. Thank
2546 you.

2547 Thank you, Mr. Chairman.

2548 Mr. {Walden.} Thank you, and with that, the Committee
2549 will stand adjourned.

2550 [Whereupon, at 11:56 a.m., the Subcommittee was
2551 adjourned.]